



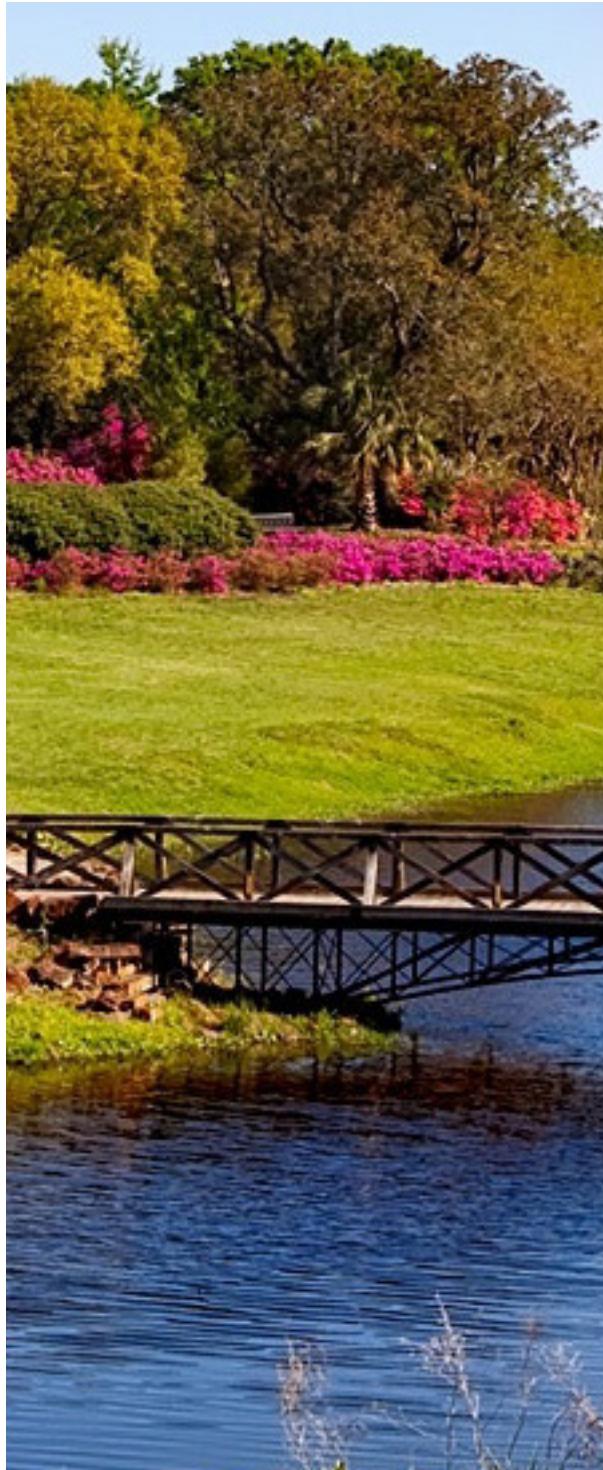
# Orientation

Oxford Blockchain Strategy Programme  
2022

# Oxford Blockchain Strategy Programme

## Orientation

---



### Table Of Contents

1.0 Blockchain Strategy Syllabus	3
2.0 Meet Your Instructors, Guest Instructors, Tutors, and Success Managers	10
3.0 About Riff	29
4.0 Welcome to Oxford Blockchain Strategy	37
6.0 Programme Requirements and Grading	47
7.0 Resources and Quick Help	52

# 1.0 Blockchain Strategy Syllabus

Welcome to Oxford Blockchain Strategy! Take a few minutes to explore this page for information about this programme.

## About This Programme

### Key Programme Objectives

Through the programme, you will learn about:

- Cryptocurrencies and blockchain technology, the connection between technology choices, the types of use cases enabled, and their impact on business strategy.
- A wide range of use cases for blockchain technology across various sectors, including finance, telecommunications, energy, entertainment, and government.
- The cryptocurrency and blockchain technology ecosystem, the key players in it, the competitive dynamics, and the differentiation between various emergent sectors of this industry.
- Leveraging tools and resources to stay up to date on the latest technology and business developments in this rapidly evolving industry.
- Various course frameworks to analyse and articulate the challenges and opportunities associated with the use of blockchain technology in a business setting.
- Formulating a suitable business case for using blockchain technology.

## Who Should Take This Programme

This programme is designed for:

- Entrepreneurs, business leaders, executives, or professionals who want the strategic insight and actionable knowledge to create new ventures or develop both short and long-term business strategies for blockchain technology; managers, directors, or professionals in either private or public sector businesses or organisations;
- Individuals who are intellectually curious and motivated and in the midst of, or aspiring towards, a career transition or looking for future-fit skills in blockchain technology and strategy;
- Individuals who want to learn alongside and build a network with fellow participants whose titles may include:

- Chief Executive Officer
- Chief Information Officer
- Chief Technology Officer
- Chief Operating Officer
- Founder or Co-Founder
- Senior Manager
- Programme Manager
- Managing Director
- Digital Innovation Officer or Manager
- Director
- Financial Analyst
- Vice President
- Project Manager
- Digital Product Director
- Compliance Officer
- Industry expert
- Regulator
- Entrepreneur
- Academic

## About the Curriculum

The Blockchain Strategy programme is designed to provide you with the knowledge you need to understand the fundamentals of blockchain technology and cryptocurrencies. This knowledge will help you to think strategically about implementing a blockchain technology solution, and equip you with the skills to understand the future of blockchain applications.

This curriculum explores the impact of blockchain technology on businesses, traditional platforms, financial services, governments, organisations, and consumers. It will introduce the following:

potential transformations and use cases in a wide range of industries; practical considerations on regulation, compliance, and governance; and a balanced perspective of challenges and opportunities in this industry. This combination enables a strategy and business case for blockchain technology. Throughout this programme, you'll hear viewpoints from:

- Policymakers and regulators
- Entrepreneurs
- Influencers
- Investors
- Academics
- Corporations and organisations
- NGOs and global institutions

You will form groups to discuss, and reflect on, the course material as well as develop a persuasive blockchain use case to show potential VC investors or an existing organisation's board of directors. This will help you to better understand the practical application of theoretical concepts you'll learn about.

By the end of this programme, you will be able to:

- Examine the basics of how a blockchain protocol works and outline a clear definition of blockchain technology.
- Understand how blockchain technology can be used as a digitally scarce asset, as a payment rail, or as a distributed ledger and evaluate whether a use case is suitable to be put on a blockchain.
- Develop strategies for engaging with the various stakeholders of a blockchain project.
- Prepare a plan to address legal, organisational, and ESG challenges for a blockchain or crypto project.
- Formulate a suitable business case for blockchain technology.
- Present a persuasive blockchain use case to potential investors or to an existing organisation's board of directors

## How You'll Learn

Our programmes interpret advanced topics into small, understandable modules that carry you on a curated learning journey to a new kind of understanding.

Each week you will engage in a mixture of:

- Viewing or listening to digital videos or audio content, augmented by written material you can download to review as you have time.
- Completing quizzes and exercises designed specifically to help you understand and retain new information.
- Participating in dialogue with expert instructors and your peers via discussion forums and small-group engagement.
- Participating in carefully crafted interactions to provide you with an engaging learning experience.
- Acquiring information in context through “worked examples” that help you understand how the concepts delivered in the programme material can be applied to your own work environment.

The Oxford Blockchain Strategy programme is designed for approximately seven to ten hours per week of effort, including a mix of videos, reading, and exercises. Supplemental or optional reading is offered for those who wish greater depth in assimilating the subject matter.

Most of the material can be self-paced; i.e. the participant can choose when to consume material and complete assignments during each week. Some work is synchronous in small groups, which has been demonstrated to deliver to executives a better understanding of the material and superior learning outcomes.

## Schedule

Programme materials become available weekly on Wednesdays at 11:00 UTC. (Try the [Time Zone Converter](#) to get your local time.)

Module	Description
<b>Orientation (1 June, 2022)</b>	Explore what you will learn and how you will learn in the programme. Learn about the Riff platform.
Time estimate: 2 hours	<b>Live Kick-off Webinar: 2 June, 2022, 12:00 UTC</b> <b>Assignments Due: 14 June, 2022, 23:59 UTC</b>
<b>Module 1 (8 June, 2022)</b> Time estimate: 7–10 hours	Recognise the scale of investment in blockchain technology and the significance of the blockchain industry. Understand the historical context that fostered the emergence of blockchain. Identify the key properties and components of blockchain technology. Outline a clear definition of blockchain and explain the potential effects this technology may have on business and society.  <b>Group Activity:</b> Meet your group. In preparation for working as a group, you will complete a short exercise where you will get to know the strengths and personalities of your group members in order to create an effective group dynamic. You'll also be invited to a live tutorial session with your Tutor to prepare for your first assignment submission in Module 2.  <b>Assignments Due: 14 June, 2022, 23:59 UTC</b>  <b>Live Webinar—Web3 Identity: 16 June, 2022, 12:00 UTC</b>
<b>Module 2 (15 June, 2022)</b> Time estimate: 7–10 hours	Recognise the types of use cases blockchain technology enables. Evaluate whether a use case is suitable to be put on a blockchain. Describe how blockchain technology can be used as a digitally scarce asset, as a payment rail, or as a distributed ledger. Compare different business models of blockchain use cases.  <b>Group Activity:</b> Define blockchain technology in your own words and use the suitability criteria in Module 2 to rationalise your chosen use case.  <b>Assignments Due: 21 June, 2022, 23:59 UTC</b>

Module	Description
<b>Module 3 (22 June, 2022)</b>	<p>Identify the key players in the cryptocurrency and blockchain technology ecosystem. Learn how to develop a stakeholder engagement strategy for a specific blockchain project. Compare the incentives, as well as the organisational and competitive dynamics between blockchain stakeholders.</p>
Time estimate: 7–10 hours	<p><b>Group Activity:</b> In a live tutorial session with your Tutor, you'll go through a stakeholder mapping exercise and discuss challenges using a use case example. This is to prepare for your submission in Module 4.</p>
<b>Assignments Due: 28 June, 2022, 23:59 UTC</b>	
<b>Module 4 (29 June, 2022)</b>	<p>Recognise how securities, data, privacy, anti-trust, and tax laws impact the use of blockchain technology. Compare blockchain regulations in Europe/UK, US, and China. Identify organisational challenges that may arise when adopting blockchain technology and new operating models. Formulate a plan to address legal, organisational, and ESG challenges for a blockchain or crypto project. Recognise the Environmental, Social, and Corporate Governance challenges within blockchain technology projects.</p>
Time estimate: 7–10 hours	<p><b>Group Activity:</b> Complete a stakeholder mapping exercise using the stakeholder mapping template from Module 3. Show the best way to engage each stakeholder to earn their support. Address any ESG, organisational, legal and regulatory challenges and create a plan for your use cases using the framework in this module.</p>
<b>Assignments Due: 5 July, 2022, 23:59 UTC</b>	
<b>Module 5 (6 July, 2022)</b>	<p>Evaluate the benefits and risks of bringing blockchain technology into a particular project. Learn how to develop a business case for blockchain technology in a startup or an existing organisation. Identify the various types of financing and funding available for blockchain-focused projects and businesses.</p>
Time estimate: 7–10 hours	<p><b>Group Activity:</b> In a live tutorial session with your Tutor, you'll go through a business case framework and use case viability to prepare for your final submission in Module 6.</p>
<b>Live Mid-Programme Q&amp;A Event: 30 June, 2022, 12:00 UTC</b>	
<b>Assignments Due: 12 July, 2022, 23:59 UTC</b>	

Module	Description
<b>Module 6 (13 July, 2022)</b>  Time estimate: 7–10 hours	Present a persuasive blockchain use case to potential investors or to an existing organisation's board of directors.

**Group Finale:** Assess the cost structure and revenue model of your blockchain use case. Focus on module 5's business case framework to determine your business case viability and rationalise your findings. If you decide your use case is not a good use case, after all, you can motivate why it is not by using the same criteria you would use to explain why a use case is a viable solution.

**Assignment Due: 19 July, 2022 23:59 UTC**

## 2.0 Meet Your Instructors, Guest Instructors, Tutors, and Success Managers

Our programme brings together thought leaders from the University of Oxford and guest industry experts, facilitating the rapid application of theory to practice. Our Tutor and Success Teams are here to support you throughout the programme.

**Please Note:** Programme Directors, Academic Directors, Faculty, Guest Speakers, and Tutors cannot provide academic references to learners of this programme. You may contact [registrar@esmelearning.com](mailto:registrar@esmelearning.com) to request proof of attendance once you have completed the programme.

### Instructors



**Meltem Demirors**

**Programme Director; Chief Strategy Officer at CoinShares**

Meltem Demirors is an expert in digital asset investing with significant experience in accelerating growth and acceptance of the asset class. At CoinShares, a publicly listed (Nasdaq Nordic \$CS) digital asset investment firm with \$5B in assets under management, Meltem leads investment and corporate strategy. She is also a founding member and Co-Chair of the World Economic Forum Cryptocurrency Council, and she works closely with organisations across the cryptocurrency ecosystem. Meltem was integral to the growth of Digital Currency Group, the world's largest digital asset investment firm, and previously worked in the oil and gas industry in corporate treasury, trading, and M&A.

**Teaches in:** Modules 1–4



### Martin Schmalz

#### **Academic Director; Professor of Finance and Economics, Saïd Business School, University of Oxford**

Martin Schmalz is a Princeton-trained financial economist and tenured Professor of Finance and Economics at Saïd Business School, University of Oxford, where he teaches cutting-edge subjects like “The Business of Big Data” and AI applications in Oxford’s business, law, engineering, and executive programs. Martin has published research on consensus protocols since 2006, has been a Bitcoin investor since 2011, and helped oversee cryptocurrency trading strategies for a quantitative hedge fund in which he was a partner before focusing full-time on his current commitments. Outside of Oxford, Martin coaches top-level executives and policymakers and consults with family offices and UHNWI on asset management and succession planning. His research on how the ownership structure of firms affects firm behaviour and market outcomes has affected policy-making and antitrust enforcement worldwide.

**Teaches in:** Modules 5 & 6



### Andrew Baum

#### **Emeritus Professor, Saïd Business School, University of Oxford; Senior Research Fellow, Green Templeton College, University of Oxford**

Andrew Baum led the school’s teaching activity in real estate from 2009–2021 (MBA, EMBA and executive education), and in 2017 he established the Oxford Future of Real Estate Initiative, an industry-supported research programme focused on the 2025–2030 impact of innovation and technology on the global real estate industry. Andrew is Chairman of Newcore Capital Management, a real estate fund manager focused on alternatives, and advisor to several property organisations. He founded RES (a property research company) in 1990 and (with his partners) sold the business to Henderson Global Investors in 1997. In 2001 he founded OPC, a property research and investment company that was sold to CBRE Investors to create CBRE Global Investment Partners. Andrew’s groundbreaking report detailing the dramatic changes facing the real estate industry—PropTech 3.0: The Future of Real Estate—was the most downloaded Oxford Saïd report in 2017 and became the most downloaded PropTech report on Infabode. Andrew was also voted one of the top 3 most influential people in PropTech in the 2017 Lendinvest list.

**Teaches in:** Modules 2, 3, 4 & 6



**Bill Roscoe**

**Professor of Computing Science, University of Oxford**

Bill Roscoe has held various roles at the University of Oxford throughout his career, where he currently works part-time and where he served as head of the Computer Science department from 2003–2014. He currently works with various organisations to apply his research. Just about all of Bill's research, including that on blockchain, derives from his study of concurrency (how independent parties interact). One of the major applications of his concurrency work is over 25 years research on computer security.

**Teaches in:** Modules 1, 4 & 6



**Felipe Thomaz**

**Associate Professor of Marketing, University of Oxford**

Felipe's research focuses on empirically modelling marketing strategy issues, including the incorporation of social networks into the understanding of black markets (digital or otherwise) and strategies developed to stunt their growth and proliferation. His research also involves questions of social networks' impact on brand and firm performance, the behaviour of consumers in digital marketplaces and interactive marketing channels, and the development of managerial metrics that rely on abundant and timely social media data. This research on social media, digital markets, and strategic firm and brand networks includes publications in the Journal of Marketing and Journal of Service Research.

**Teaches in:** Modules 4, 5 & 6



**Dr. Mimi Zou**

**Director of Studies in Law; Regent's Park College, Oxford**

Dr Zou, is an English and Australian qualified lawyer with nearly two decades of experience in legal practice, financial services, government, and international organisations. She has extensive expertise in lawtech, and co-founded an AI company (Deriskly Ltd) with a team of computer scientists from Oxford University. She advise/have advised the UK Government, World Economic Forum, World Bank, UNIDROIT, WIPO, LawtechUK, Asia-Pacific Legal Innovation and Technology Association, and other prominent organisations on deep technologies, law, and policy issues. Dr Zou's research focuses on commercial law issues in the contexts of China's digital economy and Chinese outbound foreign investments (especially relating to the Belt and Road Initiative). She has worked in legal practice in Sydney, Hong Kong, and London, as well as in a number of international organisations, government departments, and financial institutions in Asia-Pacific and Europe for over 15 years. In 2016, the Asia Society named Dr Zou as an 'Asia 21 Young Leader', which recognises the accomplishments of rising change-makers in the region. Her research has won international awards and been covered by media outlets including The New York Times, BBC, The Guardian, Reuters, VICE, China Daily, and South China Morning Post.

**Teaches in:** Module 4

## Guest Instructors



**Mason Borda**

**CEO & Co-Founder, Tokensoft**

Mason Borda started his career at technology companies such as Boeing, SSL, and Broadcom. He entered the digital asset space in 2013, designing and building the infrastructure for a dollar-based blockchain. In 2014, Mason co-founded a payroll automation company, Payroll Integrations, whose clients today comprise 14% of the US 401(k) market. In 2016, he built the first commercially viable custody solution on the Ethereum network. Currently, Mason guides the Tokensoft team in business strategy, business development, and market planning.

**Teaches in:** Modules 2, 4 & 6



**Kathleen Breitman**

**Co-Founder & CEO, Tezos**

Kathleen Breitman is a co-founder of Coase, a software company that aspires to lower transaction costs using cryptocurrencies. She previously co-founded Tezos, a smart contract platform and cryptocurrency with an on-chain governance mechanism to coordinate and push upgrades to its network. Kathleen holds a degree from Cornell University and advises a variety of companies and venture capital firms, including several in the burgeoning NFT space.

**Teaches in:** Module 2



**Matt Brown**

**VP, Corporate Development at LO3 Energy**

Matt leads global commercial functions for Portland, OR-based LO3 Energy, including business development, customer success, and corporate strategy. He has over a decade of experience in early and growth-stage climate tech development spanning functional roles in early-stage investing, federal policy, and as an operator. Matt has focused on the commercialisation of distributed renewables, energy storage, and market dynamics related to grid modernisation and advanced transportation. Matt previously lead clean energy investment research and analysis at the CREO Syndicate and served as a consultant to Braemar Energy Ventures. Prior to that, he was a VP at McBee Strategic Consulting in Washington, D.C., where he managed a portfolio of energy sector clients comprised of startups, multinational energy majors, and venture capital firms. His career started in climate policy with a focus on cap-and-trade mechanics. Matt has a B.A. in Environmental Economics from Colgate and an MBA from Columbia Business School.

**Teaches in:** Module 3



## **Nelly Chatue-Diop**

### **CEO and Co-Founder, Ejara**

Nelly Chatue-Diop is the CEO and co-founder of Ejara, a blockchain-based saving and investment app for people in Francophone Africa and the diaspora. She has spent the last 15+ years across Europe and the United States, during which time she built a unique experience in Tech, traditional Finance, and Web 3.0 (IA, Blockchain) within several executive committees and boards of directors. Nelly holds a computer science engineering degree and completed her MBA at HEC Paris and London Business School. She is a renowned Data leader and an outspoken Blockchain advocate for Africa and with Africans.

**Teaches in:** Module 2



## **Emilie Choi**

### **President and Chief Operating Officer, Coinbase**

Emilie Choi oversees operations at Coinbase, including Corporate and Business Development, Ventures, Security, Institutional Sales, International, IT and Data, and Marketing and Communications among other functions. Prior to becoming President & COO of Coinbase in November 2020, Emilie served first as VP of Business, Data, and International, and then as COO. Before joining Coinbase, Emilie spent more than eight years at LinkedIn as the VP of Corporate Development. She has also worked in corporate development and strategy roles at Warner Bros. and Yahoo!. Emilie also sits on the boards of Naspers, Ltd., and ZipRecruiter.

**Teaches in:** Modules 3, 4 & 5



## **Marguerite deCourcelle**

### **CEO, Blockade Games**

Marguerite deCourcelle, aka COIN ARTIST, is an artist, creative technologist and game designer who has created many firsts within the blockchain creator economy since 2014. She is internationally recognised by the BBC, MIT, NASA, Bloomberg, and CNBC for cultivating crypto art, and she is credited for inventing cryptopuzzles. Marguerite has been the CEO of one of the earliest NFT game companies, Blockade Games, since 2018. Her most renowned artwork is known as Torched H34R7S. She recently auctioned an interactive NFT during Christie's first NFT showcase.

**Teaches in:** Module 2



**Priyanka Desai**

**Vice President of Operations, OpenLaw**

Priyanka Desai is currently leading operations for OpenLaw, which launched The LAO, Flamingo, Neptune, MUSE0, and more. Prior to working for OpenLaw, Priyanka spent time at blockchain FinTech consortium R3. In addition, she worked for the New York State Department of Financial Services, assisting the Capital Markets division on cryptocurrency enforcement and “Bit Licensing” of various New York-based blockchain startups. Prior to her time at the Benjamin N. Cardozo School of Law, Priyanka worked for the House Foreign Affairs Committee and a large law firm.

**Teaches in:** Modules 4 & 6



**Yaya J. Fanusie**

**Founder and Chief Strategist, Cryptocurrency AML Strategies**

Yaya J. Fanusie is an Adjunct Senior Fellow at the Center for a New American Security (CNAS). His research focuses on the national security implications of cryptocurrencies and blockchain technology. Yaya spent seven years as both an economic and counterterrorism analyst in the CIA, where he regularly briefed federal law enforcement, U.S. military personnel, and White House-level policymakers—including President George W. Bush whom he personally briefed on terrorism threats. In 2009, he spent three months in Afghanistan providing analytic support to senior military officials. Yaya is also founder of Cryptocurrency AML Strategies, an advisory firm that helps financial institutions and technology firms address money laundering and terrorist financing risks associated with digital assets. In 2018, he developed and taught an Introduction to Blockchain Technology course at Morgan State University in Baltimore. Yaya has testified before Congress multiple times on illicit financing issues. He has appeared on CNN, Fox News, CNBC, Bloomberg TV, and has been quoted in the New York Times, the Wall Street Journal, and The Washington Post.

**Teaches in:** Module 4 & 6



## Alex Gladstein

### Chief Strategy Officer, Human Rights Foundation

Alex Gladstein is Chief Strategy Officer at the Human Rights Foundation. He has also served as Vice President of Strategy for the Oslo Freedom Forum since its inception in 2009. Alex has connected hundreds of dissidents and civil society groups with business leaders, technologists, journalists, philanthropists, policymakers, and artists to promote free and open societies. Alex's writing and views on human rights and technology have appeared in media outlets across the world including The Atlantic, BBC, CNN, The Guardian, The New York Times, NPR, TIME, The Washington Post, WIRED, and The Wall Street Journal. He has spoken at universities ranging from MIT to Stanford and briefed the European Parliament and US State Department, and he serves as faculty at Singularity University and as an advisor to Blockchain Capital, a leading venture firm in the fintech industry. He frequently speaks and writes about why Bitcoin matters for freedom, and he co-authored *The Little Bitcoin Book* in 2019.

**Teaches in:** Modules 3, 4 & 6



## Anand Gomes

### Founder, Paradigm

Anand Gomes is the Co-Founder and CEO of Paradigm, an automated OTC platform for institutional digital asset traders. Anand has spent most of his career in the OTC markets, where he helped build trading businesses across interest rate, commodities, and credit markets. Anand graduated with an MBA and an MS in Finance from Case Western Reserve University and also has a BS in Computer Science and a Diploma in International Business from the University of Pune. Prior to graduate school, Anand spent 3+ years running manufacturing operations for his family's middle-market, industrial firm in India. He is passionate about music, psychedelic art, distributed systems, AI, mountains, motorcycles, and a lover of all art and expression.

**Teaches in:** Module 2



## Eva Kaili

### **Greek Socialists & Democrats Delegation in the European Parliament**

Eva Kaili is a Member of the European Parliament and a part of the Hellenic S&D Delegation since 2014. She is Chair of the Future of Science and Technology Panel in the European Parliament (STOA) and a member of the Industry, Research and Energy committee (ITRE), the Economic and Monetary Affairs Committee (ECON), and the Budgets Committee (BUDG). Eva has worked intensively on promoting innovation as a driving force in the establishment of the European Digital Single Market. She has been the draftsperson of multiple pieces of legislation in the fields of blockchain technology, online platforms, big data, fintech, AI and cybersecurity, and more recently, the Invest EU programme. She is also the founder of the Future Forum, a network of influential politicians, officials, and public figures promoting innovation.

**Teaches in:** Module 4



## Tegan Kline

### **Co-Founder and Business Lead, Edge & Node; Former Business Lead, The Graph**

Tegan Kline is the Co-Founder and Business Lead of Edge & Node and former Business Lead at The Graph, an indexing and query protocol organising the world's open blockchain data and making open data a public good. Tegan met Yaniv Tal in San Francisco and met Brandon and Rodrigo at Devcon Prague, where the vision of The Graph's decentralised indexing layer came to life in her mind. Tegan is the former International Business Development Manager and OXT Relations Lead for Orchid, an A16z and Sequoia-backed blockchain company that created tools and protocols for users to obtain digital freedom and an open and accessible internet. Prior to her time at Orchid, Tegan was the Executive VP of a patent marketplace powered by blockchain and analysed by AI. She began her career in Investment Banking at BAML and, prior to her work with blockchain, worked in Sales and Trading at Barclays

**Teaches in:** Module 4



## **David Lighton**

### **Co-Founder, SendFriend**

David Lighton is a Co-Founder of Lithium Finance, a DeFi pricing oracle, and SendFriend, a blockchain-payment platform. As a co-founder and former policymaker, David is inspired by the power of Blockchain technology improving financial systems and people's lives. He is a Fellow at Yale University and a Former World Bank staff, where he developed financial inclusion strategies for Central Banks.

**Teaches in:** Module 4



## **Morgan Mercer**

### **Founder and CEO, Vantage Point**

Morgan Mercer is a thought leader, two-time founder, angel investor, and visionary whose technology company, Vantage Point, is recognised globally for its contributions to Diversity, Equity, and Inclusion. After starting Vantage Point at the age of 23, Morgan became one in three dozen Black women to raise over \$1M in venture capital funding—a feat achieved by .006 percent of Black female founders. She has been featured in over 135 national and international publications, including Vogue UK, Forbes, The Guardian, NPR, WIRED, BBC, and Bloomberg. As an advisor and speaker, she has spoken at over 40 conferences and has been a guest lecturer at The London School of Economics, The University of Maryland, and UN Women. She is a Network Advisor and a Program Judge for Headstream Accelerator, backed by Melinda Gates as well as Trill Project and Dr. Haynes Collective.

**Teaches in:** Module 4



**Aya Miyaguchi**

**Executive Director, Ethereum Foundation**

Aya Miyaguchi originally became fascinated in the blockchain space for its potential to impact financial inclusion in emerging economies. In early 2013, she joined Kraken and educated the public, VCs, and regulators on cryptocurrencies and blockchain innovation globally as Managing Director for Japan. Aya now leads the Ethereum Foundation, which supports projects in the Ethereum ecosystem, including core Ethereum protocol research and development and educational efforts aimed at further expanding the world's largest blockchain ecosystem. In 2019, she was appointed to the World Economic Forum's Blockchain Global Council and named a Board Member of Ethereum Enterprise Alliance.

**Teaches in:** Modules 3 & 6



**Marek Olszewski**

**Partner, cLabs**

Marek Olszewski is the co-founder and CTO of cLabs, one of the companies contributing to the Celo Protocol. He also co-founded Locu, a machine learning venture-backed company started out of MIT that was acquired by GoDaddy. He is an MIT PhD alumni and a former Facebook Fellow and has previously worked at Google, Microsoft Research, and Sun Labs.

**Teaches in:** Module 2



**Matt Prewitt**

**President, RadicalxChange Foundation**

Matt Prewitt is the President of RadicalxChange Foundation. Matt is a frequent writer on blockchain, technology, institutions, and governance, and he serves as an advisor to Amentum Investment Management. He is also an antitrust and consumer litigator and a former law clerk at the United States District Court for the Southern District of New York.

**Teaches in:** Modules 4 & 6



## Konstantin Richter

### **CEO and Founder, Blockdaemon**

Konstantin is a serial entrepreneur and investor. He has led several SaaS B2B companies towards meaningful exits in the media and advertising space, most notably Audiotube, Lookbooks, and Wiredrive. He also is an advisor to the blockchain company Gem, and he serves on the board of MadHive, a leading media/advertising blockchain business. He currently serves as the CEO and founder of Blockdaemon, the leading independent blockchain node infrastructure to stake, scale, and deploy nodes with institutional-grade security and monitoring.

**Teaches in:** Modules 5 & 6



## Edmund Schuster

### **Associate Professor of Corporate Law, London School of Economics**

Edmund Schuster is an Associate Professor of corporate law at the LSE. His research focuses on corporate law, law and finance, takeover regulation, and the economic analysis of law. He has prepared studies for the European Commission on the reform of corporate governance and private international law. In 2014, Edmund was awarded the Modern Law Review Wedderburn Prize for his article on the law and economics of the mandatory bid rule. Edmund studied law at the University of Vienna and at the LSE. Prior to joining LSE, Edmund practiced corporate law in London and Vienna, and he was head of office at the Austrian Takeover Commission. Alongside his academic work, Edmund regularly advises the M&A team of Baker & McKenzie Austria.

**Teaches in:** Modules 4 & 5



## **Christophe Spaenjers**

### **Associate Professor of Finance, HEC Paris**

Christophe Spaenjers is Associate Professor of Finance at HEC Paris and an academic expert on the investment characteristics of real estate, art, and other “real assets”. He graduated with a Ph.D. in Finance from Tilburg University (the Netherlands) in 2011. His research has been published in leading journals such as American Economic Review, Review of Financial Studies, Journal of Financial Economics, and Management Science. His research has also been covered extensively in the popular press, including The Economist, Financial Times, New York Times, and Wall Street Journal. Currently, Christophe teaches in the MBA programs at HEC.

**Teaches in:** Module 2 & 6



## **Federico Spagnoli**

### **Regional President, Prudential International Insurance**

Federico Spagnoli is the Emerging Markets Ecosystems Product Head and Regional President of Argentina, Mexico, Chile, Peru, and Colombia for Prudential International Insurance (PII). In this role, Mr. Spagnoli has direct responsibility for the development of Total Wellness Ecosystem and Product Development across Emerging Markets, as well as direct responsibility for Prudential Seguros Argentina and Prudential Seguros Mexico, and he supervises the relationship of PII with ILC and AFP Habitat. Prior to joining Prudential, Mr. Spagnoli spent twelve years in various senior positions within AIG's international subsidiaries.

**Teaches in:** Modules 1, 2, 4, 5 & 6



**Yaniv Tal**

**Project Lead, Graph Protocol**

As Co-Founder for The Graph and Project Lead for Edge & Node, Yaniv Tal has successfully led The Graph team and community of Indexers and Curators to where they are today. Yaniv believes that decentralisation will fundamentally transform how humans cooperate, and that this will only be possible once a fully decentralised protocol stack is in place, with incentives for allocating talent and resources. Excited to be part of the decentralisation movement, Yaniv has identified an open data layer that developers and users can collaborate on in a decentralised way was the missing piece to realising Web3. Prior to starting The Graph, Yaniv worked at Mulesoft (an API developer company acquired by Salesforce) and co-founded a developer tooling startup using immutable databases.

**Teaches in:** Modules 1 & 2



**Abbey Titcomb**

**Co-Founder, Radicle**

Abbey Titcomb is the Community Lead at Radicle, a decentralised network for code collaboration. Abbey began her career in venture capital at Underscore VC, an early-stage firm investing across the stack in enterprise open-source, AI/ML, blockchain, and more. Since then, Abbey has been building in the Ethereum ecosystem, working with venture studios and startups building decentralised technologies. At Radicle, Abbey cultivates the project's open-source community and manages partnerships to support the growth of the Radicle ecosystem.

**Teaches in:** Module 3



**Darshan Vaidya**

**CEO & Co-Founder, X-Margin**

Darshan Vaidya has over a decade of experience trading derivatives across fixed-income, FX, and oil. He co-founded one of the first crypto options funds in the space and is now the CEO and co-founder of X-Margin. X-Margin is a pioneer in applying privacy-preserving technology to credit and financial market risk to bring greater efficiency to financial markets and disintermediate the current prime and clearing solutions.

**Teaches in:** Module 2



## **Robert Viglione**

### **Co-Founder & CEO, Horizen Labs**

Robert Viglione is the co-founder and CEO of Horizen Labs, as well as the co-founder and team lead of the Horizen public blockchain. Horizen Labs is a blockchain development company that makes blockchain technology accessible for businesses by enabling them to create distributed ledger solutions that are fast, secure, private, and scalable. Rob is a former physicist and mathematician with experience working on Bitshares, BlockPay, Zclassic, Seasteading, and Bitgate. Previously, Rob has been an advisor to Aave and HeroEngine and has worked as a software project manager for the U.S. Air Force.

**Teaches in:** Module 5



## **Anatoly Yakovenko**

### **Founder, Solana**

Anatoly Yakovenko is the Co-Founder of Solana and creator of Proof of History. Previously, he was the team lead for operating systems development at Qualcomm, distributed systems at Mesosphere, and compression at Dropbox. He was also the Co-Founder of VOIP startup Alescere, where he led development of SIP and RTP protocol stacks and server components for a VoIP system for small businesses. Anatoly holds 2 patents for high-performance Operating Systems protocols, was a core kernel developer for BREW, which powered every CDMA flip phone (100m+ devices), and led development of tech that made Project Tango (VR/AR) possible on Qualcomm phones.

**Teaches in:** Modules 1 & 4

## Tutors



### **Matt Zarracina**

#### **Head Tutor**

Matt leads True Tickets, a B2B enterprise SaaS startup providing secure contactless digital ticketing for live events. Prior to co-founding True Tickets Matt served as a Director of Innovation in Thales Group's "Thales xPlor". He applied Design Thinking concepts to identify, assess, & develop disruptive innovations for broader commercial applications (Blockchain & DLT, AI, Autonomous Vehicles, Augmented Reality, & Big Data). Prior to xPlor, Matt was a Senior Manager at Deloitte Consulting where he led growth, M&A, & innovation projects. Matt also served as a helicopter pilot in the US Navy. He is based in Massachusetts, USA.



### **Simon Bowles**

#### **Tutor**

Simon is the Head of Tokens at both XONE and Unbanx, and a mentor at Techstars. He started his career in venture capital followed by trading at global hedge funds in London, and since 2016 has worked in various countries in Europe within FinTech/Blockchain, including twice as CEO. He currently sits on the advisory board of six blockchain companies, from start-ups to unicorns, where he helps with strategy, growth, and tokenomics, and he has also been used as a subject matter expert for the UK courts. Simon is based in Limassol, Cyprus.



### **Avinash Vora**

#### **Tutor**

Avinash Vora is an entrepreneur and innovator with over a decade in business leadership and management. He is a specialist at business turnaround and fast profitability and has extensive experience in industrial manufacturing operations, treasury management, agriculture, and business development across Asia, Africa, Europe, and North America. Having focused on product development across the apparel, agriculture and FMCG industries, Avinash has a focus on ecological sustainability, future-proofing, and market understanding. He studied economics at the University of Michigan and enjoys technology, college sports, and RPGs. Avinash is based in Dubai, UAE.



## Tyron Fouche

### Tutor

Tyron Fouche is a Fellow of the Institute and Faculty of Actuaries with over 12 years of experience in the financial services and digital innovation space. Having founded multiple ventures, he has developed insights into bringing new innovation into established markets and has developed a strong entrepreneurial toolkit from raising funding, to establishing product-market fit to exiting a business successfully. Tyron is the Head of Innovation at MBE consulting where he helps UK insurers embrace digital innovation. He is a co-founder at The DeFi Lab, a Web 3.0 studio in the Start-up Lisboa incubator, and co-founder at Nuovalo, a US based consultancy focussed on creating innovative decumulation stage retirement products. Tyron has previously served as a Subject Matter Expert on the Oxford Fintech, Blockchain Strategy and Venture Finance programmes and has been endorsed as an “Exceptional talent” in the global digital technology industry by Tech Nation. Tyron is based in Lisbon, Portugal.

## Success Team



### Gabriel Smith

#### Lead Success Manager

Gabriel Smith has worked with Oxford Digital Finance Portfolio Programme learners as a Success Manager since the summer of 2020, and prior to that he worked as programme coordinator for Pioneer Academics and as a freelance tutor for high school and university students. He has overseen online classes in subjects ranging from Greek philosophy to business leadership strategy, and he has guided students to top grades in their coursework. His own academic record includes a BA from the University of Exeter and an MA from the University of Edinburgh. He has also spoken at literary conferences in London and Paris and published work in a peer-reviewed academic journal. Gabriel is based in Yorkshire, UK.



## **Paris Chung**

### **Success Manager, APAC**

Paris Chung has been supporting Oxford Programme learners as a Success Manager and technical writer since Summer 2020, and is a certified executive coach and mentor with degrees in Computer Science and Business Administration. She holds her BS and MBA degrees from Assumption University of Thailand. Paris has spent time as a quality assurance tester, and has technical proficiency and leadership experience. She is an agile coach who has a proven record of supporting and guiding individuals to learn effectively. Paris is based in Bangkok, Thailand.



## **Rachael Johnston**

### **Success Manager, EMEA**

Rachael Johnston is an educator who has taught Biology, Chemistry, and English as a Second Language. She has also acted as a peer mentor as part of the YCSA Control Alt Delete program helping young BME people with education and employment goals. Rachael earned her Bachelor's in Veterinary Biosciences at the University of Glasgow and her TQFE in Biology and Chemistry at University of Stirling. She is passionate about giving learners the best possible learning experience to help unleash their potential. Rachael is based in Glasgow, Scotland.



## **Kim Potter**

### **Success Manager, AMER**

Kim Potter is a retired educator who served multiple school districts in Michigan for 25 years. For the majority of her career in public education, Kim held the positions of reading specialist and special education teacher as she worked one-on-one and with small groups of students. To ensure student success, Kim worked directly with classroom teachers on instructional strategies to meet the needs of diverse learners. Before and after the school day, Kim also tutored students in academics and served on various school improvement committees. Kim resides in Colorado, USA.

## 3.0 About Riff

### AI-Enabled Knowledge Acceleration to Build Collective Intelligence at Scale

#### Guest Video: Introducing Riff

In this video, Beth Porter discusses the benefits of using Riff Edu platform to enhance collaboration during your programme experience. She explains how Riff Edu gives you personal feedback on your group meetings. This feedback raises your awareness of group dynamics and helps you improve your collaboration skills.



Hi, my name is Beth Porter, and I'm going to be talking to you about how we use the Riff platform in this programme. You will use Riff to meet in small groups to collaborate on shared tasks, and you will connect with other programme participants to share ideas in a community of practice.

Collaboration is an important element of the course experience. When you work together towards shared goals on group assignments, you're modelling what you do in a work environment. Riff is a communication platform designed to foster collaboration.

In the Riff platform, you will use video chat and text chat to communicate in real time, and throughout the programme. In peer learning groups, you will work on structured activities, but we hope and expect you to build social connections with other participants and course staff. Collaboration is a hallmark of this programme. Connecting with others will help you stay engaged, build workplace skills, and forge lasting connections with new colleagues across industries that we hope will last well beyond this course.

When you're in a Riff video meeting, Riff is measuring vocal activity; not what you say, but when and how you say it. This vocal activity tells us a lot about the dynamics of the group. We can measure: dominance, who is speaking the most and how often; influence, who is speaking after whom; interruption, what happens when another person grabs the mic; and affirmations, which are little vocal gestures that usually indicate how engaged people are. These are just some of the different kinds of human signals that people give off when they're meeting and collaborating together.

When you meet in person, you exhibit a lot of human signals. This helps you understand whether somebody trusts you, whether they're listening to you, whether they're engaged in what you're saying. When you're on a video, it's much harder to pick up on these signals.

In Riff, we give you an onscreen indicator which tells you who is dominating the call in real time, among other things. Immediately after the call, we surface additional metrics that give you more detailed information.

Armed with this information, you and all your teammates will start to understand when to interject and when to hold back. This awareness will help your team become more effective, accomplishing shared goals such as complex, challenging tasks that give you a reason to work together.

## The Riff Platform

Using artificial intelligence, we are re-architecting the experience of group collaboration through a new breakthrough technology.

The most effective learning experiences occur within small groups engaged in problem-solving exercises. However, in a digital/distributed work environment, how does one make this effective? Video conference calls cause people to tune out of the discussion.

Using artificial intelligence, we are redesigning the experience of group collaboration. This new capability changes the way your team members interact with one other in real time, as the video call is happening. We find that using Riff has enabled us to provide digital learning (online course) experiences with a Net Promoter Score more than 12X higher than conventional MOOCs on platforms like edX or Coursera, with a completion rate (% of those who start, versus those who finish the programme) 18X greater.

With a simple on-screen cue, people can have more effective team interactions.

## Personalised Feedback

The Riff Platform analyses interactions to create a confidential, personalised dashboard that you can use to assess your own work. This report will not be shared with anyone, but enables you to better understand your work, interactions, and group dynamic.

## Riff Chat

When you log into Riff, you will enter a chat application, much like Slack. Riff's chat feature is powered by [Mattermost](#), an open-source chat platform.

Riff's chat features three different types of channels.

**Public Channels** are channels that everyone can join. You will be automatically enrolled in a number of public channels. For example, "Town Square" is where informal conversations about the programme can happen. There will also be a public Programme Support channel for general questions about the programme.

**Private Channels or Small Group Channels** are channels that only invited members can access. This is where you will do your small group work. The channel activity can only be accessed by your small group, but will be monitored by a Success Manager, a Tutor, and some other Programme staff.

**Direct Messages** are conversations initiated by a learner with one (or more) other users on Riff. These may also be monitored by the Programme Team.

Any messages you send in Riff Chat should follow the learner behaviour guidelines outlined in the Learner Handbook and Honour Code.

You can receive and respond to your chat messages on your mobile device by using Mattermost, a third-party app that is available from Google Play and the Apple store. When you open the app, enter <https://said-oxford.riffedu.com> as the URL, and enter the user name and password that you created the first time that you accessed the Riff platform.

## Updating Your Personal Settings

To change your personal settings, click the main menu next to your name, and then click **Account Settings**. On this page, you can specify how you'd like to stay informed of Riff chats throughout the course, add your profile picture, and customise other settings.

## Riff Video

You will use Riff Video to conduct video meetings with your small group, connect with tutors, success managers, and each other. You'll be able to start a video meeting from within the chat window. More information on how to do that is below.

## System Requirements

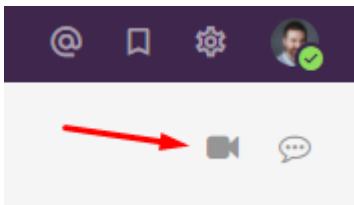
- A modern desktop or laptop computer with the following features. (Other devices are not supported.)
- The Windows or MacOS operating system.
- The latest version of Google Chrome, Mozilla Firefox, or Microsoft Edge.
- An enabled camera and microphone, to use with Riff.
- An internet connection with a minimum speed of 3 mbps for both upload and download (10 mbps is recommended).
- Please note: If you experience a loss of bandwidth during a Riff video meeting, Riff will automatically mute your video feed to improve performance.

## Starting and Joining a Riff Video Meeting

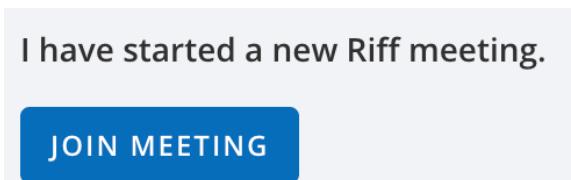
Usually, your small group leader will start the video chats for your team, though any member of the team can start a chat.

- Launch Riff Edu via any of the group exercises in the course, from the link at the top of this page, or by going directly to the Riff website.
- Open the channel where you want to have the video chat—usually that's your small group channel or in a direct-message window.

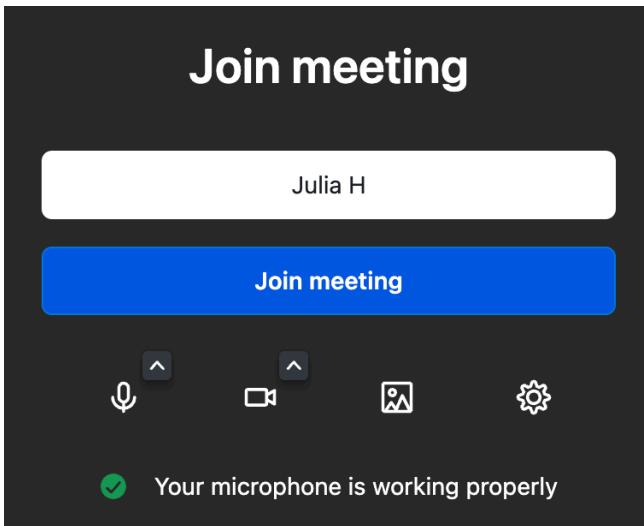
- In the top right corner of the page, click the video icon.



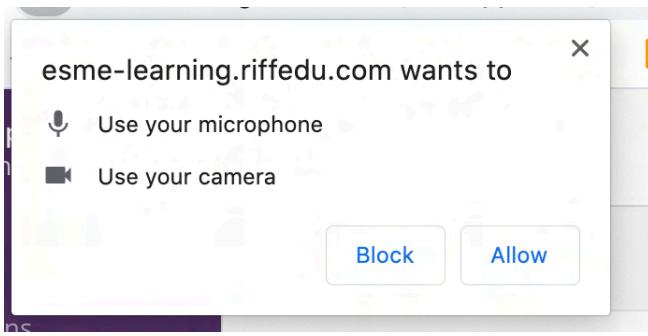
- If you are first to start a meeting, the video screen will overtake your chat screen and prompt you to join the meeting with video and audio on or muted.
- A **Join Meeting** button appears in the center of the channel page. **Note:** Anyone in the channel may join the meeting in progress. No one will be allowed to create a NEW meeting in the same channel while a meeting is already in progress.



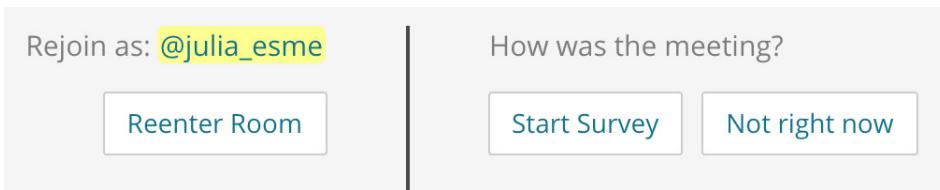
- Click **Join Meeting** to enter. You'll get a prompt asking you to confirm entry into the room.



- Make sure your camera and mic are working. The first time you join a video meeting in Riff, you'll be prompted to allow camera and microphone access. Click **Allow**.



- While in the meeting, you can expand your screen to see more of your group members or shared document, or collapse your screen to see the channel text chat window by clicking the expand-collapse icon in the top right.
- If you leave the meeting, you'll be given an option to re-join the meeting or view your meeting metrics.



- After the meeting, look at your Riff metrics in the Dashboard by clicking the **Riff Metrics** channel on the left side of the Riff Edu page or explore your connections to classmates by clicking **Connections**.



That's it! Enjoy your meeting!

## A word on privacy

Riff Video doesn't record any content. MIT research reveals that the pattern of communications between individuals and within a group are far more predictive of outcomes than the content. So Riff tracks who speaks, not what they say, to help optimise group performance while preserving personal privacy.

## Troubleshooting

A number of external factors can influence Riff's performance. If you have trouble, try the following suggestions before you contact support.

- Check your internet connection, including the speed. Riff requires at least 3 mbps of upload and download speed. Search for “internet speed test” on Google to find utilities that test your connection speed.
- Close all unnecessary applications.
- Use Chrome. Chrome limits the frame rate of the video without significantly degrading picture quality.
- If you've tried these suggestions and are still having trouble, email [oxfordsuccess@esmelearning.com](mailto:oxfordsuccess@esmelearning.com).

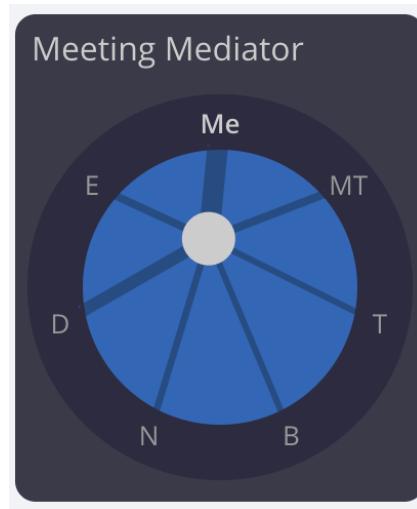
## Using Riff Metrics

Riff Edu provides feedback in two ways: during your video calls in the Meeting Mediator, and after your meetings on the Riff Edu dashboard. In the Meeting Mediator or on the dashboard, click the info button on any metric for details about what it measures and how to use it.

To learn more about Riff metrics, download [this document](#).

## Meeting Mediator

The Meeting Mediator measures your conversations in real time and gives passive feedback to the group.



Use the Meeting Mediator to see:

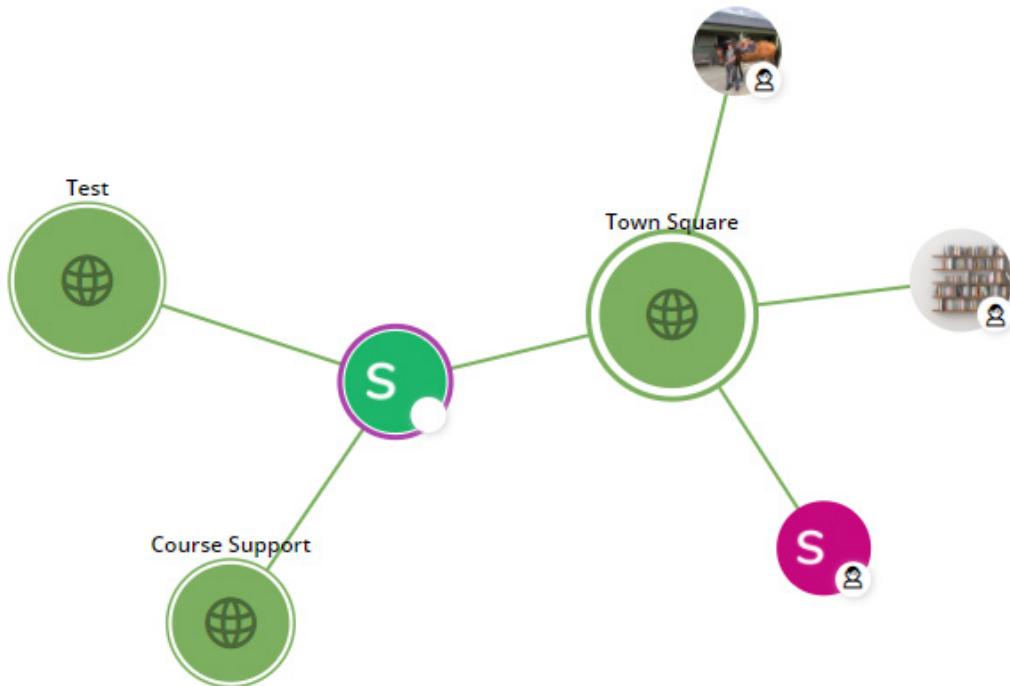
- How the conversation changes as it's happening: the central node moves towards whomever is speaking the most. Consistent thick lines and close proximity to a single user indicates conversational dominance.
- If people are over- or under-contributing: hover over a user node to see how much a person has spoken recently.
- How engaged participants are: hover over the centre node to see how many exchanges your group has had. A higher number represents a more energetic conversation, indicated by a darker shade of purple.

## Dashboard

The **Connections** link from the Riff Metrics dashboard shows you how your connections grow over the duration of the programme, and **Meeting Metrics** provides data about each of your video meetings.

### Connections

The network graph shows you how connected you are with your teams and others in the programme, and in which channels you are most active.



## Meeting Metrics

After each Riff video call, Riff will display a set of metrics about the conversation. Use this data to see:

- How balanced your speaking time was—whether you or other group members dominate the conversation, or need to speak up more.
- Do you engage with each group member equally or if there are some individuals you have a relatively strong connection with.
- Information about your interruptions and interjections.
- Did your meeting have a lot of turn taking (Energy) and if your entire group was engaged for a majority of the time.



# 4.0 Welcome to Oxford Blockchain Strategy

## 4.1.1 Getting Started

### Welcome to Your Online Learning Campus!

Welcome to the Oxford Blockchain Strategy Programme. Please take a moment to watch the following video that introduces you to your Online Learning Campus and how to navigate through the programme.

Thank you for joining Esme Learning, and welcome to the Online Learning Campus. This programme environment might be new to you. Please take a few minutes with this video to learn how to navigate the programme successfully. Note that the specific programme you see in this video may differ from the one you are enrolled in.

[ON SCREEN: Navigating the Programme]

After you sign in, select the programme on your dashboard. Once you have entered the programme, choose an item from the programme outline. We recommend beginning with the orientation. Programme content is organised into modules and lessons. A module lasts one week, and contains several lessons.

When you work through the programme, the pane on the left shows the module that you're working through along with the lessons in that module. In the centre of the page, you will see the content. At the top, the individual pages in each lesson are visible in the navigation bar. You can hover over the lesson to see its title, or if you are on a mobile device, you can long-press the lesson to reveal the title.

To ensure that you view every page in each lesson, use the "Previous" and "Next" buttons in the navigation bar, or at the bottom of each page, to progress through the programme. As you progress through the programme, you can check your progress by selecting the "Progress" tab.

[ON SCREEN: Types of Programme Content]

Throughout the programme, lessons are presented in a variety of formats, including text and video. To access programme materials, you simply need a modern browser. For learning on the go, most content loads well on a mobile device. To watch programme videos, click one of the two "Play" buttons. These buttons are located in the centre of the video window and in the lower left corner of the video window.

To change the video speed, click the "Settings" option in the lower right corner of the video window and then select the speed you want, from half speed up to twice the regular speed. To turn captions on or off, click the CC icon in the lower right corner of the video frame.

To view a transcript, click the "Download Transcript" button underneath the video player. The transcript will open as a separate browser page that you can print, or save as a PDF file in most modern browsers.

At the end of each lesson, there may be several ungraded knowledge check questions meant to reinforce the learnings of the current lesson. Note that these knowledge check questions do not impact your grade.

#### [ON SCREEN: Completing Assignments]

In your programme, you will complete a variety of assignments, including quizzes, individual reflections, and group exercises. These graded assignments factor into your final grade. All module assignments are due by the end of the module: Tuesday at 11:59 pm, Coordinated Universal Time. Note that the Online Learning Campus will translate that time to your local time zone based on your computer settings.

For quizzes, select the answers that you want and then click the “Submit” button. You will receive your score on the same page immediately, along with feedback to support your learning. The number of attempts per question is shown next to the “Submit” button.

For individual reflections, you submit your work by writing in the text box below the description. Note that once these assignments are submitted, they cannot be edited. For group exercises, you work with your peer learning group in a web-based, AI-enabled collaboration platform called Riff Edu. Here, you can easily connect with your group to discuss the exercise, or anything else related to that week’s content.

Below each team exercise, there is a button directing you to Riff. See the “About Riff” section at the top of the programme for more information.

At any time, you can check your progress through the programme by selecting the “Progress” tab. The “Progress” tab is separated by assignment type. Note that the assignment type average columns and total column to the far right are additive and will increase as you receive scores for graded assignments. When the total column passes the horizontal pass line, you will receive a certificate of attendance at the end of the programme.

Please reach out to your success team if you need any assistance during the programme. Good luck on your learning journey.

## Welcome to the Oxford Blockchain Strategy Programme!

You are embarking on a journey that is so much more than ordinary professional development. Using next-generation artificial intelligence (AI)-enhanced learning, you will gain actionable knowledge from experts in the field and build your professional network through engaging with other learners. Upon completing the Oxford Blockchain Strategy Programme, you’ll receive a prestigious certificate and join a global network of e-lumni with access to opportunities and events through Saïd Business School, University of Oxford.

As you pursue this certificate, we are invested in seeing you upskill, develop, and succeed! Throughout the programme, you will have a dedicated success team supporting you and cheering you on. You will learn more about this team and the Oxford Blockchain Strategy Programme in the orientation.

Let’s get started!

## Goals for the Week

Remember, if in doubt, just use the < Previous or Next > buttons located at the top and bottom of the page. This will ensure you're accessing every lesson.

Goals for the week are to:

- Verify your **identity**.
- Accept the **Honour Code, Terms of Service and Privacy Policy**.
- Understand **what you will learn** in the programme, and **how you will learn**.
- Document your **expectations** for the programme.
- Understand the **Capstone** project.
- Meet your **Success Manager** and **Tutor** and find out how to get support throughout the programme.
- Familiarise yourself with the **Riff Edu** collaborative platform.

Have questions? Need support? You can reach us at [oxfordsuccess@esmelearning.com](mailto:oxfordsuccess@esmelearning.com).

### 4.1.2 Welcome to the Programme

#### Faculty Video: Welcome to the Blockchain Strategy Programme

In this video, your Programme Director, Meltem Demirors, and Academic Director, Martin Schmalz, welcome you to the programme and give you an overview of what to expect.



Welcome to the Oxford Blockchain Strategy Programme. I'm so excited to be here with you today. My name is Meltem Demirors, and I will be your programme director. I've spent the last seven years building businesses in the blockchain technology ecosystem, and currently run a publicly listed investment firm called CoinShares.

Now, over the last seven years, I've gone through the same journey that you are about to embark on. The cryptocurrency space in the blockchain technology ecosystem is an interesting one, filled with new terminology, new words, and new concepts. And my job is to help you navigate this new and interesting world.

Throughout the course of the next six weeks, you'll walk through a variety of different modules, where you'll learn about some of the key components of blockchain technology, some of the benefits and challenges associated with this technology, and how you can best articulate the benefits of your specific use case. Now, in order to get the most out of this programme, I recommend you set aside 7 to 10 hours per week to really engage with the content and your peers. I'm looking forward to seeing you at the end of this journey and hearing about all you've learned along the way.



- Hello, and welcome. My name is Martin Schmalz. I'm an Associate Professor of Finance at Said Business School at the University of Oxford. I'm your academic director for this programme. And like Meltem, I'm excited that you're taking this journey with us.

I have a long history with the subject. I've published papers on consensus protocols, which is a crucial part of distributed ledger technologies, as early as 2007, when I was still a master's student. And I have invested in Bitcoin as early as 2011.

The reason I invested back then was, of course, mainly because spending time on cryptocurrencies was a more exciting way of spending time than working on my PhD dissertation in Economics at Princeton. But in the end, I got both. And as you will see in this programme, having learned both economics and blockchain technology comes with quite a few benefits that I do want to share with you in this programme.

So some advice I'd like to give you as you get started with this programme and learning about blockchain technology is the following: This is a fairly technical subject, and there's a lot to learn. Not only in terms of concepts, but also in terms of simple vocabulary.

But the team here did the best job imaginable to make the content accessible. So I encourage you to simply engage with the programme and spend time with it. Trust that you will absorb the content, not necessarily on the first time you hear it, but with extended and repeated exposure. And have fun. That's the best way of learning, anyways. With that, let's take it away.

## 5.1.3 What the Programme Will Cover

### What The Programme Will Cover

The Oxford Blockchain Strategy Programme is designed to provide you with the knowledge you need to understand the fundamentals of blockchain technology and cryptocurrencies, to think strategically about implementing a blockchain technology solution, and to understand the future of blockchain applications.

This curriculum explores the impact of blockchain technology on businesses, traditional platforms, financial services, governments, organisations and consumers. It will introduce potential transformations and use cases in a wide range of industries; practical considerations for regulation, compliance, and governance; and a balanced perspective of challenges and opportunities in this industry to enable you to propose a strategy and business case for blockchain technology.

To better understand practical applications for the theoretical concepts you'll learn, you will form groups to discuss and reflect on the course material and develop a persuasive blockchain use case for potential venture capital (VC) investors or an existing organisation's board of directors. You will obtain guidance from programme instructors and tutors, including discussions and webinars outside of core videos and exercises.

Through the programme, you will learn about:

- Cryptocurrencies and blockchain technology, the connection between technology choices, and their impact on business strategy.
- A wide range of use cases for blockchain technology across various sectors, including finance, telecommunications, energy, entertainment, and government.
- The cryptocurrency and blockchain technology ecosystem, the key players and competitive dynamics in the ecosystem, and the differences between emergent sectors of this industry.
- Tools and resources you can leverage to stay up to date on the latest technology and business developments in this rapidly evolving industry.
- Course frameworks to analyse and articulate the challenges and opportunities associated with the use of blockchain technology in a business setting.
- Formulating a suitable business case for using blockchain technology.

## Module Breakdown

### Module 1

In Module 1, you'll discover the components of a blockchain network, including protocols and different consensus mechanisms, how these components work, and the implications for different use cases. A key use case is currency, and in particular, Bitcoin. You'll explore the history of money, gold, and banking as a bridge to understanding the fundamentals of cryptocurrency, blockchain technology, and Bitcoin.

### Module 2

In Module 2, we will dive deeper into applications for blockchain technology in a variety of industries and learn how companies are blending new and traditional business models to monetise their blockchain solutions.

### Module 3

In Module 3, you'll explore the key players in the cryptocurrency and blockchain technology ecosystem, their roles, and their influence in this industry. You'll also identify the most relevant internal stakeholders involved in your project, business, or organisation, as well as the external stakeholders that are key to developing a blockchain technology solution.

## **Module 4**

In Module 4, you will examine organisational considerations related to decentralised authority and its challenges in the legal, regulatory, and environmental, social, and governance (ESG) areas of a blockchain project. Through this exploration, you will discover the dynamics of platform strategies and learn how to frame your blockchain project by addressing these considerations.

## **Module 5**

In Module 5, you will evaluate the benefits and risks of launching a blockchain startup, or bringing blockchain technology into an organisation, and will learn how to outline a business case for blockchain applications.

## **Module 6**

This week is designed for you to focus on completing your Capstone project. All of the sections in this material are voluntary and are structured as a “choose your own adventure” where you can read as little or as much about these applications as you would like. They include deeper dives into some of the topics that have already been covered as well as a few new ones, including a forward-thinking case study about blockchain for the public good. Pace any additional learning here with the time you need to finish and deliver your Capstone project. Module 6 will present an opportunity to explore what the future may look like for some of the leading-edge blockchain applications, including how to get involved in a blockchain ecosystem and how to keep your skills fresh. This module will also outline some of the ways you can become more involved in the global blockchain community, including the tools, resources, and references that you can continue to use after the course.

## **Programme Learning Outcomes**

At the end of this programme, you will be able to:

- Examine the basics of how a blockchain protocol works and outline a clear definition of blockchain technology.
- Understand how blockchain technology can be used as a digitally scarce asset, as a payment rail, or as a distributed ledger and evaluate whether a use case is suitable to be put on a blockchain.
- Develop strategies for engaging with the various stakeholders of a blockchain project.
- Prepare a plan to address legal, organisational, and environmental, social, and governance (ESG) challenges for a blockchain or crypto project.
- Formulate a suitable business case for blockchain technology.
- Present a persuasive blockchain use case to potential investors or to an existing organisation’s board of directors.

## 4.1.4 Your Capstone Project and Group Work

### Overview: Capstone Project and Group Work

Starting in Module 1, you will work with a group of your peers to complete a Capstone project. You and your group will work together to present a persuasive blockchain use case to potential investors or to an existing organisation's board of directors. Week to week, you will meet with your group and Tutors to complete exercises together that will lead into the final Capstone project in Module 6. This will allow you to get feedback along the way from the programme Tutors as you develop your ideas. The final submission in Module 6 is submitted as a blog post where you'll describe the viability of your use case and rationalise your findings. If you decide your use case is not a good use case, after all, you can motivate why it is not by using the same criteria you would use to explain why a use case is a viable solution.

Each week, a group exercise will build toward completing your Capstone project:

Module	Group Exercise
1	<p>Optional tutorial discussion with Tutor: Blockchain Technology definition and use case selection. This exercise is ungraded and will be recorded.</p> <p>Meet your group. In preparation for working as a group, you will complete a short exercise where you will get to know the strengths and personalities of your group members in order to create an effective group dynamic. You'll also be invited to a live tutorial session with your Tutor to prepare for your first assignment submission in Module 2.</p>
2	<p>Submit Capstone assignment for grade (0% to 100%).</p> <p>Define blockchain technology in your own words and use the suitability criteria in Module 2 to rationalise your chosen use case.</p>
3	<p>Optional tutorial discussion with Tutor: Stakeholder mapping and ESG challenges. This exercise is ungraded and will be recorded.</p> <p>In a live tutorial session with your Tutor, you'll go through a stakeholder mapping exercise and discuss challenges using a use case example. This is to prepare for your submission in Module 4.]</p>

- 4 Submit capstone assignment for grade (0% to 100%).
- Complete a stakeholder mapping exercise using the stakeholder mapping template from Module 3. Show the best way to engage each stakeholder to earn their support. Address any ESG, organisational, legal, and regulatory challenges and create a plan for your use cases using the framework in this module.
- 5 Optional tutorial discussion with Tutor: Business case and blockchain solution viability. This exercise is ungraded and will be recorded.
- In a live tutorial session with your Tutor, you'll go through a business case framework and use case viability to prepare for your final submission in Module 6.
- 6 Submit Final Capstone assignment for grade (0% to 100%).
- Assess the cost structure and revenue model of your blockchain use case. Focus on Module 5's business case framework to determine your business case viability and rationalise your findings. If you decide your use case is not a good use case, after all, you can motivate why it is not by using the same criteria you would use to explain why a use case is a viable solution.

## Faculty Video: Capstone Project

In this video, your Programme Director, Meltem Demirors, introduces the Capstone project you'll work on throughout this programme.



Oh, hi, there. I'm really excited to introduce you to your capstone project. Now one of the best ways to learn is not just by sitting here and listening to people like me talk, it's by actually doing. So what you'll be doing, together with your peers in this course, is designing your own blockchain use case. Throughout the course of this programme, you'll be going through each module and working on developing your own blockchain use case, and actually implementing the frameworks, strategies, and lessons that you're receiving.

So you'll learn how to actually construct a use case. You'll learn how to talk about some of the technology decisions you'll make associated with enabling that use case. You'll learn how to articulate some of the benefits as well as some of the challenges associated with your use case. And you'll learn how to talk about the business model and some of the key metrics that you might utilise to measure the success or an efficacy of your specific use case.

Now you'll be using something called the Riff platform to communicate with your classmates throughout this programme. And you'll have support from the Esme learning team. So don't worry, you're going to get a lot more detail and a lot more instruction on how this all works. I'm really excited to see what you come up with as you go through your capstone project. And I can't wait to see all of your submissions at the end of the course. Have fun!

## 4.1.5 How You Will Learn

### Guest Video: Pedagogy

In this video, Beth Porter, President & COO of Esme Learning Solutions, describes the various ways you will learn in this programme, including reinforcement exercises, a collaboration that consists of peer learning and exercises with your group, and experiential learning modeled on real-life scenarios..



In this video, I'll be talking about some of the pedagogy that guides this course. This programme is based on cognitive science to help you remember concepts long after the programme is over. We use techniques such as reinforcement learning, collaborative work, peer learning, and experiential learning to guide the development of our exercises.

You will work repeatedly in peer groups on real-world problems that mimic workplace conditions, such as time simulations, in order to help you develop relationships and build communication skills.

When people watch videos or read materials online, they tend to forget concepts very quickly. We use reinforcement learning to let you apply what you have watched, heard, or read immediately. You will then have a much higher likelihood of remembering it later and being able to apply it to your work scenarios.

We also incorporate topically relevant, realistic activities into the course, like those you're likely to encounter at work. Whether you're working through an interactive simulation, putting together a case study, or preparing for a group presentation, you'll get to experience things collectively with other course participants, and you'll be able to practice skills like immediate application of concepts, communications, and team building.

The Esme approach combines lessons from peer-reviewed research in cognitive and neuroscience on such topics as attention span, varied practice, memory and retention, activity-based learning, scaffolding, and worked examples. These approaches result in better learning experiences and lead to better outcomes.

## 4.1.6 Live Event Information and Registration

### Attend the (Optional) Live Online Kick-Off Event

We would like to formally invite you to the Oxford Blockchain Strategy Programme Kick-Off Event, occurring on **Thursday, 2 June, 2022** from **12:00 to 13:00 UTC**. (Try the [Time Zone Converter](#) to get your local time.)

The optional but recommended online live kick-off event will:

- Welcome you to the programme.
- Introduce you to the key members of your support team.

- Allow you an opportunity to connect and network with other learners in the programme.

[Registration](#) is required to attend. Once you register, you will receive an invitation with your unique URL to join. The event will be recorded for those who are unable to attend. We hope to see you there!

## Oxford Blockchain Strategy Webinar: Web3 Identity

We are excited to have you join us for this live event on Web3 Identity. In this session, we'll hear from Meltem Demirors and the following panelists:

- Evin McMullen, the CEO of Disco.xyz
- Kim Duffy, the Director of Identity and Standards at Centre

We will discuss some of the unique considerations and constraints in design, and some of the approaches being taken today, as well as emerging standards and best practices when it comes to designing more flexible, self-sovereign systems to help us manage our most valuable asset - our identity and our reputation.

The session will be recorded for those who are unable to attend.

The Live Webinar will be held on **Tuesday, 16 June, 2022 from 12:00 to 13:00 UTC**.

[Registration](#) is required to attend. Once you register, you will receive an invitation with your unique URL to join. The event will be recorded for those who are unable to attend. We hope to see you there!

## Attend the (Optional) Live Mid-Programme Q&A Event

Programme Director Meltem Demirors and Academic Director Martin Schmalz will host an Oxford Blockchain Strategy Programme Live Q&A Event, occurring on **Thursday, 30 June, 2022 from 12:00 to 13:00 UTC**.

In this optional-but-recommended online event, programme faculty will answer questions we've collected in the Riff Edu platform.

[Registration](#) is required to attend. Once you register, you will receive an invitation with your unique URL to join. The event will be recorded for those who are unable to attend. We hope to see you there!

# 6.0 Programme Requirements and Grading

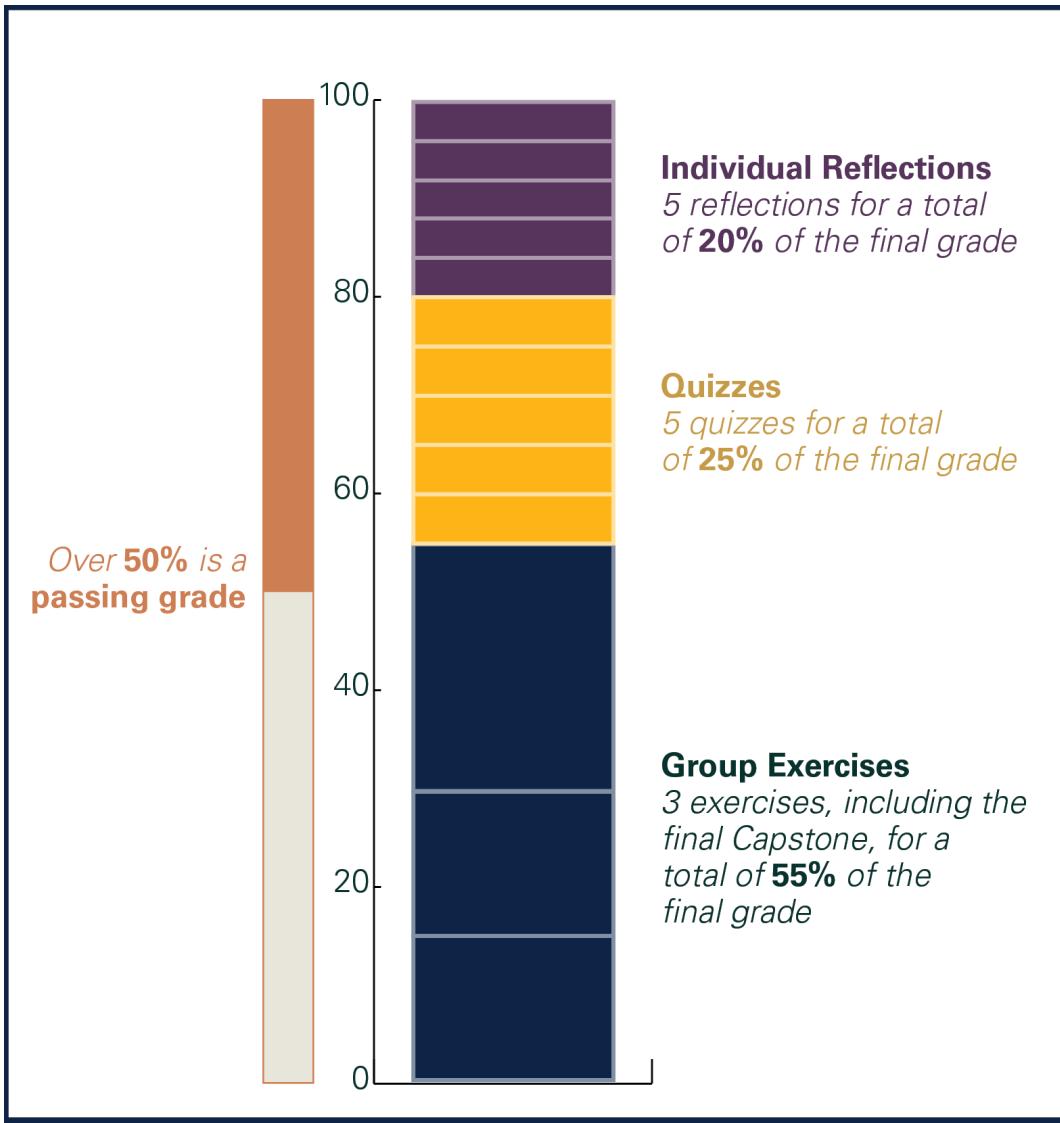
## 6.1.1 Requirements and Grading

### Programme Requirements

Your participation in the periodic quizzes and written reflections is required.

Throughout the programme you will also find optional discussion questions and prompts, which are not required but are encouraged.

As part of this programme, you will work with a group on a Capstone project. The group will work together week by week to create a blockchain project proposal presentation for a business of their choice.



## Grading

The following table shows how grading is calculated for the programme. You can see your grades on the **Progress** page.

<b>Group Exercises</b>  3 exercises for a total of <b>55%</b> of the final grade	<p>Longer questions, essays, or other content, created in collaboration with your group.</p> <p>Submitted in Modules 2, 4, and 6.</p> <p>Modules 2 and 4 are worth 15% of the final grade each, and Module 6 is worth 25% of the final grade.</p> <p>The Capstone project in Module 6 is a culmination of the group exercises and is submitted as a blog post.</p> <p>Group exercises are graded by programme Tutors. These assignments will be returned with tutor feedback and a grade (0% to 100%) one week after they have been submitted. Here is a breakdown of group assignments:</p> <ul style="list-style-type: none"><li>• Module 2: Submit Capstone assignment for grade (0% to 100%)</li><li>• Module 4: Submit capstone assignment for grade (0% to 100%)</li><li>• Module 6: Submit Final Capstone assignment for grade (0% to 100%)</li></ul>
<b>Quizzes</b>  5 quizzes for a total of <b>25%</b> of the final grade	<p>Answers to questions about key concepts and takeaways.</p> <p>Submitted in Modules 1–5.</p> <p>Answers are automatically graded.</p>

<p><b>Individual Reflections</b></p> <p>5 reflections for a total of <b>20%</b> of the final grade</p>	<p>Short essays (200 to 300 words) that allow you to reflect on, and put into your own words, the content of the module.</p> <p>Submitted in Modules 1–5.</p> <p>Programme staff review your reflections. You are not graded on the specifics of your reflection; you are graded on whether you submitted a response that shows thoughtfulness and a reasonable effort, for which you can receive:</p> <ul style="list-style-type: none"> <li>• 5 points (100% for the assignment) for a full effort.</li> <li>• 3 points (60%) for a partial effort.</li> <li>• 0 points (0%) for no submission.</li> </ul>
<p><b>Optional Tutorial Sessions (Ungraded)</b></p> <p>These are live sessions with Tutors that help you prepare for your capstone assignments submitted in Modules 2, 4, and 6.</p> <p><b>Note:</b> These sessions will be recorded.</p>	<p>Module 1: Optional Tutorial discussion with Tutor: Blockchain Technology definition and use case selection</p> <p>Module 3: Optional Tutorial discussion with Tutor: Stakeholder mapping and ESG challenges</p> <p>Module 5: Optional Tutorial discussion with Tutor: Business case and blockchain solution viability</p>

For you to pass the programme and receive a certificate, your final score must be at least 50%.

The 50% pass rate does not mean that this UK-based course is easier than an equivalent US-based course. In many (but not all) US institutions, a 70% grade is a “C” or a “D”, or a low passing grade. In the UK, the passing grade in many (but again, not all) institutions is 50%, and 70% is considered an “A”, or a high passing grade.

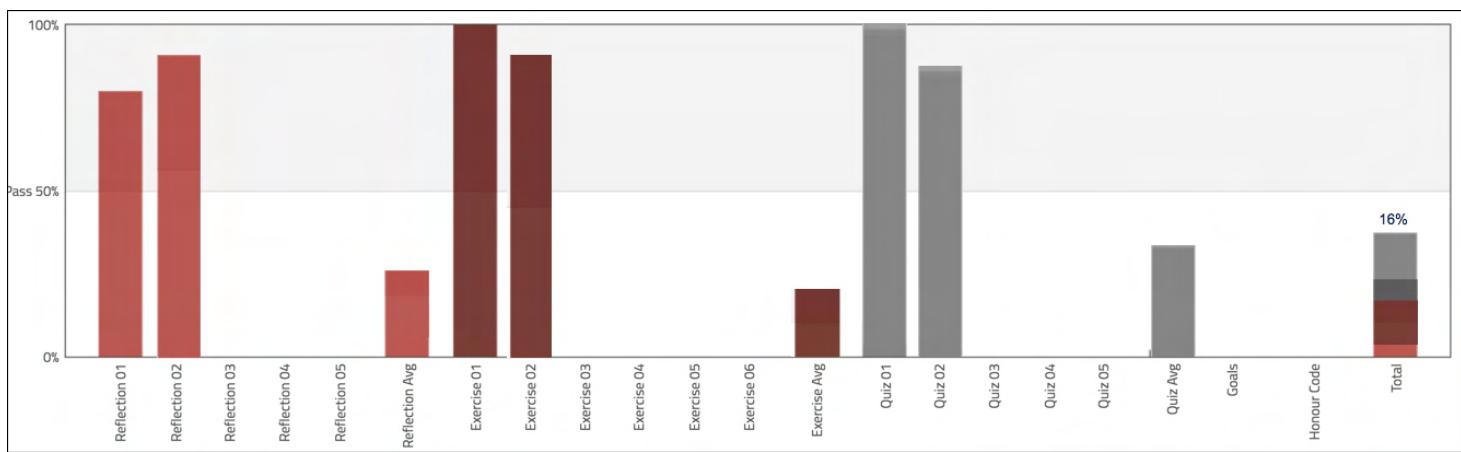
One system is not harder than the other; rather, the grading scales are different. If you took the same class in the US and in the UK, a passing grade could be 70% in the US and 50% in the UK.

## Viewing Your Grades

You can see your scores for graded assignments on the **Progress** page. The **Progress** page contains a chart of all graded assignments in the course. (Ungraded assignments, such as Knowledge Checks, are not shown in the graph, but are listed beneath it.)

You see the score for each graded assignment you have submitted. Note that the scores are grouped by type of assignment (Reflection, Exercise, Quiz), not by the sequence in the programme. Each bar shows your score on that assignment, from 0% to 100%. In this programme, each assignment is worth 10 points; therefore the bars will show scores in 10% increments.

In the following example, the learner has completed different assignments: the Reflection, Exercise, and Quiz through Module 2.



The “average” for each type of assignment and “Total” column at the right end of the progress chart are **additive**. This means that the “average” and “Total” columns reflect those amounts as if all assignments (whether completed or not) are graded. The Total column is calculated based on the weighting of the different types of assignments, described in the table above.

When the total score goes over the **Pass** line (50% in this programme), you have earned a certificate.

## Interpreting Your Progress Page

Below the **Progress** graph, you’ll see a breakdown of the entire programme. This breakdown lists every single section in the programme, and lets you know which sections have assignments:

- A section that says “No problem scores in this section” has no assignments.

Module 1: Introduction to Fintech	1.1 About Module 1
	<i>No problem scores in this section</i>

- Practice Scores represent the Knowledge Check problems. They are scored but do not affect your grade. You'll see whether or not you attempted these, and how you did.

1.2 Foundations of Fintech I (0/1)
<hr/> <hr/>
<b>Practice Scores:</b>
0/0   0/0   0/0   0/1

- Problem scores represent the quiz and written assignment scores that count toward your final grade. You'll see whether or not you attempted these, and how you did.

1.10 Quiz (0/13)
<hr/> <i>Quiz due Nov 10, 2020 18:59 EST</i>
<b>Problem Scores:</b>
0/1   0/1   0/1   0/1   0/1   0/1   0/1   0/1   0/1   0/1   0/1   0/1   0/1

**Note:** Scores for tutor-graded assignments, such as the individual exercise and group exercises (not the individual reflections), will appear on your **Progress** page by the Wednesday a week after the assignment due dates. Feedback for group assignments will be provided in your group's Riff channel. Feedback for individual assignments will be emailed to you.

# 7.0 Resources and Quick Help

## Orientation Recap

In this orientation, you learnt:

- About the expectations for learner behaviour in the programme.
- How to navigate the online programme.
- About the content and pedagogy in the Oxford Blockchain Strategy Programme.
- How to use Riff to meet with your classmates through chat and video.
- Ways to get support throughout the programme.
- About the Capstone project.

We hope you are looking forward to diving into Blockchain Strategy in Module 1.

## Downloads

[Honour Code](#)

[Terms of Service](#)

[Privacy Policy](#)

[Learner Handbook](#)

## Quick Help

You may reach your Success Manager by emailing [oxfordsuccess@esmelearning.com](mailto:oxfordsuccess@esmelearning.com).



Module 1:

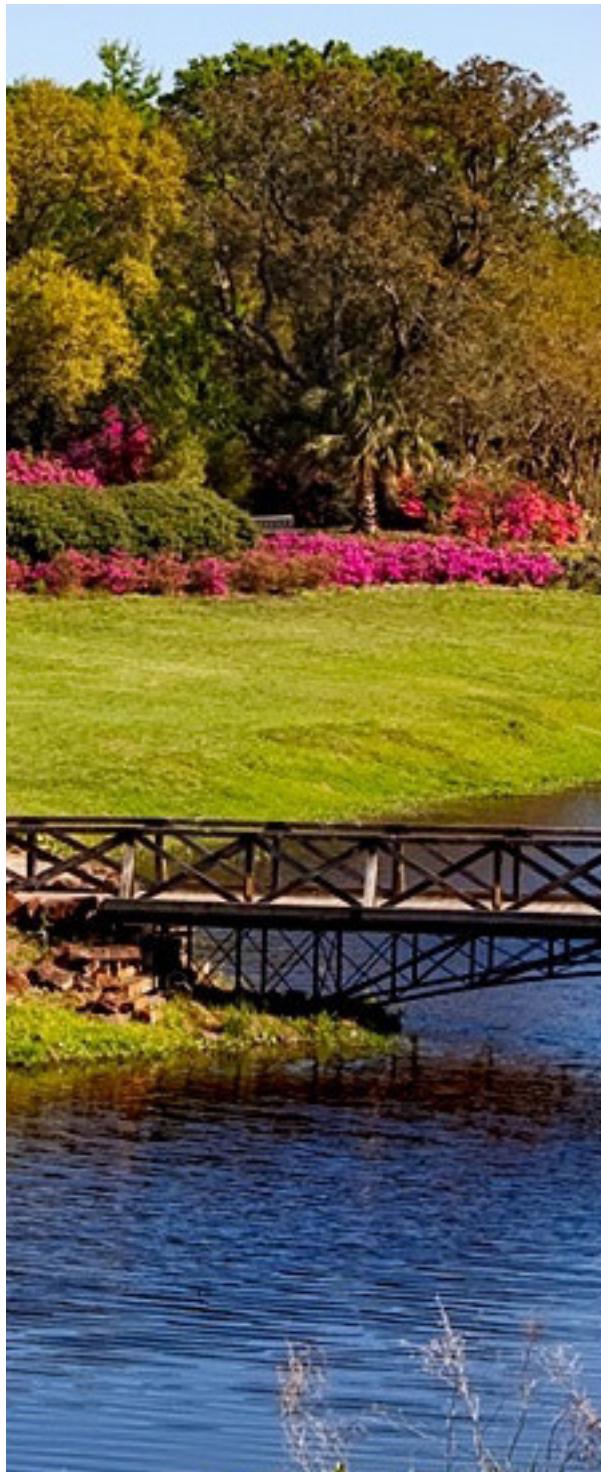
# Fundamentals: Blockchain Protocols, Networks, and Cryptocurrencies

---

Oxford Blockchain Strategy Programme  
2022

# Oxford Blockchain Strategy Programme

## Module 1: Fundamentals: Blockchain Protocols, Networks, and Cryptocurrencies



### Table Of Contents

<b>1.1 About Module 1</b>	<b>3</b>
1.1.1 Overview of Module 1	3
1.1.2 Animation: What is a blockchain?	6
1.1.3 Interest Groups	6
<b>1.2 Understanding Money as a Technology</b>	<b>8</b>
1.2.1 The Origins of Money	8
1.2.2 Flash in the Pan: The Rise and Demise of the Gold Standard	10
1.2.3 The Advent of Banking and the Creation of Money	11
1.2.4 Key Takeaways and References	13
<b>1.3 The Pursuit of Digital Money</b>	<b>16</b>
1.3.1 The Emergence of Digital Money	16
1.3.2 Digital Money Pioneers: Laying the Foundations	18
1.3.3 Who Runs the Ledger?	21
1.3.4 Key Takeaways and References	22
<b>1.4 Cryptography's Role in Blockchain Technology</b>	<b>25</b>
1.4.1 The History and Foundations of Cryptography	25
1.4.2 Cypherpunks and the Crypto Wars	29
1.4.3 Key Takeaways and References	30
<b>1.5 Introduction to Bitcoin</b>	<b>33</b>
1.5.1 Introduction to Bitcoin	33
1.5.2 The Birth of Bitcoin	35
1.5.3 The Evolution of Bitcoin	37
1.5.4 Key Takeaways, References, and Optional Reading	40
<b>1.6 Bitcoin as a Protocol, Network, and Asset</b>	<b>42</b>
1.6.1 The Bitcoin Network	42
1.6.2 Bitcoin Protocol	44
1.6.3 Bitcoin, the Asset	44
1.6.4 Key Takeaways, References, and Optional Reading	46
<b>1.7 Blockchain Technology Explained</b>	<b>49</b>
1.7.1 Components of Blockchain Technology	49
1.7.2 Consensus Mechanism	51
1.7.3 Smart Contracts	55
1.7.4 Token	56
1.7.5 Development and Maintenance	57
1.7.6 Growth in Bitcoin Tokens	59
1.7.7 Programming Language	60
1.7.8 Network	60
1.7.9 Key Takeaways, References, Optional Reading, and Additional Video	62
<b>1.8 Case Study: Venezuela's National Cryptocurrency – The Petro - Can a State-Backed Crypto Succeed on Crypto Terms?</b>	<b>88</b>
1.8 Case Study: Venezuela's National Cryptocurrency – The Petro	88

# 1.1 About Module 1

## 1.1.1 Overview of Module 1

### Overview

Welcome to Module 1 of the Blockchain Strategy Programme!

In Module 1, you'll discover the components of a blockchain network, including protocols and different consensus mechanisms, how these components work, and the implications for different use cases. A key use case is currency, and in particular, bitcoin. You'll explore the history of money, gold, and banking as a bridge to understanding the fundamentals of cryptocurrency, blockchain technology, and Bitcoin as a protocol.

You'll study the following key concepts in this module:

- The key properties and components of blockchain technology
- Blockchain protocols and consensus mechanisms
- Financial technology and the information revolution
- The history of money and gold
- The evolution of bitcoin
- The roles of bitcoin, Satoshi Nakamoto, and the Nakamoto white paper in the development of blockchain technology

Through an exploration of Venezuela's adoption of the petro as its national currency in this module's case study, Module 1 will also prepare you to dive deeper into other use cases and possibilities that the blockchain ecosystem offers.

## Programme Director Video: Module 1 Overview

In the following video, Meltem Demirors describes what to expect in the course and walks you through the subjects you will learn about this week.



Hi, and welcome to module one of the Oxford Blockchain Strategy Programme. I'm excited for you to learn about the basics of blockchain technology. We'll begin in the year 2008, when a pseudonymous individual named Satoshi Nakamoto published a white paper to the Cypherpunk mailing list outlining a new cryptographically-based currency system called Bitcoin.

In the years and decades that have followed since then, the world has seen the emergence of a variety of different types of blockchains utilising different consensus mechanisms. In this module, you will learn some of the basics of these different types of technologies, how they've worked, and what the implications are for the different types of use cases enabled by this technology.

You'll hear from technologists who are building new types of blockchain technology, utilising different cryptographic techniques, and some of the inherent trade-offs and scalability, security, and usage that result from these technological choices. Throughout this module, you'll learn some of the basic building blocks that comprise cryptocurrencies and the underlying blockchain networks on which they operate, as well as some of the computational infrastructure that's required to support blockchains at scale.

I'm excited for you to take this module and delve into some of the unique characteristics of this new technology that will be important for you to understand as you think about developing your own blockchain technology-driven business strategy.

## Learning Outcomes

By the end of this module, you will be able to:

- Recognise the scale of investment in blockchain technology and the significance of the blockchain industry.
- Understand the historical context that fostered the emergence of blockchain.
- Identify the key properties and components of blockchain technology.
- Outline a clear definition of blockchain and explain the potential effects this technology may have on business and society.

## Vocabulary

In each section, you will learn several new terms that are associated with blockchain technology. Develop a strategy to easily access the terms and their meanings as you move through this programme, employing memorisation techniques so that the terms become second nature to you.

## Graded Assignments

You will complete individual and group assignments, which count towards your completion of the programme. This week, you will:

- Complete a quiz on the module's content and key takeaways.
- Reflect on what you have learnt by applying it to your personal or professional experiences.

You must submit all graded assignments in Module 1 by **14 June 2022, 23:59 UTC**. (Try the [Time Zone Converter](#) to get your local time.)

## Additional Activities

In each module, we present additional activities related to the core learning. This week, you will:

- Discuss Venezuela's national cryptocurrency with your peers.
- Meet with your group in the Riff platform to complete an ungraded team exercise ahead of starting on your Capstone project in Module 2. See 1.9.1 for more information. We suggest you start a discussion in your small group channel soon to identify possible times for a 1-hour meeting this week.

## Time Commitment

Plan to spend seven to ten hours on Module 1 this week. As there is a lot of reading material and video content, you might want to divide your work into several sessions. The module is broken up into sections by theme, giving you potential break points.

Make sure you plan time to meet with your team and to complete the assignments.

## 1.1.2 Animation: What is a blockchain?

### Animation: What is a blockchain?

The following animation video introduces the fundamentals of blockchain technology.

What is a blockchain? As Bitcoin becomes more widely recognized, interest in blockchain, the underlying technology, is growing. But what is a blockchain? Put simply, a blockchain is a ledger, a set of records. Most ledgers are centralized. A single authority, such as a bank, controls the ledger. But blockchains use distributed ledger technology, or DLT. In a distributed ledger, no central authority needs to exist. Instead, each of the computers in a network, each so-called node, has a complete copy of the ledger.

Why the term blockchain? A block is a set of data, similar to a ledger entry. Blocks can store different kinds of information-- from financial transactions to medical records. Each block includes the transaction data, a timestamp, and a hash that identifies the previous block. A chronological series of blocks, or chain of blocks, makes up a blockchain.

Blockchain offers several potential security benefits compared to centralized ledgers. A blockchain keeps full copies of the ledger on every node. When a user submits a new block, a majority of the nodes on the blockchain must achieve consensus. They must agree that the transaction is valid before the block can become part of the chain. Blockchains are immutable, or unchangeable. Users can only add new transactions.

Attempting to modify a block corrupts the hash identifier, which breaks the connections between blocks and alerts the network. While the technology is still emerging, blockchains are now being used in applications that go far beyond cryptocurrency, such as tracking products, from start to finish, in global supply chains.

## 1.1.3 Interest Groups

### Interest Groups

Part of the value of this programme is realised by connecting with and learning from others from around the world with similar interests. As discussed in the Orientation, one way you will form connections with other learners is through the Capstone project. Each week you will work with your Capstone Group to develop a blockchain technology solution. This collaboration is an opportunity to learn from your peers and mirrors most on-the-job situations, in which you will work with others.

We also recognise that learners want to connect with and share ideas on certain topics with classmates outside of their Capstone Groups. For example, you might want to connect with other learners who are most interested in decentralised finance, who may or may not be in your Capstone Group.

To facilitate these connections, we will also set up Interest Groups in Riff, where you can share ideas with those with similar goals. The Interest Group channels are public, and you can join those in which you are interested. This is a space where you can share your thoughts on the programme's content to the degree you are comfortable, as an opportunity to get feedback on your ideas. You are also encouraged to provide feedback on the ideas of others in the Interest Group.

You will also see the Interest Group channels in the Riff navigation pane. You may want to limit the number of groups you join so you can fully participate in the discussions.

**Note:** When discussing your own business activities, carefully consider the information you share. Do not share confidential information that you do not want public.

# 1.2 Understanding Money as a Technology

## 1.2.1 The Origins of Money

### Overview

To understand how blockchain and its unique technological properties are helping to facilitate bitcoin, and its decentralised idea of money, it is helpful to look back at how money has evolved.

With a solid foundation of the origins and functions of money, its value in society, the rise and fall of the gold standard, the advent of banking and the global financial system itself, learners will understand what the original Bitcoin white paper proposed to solve and how and why blockchain developed into the technology that underpins bitcoin and other cryptocurrencies today. By extension, learners will then be able to ascertain how to apply blockchain technology to other virtual uses beyond cryptocurrencies.

**Note:** “Bitcoin”, as a term, can refer to bitcoin, with a lowercase “B”, as an asset, or to Bitcoin, with a capital “B”, as an environment that includes a network and a protocol, or set of rules for transferring data.

### Vocabulary

This section introduces the following terms:

- [double entry accounting](#)
- [medium of exchange](#)
- [unit of account](#)
- [store of value](#)

### The Origins of Money

Over the millennia, money has taken many forms: cowry shells, amber beads, gold coins, paper bills, and, in mediaeval England, eels. No matter what form money takes, its value in society is derived from its ability to serve three main functions: as a medium of exchange, a unit of account, and a store of value.

Today, money has evolved into one of the world’s most useful tools, or technologies, allowing the movement of value across vast distances of space and time, facilitating the exchange of value

between strangers with little or no history of interaction or trust between them, and making value a mutable, portable concept. Money has made trade and, indeed, all human economic activity possible—first between early societies and civilisations, and, today, in a globalised economy spanning both geographical regions and online.

But where did money come from? Economists, including Adam Smith, the 18th-century philosopher and economist, have long held that money evolved from bartering (Smith, 2018). Consider the hunter-gatherer who has killed a bison. Unless the meat was shared with the tribe, there was a risk that the meat would rot before its value—in the form of calories—could be extracted. But what if some of that meat could be exchanged for something else? Hunter-gatherers rarely had the surplus to trade, but by the Neolithic era, 12,000 years ago, as nomadic tribes learned to cultivate crops and domesticate animals and settled into larger groups, bartering and trading emerged. Meat, for example, might be swapped for grain.

As societies grew and migrated across larger distances, the limitations of bartering became evident. A farmer might want to trade their excess meat for grain, but what if the wheat farmer had enough meat and wanted instead to trade grain for tools? Keeping track of these trades between an ever-expanding number of partners was also increasingly unwieldy.

To solve the problem of tracking trades, residents of the ancient Mesopotamian city of Uruk used physical tokens to represent objects, including sheep and grain and created a written form of information about the exchange and store of value on clay containers and tablets. As this early form of accounting evolved, it eventually helped spawn an abstract system of symbols to represent quantities—that is, numbers.

By the mid-6th century BCE, the Mesopotamian shekel, physical coinage in the form of silver and gold, also began to appear. These coins could now be used to express value. Farmers could put a price on their meat or grain. Those performing services, such as carpenters, could put a price on their skills. Money, especially in the form of durable, nearly indestructible metal coins, also made it possible for the farmer or carpenter to store the value of their harvest or labour, accumulate wealth and carry the value of that wealth into the future, or transfer it to their descendants.

These early innovations that formed the basis of the early economies of Mesopotamia—money, mathematics, accounts, and writing—would eventually be replicated the world over, allowing

## Money

**Money is a technology to move value across space and time.**

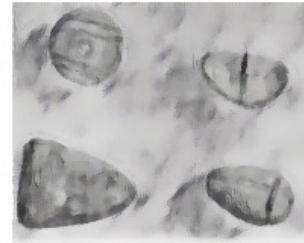
money has three core functions

a medium of exchange      a unit of account      a store of value



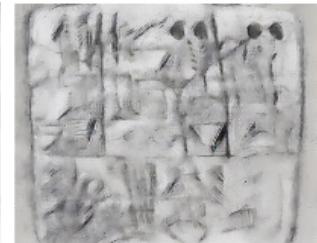
money provides two ways to keep track of who owes what to whom

tokens represent things



ancient Uruk tokens

ledgers represent the state of the world at a given time



ancient Uruk ledger

civilisations to manage obligations and other contractual commitments among parties who, essentially, had no reason to trust each other, who had never met and might not ever meet (Harford, 2017).

## 1.2.2 Flash in the Pan: The Rise and Demise of the Gold Standard

### Flash in the Pan: The Rise and Demise of the Gold Standard

Throughout history, gold has been prized for its inherent, unique qualities. Ancient civilisations revered gold as a beautiful, naturally rare, durable, and untarnishable metal. Because of its density and colour, gold is difficult to counterfeit, yet, it is malleable, meltable, and easily split into smaller units. The ancient Egyptians believed gold to be the “flesh of the gods,” and throughout many cultures across the world, it has been used to symbolise immortality, wealth, purity, and prestige (Schorsch, 2017). Gold, along with other metals, including silver and bronze, were eventually used to create coins, or currency, allowing value to be accumulated and transferred across space and time.



From the 19th century onwards, gold began to play a more central role in the world economy as countries adopted the gold standard, a monetary system that ties the value of a country's currency to a specific measure of gold, with a government guarantee that banknotes could be exchanged for their gold equivalent. In 1816, England became the first country to adopt the gold standard, followed by Germany and the United States in 1873. During its late 19th century rise, the gold standard was viewed as a symbol of a disciplined treasury. Under the gold standard, governments are constrained in their ability to freely print money (and devalue their currency) unless they have, or obtain, the gold to back it up. By the late 19th century, all of the world's major economies had joined the gold standard and, by pegging their currencies to gold, tied their currencies to one another. This helped facilitate trade and investment and usher in the first age of globalisation. The “golden age” of the gold standard lasted until World War I, when countries suspended it to fund their war efforts, causing the system to collapse (Crabbe, 1989). While Britain returned to the gold standard in 1925, the country abandoned it completely in 1931, in the face of complex economic challenges.

In 1944, near the end of World War II, 44 countries established an international monetary system called the Bretton Woods System. This model kept the US dollar fixed to gold and the other 43 countries' currencies fixed to the US dollar. This system remained in place until 1971, when, facing high unemployment and a slew of economic challenges, President Nixon ended the Bretton Woods System and, in doing so, the convertibility of the US dollar into gold (Ghizoni, 2013).

The gold standard eventually gave way to a system through which governments have more flexibility in setting monetary policy and responding to economic crises, using a wider range of tools, such as the setting of interest rates to stimulate or cool the economy. This flexibility allowed the US and UK governments, for example, to bail out a number of financial institutions following the Global Financial Crisis, under the rationale that allowing these key banks to fail would risk the collapse of the entire system.

While most mainstream economists believe that returning to the gold standard would harm the economy by inhibiting the ability to quickly and flexibly respond to a country's economic challenges, the idea has recently gained more support, mainly from those who see it as a check on government power and as a symbol of discipline and prudence (Stewart, 2020). This idea that governments should be limited in their ability to shape monetary policy, leaving it instead to the market to self-correct, is also a central tenet of the decentralised nature of bitcoin and other cryptocurrencies.

### 1.2.3 The Advent of Banking and the Creation of Money

#### The Advent of Banking and the Creation of Money

Modern banking has its roots in a system of accounting that gained widespread use in Renaissance Italy. In the late 1300s, double-entry accounting, a system of bookkeeping where an entry to one account has a corresponding entry to another account, emerged among Venetian merchants and banks as a way to track the increasingly complex web of credits and debts that their trading activities spawned (Sangster et al., 2012).

The Medici Bank (Banco de' Medici), owned by the powerful Medici family, for example, employed double-entry accounting, increasingly known as *alla veneziana*, or the Venetian way (Fazzini et al., 2016). It was not until 1494, however, that the complicated system gained widespread adoption after Luca Pacioli, a Franciscan friar and mathematics professor, published his textbook, *Summa de arithmeticā, geometriā, proportioni et proportionalitā*, which included a detailed, 27-page description of how to set up and use double-entry accounting. The innovative system is now heralded as one of the world's greatest inventions and has helped facilitate the rise of modern capitalism.



How did it do this? Double-entry accounting helped foster closer scrutiny and a deeper understanding of a business's operations by giving a complete view of its general ledger, a practice that became increasingly popular during the industrial revolution. In 1772, Josiah Wedgwood, founder of the extant pottery company, revived his failing business through his use of double-entry accounting. The careful recording of credits and debits allowed him to identify where his profits were made and to grow them, but it also gave him an entire, up-to-date view of his balance sheet or the complete value of his assets and liabilities (Hartford, 2017).

This accounting system persists today: when a bank customer makes a deposit (credit) to their account, for example, the bank must then record a corresponding liability (debit) to the bank's general ledger account. As more banks adopted double-entry accounting, banks began to accept deposits and extend credit based on risk (Demirors, 2020). Modern banks may look very different from their 15th-century counterparts, but their core purpose remains much the same.

## The Creation of Money

Today, money is created by both a nation's central bank and private sector commercial banks. Central banks manage the country's economy through monetary policy and a nation's money supply, while commercial banks provide financial services to consumers and businesses.

But what does it mean to "create money", and what is the role of the money that they create?

Two types of money exist in the financial system: outside money, or the money that the central bank issues, and inside money, or money that the private sector, such as commercial banks, create and that circulates among private consumers and businesses. Outside money is also known as "fiat currency" or "fiat money" because it derives its value from the trust that people place in the central bank or government backing it. That is, because the government decrees by fiat or formal authorisation that it is legal tender, people trust the currency will lawfully be accepted by other people to settle their debt obligations (Prasad, 2021, p. 26).

Today's money exists as credits and debits that take an electronic form in a central bank database instead of physical coins that move around a royal treasury and empire. Because money today is largely represented as information, central banks, to support monetary policy objectives, can influence the amount of money in the economy by adjusting short-term interest rates, which affects the availability of credit to commercial banks, and sets the deposit reserve requirements the commercial banks must hold in liquid assets.

Private commercial banks create money by extending loans to consumers and businesses. When a bank extends a loan to a consumer, the bank deposits the loan amount into the consumer's account, creating money. (In keeping with double-entry accounting rules, the bank must also create and record a corresponding liability on their balance sheet.) When the consumer makes a payment on the loan, the bank debits (decreases) their liability account which in essence destroys and removes the money from circulation. Private commercial banks have accounts with their central banks and transfer money back and forth.

Cryptocurrencies represent an attempt to create money outside the central bank system and governments. Bitcoin, to a great extent, was created in opposition to fiat currency and all that it represented. It is a system designed to allow parties to transact with each other without the need for a trusted third party, such as banks or governments. In an introduction to bitcoin, Satoshi Nakamoto, its pseudonymous creator, wrote, “The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible”.

As bitcoin and cryptocurrencies have gained ground, they have raised profound questions on the impact that they will have on the entire financial system and on the social and political implications of what it means to create money. Who gets to create and control money? How will a largely unregulated shadow currency impact fiat currency and financial stability? How should such a system be regulated? How should governments, central banks, and commercial banks respond to cryptocurrencies? How will cryptocurrencies impact how central banks carry out monetary policy? Do cryptocurrencies like bitcoin live up to the promises outlined in Nakamoto’s introduction? Do cryptocurrencies have a better track record than fiat currencies with regard to breach of trust?

## 1.2.4 Key Takeaways and References

### Key Takeaways

Let's review the key points of this section:

1. Money is a medium of exchange, a store of value, and a unit of account. The development of money helped people move value across time and space. As social groups became larger and more spread out, it became difficult to track credits and debts. Money resolved that issue.
2. Money was a way to move value across distances in societies without written systems of record. Before most people could read and write, information was difficult to preserve. Through money, value could finally be passed down from generation to generation.
3. Gold emerged as an early form of physical money. Gold's specific characteristics made it valuable. It is durable, portable, divisible, verifiable, and scarce. Later, gold would be used to back the currencies of the major world economies in what was called the gold standard.
4. Banks evolved out of needs driven by physical money, which was dangerous to transport and store, and took different forms by region. Rather than exchanging physical money, rich and poor alike relied on a system of reciprocity. This informal system evolved into banking, which relies on centralised institutions taking deposits and extending credit based on risk.

5. Double-entry accounting, which emerged in 14th century Italy, is a bookkeeping practice that allows an up-to-date understanding of a company or bank's balance sheet, that is, the complete value of its assets and liabilities. Banks continue to use double-entry accounting today.
6. Today, money is created by both a nation's central bank and private sector commercial banks. Central banks manage the country's economy through monetary policy and a nation's money supply, while commercial banks provide financial services to consumers and businesses.
7. Cryptocurrencies represent an attempt to create money outside the central bank system and governments.
8. Bitcoin and cryptocurrencies raise profound questions on the impact that they will have on the entire financial system and on the social and political implications of what it means to create money.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

### 1.2.1 The Origins of Money

Harford, T. (2017, 12 June). How the world's first accountants counted on cuneiform. *BBC*. <https://www.bbc.com/news/business-39870485>

Smith, A. (2018, 5 February). An Inquiry into the Nature and Causes of the Wealth of Nations. *Library of Economics and Liberty*. [https://www.econlib.org/library/Smith/smWN.html?chapter\\_num=7#book-reader](https://www.econlib.org/library/Smith/smWN.html?chapter_num=7#book-reader)

### 1.2.2 Flash in the Pan: The Rise and Demise of the Gold Standard

BBC. (2020, 5 August). Gold price rises above \$2,000 for first time. <https://www.bbc.co.uk/news/business-53660052>

Crabbe, L. (1989, June) The International Gold Standard and U.S. Monetary Policy from World War I to the New Deal. *Federal Reserve Bulletin*. <https://fraser.stlouisfed.org/files/docs/meltzer/craint89.pdf>

Ghizoni, S. (2013, 22 November). Nixon Ends Convertibility of U.S. Dollars to Gold and Announces Wage/Price Controls. *Federal Reserve History*. <https://www.federalreservehistory.org/essays/gold->

## convertibility-ends

Glint. (2019, 14 April). The History of Gold as Money. [https://glintpay.com/en\\_us/blog/gold-diversify-portfolio-2](https://glintpay.com/en_us/blog/gold-diversify-portfolio-2)

Schorsch, D. (2017, January). Gold in Ancient Egypt. In Heilbrunn Timeline of Art History. New York: The Metropolitan Museum of Art, 2000-. [http://www.metmuseum.org/toah/hd/egold/hd\\_egold.htm](http://www.metmuseum.org/toah/hd/egold/hd_egold.htm)

Stewart, E. (2020, 17 November). Why Trump and McConnell are trying — and failing — to push through Fed pick Judy Shelton. Vox. <https://www.vox.com/policy-and-politics/2020/11/17/21569992/judy-shelton-federal-reserve-trump-nominee>

### **1.2.3 The Advent of Banking and the Creation of Money**

Demirors, M. (2020, 14 May). The Great Race for Assets. *Meltem Writes Things*. <https://meltdem.substack.com/p/the-great-race-for-assets>

Fazzini, M., Fici, L., Montrone, A., Terzani, S. (November-December 2016). A Modern Look At The Banco De' Medici: Governance And Accountability Systems In Europe's First Bank Group. International Business & Economics Research Journal, 271-286. <https://clutejournals.com/index.php/IBER/article/download/9827/9921/36514>

Fontevecchia, A. (2010, 19 November). How Many Olympic-Sized Swimming Pools Can We Fill With Billionaire Gold? *Forbes*. <https://www.forbes.com/sites/afontevecchia/2010/11/19/how-many-olympic-sized-swimming-pools-can-we-fill-with-billionaire-gold>

Hartford, T. (2017, 23 October). Is this the most influential work in the history of capitalism? BBC. <https://www.bbc.co.uk/news/business-41582244>

Hobrow, T. (2017, 2 June). From Double-Entry to Blockchain. *VenturesOne*. <https://venturesone.com/double-entry-blockchain>

Nakamoto, S. (2009, 11 February). Bitcoin open source implementation of P2P currency. *P2P Foundation*. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>

Prasad, E. S. (2021). The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance. The Belknap Press of Harvard University Press.

Sangster, A., Stoner, G., De Lange, P., O'Connell, B., & Scataglini-Belghitar, G. (2012). Pacioli's Forgotten Book: The Merchant's "Ricordanze". *The Accounting Historians Journal*, 24–44. <http://www.jstor.org/stable/43486714>

# 1.3 The Pursuit of Digital Money

## 1.3.1 The Emergence of Digital Money

### Overview

A number of early attempts to digitise money laid the intellectual and technological groundwork for bitcoin. In this section, we identify the most important pioneers and examine their contributions that led to bitcoin. In later sections, we will delve more deeply into these technological concepts. We will also closely examine the role that cryptography, in particular, played in the conception of a privacy-preserving, decentralised digital currency and the players who drove this idea forward.

### Vocabulary

This section introduces the following terms:

- [exchange value](#)
- [fiat currency](#)
- [Information Revolution](#)
- [informational value](#)
- [use value](#)

### The Emergence of Digital Money

One of the biggest paradigm shifts and drivers of wealth creation in the last century has been the information revolution, enabled in part by the advent of the internet and the surge in big data. Since the beginning of the 21st century, our ability to collect, store, and process data has been unprecedented: Data is now ubiquitous. And, while its widespread use today raises questions of privacy, the high volume analysis of data and the novel ways to process analytical outcomes are fuelling the information revolution we are now experiencing. In turn, the information revolution is driving the emergence of new business models.

Last century's information revolution, along with the advent of the internet, paved the way for the radical transformation of several industries, from media and entertainment, retail and mobility, travel and hospitality, and finance and banking.

Innovation around money, however, remained limited and elusive, despite numerous attempts starting as early as the late Eighties to “[digitise]...the final mile of electronic money, where the coin and dollar

bill go the way of the vinyl LP..." (Levy, 1994). Digital cash pioneers believed that electronic money would one day allow people to pay one another online as easily as they paid each other in cash. People would be able to send money across nations and borders to whomever they choose, without banks or credit cards acting as intermediaries, charging high transaction fees, and imposing low spending limits on microtransactions. Early electronic cash proponents also insisted that any digital form of money should preserve the privacy of its users, just as physical cash does.

Creating digital money caused two immediate challenges: how to preserve the anonymity of the user; and how to ensure that a unit of digital money, now represented as bits and bytes, remains "scarce" and cannot be copied and spent again (and again)—a risk referred to as the "double spend problem".

In the physical world, cash protects the anonymity of both the spender and creditor. Moreover, when paying cash, an individual cannot double-spend or pay the same coin or token to more than one creditor. In today's digital world, the double-spend problem is solved by banks, acting as trusted central authorities that check and authorise transactions on their ledgers. Indeed, much financial technology today deals with the problems that arise from double-spending and reconciling vast amounts of financial data across centralised, siloed databases.

Throughout the Nineties and early Noughties, several initiatives emerged to tackle the challenges of digital money. While none gained significant mainstream use, and some never moved beyond the conceptual stage, these pioneering attempts laid down the technological and intellectual groundwork for future efforts, eventually leading to Bitcoin.

## The Impact of Information on Modern Economics

The information revolution has also had a significant impact on modern economics. Information has become a critical systems input alongside other common economic modalities, such as labour or capital. It has also been monetised or converted into a commodity or product that is bought and sold (Veneris, 1990). As a product, information acquires use value and exchange value, and therefore a price. All products have use value, exchange value, and informational value. For example, cars have a use value because they provide transportation, and they have an exchange value because people buy cars for a price. Cars also have an informational value, as the knowledge to produce, market, and distribute cars requires the investment of time and money.

The management of information led to the need for bureaucrats, so-called "white-collar workers" who could stay atop of this wealth of data. Information-related activity, in fact, comprises its own sector of the economy, distinct from extractive activities like farming or mining or manufacturing activities like food production or auto fabrication (Veneris, 1990). New information, in turn, leads to technology innovation, and the dissemination (or "diffusion") of this innovation can create crisis and renewal, a process which Joseph Schumpeter called "creative destruction" (Caballero, 2008).

With innovations in technology, access to information becomes more widespread and plentiful. There are many outlets via the internet where information is disseminated - news channels, online libraries, and social media, to name a few. In addition, the speed at which this information becomes accessible is near-instantaneous in many cases like current events and financial transactions. For example, earlier

this century, banks stopped trading actual checks in the clearing process and instead began trading images and data or information. That new process became a game-changer in the financial world, and the competitive forces have consistently improved upon this process ever since. Through what is now the traditional online banking process, consumers and businesses can access this same information with unprecedented speed and accuracy. These innovations created the foundations from which digital money could evolve, and they ultimately underscored the platform on which bitcoin was built.

### 1.3.2 Digital Money Pioneers: Laying the Foundations

#### Digital Money Pioneers: Laying the Foundations

In 1989, David Chaum, a computer scientist and cryptographer, founded DigiCash. Chaum, a long-time privacy advocate, was insistent that digital cash had to preserve a person's anonymity, noting as early as 1983 that the ever-expanding electronic data trail that a person's digital transactions left behind made it easy to reveal "...a great deal about the individual's whereabouts, associations and lifestyle" (1983).

Digicash created a system of currency called cyberbucks that could be used to make secure, online payments, free of the low payment limits that credit cards often imposed. Most importantly, DigiCash preserved the anonymity of the user. DigiCash, based on Chaum's seminal 1982 paper, Blind Signatures for Untraceable Payments, used cryptography to create blind digital signatures, which allowed users to sign off on transactions without identifying who they were (Chaum, 1983).

To use cyberbucks, DigiCash customers had to convert money from their bank account into the digital currency, which was then stored on their hard drive. Transactions were cleared through the DigiCash platform, which confirmed that the digital signatures were valid and, thus, that the transactions were authorised.

Despite garnering respect in both the tech and financial sectors, as well as a partnership with Mark Twain Bank, a regional institution, DigiCash declared bankruptcy in 1998. Ultimately, the platform was unable to gain traction with either merchants or consumers, both of whom saw little need for it (Hussey, 2019). Moreover, while DigiCash cemented the use of cryptography to keep electronic money private and secure, it still acted as a centralised gatekeeper to ensure that transactions were valid and cyberbucks were not double-spent.

The next significant development to emerge in the digital money space was Hashcash. The brainchild of British researcher Adam Back in 1997, Hashcash was originally conceived to prevent spam email and denial-of-service (DoS) attacks from malicious entities. Back's platform, which acted as a proof-of-work system, used cryptographic hash functions to solve the challenge of people repeatedly using a digital file (Back, 2002).

To produce one unit of Hashcash, users had to solve mathematical equations that required brute-force computing power. Hashcash, as a digital currency, was never implemented, as a unit of Hashcash could be used only once, thereby suffocating its usefulness as a medium of exchange (Popper, 2016, p. 18).

One year later, Nick Szabo, a computer scientist and cryptographer, came up with the concept of “bit gold”, a token that required Hashcash’s proof-of-work functionality, but could also be used more than once. Hal Finney, another computer scientist and collaborator of Szabo’s, proposed his own solution, which he called Reusable Proofs-of-Work (RPOW). Another American computer scientist, Wei Dai, proposed, though never implemented, b-money, a digital currency that not only required proof-of-work but that it be verified on a shared community ledger (Reiff, 2018).

Despite the best efforts of these early pioneers, digital money stalled until 2008 due to its inability to surmount several key obstacles. In particular, none of the experiments found a way to bypass a central authority figure that was either regulated by the government (banks) or invulnerable to an attack (or bankruptcy) that could destroy the entire system. As Nathaniel Popper noted in Digital Gold (2016), by the late 2000’s, “The goal of creating digital money seemed as much of a dream as turning coal into diamonds”.

## Enter Bitcoin

In 2008, six weeks after Lehman Brothers, the fourth-largest US investment bank at the time, collapsed and plunged the world into economic crisis, a person, or group of persons, identifying themselves as Satoshi Nakamoto posted a message along with a nine-page white paper to a cryptography listserv.

“I’ve been working on a new electronic cash system that’s fully peer-to-peer (P2P), with no trusted third party,” Nakamoto wrote by way of introduction (Nakamoto, 2008).

The paper outlined the workings of Bitcoin, which took the work of the earlier digital money pioneers and built upon it by proposing a solution to the challenge of a centralised authority. Now, participants could be pseudonymous (as a public ledger, anyone can view basic transaction details, including the sender and receiver’s public key address) through encrypted digital signatures; coins could be spent online and were reusable, using HashCash’s proof-of-work concept; and the double-spend problem was resolved through a P2P network. Specifically, Bitcoin proposed to prevent double-spending through a “peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions” (Nakamoto, 2009).

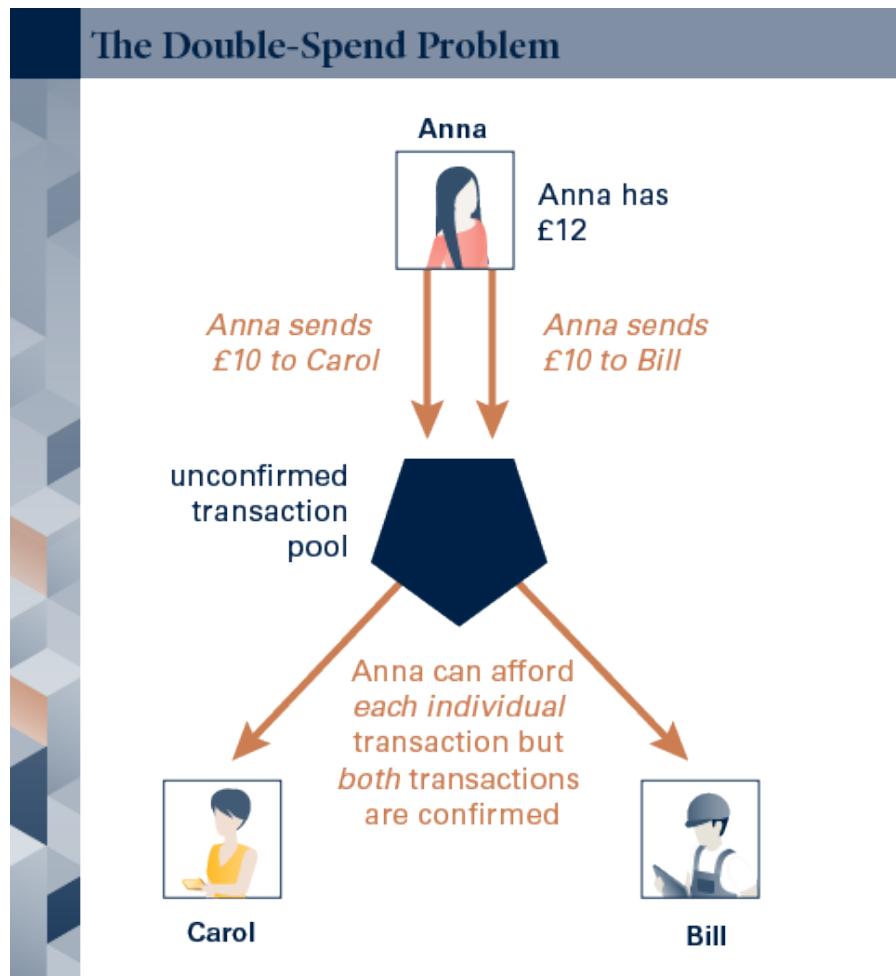
## Double-Spending

In an earlier section on the Advent of Banking, we referenced double entry accounting and its role as a bookkeeping method in banking. Yet, money in the form of ledger entries instead of physical currency leads to the “double-spend” risk (Gigi, 2021). Let’s say Anna has £12 in her account. She wants to send money to Carol and Bill and initiates two transactions simultaneously, both for £10. If there is a breakdown in the ledger accounting system, £20 would be sent from her account when there is only £12 available to send. This represents the “double-spend” problem.

This risk does not exist in the physical world, where an individual cannot “double-spend” or pay the same coin or token to more than one creditor. In today’s digital world, central banks and large financial

institutions—the record keepers—centralise the process of giving and receiving money. However, as information in a ledger now represents money without a corresponding physical token, how do we know that the ledger accurately represents our money?

Much financial technology today deals with the problems that arise from double-spending and reconciling vast amounts of financial data across centralised, siloed databases.



## The Ledger

In accounting, the ledger represents the listing and summaries of the debits and credits for a business entity of any kind. A bank or a bank account operates with a ledger. A ledger balance, then, is calculated at a point in time by aggregating all of the debits and credits against the previous point in time's balance. A breakdown in this process is what allows Anna to send more money out than what she actually has in her account.

### 1.3.3 Who Runs the Ledger?

#### Who Runs the Ledger?

Creating money as information was one of the core challenges facing internet pioneers when they built digital money systems to connect financial transactions with the online experience. Creating and maintaining trust remains a core challenge.

When one party presents information about money to a second party, the second party needs to be able to trust that the information accurately reflects reality. Additionally, a trusted third party is necessary to update the information as soon as the money is transacted.

This third party, who controls the ledger, must keep accurate information: With currency backed by physical tokens, people can't spend money that they don't have or that they already spent (Gigi, 2021). Traditional money is backed by physical laws, such as when it is issued, its denominations, and what form that issuance takes. In the digital realm, however, physical laws don't apply. There is no physical restriction preventing a person—or bank—from double-spending or fabricating money, from hundreds to billions of pounds, simply by adding an entry to a ledger. To keep ledgers and those who manipulate them accurate and honest, governments and other organisations must enact artificial or non-physical laws. Additionally, independent auditors must be able to verify that the information in the ledger is accurate by reading through time-stamped entries that have a clear, definite order.

#### Guest Video: Decentralising the Truth

In this video, Yaniv Tal, CEO of Edge & Node, discusses the relationship of truth and decentralised information, and the next stage in the information revolution.



A lot of this is tied to a really fundamental understanding and notion of truth, and what is truth, and how do we determine truth. At one point, the truth was whatever the church said. The church worked really closely with monarchies, and whatever the king said was truth.

Then the printing press came along, and suddenly a lot more people could contribute to what they consider to be the truth. And for some period of time, chaos ensued as people tried to figure out how do we filter through what anybody can print and what that means.

Then truth got decentralised with broadcast media. Suddenly you had newspapers, television, radio, and these broadcast media that were kind of one too many, ended up being able to define what was broadly accepted as truth.

And now the internet, of course, decentralised that when it comes to information flow. So that anybody can, again, like the printing press, print their version of the truth. But humans don't have a capacity to filter through such a large, endless stream of information to really be able to determine for themselves what is true.

And so the next stage in this evolution is blockchains, and in allowing anybody to contribute the way the internet intended to the public commons of information. But having a process by which we can converge into different forms of consensus, so that people can actually start to understand, again, the sources, where information is coming from, how to validate that information, and then have that information available to everyone.

### 1.3.4 Key Takeaways and References

#### Key Takeaways

Let's review the key points of this section:

1. Innovation around the digitisation of money was slow to develop, given the significant challenges that creating digital money posed.
2. Digital cash pioneers believed that electronic money would allow people to send money across nations and borders to whomever they choose, without banks or credit cards acting as intermediaries, charging high transaction fees, and imposing low spending limits on microtransactions. Digital cash should also preserve the privacy of its users, just as physical cash does.
3. Two challenges for digital cash pioneers included how to maintain the privacy of the user, and how to ensure that digital money could only be used once and avoid the "double-spend problem," in which a unit of digital cash is copied and spent again (and again).
4. Digital money pioneer, DigiCash, allowed its users to make secure, online payments, as well as preserving their privacy, through the use of cryptography. DigiCash, however, was still a centralised gatekeeper preventing double-spending.
5. The use of a cryptographic hash to prevent double-spending was first proposed by computer scientist and cryptographer Adam Back in 1997. Other digital money experiments or concepts to use cryptographic hashing to prevent double-spending include bit gold and b money.
6. In 2008, the pseudonymous Satoshi Nakamoto, proposed Bitcoin, an electronic cash system, that used cryptography and a P2P distributed time-stamped ledger, to offer an electronic currency that was pseudonymous, secure, could not be double-spent, and was under no central authority.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

### 1.3.1 The Information Revolution

Caballero, R. (2008). Creative Destruction. *The New Palgrave Dictionary of Economics*, Second Edition, Durlauf, S., & Blume, L. (Eds.). <https://economics.mit.edu/files/12606>

IEEE. (2021). Claude E. Shannon. *IEEE Information Theory Society*. <https://www.itsoc.org/about/shannon>

IEEE. (2021). Werner Buchholz. *IEEE Computer Society*. <https://www.computer.org/profiles/werner-buchholz>

Moore, G. (1975). Progress in digital integrated electronics. *Semantic Scholar*. <https://www.semanticscholar.org/paper/Progress-in-digital-integrated-electronics-Moore/12166e7d8e5a1a02b26e4ac21a22616e5e03dfdd>

### 1.3.2 Money Today

Back, A. (2002, 1 August). Hashcash - A Denial of Service Counter-Measure. *Hashcash.org*. <http://www.hashcash.org/hashcash.pdf>

Chaum, D. (1983). Blind Signatures for Untraceable Payments. *Advances in Cryptology*, 199-203. <https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF>

Hussey, M. (2019, 4 February). What was DigiCash? *Decrypt*. <https://decrypt.co/resources/digicash-what-is-cryptocurrency-explainer>

Levy, S. (1994, 1 December). E-Money (That's What I Want). *Wired*. <https://www.wired.com/1994/12/emoney/>

Nakamoto, S. (2008, 31 October). Bitcoin P2P e-cash paper. *Metzdowd*. <https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html>

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.org*. <https://bitcoin.org/bitcoin.pdf>

Popper, N. (2016, 24 May). *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. Harper Paperbacks.

Reiff, N. (2018, 22 June). B-Money. *Investopedia*. <https://www.investopedia.com/terms/b/bmoney.asp>

Wirdum, A. V. (2018, 12 July). The Genesis Files: With Bit Gold, Szabo was Inches Away From Inventing Bitcoin. *Bitcoin Magazine*. <https://bitcoinmagazine.com/culture/genesis-files-bit-gold-szabo-was-inches-away-inventing-bitcoin>

# 1.4 Cryptography's Role in Blockchain Technology

## 1.4.1 The History and Foundations of Cryptography

### Overview

Before we explore Bitcoin, cryptocurrencies, and blockchain technologies, we'll examine cryptography more closely. This seminal practice underpins the building blocks of bitcoin and blockchain in general. Cryptography is also the basis of a political and social movement that aims to ensure the privacy rights of citizens.

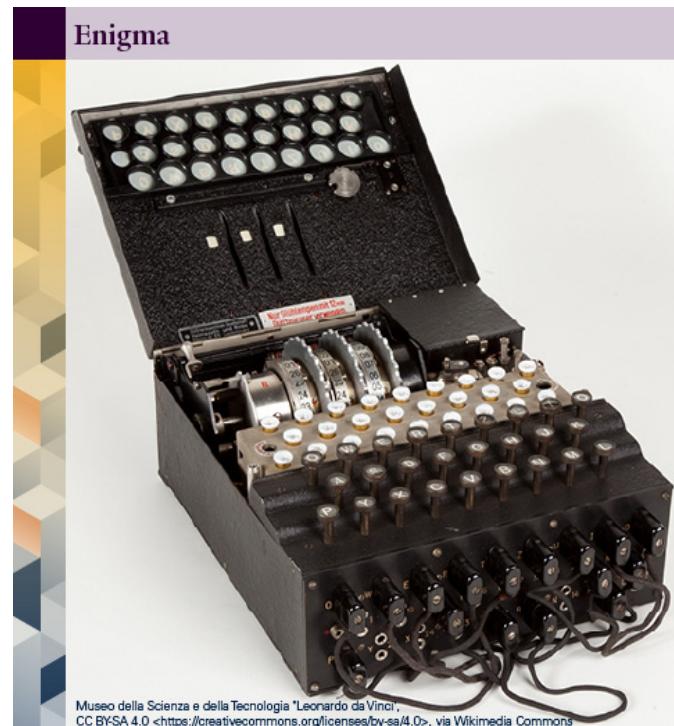
### Vocabulary

This section introduces the following terms.

- [adversary](#)
- [cryptography](#)
- [encryption](#)
- [decryption](#)
- [public key](#)
- [private key](#)

### Cryptography History

In the early 20th century, cipher devices, including the Hebern Rotor and Enigma machines, rose to prominence as the best method to conceal sensitive messages from potential espionage between nations. The Enigma machine—which was invented by Arthur Scherbius, a German engineer, in post-World War I Germany—emerged to protect sensitive communications, such as those related to the economic, commercial or military activity (Lele, 2021). Soon after its creation, the German government integrated Scherbius's invention into the nation's military infrastructure. Near the end of the 1930s, when the National Socialist German Workers'



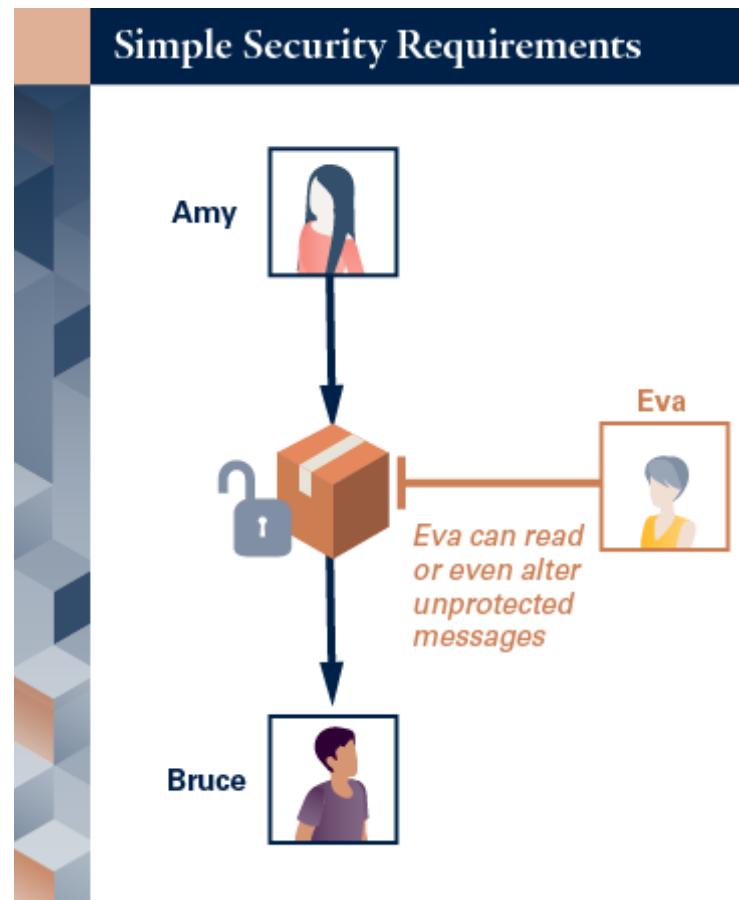
(Nazi) Party launched its offensive on Western Europe, consequently starting World War II, the German military used the Enigma machine to communicate and protect the movement of its troops, as well as the orders from high command to its submarine fleet. Through the use of the Enigma machine and its fleet of submarines, the Germans devastated the Allied forces' shipping supply chain. Via a complex cipher that was a precursor to modern cryptography, the Enigma machine-turned human-readable text into a string of characters and numbers that were not human-readable, which a receiver could decode with the same cipher.

## Cryptography Foundations

Today, in an ever-growing online world, cryptography is used to secure digital communications and to protect information and privacy. At its most basic, cryptography, through the use of algorithms, helps to secure the confidentiality and integrity of data, and to protect against the theft of data. Cryptography protects and secures the data of a number of online processes and networks: credit card numbers, online browsing, encrypted emails, and ATM transactions, to name a few.

Moreover, cryptography plays a central role in the underlying mechanics of Bitcoin; cryptography is what enables its security, scalability and immutability, and what allows it to create a decentralised network that replaces the trusted third-party gatekeeper role of banks.

For example, Amy and Bruce are friends, and Amy wants to send Bruce a message. However, Amy and Bruce have an adversary, Eva. They need to protect their message from two potential threats from Eva (Williams, 2020):

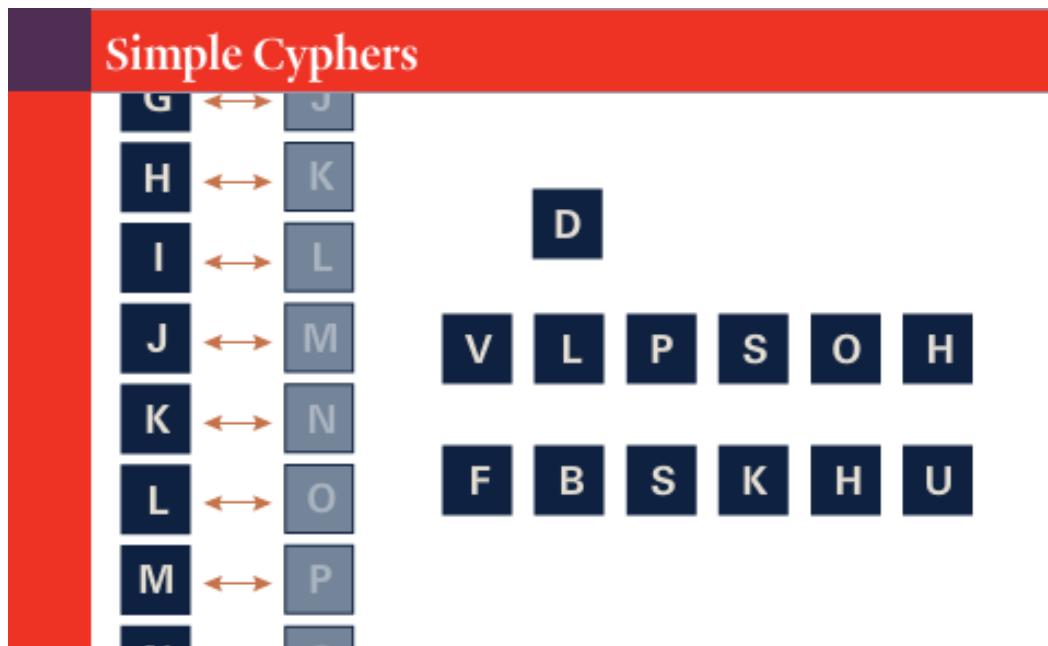


- 1. Security against eavesdropping:** Cryptography can protect the confidentiality of data. For example, if Amy is sending Bruce a credit card number, she needs to be able to trust this data will be secure.
- 2. Security against data manipulation:** Cryptography can also preserve the state of data, meaning that if someone attempts to change the data (such as when it's in transit), the recipient can become aware of the manipulation of this data. For example, if Amy is sending Bruce payment instructions, Bruce needs to know that these instructions haven't been intercepted and replaced with fraudulent instructions.

3. **Security against stolen data:** How do Amy and Bruce prevent Eva from stealing data and viewing or changing messages? Early methods relied on a shared key or code. A sender would encrypt and send a message, and the receiver decoded the message by using a key.

In “substitution”, which is a straightforward encryption method, a cipher changes units of plaintext into ciphertext by, based on a key, simply substituting one letter for another.

Initially, parties who wanted to use secure encryption to communicate first had to trade keys with each other, perhaps via written documents carried by a trusted intermediary or a physical machine and codebooks, as with Enigma.

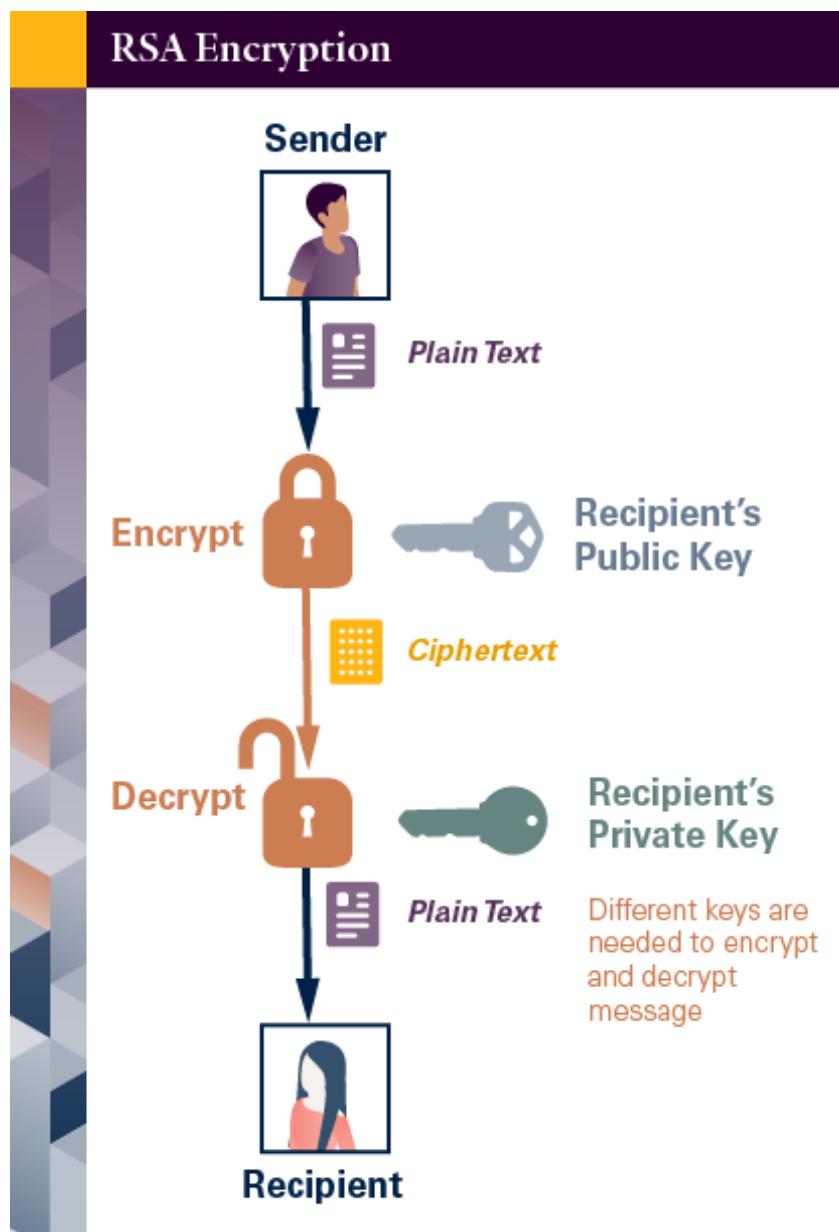


In 1976, the advent of the Diffie-Hellman-Merkle key exchange method permitted so-called “trustless” activity: Two parties who had never previously encountered each other could exchange keys using an insecure means of communication, such as the internet, and encrypt their communications (Lake, 2021). The method uses a public key, which is public information that everyone can see, and a private key that only the two interested parties know (in our prior example, only Amy and Bruce). The public and private keys combine to create a secure key that only the two parties know and can use to decrypt the information.

Following the Diffie-Hellman-Merkle method, Rivest-Shamir-Adleman (RSA) encryption became the most common algorithm for encrypting sensitive information and now powers the most secure encryption on the internet (Blanda, 2014). The RSA system provides such a high degree of security because its encryption is built around the extraordinarily difficult mathematical operation of factoring the product of two large prime numbers (known commonly as the “factoring problem”). To date, assuming the algorithm uses a large enough key, there are no published methods of decryption that can defeat the RSA system, which has withstood four decades of attacks (Castelvecchi, 2020; Blanda, 2014).

The RSA algorithm has three sequential steps: key generation, encryption, and decryption (Saravanakumar, 2013).

1. **Key generation:** The algorithm generates a public key and a private key. These are combined to encrypt and decrypt information.
2. **Encryption:** The algorithm uses the public key to make the original human-readable information unreadable—effectively rendering the information into a string of nonsensical characters. In other words, anyone can encrypt the information because the public key is accessible to all.
3. **Decryption:** The algorithm uses the private key to render the encrypted gibberish back into readable text. Only the parties who possess the private key are able to decrypt the information.



## 1.4.2 Cypherpunks and the Crypto Wars

### Quick Fact

Derived from the combination of “cyberpunk” and “cypher”, a cypherpunk today is any individual who seeks to drive political and social change through the application of cryptography and other privacy technologies (Manne, 2011). As it stands now, The cypherpunk movement works to improve privacy and security through applied cryptography.

### Cypherpunks and the Crypto Wars

In this section, we will explore the origins of the cypherpunks to provide a basis for understanding the origins and importance of their role in Satoshi’s introduction of Bitcoin.

Throughout the 1960s and 1970s, cryptographers had largely worked at universities or intelligence agencies. However, following the publication of the Diffie–Hellman–Merkle key exchange method, a community of cryptography enthusiasts began to emerge. Early cryptographers like David Chaum even wrote papers on pseudonymous reputation systems and digital cash, including a 1985 paper titled *Security without Identification: Transaction Systems to Make Big Brother Obsolete*, decades before the debut of the Bitcoin network in 2008.

By the 1980s, the notion of government and corporate control over personal privacy became evident as major developments were made in personal computing technology, and cryptographers were able to see the potential of online data control. In 1988, cryptographer Tim May authored *The Crypto Anarchist Manifesto*, a paper that outlined the emerging social and economic revolution brought on by technological advancements. The paper called for cryptographic resistance to state controls (May, 1988). At that point in time, however, only a small number of people were concerned with the political implications of personal privacy invasion (Cipher Punks, 2021).

In late 1991, three prominent cryptographers—Tim May, Eric Hughes, and John Gilmore—and approximately 30 data libertarians gathered for the first time to discuss government surveillance and its threat to online privacy. Within a week of their meeting, one of the cryptographers, Eric Hughes, developed the first secure mailing list that the group could use to communicate. The Cypherpunks, as they would later be titled, could now continue their movement through a sort of email chat room known as the cypherpunks mailing list (Cipher Punks, 2021). Hughes went on to author *A Cypherpunk’s Manifesto* in 1993, which has become a cornerstone of digital activism, stating that:

Privacy is necessary for an open society in the electronic age. ... We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy. ... We must defend our own privacy if we expect to have any. ... Cypherpunks write code. We know that someone has to write software to defend privacy, and ... we're going to write it (Hughes, 1993).

The first-ever Crypto War began as the US government tried to work around cryptographic security measures. In 1993, the Clipper Chip was introduced through a mechanism which incorporated an

algorithm called Skipjack. Designed by the United States National Security Agency (NSA), Skipjack would allow the cryptographic key of each Clipper Chip to be split in two and held in escrow by two different government agencies. Complete access to any device containing the chip would then be granted by reconstructing that device's key, thereby allowing the government to conduct surveillance on the device. The Clipper Chip program, and effectively the first Crypto War, ended in 1996 when Matt Blaze, a security researcher and Cypherpunk, exposed fundamental flaws in the chip (Crypto Museum, 2018).

While the Crypto Wars faded from the public eye in the late 1990s, they still continue today. Law enforcement and intelligence communities continue to demand access to a “backdoor” to allow them to decrypt information using a universal private key. Meanwhile, the Electronic Frontier Foundation (EFF) and other non-profits continue to defend digital privacy, free speech, and innovation. The EFF was founded by John Gilmore, one of the original Cypherpunks, and has expanded its mandate beyond fighting government censorship to activism on other applications of encrypted software (Electronic Frontier Foundation, n.d.).

### 1.4.3 Key Takeaways and References

#### Key Takeaways

Let's review the key points of this section:

1. Cryptography is the science of communication in the presence of an adversary. The two major threats are eavesdropping and data manipulation. Encryption solves those problems through the use of keys.
2. The Enigma machine, for example, used a complex cypher during World War II to securely send and decode messages. Until 1976, such communication required an exchange of physical keys.
3. In 1976, the Diffie–Hellman–Merkle key exchange method emerged, permitting so-called “trustless” activity: Two parties who had never previously encountered each other could exchange keys using an insecure means of communications, such as the internet. The Diffie–Hellman–Merkle method combines a public key to encrypt information and a private key to decrypt it.
4. RSA encryption protects most of the secure information on the internet. Rivest–Shamir–Adleman (RSA) encryption is built around factoring the product of two large prime numbers (also called the “factoring problem”), a very difficult mathematical operation. Breaking RSA encryption is known as the RSA problem, and no currently published methods can defeat the system if the algorithm uses a large enough key.
5. The Cypherpunks data privacy movement began in 1991 when three prominent cryptographers met with data libertarians to discuss ways to resist government controls over data privacy. The meeting led to the creation of the infamous cypherpunks mailing list. It allowed secure messaging between members, and the data privacy activist movement strengthened from there.

6. The first-ever Crypto War began in 1993 when the US government introduced the Clipper Chip through the National Security Agency. The government had control of the chip's private keys, which allowed for the surveillance of any device with a chip. The programme ended in 1996 when researchers exposed flaws in the chip's technology.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

### 1.4.1 The History and Foundations of Cryptography

Chaum, D. (2021, 14 November). Without quantum security, our blockchain future is uncertain. *Cointelegraph*. <https://cointelegraph.com/news/without-quantum-security-our-blockchain-future-is-uncertain>

Williams, E. (2020, 3 March). Cryptography 101: Symmetric Encryption. *Medium*. [https://medium.com/@emilywilliams\\_43022/cryptography-101-symmetric-encryption-444aac6bb7a3](https://medium.com/@emilywilliams_43022/cryptography-101-symmetric-encryption-444aac6bb7a3)

Blanda, S. (2014, 30 March). RSA Encryption – Keeping the Internet Secure. *AMS Blogs*. <https://blogs.ams.org/mathgradblog/2014/03/30/rsa>

Castelvecchi, D. (2020, 30 October). Quantum-computing pioneer warns of complacency over Internet security. *Nature*. <https://www.nature.com/articles/d41586-020-03068-9>

Lake, J. (2021, 23 March). What is the Diffie–Hellman key exchange and how does it work? *Comparitech*. <https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange>

Lele, A. (2021). *Quantum Technologies and Military Strategy*. Springer Science and Business Media LLC.

Saravanan Kumar, V. (2013, July–August). ERSA: Secure and Enhanced RSA. *International Journal of Engineering Research and Applications* vol. 3, issue 4, pp. 508–510. [https://www.ijera.com/papers/Vol3\\_issue4/CH34508510.pdf](https://www.ijera.com/papers/Vol3_issue4/CH34508510.pdf)

### 1.4.2 Cypherpunks and the Crypto Wars

Cipher Punks. (2021, 20 October). The Birth of CypherPunks. *Medium*. <https://medium.com/@cipherpunks/the-birth-of-cypherpunks-311a5a458598>

Crypto Museum. (2018, 25 November). Clipper Chip: Cryptographic Key Escrow. <https://www.cryptomuseum.com/crypto/usa/clipper.htm#:~:text=Cryptographic%20Key%20Escrow&text=This%20would%20allow%20law%20enforcement,defunct%20by%201996%20%5B1%5D.>

Electronic Frontier Foundation. (no date). A History of Protecting Freedom Where Law and Technology Collide. <https://www.eff.org/about/history>

Hughes, E. (1993, 9 March). A Cypherpunk's Manifesto. *Activism*. <https://www.activism.net/cypherpunk/manifesto.html>

Manne, R. (2011, March). The Cypherpunk Revolutionary. *The Monthly*. <https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary>

Matthews, T. (2019, 2 April). The Clipper Chip: How Once Upon a Time the Government Wanted to Put a Backdoor in Your Phone. *Exabeam*. <https://www.exabeam.com/information-security/clipper-chip>

# 1.5 Introduction to Bitcoin

## 1.5.1 Introduction to Bitcoin

### Overview

In this section, we introduce Bitcoin, as it is the most well-known use of blockchain technology. As the first completely open payment network, Bitcoin's creation inspired further cryptocurrencies and blockchain technologies that became foundational in establishing a new industry.

### Vocabulary

This section introduces the following terms.

- [backdoor](#)
- [Bitcoin](#)
- [bitcoin](#)
- [cyberpunk](#)
- [decentralised](#)
- [key escrow](#)
- [ledger](#)
- [peer-to-peer](#)
- [pseudonymous](#)
- [pseudonymity](#)
- [wallet](#)

## Programme Director Video: Why Is it Important to Understand Bitcoin?

In this video, Meltem Demirors explains why the cypherpunks and other internet pioneers are relevant to secure communications over the internet, and why it is important to understand Bitcoin.



Now, why is it so important to understand Bitcoin? Well, earlier I mentioned the cypherpunk mailing list. And I just want to briefly talk about who the cypherpunks were, and why this is relevant.

In the early '90s, cryptography became widely utilised in communication. In the early days of the internet, internet pioneers realised that, for the internet to remain a free and open space where information could proliferate and be shared, we needed the ability to communicate with privacy.

And there, cryptographic innovations allowed us to communicate securely, which made online payments possible. It also made email possible, and a whole lot of other things that we take for granted today. But the one thing that the internet pioneers were not able to do, despite their best efforts, was create internet money.

Now, money typically has been the right of nation-states—people with armies to defend their currency. Bitcoin is the first digital nation-state with its own currency.

Now, according to estimates, there are between 100 and 300 million Bitcoin users in the world today. And it's challenging to estimate that number because a wallet address is not equivalent to a user. One user could have multiple wallet addresses, and finding identifying information about users of the Bitcoin network can be challenging.

But imagine there are 300 million people around the world today who are using one internet currency called Bitcoin. It doesn't have a government. There's no leader. There's no ruling party. There's no central authority. There's just millions of people around the world running the Bitcoin code, operating the Bitcoin network, and using the Bitcoin software.

In addition, there are thousands, if not hundreds of thousands, of entrepreneurs who've been able to build businesses on this open, permissionless money system. That's really powerful, and I think it reflects the broader shift that's happening in our world today.

As our world goes from being defined by physical borders to being digital, global, and interconnected, a currency like Bitcoin enables us to do unique things we haven't been able to do in the past.

For example, let's say I want to build a company and I need to hire software engineers. Historically, I would have hired those engineers in the jurisdiction where I'm located. So, say I'm sitting in New York. I would hire engineers and developers in New York, and pay them in dollars.

Now, what Bitcoin allows me to do is, it doesn't really matter where I hire my developers or engineers anymore, they could be anywhere in the world. And instead of me trying to figure out how to send money to Argentina, or Poland, or Sri Lanka, or Malaysia, I can now send Bitcoin to people without even needing to know their identity.

This is really cool, and allows us to think about how we collaborate in digital space in new and novel ways that we haven't been able to do before.

## 1.5.2 The Birth of Bitcoin

### The Birth of Bitcoin

At its inception, Bitcoin stood apart as a revolutionary idea: Housed on a blockchain with no single or central controlling owner, Bitcoin was an open payment network designed specifically for the internet (Coinbase, n.d.). The currency circumvented central banks and private companies entirely, with immutable records stored on a decentralised ledger that anyone who had an internet connection could view and to which they could contribute. The Bitcoin blockchain is effectively money with memory, which is verifiable through cryptographically signed transactions on a globally shared database.

### Programme Director Video: Introduction to Blockchain Technology and Satoshi Nakamoto

In this video, Meltem Demirors introduces blockchain technology by describing how Bitcoin came about.



Now, you might be asking yourself, what is a blockchain? In order to understand this, let's start with Bitcoin. Now, how did Bitcoin come about?

In 2008, a pseudonymous individual named Satoshi Nakamoto published a white paper to the cypherpunk mailing list, which was a mail server dedicated to people working on cryptographic technologies to preserve freedom of speech. Now, in this white paper, Satoshi, whoever he, she, or they were, outlined, in nine very succinct pages, a concept for a peer-to-peer electronic cash system called Bitcoin. Several months later, Satoshi also introduced the Bitcoin code to the world.

Now, Bitcoin is comprised of three things. First, there's the code itself. Bitcoin is an open-source software protocol. The protocol is the rules that dictate what happens within the Bitcoin system. And the Bitcoin protocol has been developed over the last 11 years as an open-source technology, meaning it's maintained by a set of volunteers who contribute code and continually develop and upgrade the code through an open-source software development process.

Now, Bitcoin is also a network. Code, in and of itself, isn't really functional. In order for code to be functional, it must be run. Now, the way that the Bitcoin software is run is on a specialised type of hardware called an ASIC. This process is known as mining. So when you hear people talking about ASICs or Bitcoin mining, really what they're talking about is running the Bitcoin code on computational devices, where electricity and silicon meet together with code. That's how software is created.

So really, what the Bitcoin network is, it's a giant network of specialised computers around the world running the Bitcoin code. Now, Bitcoin functions on something known as proof of work consensus. What this means is computers are doing mathematical and cryptographic work in order to secure the network. And Bitcoin's security guarantees come from something called Bitcoin's hashrate. You'll learn more about how this functions from some of the speakers throughout this module.

Lastly, Bitcoin is also an asset. Bitcoin is a cryptocurrency. That means it can be used as both a medium of exchange and a store of value. Now, on the Bitcoin network, effectively what you have is a history of every Bitcoin transaction since the beginning of time. So when you download the Bitcoin software and the Bitcoin blockchain, effectively what you have is a record of all Bitcoin transactions since the beginning of the Bitcoin network.

Now, the way that transactions function in the Bitcoin network is really unique and really important to understand. Unlike a traditional financial transaction where I would need to know your name, your address, your bank account information, and a lot of other detail about you, on the Bitcoin network I only need to know one thing. I don't need your name. I don't need to know where you live. In fact, you might not even be a person.

On the Bitcoin network, a wallet address is your location on the Bitcoin network. Think of it like a mailbox that you can receive money to. Now, what makes this so unique is that Bitcoin allows for pseudonymity, not anonymity, but pseudonymity. And the pseudonymity is what makes Bitcoin so useful in a wide range of applications.

Now, before we leave Bitcoin, I want to talk about one other important concept that I think will really be helpful in understanding why the Bitcoin ledger itself is such a useful tool, and for understanding why other types of blockchains have been pioneered since the advent of Bitcoin. Now, one of the unique attributes of a distributed ledger is that it stores a lot of information. And in the Bitcoin network, in particular, when you download the Bitcoin blockchain, you're getting every transaction since t equals 0 or the beginning of that network itself.

What this would be like, for example, is using Gmail and having to download every email that has ever been sent on the internet since the advent of time. Now, that's a whole lot of information. But that fidelity of data allows us to do really unique things with value and money that we haven't been able to do before.

Now, when we talk about Bitcoin, cryptocurrencies, and blockchain technology, I really want to emphasise that we're not just talking about financial assets or money or technology. We're talking about a political movement and a social movement. In Bitcoin, there is a popular turn of phrase that goes like this. Vires in Numeris. And for those of you who don't speak Latin, which I myself don't, what that means is truth in numbers.

The Bitcoin network asks us not to trust, but to verify. Proof of work gives us certain guarantees that other systems do not. And it imbues the Bitcoin network with an important characteristic known as decentralisation. And again, throughout this module, you'll learn more about some of the inherent trade-offs between the type of consensus mechanism a blockchain utilises, its inherent decentralisation, as well as some of the unique computational requirements that support that type of functionality.

## Satoshi Nakamoto's Groundbreaking Publication

In 2008, in a nine-page whitepaper called "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto outlined a way to transact with trust in a digital world without the need for banks or financial institutions. The idea was simple but groundbreaking.

The Bitcoin whitepaper was not released in an academic journal or by a university department or government agency. It was published on a fairly obscure mailing list under the pseudonym Satoshi Nakamoto, and no one on the mailing list had ever interacted with "Satoshi" before. The first block of

Bitcoin was “mined” on 3 January 2009, and the transaction included a headline from that day’s paper as a timestamp (Saleem, 2018). Few people paid attention, but none of this deliberate and carefully planned release was accidental.

## Why Satoshi Matters

In the years since the Bitcoin whitepaper was released, many have attempted to determine Satoshi Nakamoto’s identity. However, one of the core ideas of Bitcoin is pseudonymity.

The cryptocurrency space remains rife with pseudonymous individuals who obscure their identities. Examples include:

- **The Dread Pirate Roberts:** The admin of the online Silk Road black market. After tracing Bitcoin transactions, the US Department of Justice claimed that a man named Ross Ulbricht was the Dread Pirate Roberts, but this has been heavily contested.
- **100TrillionUSD:** A macro analyst who writes about the Bitcoin environment and accepts donations in bitcoin but has never revealed their identity, using a voice modulator for interviews.
- **0xb1:** A trader who identifies themselves using the first four digits of a cryptocurrency wallet and publicly shares their trading performance and trade ideas.
- **Punk6529:** A non-fungible tokens (NFTs), or digital collectables, enthusiast with activist tendencies who is building a digital “army” to advocate for NFTs.

### 1.5.3 The Evolution of Bitcoin

#### Quick Fact

On May 22, 2010—now known as Bitcoin Pizza Day—a famous bitcoin transaction took place on Bitcointalk, an online forum, when Laszlo Hanyecz paid for two pizzas with 10,000 bitcoin (worth around US \$41 at the time) in the first use of bitcoin as a medium of exchange (DeCambre, 2021). The same number of bitcoin was worth close to US \$450 million in September 2021 (Ex-Rate, 2021).



#### The Evolution of Bitcoin

In the earliest days of the Bitcoin network, interacting with the bitcoin cryptocurrency required a steep learning curve and some technical competence, as users had to run a software client

using their terminal. Today, an ecosystem of application developers are working to make bitcoin easier to use and more accessible to a broader set of users.

## The Bitcoin Application Ecosystem

Bitcoin has primarily been a “bottom-up” movement led by retail investors and market participants outside the existing financial system. As a result, Bitcoin and crypto markets have developed their own unique market structures that do not easily integrate into traditional financial services. Crypto requires public–private key infrastructure to transfer assets, and the user experience and interface around managing private keys have created particularly challenging design constraints.

The Bitcoin application ecosystem has undergone several distinct phases. In the earliest days, the entire Bitcoin network operated on a peer-to-peer basis. Notably, LocalBitcoins was a service that allowed people to meet in person to exchange cash for bitcoin. The first Bitcoin companies backed by venture capital (VC) emerged in 2013, and in the years that followed, a great deal of consumer Bitcoin applications and core infrastructure developed. This infrastructure included:

- **Wallets:** Devices or applications that store a collection of keys and can send, receive, and track ownership of cryptocurrencies. Wallets can take many forms, be it a directory or file in a computer’s file system, a piece of paper, or a specialised device called a hardware wallet. Various smartphone apps and computer programs also provide a user-friendly way to create and manage wallets.
- **Exchanges:** Platforms that enable the buying and selling of bitcoin in exchange for fiat currencies. Some exchanges are purely crypto-to-crypto, using a synthetic dollar-peg asset or dollar IOU known as a stablecoin, where the token represents a claim on a dollar. Others are crypto-to-fiat and connect to the legacy banking system.
- **Payment processors:** Devices that enable the use of bitcoin as a medium of exchange. These devices connect bitcoin to traditional payment systems like Visa, Mastercard, PayPal, and others and make it easier for businesses to accept crypto for payment.
- **Trading venues:** Venues that enable speculative trading through derivatives (futures and options), margin lending, and other types of financial contracts. As the bitcoin market has grown and gradually been integrated into the global financial system, both consumer and institutional applications have emerged to cater to the growing audience of users. Sovereign states and economies have begun to integrate bitcoin, with El Salvador acknowledging bitcoin as legal tender and a national currency while more products are focused on expanding bitcoin’s use cases.

## Programme Director Video: Blockchain and Cryptocurrency Adoption

In this video, Meltem Demirors describes blockchain and cryptocurrency adoption and what you need to access this technology.



I also want to shift gears for a moment and talk about adoption. So how would we actually measure adoption of cryptocurrencies or blockchain technology? As we think about adoption, it's really important to remember that throughout the course of human history, the rate of diffusion of technology into society has happened at differing paces.

Typically, when a new technology is introduced, there will be a small group of innovators who are the first to adopt the technology. So, for example, when Bitcoin was first introduced to the world and the Bitcoin network became operational in January of 2009, nobody really used it for the first few years. In fact, very few people were even aware that Bitcoin existed or what it even was.

In fact, most of the people who were using Bitcoin at the time were people who were part of these technology communities and spending time on internet forums where Bitcoin was talked about. Over the subsequent years, the adoption of Bitcoin has increased as a result of both the general awareness of Bitcoin increasing, but also the number of applications, products and services, that allow people to interact with Bitcoin in a simple and easy way, have also increased. And the amount of capital going into these businesses, that allows them to grow, has also increased.

And what we typically see is once these innovators adopt this technology, there are successive waves of adoption that resemble a normal distribution with a small tail at the beginning, which includes these innovators, then a larger group coming in, called early adopters, before it reaches a majority.

In fact, the internet has been around for about 50 years now. And we're only now just to the point where the internet is really becoming ubiquitous and widely utilised. So be patient when you think about this technology, because it will take time for this new technology to diffuse into our society and to our culture, and into the way we interact with new technology.

Another thing that's really important to keep in mind is the use of blockchain technology, and the use of cryptocurrencies, is dependent on certain types of infrastructure existing. For example, in order to interact with the Bitcoin network, you need access to an internet connection or an internet-connected device. And you have to remember, only 50% of the world's population is online today.

So inherently, the ability to achieve mass adoption is going to be limited by some of the infrastructure constraints that prevent people from accessing the internet, and therefore prevent people from potentially interacting with this technology. Similarly, you need access to electricity. And so if someone doesn't have access to electricity, it's difficult to expect them to be able to interact with this new technology.

So as we think about new and novel ways that you might apply blockchain technology, just keep in mind that this tech doesn't exist in isolation. It requires other core pieces of infrastructure from compute, to telecommunications networks, to energy systems, and more for it to work properly. And keeping this in mind will help you identify what use cases are suitable for this technology at its current state of development.

## 1.5.4 Key Takeaways, References, and Optional Reading

### Key Takeaways

Let's review the key points of this section:

1. Cryptographers in the 1960s and 1970s mostly worked in government or at universities. Following the publication of the Diffie–Hellman–Merkle key exchange method, a community of cryptography enthusiasts working outside of those fields emerged.
2. In 1991, cryptographers and technologists started the “Cypherpunk Mailing List”. A *Cypherpunk’s Manifesto* focused on privacy and the necessity for people to build privacy themselves instead of trusting governments and other organisations to protect them. The Crypto Wars are ongoing, with law enforcement and intelligence communities demanding access to encrypted information using a universal private key and activists fighting for the right to communicate freely and privately.
3. Bitcoin was the first open payment network designed specifically for the internet. Bitcoin has no single or central controlling owner and is housed on a blockchain. The currency stores immutable records on a decentralised ledger that anyone who has an internet connection can both view and contribute to.
4. To create Bitcoin, Satoshi Nakamoto published a short white paper pseudonymously on an obscure mailing list. The first bitcoin was mined on 3 January, 2009. The cryptocurrency space remains rife with pseudonymous individuals who obscure their identities.
5. Initially, bitcoin cryptocurrency was not widely adopted. The learning curve to interact with it was steep. An ecosystem of more user-friendly applications is evolving to make bitcoin easier to adopt.
6. The first VC-backed Bitcoin companies emerged in 2013 with the intention of investing in and promoting core infrastructure development and consumer applications, including wallets, exchanges, payment processors, and trading venues. As the market has grown, bitcoin has become more integrated into the global financial system, with applications being developed to accommodate a wider audience.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

### 1.5.1 Overview

Wang, K. (2021, July). Measuring Global Crypto Users: A Study to Measure Market Size Using On-Chain Metrics. *crypto.com*. [https://crypto.com/images/202107\\_DataReport\\_OnChain\\_Market\\_Sizing.pdf](https://crypto.com/images/202107_DataReport_OnChain_Market_Sizing.pdf)

### 1.5.2 The Birth of Bitcoin

Coinbase. (n.d.). What is Bitcoin? <https://www.coinbase.com/learn/crypto-basics/what-is-bitcoin>

Asenbaum, H. (2018, 30 April). Anonymity and Democracy: Absence as Presence in the Public Sphere. *American Political Science Review* vol. 112, no. 3. <https://www.cambridge.org/core/journals/american-political-science-review/article/abs/anonymity-and-democracy-absence-as-presence-in-the-public-sphere/7D914F6529697778EB3D35C3C22065AE>

Library of Congress. (no date). Full Text of The Federalist Papers. <https://guides.loc.gov/federalist-papers/full-text>

Saleem, S. Z. (2018, 13 September). The 2008 global meltdown and the birth of Bitcoin. *Mint*. <https://www.livemint.com/Money/YTYMYUD7dytGK5PGSpdRTN/The-2008-global-meltdown-and-the-birth-of-Bitcoin.html>

### 1.5.3 The Evolution of Bitcoin

DeCambre, M. (2021, 22 May). Bitcoin pizza day? Laszlo Hanyecz spent \$3.8 billion on pizzas in the summer of 2010 using the novel crypto. *MarketWatch*. <https://www.marketwatch.com/story/bitcoin-pizza-day-laszlo-hanyecz-spent-3-8-billion-on-pizzas-in-the-summer-of-2010-using-the-novel-crypto-11621714395>

## Optional Reading

[Satoshi Nakamoto's whitepaper: "Bitcoin: A peer-to-peer electronic cash system"](#)

# 1.6 Bitcoin as a Protocol, Network, and Asset

## 1.6.1 The Bitcoin Network

### Overview

Now that we have introduced Bitcoin and its evolution, in this section, we will explore Bitcoin on a more in-depth level and gain an understanding of the system as a protocol, a network, and an asset.

### Vocabulary

This section introduces the following terms.

- [block reward](#)
- [full node](#)
- [hashing](#)
- [mining](#)

### The Bitcoin Network

When a transaction occurs with government-backed currency, the payer and payee banks record the transaction on each bank's private digital ledger. Other account holders on the bank's network do not have or create a record of the transaction. E-commerce services, including Venmo and PayPal, also use this traditional financial system to transfer money (Coinbase, n.d.).

Unlike a banking network, the Bitcoin network—like all blockchain networks—is designed to be decentralised. No specific party—government, financial institution, payer, or payee—controls the transaction record. Instead, every digital ledger on the Bitcoin network records every transaction, which makes transactions on the Bitcoin network immutable, or extremely difficult to corrupt because a record of a fraudulent transaction would appear and require validation on the ledgers of everyone on the network.

**Note:** While the Bitcoin network is designed to be decentralised, it is not generally known how concentrated bitcoin ownership and mining operations are.

## Transactions and Mining

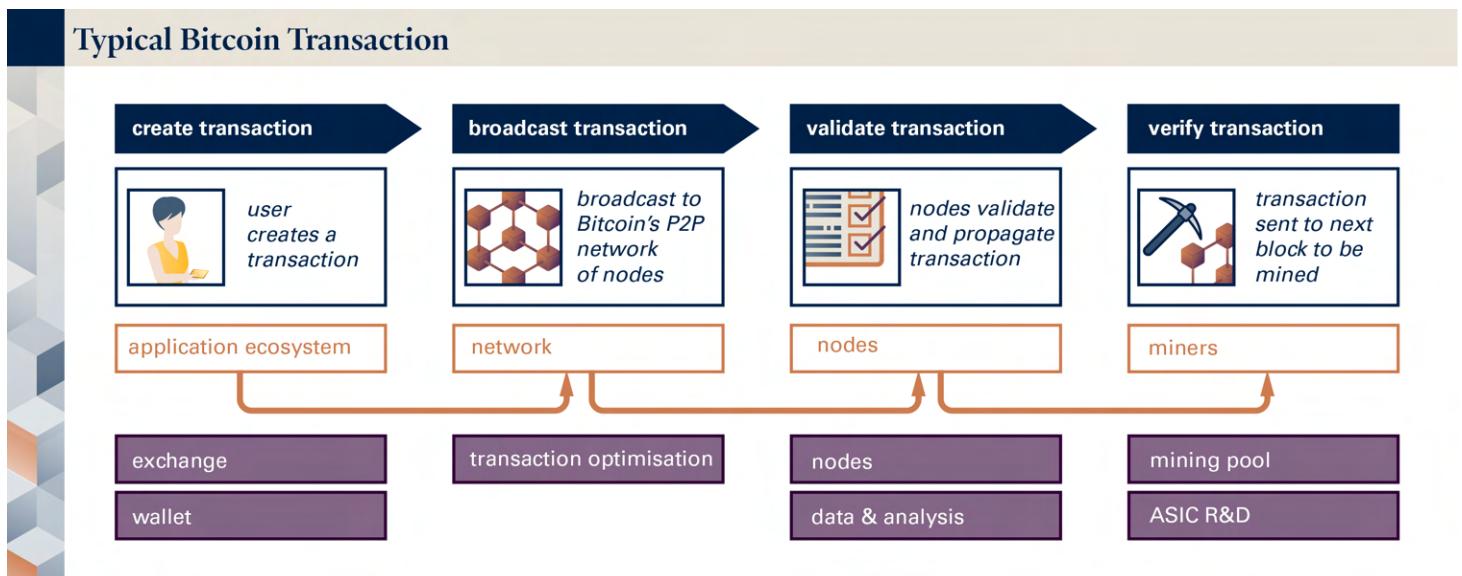
The Bitcoin network includes:

- **Users** who create transactions.
- **Bitcoin node operators** who run computers that contain a copy of the Bitcoin blockchain.
- **Miners** who facilitate and validate transactions on the network.

Miners also enforce the network rules and distribute all of the 21 million bitcoins available.

Typically, a user creates a transaction through an application like an exchange or a wallet (although users can also create their own transactions on the network). The transaction is then broadcast to the Bitcoin network, where tens of thousands of operators, running full nodes—full copies of the Bitcoin blockchain, a record of all transactions since the beginning of Bitcoin time—review the transaction. Each transaction is ordered, and these nodes verify that each requested transaction matches the ordering of the Bitcoin blockchain to ensure that the transaction sender has not spent the same bitcoin twice or created a new bitcoin. Reviewing the history of bitcoin transactions across thousands of nodes resolves the double-spend problem.

After these nodes have validated the transaction history against the blockchain, miners who run specialised hardware batch these transactions into blocks and compete to verify them in a process known as mining, which involves hashing or performing cryptographic hashing functions to find and validate Bitcoin blocks. When a block is successfully mined, the transactions in that block become part of the blockchain and are sequentially recorded on the Bitcoin network ledger to be referenced against all future transactions. For their work, successful miners receive compensation in the form of a new bitcoin.



## 1.6.2 Bitcoin Protocol

### Quick Fact

Originally, Satoshi Nakomoto wanted to call the Bitcoin blockchain the “timechain”. Centralised data systems organise data according to time, but people can fairly easily change a record of time—by altering a system clock, for example. Instead of depending on a computer clock, however, Bitcoin creates a time record based on the order in which transactions are placed on the blockchain (Gigi, 2021). The “present” is simply the longest verified chain.

### Bitcoin Protocol

The Bitcoin protocol is the set of rules that govern how the Bitcoin system validates transactions, preventing double-spending and other types of fraud. The foundation code for the Bitcoin protocol and system is open source, which means anyone can download and use the code, and any developer can contribute to it (Antonopoulos, 2017). The community has grown from a single developer, the still-anonymous Satoshi Nakamoto, into more than 400 contributors. The authoritative version of the code, Bitcoin Core, controls “all aspects of bitcoin, including wallets, a transaction and block validation engine, and a full network node in the peer-to-peer bitcoin network” (Antonopoulos, 2017).

### The Bitcoin Core Code Repository

The Bitcoin Core code repository maintains and releases Bitcoin client software for the nodes that validate transactions on the network and for the bitcoin wallet. It is a direct descendant of the original Bitcoin software released by Satoshi Nakamoto after he published the Bitcoin whitepaper. This open-source project has a large developer community that contributes code, and it is also supported by other contributors in research, peer review, testing, documentation, and translation. The community selects a small group to act as project maintainers, and they are responsible for updating the proposed code changes and other maintenance duties (Bitcoin Core, 2021).

## 1.6.3 Bitcoin, the Asset

### Bitcoin, the Asset

The monetary unit in the Bitcoin environment is a bitcoin, also expressed as XBT, ₿, or BTC. A satoshi, also known as a sat, is a monetary unit that equals a hundred millionth of a bitcoin, or 0.00000001 XBT (Thompson, 2019).

When a miner creates a new block on the blockchain, the miner receives the “block reward”, or payment, in two ways: through transaction fees paid by other users and through mining rewards

paid by the Bitcoin protocol. The Bitcoin protocol specifies that the block reward will be halved every 210,000 blocks.

All bitcoins in existence will likely be mined by 2140 (Phillips & Chipolina, 2021). As of August 2021, roughly 18.77 million bitcoin, or nearly 90% of the supply, has been mined, and about 310,000 bitcoin will be mined every year for the next four years. The last bitcoin halving took place in May 2020 (Godbole, 2020). Halving takes place every four years . It refers to the reduction of the block subsidy provided to miners by half and is a process that ensures the issuance rate of new coins is steady until its maximum supply is reached.

## Characteristics of Bitcoin

Bitcoin has the following characteristics:

- Decentralised
- Autonomous
- Programmable

How do these characteristics compare with those of fiat money? Let's explore this:

### Decentralised

Money is centralised because it has an intermediary and is controlled by a central bank and its government. Bitcoin is decentralised, meaning anyone can view the Bitcoin code, join the Bitcoin network, mine bitcoin, or use the Bitcoin network to send a transaction, and has no controlling authority.

### Autonomous

Bitcoin is autonomous and self-governing as an asset, with no central authority, whereas money is issued and controlled by governments.

### Programmable

Money is somewhat programmable because it can be converted into digital form and operated on, as in an electronic funds transfer (EFT) from one person's bank account to another. The bitcoin asset is programmable, as bitcoin is digitally native and has no physical materiality.

## Characteristics of Money

Money is a:

- Medium of exchange
- Store of value
- Unit of account

How do these characteristics compare with bitcoin? Let's explore this:

### Medium of exchange

Money is used to buy and sell goods and services and is accepted in nearly all transactions. Bitcoin is used as a medium of exchange in a limited number of online marketplaces and payment processing solutions. For bitcoin to become a true medium of exchange, it must become a much more widely accepted form of payment.

### Store of value

A store of value is an asset that retains its purchasing power and can be used predictably in the future. Money retains its value and its capacity to be used to buy and sell goods and services far into the future. The predictability of bitcoin's value is very much in question, and while bitcoin can be used to purchase goods, acceptance of bitcoin is not widespread, which limits its utility as a store of value.

### Unit of account

A unit of account is a standardised unit of measurement used as a base to determine and compare value. Money is a unit of account that can be used to compare the value of goods and services in the same currency. Bitcoin is also a unit of account, as it can be used to measure the value of some goods and services.

## 1.6.4 Key Takeaways, References, and Optional Reading

### Key Takeaways

Let's review the key points of this section:

1. The Bitcoin network includes users who create transactions, operators who run nodes with a full copy of the Bitcoin blockchain, and miners that facilitate and verify transactions.

2. In a typical transaction, a user creates the transaction, which is then broadcast to the Bitcoin network. Operators who run full nodes review the transactions, making sure that the transactions occurred in the order that the blockchain specifies. Miners then batch and verify the transactions by performing cryptographic hashing functions. Once the block is mined, the transactions become part of the blockchain, recorded in the ledger from that point forward.
3. Bitcoin is an open-source software project. Anyone can download and use the source code for free. Bitcoin is developed by an open community of volunteers that has grown from one (Satoshi) to over 400 contributors.
4. Bitcoin Core is the Github repository that stores and manages Bitcoin's code.
5. When a miner creates a new block on the blockchain, the miner receives payment in the form of transaction fees and mining rewards. All the bitcoin in existence will likely be mined by 2140. Nearly 90% has been mined to date.
6. Bitcoin is decentralised, autonomous, and programmable.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

### 1.6.1 The Bitcoin Network

Coinbase. (n.d.). What is Bitcoin? <https://www.coinbase.com/learn/crypto-basics/what-is-bitcoin>

Gigi. (2021, 14 January). Bitcoin is Time. *Der Gigi*. <https://dergigi.com/2021/01/14/bitcoin-is-time>

### 1.6.2 Bitcoin Protocol

Antonopoulos, A. M. (2017). 3. Bitcoin Core: The Reference Implementation. In *Mastering Bitcoin*. <https://cypherpunks-core.github.io/bitcoinbook/ch03.html>

Bitcoin Core. (2021). About. *Bitcoin Core*. <https://bitcoincore.org/en/about>

Thompson, P. (2019, 9 June). What Is a Satoshi, the Smallest Unit on the Bitcoin Blockchain? *Cointelegraph*. <https://cointelegraph.com/news/what-is-a-satoshi-the-smallest-unit-on-the-bitcoin-blockchains>

### **1.6.3 Bitcoin, the Asset**

Godbole, O. (2020, 12 May). Third Halving Turns Out to Be Non-Event for Bitcoin's Price. *CoinDesk*. <https://www.coindesk.com/markets/2020/05/12/third-halving-turns-out-to-be-non-event-for-bitcoins-price>

Phillips, D., & Chipolina, S. (2021, 20 April). What Will Happen to Bitcoin After All 21 Million are Mined? *Decrypt*. <https://decrypt.co/33124/what-will-happen-to-bitcoin-after-all-21-million-are-mined>

### **Optional Reading**

[The Electronic Frontier Foundation website](#)

[A Hypothetical Attack on the Bitcoin Codebase](#)

[FEDS Notes: What is programmable money?](#)

# 1.7 Blockchain Technology Explained

## 1.7.1 Components of Blockchain Technology

### Overview

Blockchain technology encompasses many elements that drive and sustain its functionality. From its roots in cryptography to the variety of use cases employed today, blockchain's underlying concepts are complex. This section will provide an overview of the major components of the technology and establish a base from which you can further explore after this programme and enrich your own comprehension.

When evaluating blockchain technology for building a project on top of an existing blockchain or for creating a completely new blockchain, consider the following:

- **A consensus mechanism:** Since a blockchain is a distributed ledger with no point of authority, who validates the transactions and records on the network?
- **Smart contracts:** A prominent blockchain application that establishes contract rules in code that automatically executes when certain events occur.
- **A token:** What form should the unit of account and the medium of exchange take?
- **Development and maintenance:** Who maintains the code, and where is the code stored?
- **Issuance of new tokens:** How will new tokens be issued? Will there be a finite or infinite number of tokens issued?
- **Programming language:** Which programming languages have an existing community of developers and other talent, and which are the least likely to introduce security risks?
- **Network:** What technological and geopolitical constraints affect the infrastructure for the blockchain?

As an organisation or business considers whether to adopt or create a blockchain, they should examine the use case carefully: Many firms and companies have attempted to apply blockchain technology to use cases where a database would suffice. The information that a blockchain manages should have an economic value, as operating a decentralised, secure, immutable blockchain always incurs costs.

## Vocabulary

This section introduces the following terms.

- [code repository](#)
- [consensus mechanism](#)
- [compute and connectivity](#)
- [decentralised app \(dApp\)](#)
- [decentralised finance \(DeFi\)](#)
- [initial coin offering \(ICO\)](#)
- [pre-mine](#)
- [pre-sale](#)
- [proof of authority \(PoA\)](#)
- [proof of elapsed time \(PoET\)](#)
- [proof of space](#)
- [proof of stake \(PoS\)](#)
- [proof of work \(PoW\)](#)
- [smart contract](#)
- [scalability trilemma](#)
- [stablecoin](#)
- [token](#)

## Traditional Protocols and Blockchain Protocols

Generally, blockchain protocols differ from traditional data protocols in two important ways:

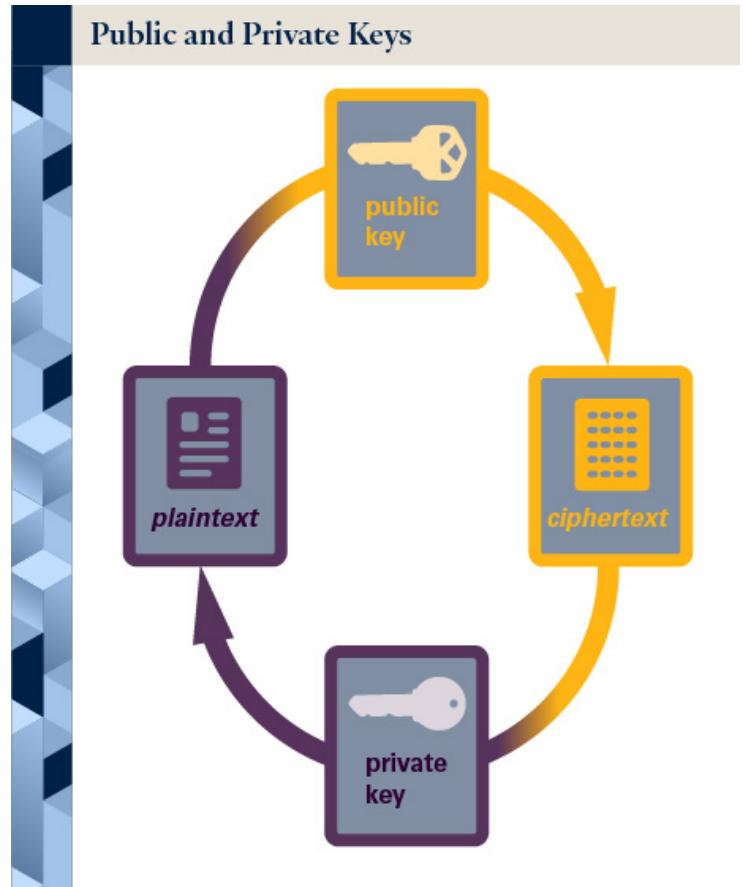
- Blockchain protocols use a ledger maintained through consensus rather than a centralised entity. The ability to alter the ledger varies based on the type of consensus and the level of decentralisation in establishing consensus. You'll learn more about consensus in this section.

- Instead of requiring real-world identities and admin-based permissions, blockchain protocols allow for anonymity among users by using public–private key cryptography to assign ownership to tokens on the ledger.

## Public-Private Keys

Most blockchains use public–private key cryptography to tie ownership to tokens on the ledger, allowing for anonymity among users. Algorithms (cyphers) generate a public key and a private key. Using encryption, they change units of plaintext (the public key) into ciphertext by simply substituting one letter for another. Algorithms then use the private key to render the encrypted text back into readable text. Only the parties who possess the private key are able to decrypt the information. As Coinbase explains of Bitcoin (n.d.):

Each person who joins the bitcoin network is issued a public key, which is a long string of letters and numbers—sort of like an email address—and a private key, which is equivalent to a password. Anyone can send bitcoin to you via your public key, but only the private key holder can access it in the “virtual vault” once it’s been sent.



### 1.7.2 Consensus Mechanism

#### Consensus Mechanism

A blockchain is a decentralised peer-to-peer system with no central authority figure. At first glance, this system presents a major problem: Without an organisation or leader making decisions, who will validate transactions on the network, and how are records verified?

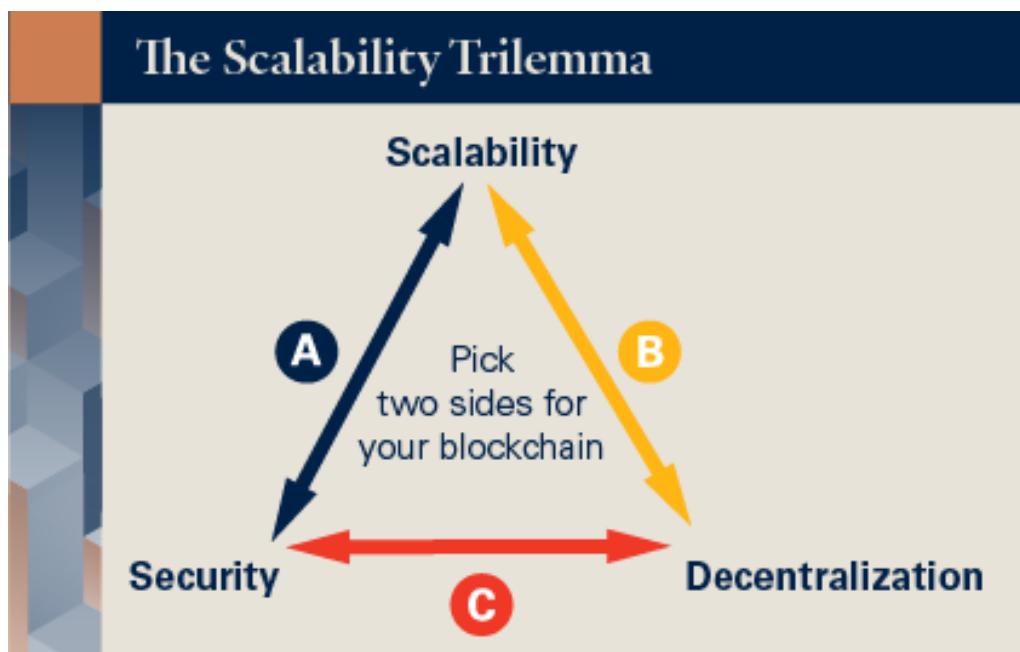
In short, users on the blockchain network validate these transactions via the consensus mechanism, which is also known as the consensus protocol or consensus algorithm. In blockchain technology, the consensus mechanism dictates the conditions that nodes and validators in the network have to meet to add new blocks to the blockchain, helping keep the network secure.

## The Scalability Trilemma

Different consensus mechanisms enable various types of functionality and properties, and each has advantages and disadvantages. Three important considerations for consensus mechanisms are the scalability, security, and decentralisation that it allows. However, these three considerations affect one another. Ethereum founder, Vitalik Buterin, describes this relationship as the scalability trilemma model to illustrate the interplay between choices for a consensus mechanism and the resulting effects those choices have on the network. The results can influence potential use cases and product design constraints.

In the scalability trilemma, a consensus mechanism can perfectly satisfy at most two of the following network features:

- Security (safety of the network)
- Scalability (in the form of transaction throughput)
- Decentralisation (in the form of fault tolerance, or the ability of the network to continue operating despite failures or malfunctions in individual nodes.)



Because perfectly satisfying all three objectives simultaneously has, to date, been technologically unachievable, the best consensus mechanism for any blockchain depends on the optimisation and purpose of the blockchain. For example, for a hypothetical blockchain that processes a high volume of low-value payments, optimising scalability and cost are important, while transaction-level security is less critical. However, security might be the main concern for a blockchain that records a low volume of high-value payments.

In another example, Bitcoin uses a mechanism that requires each node in the network to store the entire state of the network—including account balances, contract code, and metadata—and process all transactions. This consensus mechanism provides a large degree of security and decentralisation but limits scalability: The blockchain cannot process more transactions than a single node can, and even the most powerful hardware can only process a limited number of transactions per second. A less decentralised solution could increase speed and scalability but reduce security.

It is important to factor in the following considerations when analysing consensus mechanisms:

- **Costs** associated with the choice in consensus mechanisms should be evaluated. Costs could be tangible expenses that a high level of security would impact—energy costs, for example. Or costs could relate to the lack of centralisation when issues arise and are difficult to solve in a decentralised environment.
- **Speed** in processing transactions is becoming a vital competitive element in a blockchain's success. It is particularly relevant to the scalability of a network and is commonly measured in transactions per second (TPS).

## Types of Consensus Mechanisms

Blockchain networks implement their consensus mechanisms in several ways. Below is a brief summary of the most commonly used consensus mechanisms in public blockchain networks:

### Proof of work (PoW)

PoW, first used by Bitcoin's blockchain, is one of the most common consensus mechanisms. On a PoW blockchain, miners—who may not be associated with the network—compete to validate transactions and receive block rewards. Validating transactions involves solving very difficult computational problems, which requires vast amounts of computing power, hardware, and energy—as of September 2021, the annual amount of energy used to validate Bitcoin transactions was comparable to that of the entire country of Poland—and raises environmental concerns (Digiconomist, 2021). PoW allows the separation of the roles of those who own the network's cryptocurrency and the miners who validate transactions on the network. Moreover, although a single entity could try to gain control of the blockchain by taking over 51% of the network, the system's incentives are designed to reduce the likelihood of such an effort being profitable.

### Proof of stake (PoS)

Unlike PoW, in which miners who may not otherwise be involved in the network verify transactions, PoS requires participants who want to verify network transactions to stake their own network currency for a chance to do so. An algorithm then randomly chooses which validator will verify the block. Because PoS does not require validators to solve computational problems, PoS requires no expensive hardware or energy—theoretically attracting more validators, decentralising the network even further and better protecting against a 51% attack (wackerow, 2021). Not only would you need

51% of computing power to take control, you'd also need to control 51% of the staked currency, which is expensive and may reduce the incentive to manipulate a blockchain that may lose value when attacked. Moreover, with PoS, token holders have an incentive to vote for things that maximise the long term value of the protocol. In some PoS blockchains, participants who engage in malicious behaviour have their stake slashed or have their assets taken. Proof of Stake critics, however, warn that having network currency holders as the validators gives the capital owners of the network too much control.

## **Proof of space**

Also called proof of capacity (PoC), Proof of Space uses storage space rather than computational power to verify transactions and is thus more energy efficient. Rather than work towards a solution to a challenge, block validators have the solutions to the challenges placed on their dedicated storage space. In theory, the more storage space a validator has dedicated, the more solutions they can hold, and thus the greater their chances of cracking the challenge and collecting the block award (Mellor, 2021).

## **Proof of elapsed time**

PoET emerged from work conducted by chip giant Intel to offer an alternative to PoW. Proof of elapsed time networks solve a “random leader election” challenge by assigning participants a random waiting period. The first participant to complete their wait time is chosen as the leader of a new block. Importantly, according to Intel, the system uses a “trusted execution environment” to create random wait times, meaning that some trust has to be placed into that environment (Hyperledger Sawtooth, 2017).

## **Proof of authority**

PoA is similar to PoS, but instead of staking their network currency, validators stake their reputation (Binance Academy, 2018). As such, validators are required to disclose their identity and comply with a set of rules to prove their trustworthiness, limiting the network's claims to decentralisation and anonymity. PoA is more common for private blockchains.

## **Maintaining Trust and Consensus**

Because blockchains exist on decentralised networks, a consensus protocol must have a cost for the network to remain secure. These costs are realised as incentives or rewards paid to stakeholders such as token holders or miners. Without economic value at stake, the stakeholders have no incentive to collaborate on maintaining consensus. For example, there has to be a cost to vote on the state of the network in order to keep the distributed ledger synchronised. Moreover, the consensus mechanism should be costly enough to incentivise participants to remain honest and ensure that most nodes are not malicious.

## Guest Video: Solana

In this video, guest speaker Anatoly Yakovenko, CEO and Co-Founder of a high-performance blockchain, talks about blockchain scalability and consensus mechanisms.



Solana is a high-performance blockchain. It is a smart cloud contract platform like Ethereum, but it's designed for high-performance execution of smart contracts. And the goal is to go as low latency, highest throughput without any sharding, or subcommittees, or any kind of state splitting. So our goal is really to open up this censorship resistance with—the main use case that I think the stuff is really obviously good at is price discovery.

If you have a cryptographically-driven smart contract platform anybody can post their code, that does some financial application, and you have this entire world that can access it now. And we have this transparency that guarantees the access is fair and open. Can you actually implement global price discovery, execution clearing at a global level for the entire world? So that's the interesting question and the one that we're working towards. So it's a hard engineering problem. The way that Solana is designed, we've been thinking about this really from day one.

### 1.7.3 Smart Contracts

#### Smart Contracts

In 2013, a 19-year-old Canadian–Russian programmer, Vitalik Buterin, released a whitepaper proposing a new network called Ethereum. Buterin's goal was to design a network that would allow developers to build decentralised applications ("dApps") (Filiba, 2018). At the time, this functionality was limited to currencies on the Bitcoin blockchain. The young programmer's groundbreaking idea was a concept he called "smart contracts"—a collection of code and data, or programs, stored on the network that automatically runs when certain terms and conditions written into the code are met and verified. Because they are "self-executing", smart contracts eliminate the need for an intermediary while also giving participants immediate assurance of the outcome. For example, smart contracts could set in motion the releasing of funds, sending alerts, issuing a ticket, or registering a vehicle when certain conditions are met. These self-executing actions are recorded on the blockchain, which updates when the transaction has been completed (IBM, 2021).

The elements of a smart contract include those in the following theoretical real estate transaction:

- **The contract:** The program including details and terms of the agreement which are written into the code.
- **Distributed ledger:** The contract program uses blockchain and distributed ledger technology and is immutable.

- **Contract execution:** When both parties meet the contract's terms, the contract is executed, and cryptocurrency funds held in escrow would automatically move from the buyer's digital wallet to the seller's digital wallet.

Smart contracts are not meant to replace legal contracts that set forth the legal terms of a deal; instead, they help automate certain conditions without the need for an intermediary (Ethereum, 2021). While Ethereum was the first platform to offer smart contracts and hosts the majority of smart contracts today, many public blockchains, including Bitcoin, now offer smart contracts. Today, smart contracts are being employed in simple transactions, such as automatically triggering insurance payouts to more complex transactions involving fractional ownership and trading of real estate. New business models are being created as more uses for smart contracts emerge. One particular area that has benefitted has been financial services, where the use of smart contracts is in part driving the explosion in decentralised finance (DeFi). DeFi is a category of financial services, such as borrowing and lending, that operate via applications on decentralised public blockchain networks and that do not involve intermediaries, such as banks.

## 1.7.4 Token

### Overview

In every blockchain network, the native token serves as both the unit of account and the medium of exchange. Transactions on the network are priced in terms of the token, and the entire system is typically denominated in its own native currency. For example, in the Bitcoin network, transaction fees are priced in bitcoin. In addition, because the token is also the medium of exchange, users who want to exchange value with someone on a blockchain must do so using the token on that ledger.

However, tokens aren't limited to cryptocurrency. Starting around 2013, the types of tokens that can exist on the same blockchain network began to rapidly increase.

### From Cryptocurrency to Corporate Stablecoins

In 2013, stablecoins emerged as the first new token. Stablecoins, which are pegged to an asset such as gold or a fiat currency, are meant to stay relatively constant in value—unlike bitcoin, which has seen marked value fluctuations over the years (Vair & Vasisht, 2021). The first stablecoin, Tether, enabled bitcoin traders to easily move cash into the crypto ecosystem. Effectively, Tether took the dollars in at one endpoint and digitised them in a way that was compatible with Bitcoin. Today, US \$100 billion of stablecoins are in circulation. Stablecoins enjoy the same transfer speeds and settlement guarantees as other cryptocurrencies, and unlike wiring money, sending a stablecoin transaction requires only the recipient's public wallet address.

The next concept to emerge was the initial coin offering (ICO), where a token that operated on top of an existing blockchain network would be sold in exchange for the unit on that network. Many of these

tokens have a specific utility in a decentralised application, where the token can pay for services or be used in governance.

In 2018 and 2019, many firms chose to experiment with the issuance of tokenised securities like stocks and bonds, but with minimal success: Because US securities are subject to securities laws and complex issuance rules, they are not yet compatible with the crypto-finance ecosystem. More recently, a form of “synthetic” tokenised stocks have emerged, but these stocks do not offer direct ownership. Rather, they are a “tokenised representation” of the stock, with the price mirroring that of the original stock (Ossinger, 2021).

Currently, several corporations, including JPMorgan and Facebook, are experimenting with corporate stablecoins. JPMorgan’s JPM Coin is an internal unit of account that represents dollars on the company’s balance sheet but can easily move between functions and departments within the bank on a private, internal ledger. Meta (formerly Facebook) was experimenting with Diem, a stablecoin that will exist within the Meta application ecosystem and its three billion users. However, significant regulatory issues, outcry, and development delays have prevented Diem from making its public debut. Since then, Diem’s assets have been sold to Silvergate Capital (Business Standard, 2022).

## Management Without Managers

As all the nodes on a public blockchain are widely distributed and contain the same ledger information, no central management is required to operate the network. The nodes will all participate in validating transactions, and the blockchain’s consensus mechanism establishes the rules that enable the management of the ecosystem.

### 1.7.5 Development and Maintenance

#### Development and Maintenance

In developing, maintaining, and upgrading a blockchain protocol’s code, there are four important considerations:

- Who is responsible for maintaining and upgrading the code?
- How is the maintenance, development, and upgrading financed, and how is the financing held and managed?
- Do upgrading and development have a formalised process?
- Who manages the code repository and how?

Questions of code maintenance and funding often arise in open source software: Many open source communities are driven by both volunteers and companies who employ internal contributors to a

project. In the world of blockchain protocols, code maintenance and funding are even more important, as these protocols can hold trillions of dollars of economic value and facilitate billions or even trillions of dollars of commercial and financial activity.

In Bitcoin's case, development for the Bitcoin Core repository has no formal funding mechanism, and much of Bitcoin is funded through donations, grants, and other community-driven activities. Prior to its launch, Bitcoin also had no pre-mined or pre-sold coins—coins or tokens set aside for project contributors and early investors. Rather, anyone who wanted to mine bitcoin with their computer started from zero. Since the launch of the Bitcoin blockchain, however, pre-mining and pre-sales have become fairly popular. Typically, the proceeds of these pre-sales go to non-profit foundations that are stewards of the protocol's code base, and pay developers to manage and maintain the code base, sometimes as direct employees, sometimes via grant programmes, and often as a combination of both.



In contrast, the code repository for another well-known blockchain, Ethereum, is maintained by the Ethereum Foundation, which raised capital by pre-selling tokens for bitcoin and allocating a significant portion of ether (ETH), the blockchain's cryptocurrency, to early project contributors and developers. The Ethereum Foundation is a Swiss non-profit with its own staff, including a marketing and communications team.

Another way a blockchain might receive funding is through an initial coin offering (ICO).

While some ICOs have succeeded, others have resulted in the misuse of investor funds and little actual product development. Fundraising via ICOs began to decline in 2018, following a period that included legitimate projects, failed projects, and outright scams. Some projects are turning to initial exchange offerings (IEOs), where they list on an existing cryptocurrency exchange rather than creating an entirely new platform for their tokens. Others are opting for security token offerings (STOs), which are asset-backed and listed on existing exchanges and must comply with securities regulations (Kharif, 2019).

Are these forms of token financing a boon for open source? Open-source software has gone through a few different eras—from free software in the 1980s and 1990s to open-source software in the early 2000s to the commercialisation of open source in the 2010s, and now, the introduction of token-based financing models. However, while many foundations have raised billions of dollars, how sustainable these models are remains to be seen.

## Upgrading the Code

Blockchains require constant development, monitoring, and maintenance as well as upgrades. Many blockchain ecosystems have a somewhat formalised procedure known as the “improvement process”, which documents how changes are suggested, evaluated, and implemented into the code. Bitcoin and Ethereum have the bitcoin improvement proposal (BIP) process and Ethereum improvement proposal (EIP) process, respectively. Other protocols don’t have formalised improvement processes or have development teams that manage upgrades and maintenance themselves, with minimal input from external parties.

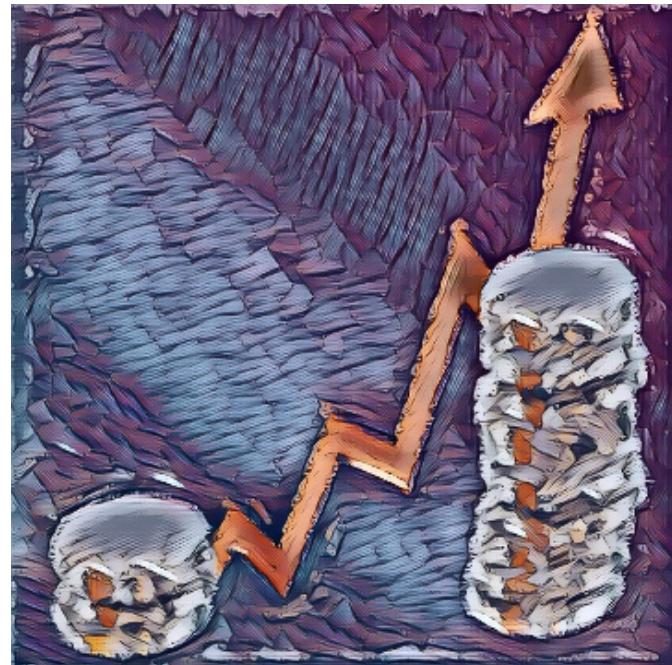
## Managing the Repository

Those who maintain the code must decide how to manage the code repository for the protocol or project. Code collaboration typically requires a set of administrators who can accept or reject changes that users suggest to the code, but questions can arise around who among the many users of the protocol has administrative rights.

### 1.7.6 Growth in Bitcoin Tokens

#### Issuance of New Tokens

Those who choose or design a blockchain protocol must decide how the protocol will handle the inevitable growth in the number of tokens that will occur—which can affect choices, including how many tokens will exist upon launch and how many tokens network participants will receive as a reward for participating in consensus. Some protocols, like Bitcoin, have a fixed issuance schedule and a hard supply cap. Since there will only ever be 21 million bitcoin in existence, the bitcoin supply schedule is pre-determined in the protocol itself. In contrast, other protocols don’t have supply caps and have dynamic rates of issuance that fluctuate based on different parameters.



For example, Ethereum’s ether (ETH) does not have an overall cap. The total supply of ETH and its rate of issuance was instead determined in the Ethereum 2014 pre-sale, which saw 60 million ETH created for contributors, 12 million ETH created as a development fund, and the annual issuance capped at 18 million ETH per year. While the total annual issuance of ETH is fixed at 18 million, this means relative growth decreases every year. For example, if there were hypothetically 75 million ETH in existence, an annual issuance of 18 million ETH would see the supply increase by 24%. However, in one year’s time, the total supply would be 93 million ETH, so issuing another 18 million over the next year would only represent an increase of 19.35%.

Every protocol has some form of growth in the number of tokens hard-coded into it, and that growth is allocated in different ways. In Bitcoin and Ethereum, which both operate on proof of work (PoW), issuances go to miners as compensation for performing work. In Tezos, a blockchain that operates on proof of stake (PoS), issuances go to token holders who are participating in staking, and they earn a pro-rata share of network growth. This means that any token holder who actively stakes their tokens will maintain their pro-rata share of the network since they earn a proportional share of the growth.

## 1.7.7 Programming Language

### Programming Language

Another important component of each protocol is the programming language for the protocol, as the right language helps ensure access to talent, platform growth, and security. If programmers have to learn an entirely new language, it could take more time for the developer community to grow and for applications to be built. In addition, new types of programming languages could create potential security loopholes or unpredictable edge cases where programs don't function as intended and errors are difficult to spot.

Existing blockchains use a variety of languages. Bitcoin uses C++, a common coding language, and GoLang. Ethereum utilises its own programming language, Solidity, which has common elements with JavaScript, a popular language used to create the user-facing portions of websites. Another blockchain, Solana, utilises Rust, which is a well-known programming language in security-focused programming communities. Another popular blockchain protocol, Polkadot, uses its own programming language, Substrate, but has applications that enable easy translation from Ethereum's Solidity language into Substrate.

## 1.7.8 Network

### Network

Although a blockchain protocol, or code, can be written in a matter of days, once the protocol is written, it has to run on a network—and networks require infrastructure to operate. Blockchain networks are typically asset-heavy and expensive, as they require specialised semiconductors or chips, as well as energy and facilities to house their validation activities. All of these call for a significant investment of capital and time: Building a large data centre or developing a new type of chip requires months or even years. Additionally, blockchain networks and infrastructure are subject not just to technological constraints but also to business and geopolitical climates.

## Technological Constraints

Blockchains require chips to perform the computations that enable them to achieve consensus or create and validate transactions. Two popular chips are application-specific integrated circuits (ASICs), which Bitcoin and other blockchains utilise, and graphic processing units (GPUs), used by Ethereum. The rapid growth of blockchain networking infrastructure has resulted in global shortages of these chips. According to research published by *The Economist*, GPU prices since 2017 have skyrocketed alongside Ethereum's price—GPUs that would normally retail for US \$700 are sold secondhand for US \$2400 or more (*The Economist*, 2021).

As these blockchain protocols perform computations, they also require energy. Some blockchains require more computational power, and thus energy, than others—including Proof of Work (PoW) blockchains such as Bitcoin. This need for a constant supply of inexpensive energy has had a profound effect on some nation-states. Until recently, China was the site of over 70% of bitcoin mining. Today, much of that activity has shifted to countries like the US and Kazakhstan.

## Growth of an Industry

Because of the costs involved in computational power, energy, and building the specialised hosting facilities that the computing machines require, blockchain infrastructure is increasingly the domain of large-scale operators who can provide the expertise required and achieve economies of scale that maximise profits. Large-scale operations dissuade smaller operators from participating in blockchain and lead to a more centralised infrastructure overall. Today, a lot of the mining on the Bitcoin blockchain is done on behalf of third parties; in North America, which has several publicly listed bitcoin mining companies with multi-billion dollar market caps, over 70% of the mining is accomplished via third-party hosting. But even proof of stake (PoS) protocols have this issue—large, concentrated holders like investment firms and asset managers have their own unique issues when considering how to best balance their financial interests with the long-term growth of the protocol, and have increasingly started to outsource decision-making and consensus-maintenance to external experts.

Overall, the crypto networking space is a rapidly growing industry, with dozens of public companies around the world that trade at high multiples. While many of these companies operate in the compute and connectivity space, some companies are focused on providing infrastructure finance and equipment leasing to the mining space, while others seek to provide energy management or profit optimisation solutions.

## The Future of Blockchain Networks

Blockchain networks and their implementation will continue to be a matter of concern in the coming years and decades as the human experience becomes increasingly digital. As some countries contemplate using public blockchain networks as a way to secure critical data, and as cryptocurrencies become more embedded within the global compute and communication infrastructure and global financial markets, the networks that secure public blockchain protocols will continue to grow in importance.

## 1.7.9 Key Takeaways, References, Optional Reading, and Additional Video

### Key Takeaways

Let's review the key points of this section:

1. Most blockchains use public–private key cryptography to tie ownership to tokens on the ledger, allowing for anonymity among users. For example, each person who joins the Bitcoin network receives a private key and a public key. The public key makes it possible for anyone to send bitcoin, but only the private key holder can access the bitcoin.
2. Blockchain protocols achieve consensus in a number of different ways, including Proof of Work (PoW), Proof of Stake (PoS), Proof of Space, Proof of Elapsed Time (PoET), and Proof of Authority (PoA). Each comes with inherent tradeoffs and is appropriate for different use cases.
3. Smart contracts are a collection of code and data, or programs, stored on the network that automatically runs when certain terms and conditions written into the code are met and verified. They are “self-executing” and anonymous, eliminating the need for an intermediary.
4. The native token is the unit of account and the medium of exchange for a blockchain. Transaction fees on the network are priced in terms of the token. Tokens can be cryptocurrency, stablecoins, tokenised securities, and others.
5. Understanding how a blockchain’s code is maintained and funded is important. For example, volunteers maintain the Bitcoin Core repository, while the Ethereum code repository is maintained by the Ethereum Foundation, a Swiss non-profit with its own staff. Many blockchain ecosystems have a somewhat formalised “improvement process” for updates. However, questions can arise around which users have administrative rights.
6. Every protocol must take the issuance of new tokens into account. Bitcoin has a hard cap on tokens, so it has a fixed growth schedule. Ethereum does not.
7. The right programming language for a protocol helps ensure access to talent, platform growth, and security. Existing blockchains use a variety of languages.
8. Blockchain protocols run on networks, which require infrastructure in the form of semiconductors (chips), energy, and facilities. The rapid growth of blockchain networking infrastructure has contributed to global shortages of semiconductors, while the need for inexpensive energy has affected some nation states.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

### 1.7.2 Consensus Mechanism

Binance Academy (2018, 8 December). Proof of Authority Explained. <https://academy.binance.com/en/articles/proof-of-authority-explained>

Hyperledger Sawtooth. (2017, 17 July). PoET 1.0 Specification. <https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html>

Marr, B. (2018, 2 February). Blockchain: A Very Short History Of Ethereum Everyone Should Read. *Forbes*. <https://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read>

Mellor, C. (2021, 18 May). Just two weeks after launch, storage-based cryptocurrency ChiaCoin drives up disk prices. *Blocks & Files*. <https://blocksandfiles.com/2021/05/18/chia-bitcoin-disk-prices>

wackerow. (2021, 29 July). Proof-of-stake. *Ethereum*. <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos>

### 1.7.3 Smart Contracts

Deloitte. (2016, 15 May.) The DAO: Chronology of a daring heist and its resolution. [https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte\\_Blockchain\\_Institute\\_Whitepaper\\_The.DAO.pdf](https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte_Blockchain_Institute_Whitepaper_The.DAO.pdf)

IBM. (2021, 9 January). What are smart contracts on blockchain? <https://www.ibm.com/uk-en/topics/smart-contracts>

### 1.7.4 Token

Bair, S. & Vasisht, G. (2021, 21 September). Stablecoins Are Anything But Stable. *Barron's*. <https://www.barrons.com/articles/stablecoins-are-anything-but-stable-516321658950>

Business Standard. (2022, 2 February). The end: Facebook-backed digital currency Diem sold to bank. [https://www.business-standard.com/article/international/the-end-facebook-backed-digital-currency-diem-sold-to-bank122020200035\\_1.html#:~:text=A%20once%2Dambitious%20but%20now,bank%20holding%20company%20Silvergate%20Capital.&text=02%3A15%20IST-,A%20once%2Dambitious%20but%20now%20faltering%20Facebook%2Dbacked%20digital%20currency,bank%20holding%20company%20Silvergate%20Capital.](https://www.business-standard.com/article/international/the-end-facebook-backed-digital-currency-diem-sold-to-bank122020200035_1.html#:~:text=A%20once%2Dambitious%20but%20now,bank%20holding%20company%20Silvergate%20Capital.&text=02%3A15%20IST-,A%20once%2Dambitious%20but%20now%20faltering%20Facebook%2Dbacked%20digital%20currency,bank%20holding%20company%20Silvergate%20Capital.)

Ossinger, J. (2021, 9 September). DeFiChain to Offer Tokenized Versions of Apple, Tesla. *Bloomberg*. <https://www.bloomberg.com/news/articles/2021-09-09/nasdaq-joins-blockchain-based-tokenized-stock-trading-venture>

### 1.7.5 Development and Maintenance

Kharif, O. (2019, 11 February). Security Tokens Are the New Crypto – But You Probably Can't Afford Them. *Bloomberg*. <https://www.bloomberg.com/news/articles/2019-02-11/why-security-tokens-are-crypto-for-the-already-rich-quicktake>

### 1.7.8 Network

The Economist. (2021, 19 June). Crypto-miners are probably to blame for the graphics-chip shortage. <https://www.economist.com/graphic-detail/2021/06/19/crypto-miners-are-probably-to-blame-for-the-graphics-chip-shortage>

## Optional Reading

[The Future of Fundraising? What We Need to Fix About Token Investing](#)

[Token Financing: How Tokenization Will Change the Economy](#)

## Additional Video 1

In this video, Meltem Demirors hosts a mini fireside chat with industry experts to explore the topic of Cross Chain Interoperability. They discuss some of the key considerations when moving assets cross-chain including security, liquidity, latency, data aggregation, and current and potential future applications of cross-chain infrastructure.

The panelists include:

- **Arjun Bhuptani, Founder, Connex**: Connex is the leading protocol for fast, fully noncustodial transfers and contract calls between EVM-compatible systems. You can use Connex to send transactions of value or calldata across chains and/or rollups. Unlike most other interoperability systems, Connex enables this without introducing any new trust assumptions or external validators.

- **Ben Jones, Co-Founder and Chief Scientist, Optimism:** Optimism is a Layer 2 scaling solution for Ethereum that can support all of Ethereum's Dapps. Instead of running all computation and data on the Ethereum network, Optimism puts all transaction data on-chain and runs computation off-chain, increasing Ethereum's transactions per second and decreasing transaction fees.
- **Emile Dubié, Founder and CEO xDeFi:** XDEFI Wallet is a multi-chain web browser extension built for DeFi users and NFT lovers. It is the world's only wallet with native integrations on THORChain, Ethereum + several EVM networks and Terra. XDEFI Wallet is a non-custodial, decentralized wallet.



**Meltem Demirors:** I'm really excited to be here. I'm even more excited that 150 people wanted to join a session on cross-chain layer 2 and interoperability. Many of you are taking the Oxford blockchain course right now. In that course we cover cross-chain interoperability and L2s briefly, but given how quickly the crypto space moves, one of the things I wanted to do this year was to do monthly sessions where we could cover special and emerging topics in the crypto space. And one of the biggest topics right now is this very topic.

I don't have the ability to screen share, Gabriel, so I don't know how you want to do that. I was having technical difficulties, but I'll go ahead and get started. In the class you've been learning, you've probably gone through the first two modules right now. And as we talked about in the kick-off two weeks ago, we put a lot of energy into module 1 and really explaining at a deep technical level how consensus and consensus mechanisms impact some of the performance parameters of blockchains, in particular in relation to speed, scalability, and transaction costs. There are inherent tradeoffs – depending on the security model and the consensus model you decide to use – on some of these parameters.

What I always like to say is, there really is no free lunch. If your objectives are to improve speed, improve the amount of throughput, and lower costs, you're going to have to make some inherent tradeoffs in your model, and one of those tradeoffs is around security. And so, here is... I'm just going to share this in full screen. One moment. Here's what I was just saying to you. We want to increase throughput, we want to increase speed, and for us to try to optimise for scalability and financial computation – which is what blockchains are – we're going to make some tradeoffs. Today, we're going to hear about a few different approaches that make different tradeoffs.

We're also going to hear from Emile, who's actually building an application to allow people to interact with cross-chain L2s more easily, about some of the unique design constraints of operating in this space. One of the really interesting things to keep in mind: interoperability in crypto is not a new concept. In fact, what I always like to say is that the first interop we built in crypto was to make dollars compatible with the Bitcoin blockchain. This happened back in 2013. One of the challenges was, dollars and bank wires settle in two to three days. They don't operate at the same speed or with the same settlement guarantees that Bitcoin transactions do. So really, the first example of interoperability in the blockchain space was taking dollars and making them compatible with Bitcoin. This was done through something called Tether.

Today, there are a variety of stablecoins. The aggregate market cap of stablecoins is over US \$120 billion. It's over 10% of the overall crypto market cap, and it's been really interesting to observe there's a lot of volume of stablecoin in circulation, but all of these are highly centralised; by far the most popular ones are highly centralised. So, one of the fundamental tradeoffs that we had to make by taking an asset, putting it on chain, and making it compatible was centralising and then also making some security compromises, in terms of the model for how assets are custodied and stored.

What we've started to see, though, over the last several months, if we think about Bitcoin as a type of financial computation, we think about Ethereum as extending that financial computation to include not only transactions, but also this programmability through smart contracts: there are now a wide range of layer 1 blockchain protocols that perform a wide variety of different types of financial computation in different ways. We've started to actually see Bitcoin itself migrating from being available only on Bitcoin – where it could be used for financial transaction processing – and being made available on Ethereum, where you can do more sophisticated types and more complex types of financial computation, and we see that with Bitcoin moving over onto Ethereum.

Starting, really, in 2018, as DeFi started to emerge, more and more Bitcoins started to move across chains in this cross-chain bridge, from Bitcoin to being available on Ethereum. However, again, one of the key challenges here is the model for that is predominantly highly centralised and fully custodial, meaning you're dependent on a third party to hold the Bitcoin for you. What we see now, as computation on Ethereum is becoming more expensive, is more and more assets are moving from Ethereum – not only Ethereum itself, but ERC-20 tokens or fungible tokens, as well as ERC-721 or non-fungible tokens – they're moving away from just being available on Ethereum for financial compute, but moving to other blockchains that are there, layer 2s or cross-chain bridges, in order to take advantage of cheaper, faster, more scalable financial computation that's available on other chains.

There's currently over US \$5 billion of Ethereum-based layer 2 value locked, and that's dominated by a protocol called Arbitrum. It's the layer 2 that's making up the majority of that volume. What's interesting about these layer 2s – and I'll talk about the differentiation between a layer 2 cross-chain bridge and some of these distinctions – but a layer 2 fully or partially derives its security model from layer 1 blockchain, meaning for Ethereum, layer 2 solutions still utilise Ethereum's consensus mechanisms. So you don't have to necessarily rely on layer 2 validators for the security of the funds.

We see similarly in the course, we cover the Lightning Network and its relationship to Bitcoin. You're still relying on the underlying security model of the original L1, but you have various optimisations you can make to make computation more efficient and cheaper, because you're using this delay between transactions happening on layer 2 and then reconciling back to layer 1's security model. So we see a lot of layer 2 activity happening on Ethereum in particular, and here you can see over the last six months, really astronomical growth of that. But it's not just about layer 2.

We're also seeing assets being bridged away from Ethereum entirely. So, US \$25 billion in total value has been bridged away from Ethereum, with US \$20 billion of that taking place over a very short period in the fall of last year. And it isn't just limited to wells or really large wallets. What's really cool about these bridges is, say for example you own just one Ether, which today is worth about US \$2,500, and you want to participate in DeFi. The average DeFi transaction on Ethereum might cost you US \$100–150, which is quite expensive, and so maybe you want to move your assets over to a cheaper chain.

Say you want to move them to Solana, where a transaction costs one one-hundredth of a cent. You do that through a one-time bridge, where you port your assets from being available only on Ethereum to being available on Solana, using a Solana bridge. Now you can use these assets in DeFi applications on top of Solana, where transaction costs are much lower, and transactions are processing faster than Ethereum because there isn't as much demand for financial computation on Solana yet; and also the throughput of that network is much higher, albeit with some security compromises and some decentralisation compromises that you're making.

One of the things I think will be interesting to cover today is, as more bridges get built; as more layer 2s get built; these volumes will continue to grow because users want speed, ease of use, and availability of financial compute. With that, I'll stop here, but I think it's just really interesting to look at how much of the volume is actually moving to layer 2s and cross-chain. And today, we're really lucky to have two experts on this.

We have Arjun from Connex. Connex is a protocol that is making data available cross-chain and enabling liquidity to move cross-chain. I'll let Arjun explain that a bit more to you, but Connex does this without relying on any new trust model, which I think is really important. And then we also have with us Emile, who's building a cross-chain wallet called XDEFI. XDEFI is utilising THORChain, which is a cross-chain protocol, for a lot of its back-end infrastructure. Emile can tell us a bit about how he's making cross-chain more usable, more functional. And then, if he joins us, we might also have Ben Jones from Optimism joining us. Optimism is another Ethereum layer 2 utilising a new type of technology called an Optimistic Rollup that's trying to make Ethereum transactions more efficient by using this new mechanism.

And so with that, maybe what I'll do... I want to start by talking about just the why. So, Arjun, maybe we'll start with you. Why did you want to build Connex? What made you realise you needed to build it? And what was the impetus for the journey you and your team have been on over the last few years?

**Arjun Bhuptani:** Thanks Meltem, and thanks for the intro and for having me here. I'm Arjun. I'm one of the founders of Connex. We started Connex about... I guess in 2017, so almost five years ago now, with this idea that you can use blockchains and other decentralised systems as mechanisms to empower users and enact widespread social change. And one of the biggest barriers that we saw to that happening was just the accessibility of this technology; the difficulty of using it in a real-world context, and at the time a big part of that conversation was focused on the scalability of chains. It's interesting that that is still a conversation right now, and it's a testament to how hard some of these problems are.

Connex was one of the first projects that actually was working on Ethereum scalability, alongside a lot of researchers from a lot of the popular L2 projects today. One of the things that we noticed was that there was this very key user experience problem that exists around scalability, and this gets down to what Meltem was talking about around tradeoffs and how there's really no free lunch. You can try to scale blockchains up by trying to make them faster, but that makes them more centralised. If you try to scale blockchains by fragmenting them out to different computing – basically, execution – environments, similar to what is happening right now, you lose this core property of being able to seamlessly interact with applications running on the same chain.

So we set out to figure out, how can we work to solve that problem? If we're headed towards this world where you are scaling Ethereum and scaling chains by moving compute and other execution to Rollups and other layer 2s, how do you enable a seamless user experience where people are still able to use applications without necessarily needing to know the details of what Rollup they're on and what chain that Rollup is attached to? That's the core thesis around Connex. We want to allow, where a developer is facing an infrastructure layer, we want to allow developers to build these powerful cross-chain and cross-L2 applications that, to the user, are still completely seamless.

**MD:** Thanks Arjun, that's really helpful, and I think one of the really cool things – and we'll talk about some of the metrics around Connex later – is how quickly usage and utilisation of Connex has grown and availability of liquidity, which I think is really interesting when you think about the potential for crypto markets more broadly. But Emile, let's move over to you, because you're sitting in a very different part of the ecosystem. You're not

building a new protocol, necessarily, but you're building an application, a user experience, that makes it much easier for people to interact with assets that might exist across different chains, so that you don't have to have hundreds of different wallets. This is a problem I have today. I have a different wallet for each chain I'm on. It's really difficult to keep track of what's where. It's actually quite embarrassing how bad I am at it. So, tell us a little bit about XDEFI and then maybe also tell us a bit more about the relationship with THORChain and how you made some of the design decisions around how you wanted to build XDEFI in particular.

**Emile Dubié:** Thanks Meltem, for sure. I'll actually start about THORChain because that's one of the main reasons why we built XDEFI in the first place. Essentially, back in 2019, as you know, I was an investor myself and I was looking at the space in 2019 and was thinking, alright, the future is multi-chain more than just Ethereum-focused, although I'm a massive fan of Ethereum, and I was trying to find some investment thesis around that. I think it was in the Synthetix charts at the time that I heard about THORChain, so I started digging a little bit more about this project, which is basically a decentralised cross-chain liquidity protocol that allows for swapping between native assets, for instance, BTC against ETH directly, without wrapping them, and invested in it early myself. So I was close to the team at THORChain, and I was thinking about how can we help with my current co-founder; the ecosystem is broken, what can we do?

After a few discussions with the THORChain team, we realised that there was a lack of infrastructure and of a wallet provider that would make it possible for users that are trying to interact with any UI interfaces that are powered by THORChain, to do so seamlessly. Why? Because back in 2020, and to some extent it's still the case today – although slightly different because you have more competition – you mainly had in the wallet extension space, MetaMask, which I'm sure we've all been using for a long time, and that is mainly focusing on Ethereum-based networks, and more specifically, Ethereum.

It was interesting to look at the wallet landscape because you had tons of mobile wallets, whether they're non-custodial, custodial only, focused on Ethereum, cross-chain, smart contract wallets with Argent, and so on. But at the end of the day – and I think it's still true today – in 2020, most of the volume in DeFi was still going via web clients. So if you want to give the flexibility to users to actually chase any yield opportunities out there, you actually need an extension. At the time, there were no cross-chain extensions, as in, you had MetaMask but you didn't have an option such as XDEFI wallet that allows you to basically store, send, and receive assets that are based on plenty of different layer 1s, and also layer 2s or sidechains.

So that's how it all started really, discussing with the THORChain team, trying to develop the ecosystem around the project, and back in July 2020 we decided to build the XDEFI wallet. Since then we've added support for 10 different chains, and we're continuing to do so. I think there were a lot of challenges to build a multi-chain wallet in a non-custodial fashion, not just from a technical standpoint, but also from a UX perspective, because each blockchain has different characteristics so you need to cater for them in the UI.

You need to try to think a little bit more: how do I actually abstract this multi-chain side of things? How can I reproduce a UX that is quite simple on a centralised exchange, but in a decentralised fashion? All of these challenges were things that we tackled along the way, and that we're still tackling. I also think that as a wallet provider, for me, wallets are vehicles, they're not destinations. So you use a wallet, it has to be reliable, secure, and fast for you to navigate across different types of web applications. And this is really what we're trying to achieve, but at the same time we want to make sure that we give some services – such as swapping and bridging from the wallet directly – a much better experience than it is today. Hence why we are integrating with people like Arjun – with Connext – and THORChain, and other protocols, because we want to allow people to

actually go L1 to L1, L1 to L2, L2 to L2 from within the wallet directly without having to interact with different bridging solutions, interfaces; and obviously trying to remove the friction around transaction signing popups, et cetera, which is obviously quite limiting from a UX standpoint.

So that's the XDEFI wallet, I guess, in a few words. Another challenge that we faced is, as we are supporting 10 different chains, from an API point of view, I don't think the API landscape was ever really designed for multi-chain products, basically, and there was a structural gap here. Because if you look at it as it stands, as of today XDEFI wallet is using more than 17 different APIs to fetch balances, transaction fees and so on, which is absolutely not sustainable and we cannot scale that way; you get rate-limited, and so on. So we've built our own cross-chain API from the ground up during the last six months, including EVM indexes, Tera indexes, NFT indexes, and so on, to make the overall performance of the product better, which was one of the main challenges that we faced. Because when MetaMask fetched a certain number of transactions, of data, we are doing the same for 10 different chains, so you can imagine how many requests we make at any given point in time. Yeah, that's me.

**MD:** Yeah, and I think actually you raise a really good point Emile, which is I think a lot of people, when they interact with applications today, they don't really think about the back-end developer tooling that goes into data availability on those applications. In fact, data availability across chains is something we don't talk about a lot, and one of the things we tried to do back in 2018 was build the first cross-chain settlement protocol. It came out of some fundamental research that was done at Boston University by a cryptographer, Sharon Goldberg. It was called Arwen, and it was basically this cross-chain atomic swap protocol. And actually the biggest challenge was, in 2018, in order to be able to swap assets cross-chain, you needed a cross-chain indexer that was continuously keeping data from across chains reconciled so that you could actually do this in a simple manner.

At that point in time, all this infrastructure, the data infrastructure, particularly in data oracles across chains, didn't exist. So not only did we have to maintain this atomic swap, we had to maintain a cross-chain indexer. Even just doing that for Bitcoin and Ethereum was a huge development lift. Today, people don't necessarily think about all of the underlying developer tooling and infrastructure that goes into building one cross-chain bridge, let alone multiple. So I think, again, this is a huge area of opportunity. This is a huge area for development and more research. And I think, one, more people don't necessarily think about the high cost of building, because I think people conceptually – when they think about a cross-chain – they view it as this finite, discrete, one-time event. But it's sort of a continuous event, because all of these protocols are continuously evolving; a blockchain is a living, breathing, evolving thing, unlike a piece of software, which may not necessarily see any fundamental upgrades for very long periods of time.

One of the things that I'd love to talk about is just the landscape. We've used a few terms, and maybe we can just delve into terminology and give people a clearer understanding. This is probably my fault for not being very precise with the terms. So there's layer 2, there's cross-chain, and there's the concept of a bridge. How do you guys conceptually organise the innovation or some of the fundamental components of this cross-chain L2 ecosystem? What is an L2 to you? What is a cross-chain bridge to you? How do you think about these separations and distinctions, and how do you start to map out the space?

I'm actually going to pull up this crazy ecosystem map that I put in our internal notes, just so people can see what I'm talking about, because it's a lot to deal with. Either of you... Don't go all at once. Here we go, here is the beautiful cross-chain ecosystem. Here we see one that's asset-specific, chain-specific, app-specific, and

generalised. And then I quite like this one that actually organises it by underlying chain, and you can see the cross-chain ecosystem, it's just absolutely bananas. And we see what's being built on each chain. It's wild. I don't know, how do you guys mentally organise this? How do you even keep track of it? Arjun, maybe you can start since you're probably looking at this space from a technical perspective.

**AB:** I guess the first thing to do is to define what an L2 is, and how do you define what an L2 is versus something that is just an entirely separate chain? Generally, the thesis behind an L2 has been a system that relies on Ethereum, or some other layer 1, for its security. The way that happens is that it basically doesn't have its own set; so with chains and consensus, one of the key things, key parts, of what keeps the chain secure is that you have economic security, and that economic security comes from either stake or utilising a bunch of computing resources in the case of PoW.

The idea with an L2 is that you don't go and bootstrap your own economic security. You leverage the economic security of a layer 1 chain, and you do that through... There's a variety of different constructions, but the most popular construction right now is a Rollup, where what you're really doing is you're taking a bunch of compute in this Ethereum-like environment, you're aggregating it into a bunch of proofs, and then you're just posting the proofs to Ethereum. It's like compression, basically. Now, the difference between that and another chain is that, of course, that other chain has its own entirely separate set of validators or miners.

When you get to cross-chain, it starts to get interesting because the information education around cross-chain – and cross-chain protocols, and in general, interoperability – is only now coming to light. My personal favourite mental model is what I call the interoperability trilemma, which is very similar to the scalability trilemma that we talked about earlier, where there is this tradeoff space around interoperability and communicating between chains, where it's difficult to simultaneously be a cross-chain protocol that is trust-minimised and also generalised – so, able to do any kind of arbitrary data transfer across chains – and also easily extensible; so, being able to be deployed to any chain.

And the reason that that's difficult is because the mechanisms that we have right now to do trust-minimised cross-chain communication rely on either something like an atomic swap, which Meltem talked about briefly, where you're swapping an asset on one chain for an asset on another chain. This is kind of also how THORChain works, but in THORChain's case there is a separate set of validators. Or they rely on something, basically, like running a light client of a chain inside of another chain, which is a much more complex activity.

In the atomic swap case, that's really largely limited to transfers of funds, and then really basic actions, so you can't get full expressivity; you can't port around any kind of data. Then on the light client side, building light clients is just incredibly difficult, and especially in this case, because you would need to build a new light client for each pair of chains that you wanted to bridge. So the complexity of that grows based on the number of chains, and things like that. The TL;DR is there's no really perfect solution, and in my cross-chain maximalist view – or I guess in my interoperability maximalist view – even things like Rollups are examples of ways to do special purpose cross-chain communication that allow you to have certain tradeoffs and certain security. But overall, as a landscape, it's complex and there are a lot of tradeoffs between different approaches.

**MD:** Yeah, I think one of the things I think about a lot, there's just an interesting way to really make this security conversation, in particular, more tangible. Over the fall, the Avalanche layer 1 blockchain started getting more and more popular, and a popular way for people to get assets from other chains into Avalanche – because you don't necessarily want to sell your ETH for dollars, take your dollars, buy Avalanche tokens just to operate on

that chain – what you can do is you can take existing assets that you have on Ethereum – and Ethereum really was the most popular chain from which people bridged or moved assets into the Avalanche ecosystem – at one point, that bridge between Ethereum-based assets and Avalanche had, I believe, over US \$6 billion of assets. And that bridge was secured by a single SGX enclave; a single key that was being used to sign, sort of, transactions.

That was a really interesting vulnerability, because here you have a tremendous amount of capital that's making up a lot of the activity on this particular chain – also comprises probably 4% or 5% of the overall assets on Ethereum and the overall monetary value on Ethereum – and people aren't thinking about when they're bridging these assets, they're dependent on the integrity and the security of one single key stored in one single hardware device. And again, I think it's not a criticism, but I think it speaks to some of these inherent tradeoffs where moving assets cross-chain or introducing new types of efficiency is going to require, to some degree, increased levels of centralisation and increased levels of security risk, because you are relying on someone in the middle, a co-ordinator in the middle, to make this possible to facilitate these types of transactions.

I thought that was a really interesting moment, because up until that point, everyone was really excited about interoperability. People were bridging assets across chains without giving it any second thought. I myself was certainly part of that cohort, or I thought, oh, this is great, I'm going to wormhole my assets from Ethereum to Solana, or then I'm going to move my assets via the Avalanche bridge from Ethereum to Avalanche; but we didn't really stop to consider some of the inherent security risks there. Again, it's not a criticism, and fortunately, there weren't any major exploits. There was no major exploit that took place, but it is something that starts to become much more relevant and much more concerning when significant volumes of capital are moving across chains, because at some point that could start to threaten or destabilise the majority-driven consensus models on some of these chains.

We saw this with Ethereum when there was a hack, or an exploit, of a smart contract in Ethereum and 15% of the Ethereum supply was suddenly controlled by an adversarial individual who had exploited the smart contract. That created fundamental risks in terms of ownership and control of the protocol, and particularly proof-of-stake protocols. If there are a lot of assets dependent on these bridges, you could see a situation where you see consensus itself being threatened by adversarial actors who are able to exploit these bridges in these L2s.

It's an interesting thought experiment, and that's where I think the challenges lie in this industry, is at these really unique edges where we don't necessarily think about the risk until it's right in our faces. And I don't know what's been done about the Avalanche bridge risk since it was discussed widely. Do you know, Arjun?

**AB:** I don't think, really, much.

**MD:** Not yet.

**AB:** I think you bring up an interesting point here. This is a more general principle from the security space, which is just that the security of all of these systems... You can spend as much time and as much energy creating a very secure blockchain... Ethereum is by far, by and large, the world's most secure chain right now, and so you can do something on Ethereum and enjoy the benefits of that security. But in any instance where you're layering these kinds of systems on top of each other, the security of the overall system is always going to be the security of the weakest link. So if you're using the Ethereum ecosystem, and then you happen to utilise a bridge to get to a Rollup, or to go between Rollups or something like that, and then that bridge has external

validators or it's using multisig – or, worst case scenario, it's using a single signing key – then that means that now your funds, or the assets that you bridged, are actually custodial. You're no longer benefitting from the chain security at all. You're now just entirely custodial.

**MD:** Exactly. Emile, I'd love to hear from your perspective, because you're dealing with consumers. Arjun, you're dealing more with app developers and people building on L2s, as well as liquidity providers and validators in the Connex... well, routers in the Connex ecosystem. Emile, you're dealing with a very different audience: people who are using these things, people who are putting their assets in XDEFI. XDEFI itself is non-custodial, but how do you think about articulating some of these concerns and some of these risks to people who are using the XDEFI wallet? Maybe believing that their assets are non-custodial, but say, for example, there's an issue where a bridge is exploited and they very quickly realise these things are not as decentralised and not, in fact, non-custodial: how do you think about some of the threats, and some of the adversarial models that you have to deal with, especially since you're dealing with people's funds?

**ED:** OK, there are several things, like there are a lot of other security issues that we can potentially have our users impacted by. I guess it all comes down to education at the end of the day. I do believe that as a non-custodial wallet, essentially what's happening is that people that are downloading our product are generally going to come with a crypto exposure already, from sites like Kraken, Binance, Bitcoin, Coinbase. They already know what a crypto is. They just haven't, basically, jumped from the centralised venues to the decentralised web.

I do believe that what happens most of the time is that we have new users that come, and have an idea of what a cryptocurrency is, but have no understanding of how a non-custodial wallet works and what does that mean to actually be in control of the security around your funds? So this is really important for us, to actually take these new joiners at the very beginning of the learning curve and bring them into the space, and try to give them all the potential knowledge for them to make sure that not only do they have a good hub spec, but they can interact safely with external interfaces.

How do we do that? It's not done yet, but we've designed something we call the "play to learn", whereby people will be able to join XDEFI wallet and learn more about how a non-custodial wallet works, and how to make sure that their funds are secure. For me, at wallet level, it starts by, if you have a little bit of funds in crypto, you should use a ledger, like a Trezor and so on. You should use a hardware wallet. I think that's the first thing. Obviously, wallet extensions are being audited, they're being reviewed, et cetera, but the extension client, as such, isn't the safest client by definition.

So my advice, and that's the advice that I'm giving to anyone putting a material amount of funds in their own wallets, is to have a ledger. Now, I think it comes with issues at the UX level, and this is something that we've been thinking about for a little while. The problem in using a hardware wallet with a multi-chain product is that a ledger itself does not really allow, per se, to have UX flows that are easy to follow for users. Why? Because every time you want to plug your ledger and load a given wallet within your extension, you basically are going to have to plug it and plug it to have several of them; or when you have to switch accounts again and again, this is really complicated from a user experience standpoint, meaning that there will be a limitation for multi-chain products and wallets in particular. At that level how do you basically make sure that people are still safe while capturing for better UX? So, some of the things we've been looking into is, for instance, non-custodial 2FA and how we can create that using TSS.

**MD:** Emile, so, 2FA – two-factor authentication – what is non-custodial TSS?

**ED:** OK, so, to give you an ID. Simply put, it's basically you split the keys between two devices, so you have one on your mobile device and you sign in with your mobile device to connect to your extension. Simply put. That's much more complicated than that. It hasn't really been done. ZenGo and Taurus have worked on PoC, but it's still to be done, so this is something we're researching right now. But essentially a little bit like you would connect to, I don't know, Google with Google Authenticator. Essentially, it would come back to the same in terms of UX.

**MD:** Yeah, and I think what you're highlighting is one of the fundamental challenges, and one of the things we cover in the course. The fundamental innovation here with blockchains is we're enabling people to prove ownership of assets using public/private key cryptography. The beautiful thing about that is it allows any asset to become tradable and to settle with finality on this global settlement protocol, which is your layer 1 blockchain, using this public/private key infrastructure, which doesn't require third parties. We've introduced third parties into the process to make the UX simpler, and to create user experiences that provide more security guarantees or more levels of redundancy; more levels of, sort of, organisational de-risking.

But, fundamentally, why does cross-chain interoperability matter? Why am I so excited about the space? Why do I think this is the future? We'll try to bring it back to a high-level concept. In my view, today we have a crypto market; it's about a US \$1.7 trillion market. These assets are very fragmented, though. About 40% of that is Bitcoin, another 20% is Ether, another 20% is the top 20 layer 1 blockchains, and then there's a long tail of assets. The issue is, liquidity in the space starts to get fragmented, and the premise has always been – for me at least – you can turn anything into an asset that you can trade anywhere, any time, with anyone, clear margin how you want, settle how you want, with finality, on a public, global distributed ledger.

That's the exciting thing. Everything in the world can now become an asset and be part of a global market; become collateral. The issue is, when you start fragmenting these markets – and again, the incentive is to fragment infinitely, because you want more layer 1 blockchain computation and you want that computation to be cheaper, faster, and more scalable, always – that starts to fragment market liquidity. And so, interoperability enables you to maintain one global pool of liquidity because it's easy now to port financial computation from one network to another while still maintaining some of the security benefits of these underlying layer 1s. So I'm very optimistic about interoperability, L2s, cross-chain. But again, hopefully this conversation has given you an appreciation for how nascent and new this design space is, and I think this design space will take decades to perfect and really understand.

And it really is at the cutting edge of theoretical security research; as well in cryptography research. So I think hearing from Arjun – who's actually building one of these protocols – and then hearing from Emile, who's trying to figure out how to enable people to actually interact with this innovation and build a better user experience; hopefully, that gives you an appreciation just for how profoundly challenging it is, but also how profoundly exciting it is, from a capability perspective, to have this technology.

## Additional Video 2

NFTs have attracted a tremendous amount of interest from collectors and investors alike, but have historically been considered illiquid assets. As we saw with the advent of DeFi or decentralised finance, holders of on-chain assets want the ability to put their financial assets to use, and being able to obtain liquidity without selling an NFT is a concept with wide appeal.

We have already seen examples of NFTs being tokenised; the next step will be “financialising” those assets using DeFi protocols, transforming NFTs into highly useful assets with increasingly numerous use cases.

In this recorded session, we’ll hear from three entrepreneurs leading the charge on the financialisation of this new asset class and the various building blocks / primitives needed to enable this vision.



**Meltem Demirors:** I'm really excited to have everyone here today. Very relevant, very timely topic. As you know, we try to address as much as we can in the course syllabus, but given that this is crypto, there's always new things happening. And so we do these occasional addendums where we get to bring in experts working at the frontier of what's happening in this industry. Today we have with us Nick, who's the CEO of Upshot. So Nick, do you want to wave? Hi to everyone. We have Andy, who's the CEO of Fractional. That's Andy there, and then we have Scott, who's the CEO of Genie, so hey Scott. It's 8:00 am here in the States, so it's pretty early for people in the crypto space. I'm happy that they've all decided to join us.

We're going to kick off today with a little short overview to just give everyone a grounding on NFTs, what they are, how they work, what we're going to be talking about. We'll weave in some of the materials that you've learned about in the first few modules in the course, and then we're going to go into discussion with our panellists, our experts here. Of course, as always, we're going to keep this informal, so I encourage you to put questions, comments in the chat. I'll try to weave them in. And really, this is an opportunity for you to learn and for you to ask questions, so please feel free to do that using the chat. With that, I'm going to go ahead and share my screen.

Let's all become JPEG connoisseurs. So I'm just going to do a little NFT 101 here. What is an NFT? At a high level, an NFT is a combination of on-chain information and off-chain information, and this is something you've learned about in the first few modules: that there will typically be two different types of data. There's a contract, typically for Ethereum-based NFTs is the ERC721 contract. It's standard, it's really common. And then there's a bunch of metadata that can be stored on-chain or off-chain, as well as rich data that's associated with the NFT. There's a lot of different use cases for NFTs, and I think we're still at the very early stages of what NFTs will be utilised for. And again, Andy, Scott, and Nick are going to be able to talk about some of the use cases they're really excited about and what they're building in this space.

But at a high level, the place where NFTs started, where we're getting the most attention, is on the collectibles side, in particular art and gaming assets. But obviously, sports collectibles like Top Shots or Topps Baseball Cards have become more popular. We're seeing names and domains emerging – so some of you may have heard of ENS domains, or Ethereum Name Service domains – but there's also a lot of other things that can be captured as NFTs in the collectibles realm.

We also have DeFi NFTs, so you can have positions in a DeFi protocol that can be represented as a unique non-fungible token, Uniswap V3 notably. Uniswap is a very popular DEX, or decentralised exchange. Uniswap V3 notably turns your liquidity position into an NFT that can be traded, which is pretty interesting. We're also seeing NFTs being utilised in insurance and other parts of the DeFi stack, and then obviously on the securities side, unique securities contracts could potentially be represented as NFTs, whether that's a real estate contract, a bond contract, or another unique financial product. Obviously emerging exciting space.

There's also an emerging on-chain credentialling space that's emerging, but here's just a high-level overview. The NFT stack is something I just want to touch on briefly. There's a lot of information here. We're not going to talk about it all, but I want to just bring together the different components that you've learned about throughout the course – particularly the protocol layer, the networking layer, and the application layer – just to give you some context as to where this all fits. Let's just dive in. So the core layer that I want to touch on first is protocols. From a layer-1 protocol perspective, a lot of NFTs today are issued on Ethereum. I think it'd be fair to say the NFT landscape to date has been dominated by Ethereum, although again, Scott, Andy, and Nick may disagree with that and may have other opinions on where the future is headed. But obviously, specific blockchains like Flow, which is focused on sports collectibles, and Solana, which is focused on bringing efficiency to transaction processing, are also starting to see more momentum.

Again, I think one of the key questions is in choosing a layer-1: what are the security tradeoffs you're making? What are the transaction fee tradeoffs you're making? And then what's the available infrastructure on these different layer-1s to support your NFT project? There's also layer-2 protocols. In our last session in February, we talked about cross-chain interoperability, and we had folks who are building in that space. One of the key things we're starting to see is some types of NFTs moving to layer-2s, primarily built on top of Ethereum and other NFT-focused blockchains, but also moving to side-chains or bridges to allow people to move their NFTs across layer-1s and utilise them in different ways.

So, Polygon, for example, has been really popular. There's a really cool type of NFT or token called a POAP, or a proof-of-participation token, which a lot of projects give out or events will give out when you attend an event. That's been migrated over to Polygon because it's much cheaper to issue on top of Polygon versus, say, in Ethereum. So you pay a cent to issue a POAP as opposed to paying anywhere from a few dollars to dozens of dollars, depending on how much is happening on the Ethereum blockchain when you want to mint your POAP.

Another thing to think about – it's really important – that we don't talk about a lot is storage. Where are you actually storing data associated with the NFT? It's a really interesting question – and again, from an infrastructure perspective, it's one that isn't talked about a lot when it comes to NFTs – but a lot of times layer-1 blockchains aren't really great places to store a lot of data; particularly large files, large images. So there are a number of different on-chain solutions that are emerging. There are storage-specific protocols like IPFS, Arweave, and SIA, and then there are also a number of service providers emerging that enable the utilisation of Web2 storage solutions and make them compatible with Web3.

But an important question is, when we think about NFTs, where is the metadata associated with your NFT stored? Where is the actual image itself stored? Important thing to consider. Then we'll get into the actual application stacks. So this starts to become interesting. We talked a little bit about the different verticals in the NFT space, and again, we'll delve into that in today's session, so I won't dwell on this. And then this is really the core topic for today, which is once we've issued all of these NFTs, all of these new assets that are represented on-chain, how do we utilise them in new and interesting ways to create new financial primitives?

This is really where I think a lot of exciting work is happening. This is where the unique attributes of NFTs really start to shine, is how can we actually start to get into the financialisation of NFTs? Unlike fine art, which has issues with provenance, with storage, with custody, with valuation, with fractionalisation even, NFTs offer us a really interesting opportunity to do a lot of these things natively. But in order to financialise NFTs, you need all of this tooling, all of this infrastructure, to make that financialisation, that productisation, that securitisation, possible. The folks we have on today are doing exactly this, and building those primitives that are going to make financialisation possible.

So, that's hopefully a helpful overview of NFTs, and just a high-level perspective of how some of the different things you've learned about in the course fit together and come together. I'll make sure we share these slides so that you can view them and read them in more detail on your own time. I know we went super fast. With that, I will stop sharing my screen, and we'll move over to actually talking about financialisation of NFTs. Why don't we start off with Andy from Fractional? Andy, tell us what Fractional is at a high level.

**Andy Chorlian:** Yeah, Fractional is a platform to fractionalise NFTs. Really high level, it's a totally permissionless, non-custodial platform where you just come with an NFT, basically say, hey, I want to turn this into a bunch of smaller tokens, call one smart contract, call and then that NFT is custodied inside of a smart contract and issues a bunch of tokens back to you. That's the really quick version.

**MD:** Yeah, and why? Why do we need to be able to fractionalise NFTs? Just give us some context as to why that might be relevant.

**AC:** Yeah, I think there's multiple reasons. Probably what we've seen so far have been a couple of different kind of baskets of why people would want to do it. One is to create, say, Collector DAOs or groups of people who all own the same thing that's been popular.

**MD:** What's a DAO, for those of us who are new to crypto?

**AC:** A DAO is a Decentralised Autonomous Organisation, so it's basically a group of people who are all rallied around, normally, some kind of cause, some end goal. And they're using a token to vote and manage, say, a treasury and kind of collective energy, and what they're spending their time on. And so we've seen that a couple of times. People have purchased an NFT together, and fractionalised it, and then used the fractional tokens that are created as the governance token for a DAO. Probably the most interesting example of this we've seen was one called FreeRoss DAO, where they bought Ross Ulbricht's Genesis NFT, and they raised a bunch of money alongside that, and they're now governing those funds and working to free Ross Ulbricht. That's one example that I think is really cool.

Obviously, you can think of a lot of reasons why people would want to own 5% of an NFT. Some of the stuff around gaming, and potential use of almost treating the NFT like a timeshare and saying, I own 10% so I can use the utility of this NFT 10% of the time. Different things like that are interesting, but those are a couple of the use cases we've seen.

**MD:** Thanks, Andy, and just give us an idea of how big Fractional is. Do you have any sort of idea how many NFTs have been fractionalised, how much market value they represent, just to help us place that in context of the broader NFT market?

**AC:** So, Fractional as of right now, there's around 75,000 unique addresses that own a fraction of an NFT from what we can tell, and a couple of thousand NFTs have been fractionalised. There's been... It's varied a ton based on the market and different things. The NFT market's been crazy. But as of right now, I think there's a little less than US \$200 million of valued NFTs on the platform, and there's been a little over US \$1.5 billion of trading volume of fractions of NFTs.

**MD:** It's amazing. Well, thanks so much. I myself have used Fractional, big fan, especially for really expensive NFTs. Maybe you don't want to spend a couple of million dollars on a picture of a rock, but you'll happily spend a couple of hundred dollars on a tiny, tiny fraction of said picture of a rock. You talked about valuation, so maybe

Nick, we'll move over to you and you can talk a little bit about Upshot and what you're building on the NFT valuation side.

**Nick Emmons:** Yeah, so at Upshot, what we're focused on is building out NFT appraisal tools. NFTs are these types of assets that don't change hands very often. They're low velocity assets, and so using market-based mechanisms as the sole means of pricing them becomes inefficient or inadequate at times. So what we've built is a number of pretty advanced machine learning models that re-price NFTs at an arbitrary, frequent cadence. What that allows us to do is build out these real-time price feeds for NFTs that can later be used to build out more exotic or expressive financial instruments.

We can start to get into things like more advanced NFT derivatives, NFT synthetics, a number of other financial primitives that are unlocked only when we're able to frequently update the prices for these assets.

**MD:** Yeah, and then a question on that, Nick. Maybe just giving people a little bit of background, a little bit of context. In the traditional art world, if I have a Picasso or a painting, there's a valuation event that typically only happens once. There's a liquidity event. So, typically, valuation is coupled with liquidity, and rare artwork or very expensive, high-end artwork sells very infrequently. Can you just talk a little bit about why valuation in NFTs is so, so different?

**NE:** Sure, so what's nice about NFTs – at least, the types of NFTs that are prominent today – is that most of them are collectibles. Most of them are defined by a finite set of traits, and so we can do this more structured analysis on the appraisals, or on the pricing, than is possible with one-off bespoke pieces of art in the physical world. We have collectibles that have different traits that are made up of different levels of rarity, and we can start to examine things at a much more granular level. We can apply this structured learning to pricing these NFTs that allows us to be much more accurate, and we have more data in that these all exist in a shared substrate of data in the blockchain, and we can do more robust analyses across social sentiment, indifferent community growth, and community sentiment, stuff like that. So we have access to just a lot more data and it's a bit more structured, at least with the types of NFTs that are prominent today. That allows us to build out much more robust appraisal mechanisms than currently exist in the physical, bespoke art world.

**MD:** Got it. And we actually have a question around verification and authenticity. So Nick, since you're already talking about valuation, we'll throw this one at you. This is a question from Sylvia around how do you go about verifying and authenticating NFTs? Because I think this is another place where NFTs just lend themselves so well to financialisation.

**NE:** Yeah, I mean, most NFTs can be verified on-chain unless we're talking about the translation of an analogue piece of art, or a kind of asset, to an NFT where there is this sort of supra-blockchain type of verification that's necessary. Verification is sort of baked into the asset class itself. So that often comes with the standard: it comes with NFTs innately. I don't know if that answers the question, but...

**MD:** I think it starts to answer the question. I think everyone here is at varying levels of knowledge, they're in different places in the course. Some people have completed it, some people are in the first module. So hopefully that makes sense. Actually, I'm going to go back to you, Andy, for a moment. I have a tough question for you. Someone asked this privately, but I think it's a really good question. They were asking when you fractionalise an NFT, do the fractions of that NFT become fungible, even though the NFT itself is non-fungible?

**AC:** Yeah, so we started out with the fractions being fungible tokens, being ERC20 tokens. For those who aren't aware, those are the general tokens that are used on Ethereum for, say, traditional DeFi protocols like Uniswap and Compound, and all of that. We then transitioned to using ERC1155 tokens, which are NFTs, but also still fungible tokens. What we're working on now is actually a little bit of a hybrid, where if you want your fractions to be non-fungible, that is going to be possible. But you also could have them be fungible ERC1155s but they will all be NFTs. One of the challenges there is, just wanting them to show up in your wallet and still look nice, and all of that. So generally, yes, they are still fungible, but soon we'll have the option to not have them be fungible.

**MD:** Awesome. Thank you. And then Scott, last but not least, you've been waiting patiently. I think Genie is sort of the last part of the stack. I can value NFTs and figure out what ones I want to buy, and what a good price to buy them at is. I can then take my NFT, split it into tons of little fungible or non-fungible pieces and sell them to the broader community online, and buy them with groups of friends, and now I want to get into the actual buying. Tell me what you're building at Genie.

**Scott Gray:** Yeah, so Genie's an NFT marketplace aggregator. We allow for users and applications to buy or sell any NFT from any marketplace. There's tons of different verticals of marketplaces. Some of them that we're talking about today are financial marketplaces like Fractional and, eventually, Upshot. But there's also primary marketplaces, secondary marketplaces. Genie brings all of those marketplaces together, and what we're solving for is liquidity fragmentation; also, information asymmetry that appears because of that liquidity fragmentation. And what's a result of those two is capital inefficiency. By using Genie, you can solve for those three problems.

**MD:** Yeah, so Scott, maybe just if you can ELI5, "explain like I'm 5", me. What does liquidity fragmentation mean? And for those of us who haven't been active on NFT marketplaces, maybe just describe to us what that looks and feels like.

**SG:** What I mean by liquidity fragmentation is when NFTs appear on different marketplaces. To give you an example, there's 10,000 CryptoPunks. Maybe 100 CryptoPunks are on OpenSea, 100 are on Coinbase, and the rest are on Larva Labs. For a user, you have to go through all those different websites to find the CryptoPunk that you want, and as non-fungible tokens have a marginal rate of substitution, because you're adopting them as your identity and as culture, you want to be able to choose the one that you really want. What Genie allows for you to do is see across all those different marketplaces and pick the NFTs that you want, and you can also batch-buy or batch-sell across those marketplaces.

**MD:** Yeah, and I've personally used Genie quite a bit when I want to buy a lot of NFTs, when I want to sweep the floor. For those of you who aren't familiar with that phrase, "sweep the floor", it's where you buy all of the lowest-priced NFTs in a collection. Genie is a really useful tool because instead of going to all of these different websites, I can buy a whole lot of NFTs in one click and one transaction. I am a sweeper, Scott. That's correct. I'm a lazy NFT collector.

OK, well, thank you so much for those intros, and I see a lot of great questions in the chat. Thanks to everyone who is asking questions. Again, feel free to throw them in there. I will try to weave them in as they're relevant. One of the things I want to talk about as a starting point is I think, again, a lot of people in the session may not be so familiar with NFTs. I think a lot of the attention we've seen in the NFT space to date, especially in popular media, is on these so-called blue chip collections or really widely-recognised, widely-collected NFT collections that tend to have really high prices and therefore, I think, not be so accessible to most everyday people who may not have, you know, half a million dollars lying around to buy an Ape, or a Punk, or one of these blue chip

assets. Can you talk a little bit about how NFTs are going to evolve across other use cases, and what the long tail of non-blue chip and blue chip NFTs might look like?

**NE:** Sure, I guess I can start. I guess the way to think of it, NFTs primarily, even though they've been represented as art and collectibles to date, are more of a structural innovation in the blockchain space. They are this standard that quite literally allows us to tokenise anything, and bring anything on-chain. Art and collectibles have captured the limelight over the past year and a half, but what we'll start to see NFTs represent more of are financial assets, more esoteric financial assets; things like bonds, annuities, commodities, things like this, or insurance, real estate. NFTs will begin to bridge into this financial world, and we'll see a large number of primitives being built around those.

So while we've seen these high-value collectibles and pieces of art capture mainstream attention up to date, we'll start to see NFTs be a much more financial asset class; and NFTs are a very broad asset class. The term NFT itself will fall out of vogue, and will fall out of the public lexicon over time as NFTs become just this abstract structural trait that these different types of asset share.

**MD:** OK. That's the first time I've heard someone say that, Nick. That's a bold prediction, so we're going to stop using "NFT". It really is interesting that we still talk in terms of NFTs because it is really a technical characterisation, as opposed to really indicative of anything related to the asset. There's a question here around the tokenisation of various types of assets. Seth asked a question around the tokenisation of physical assets, and then James had a question around NFTs representing identity assets or credentials of various types.

I guess, Andy, since you sort of sit at this interesting place where you're seeing what people are fractionalising, what do you think about the migration of physical assets on-chain and credentialling assets on-chain as NFTs?

**AC:** So, I have a bit of a coloured history with real-world assets coming on-chain. I spent a lot of time at MakerDAO, where a lot of our research was about real-world assets as collateral for Maker. And most of our research was that it's really, really hard. That was the conclusion. There are some interesting companies who are doing this model where they say, hey, send us your – typically it's for collectibles. There's one called 4K, another one, there's a bunch. I don't remember their names – where you basically send it to them, they put it in a vault, and they mint an NFT and then that NFT is tradable. Anyone can redeem it and get the item out of the vault.

The challenge there is you have this trusted third party who is actually custodizing the real-world asset. And you just have to assume that they're going to not go bankrupt, the vault is not going to be robbed, whatever. So there are challenges there, but I think we're going to continue to see it happen. I just generally am betting that it'll be a slower wave of adoption than the larger usage and excitement around digitally native assets and metaverse native assets, and just crypto native assets in general. My feeling is that the infrastructure needed and a lot of even the legal structure needed to appropriately handle this move from real-world assets to NFTs is not really fully fleshed out, and that'll take a lot longer of a time than actually building the technology needed to do it. And so my bet is that will be a bit of a slow process.

And the challenge with identity stuff, as I mentioned as well, is, one, the privacy of your identity stuff is a bit challenging. There are secret chains where everything is encrypted or zero-knowledge proofs, and that probably would be where that kind of stuff would live. We've also seen some examples of basically getting an NFT issued that essentially, where a third party says, hey, we've done KYC on this person, and they have passed the basic KYC where you could sell them goods or whatever, but doesn't actually say anything about

you. I'm interested to see how that space evolves over time. I believe that's what Bored Ape Yacht Club used for their most recent KYC for whatever is coming for them. But we haven't seen that space really blow up too much yet. I would expect that it does, but I don't really know what that looks like. I'm definitely not a KYC expert by any means.

**MD:** Yeah, I'm actually working on a research piece around the use of non-transferable NFTs in credentialling, so we'll definitely share it with the class when ready. But I think there's been a lot of discussion precisely around this issue of privacy. You don't necessarily want identity- or credential-related data represented on-chain, especially if people drop it in your wallet. And there's no way for you to verify it or remove it. I think there's been a lot of debate around whether or not NFTs are actually good for that, or if you can use verifiable credentials, which are a different standard. Definitely a topic for conversation.

We have a lot of questions, comments in here. Guys, feel free as we're chatting if you want to pop in here and respond to things. Feel free if you have suggestions for things people should look at. Feel free. Let's go over to you, Scott. Let's talk a little bit about investing strategies and ways that you can arbitrage NFTs since you're building this aggregator. I guess, what are some initial use cases you can think of with the financialisation of NFTs? That allow us to build new financial products that don't rely on us qualitatively assessing NFTs and saying, hey, I think this one specific NFT, or this one specific collection, is a good investment. But what are different ways that people can actually start to build scalable investment strategies that remove some of the subjective judgement from NFTs and actually build NFTs into an investable asset class at larger scale? What are your thoughts as you see how people are using Genie?

**SG:** Yeah, definitely. Genie sits in a really interesting place where it's agnostic to whatever valuation model the user has. I think the NFT spaces started off really simple by using rarity scores as a way to gauge if an NFT is valuable or not. And now we're seeing more...

**MD:** Scott, can you describe what rarity is? Sorry, again, we have different...

**SG:** No problem. So, rarity looks at the metadata of an NFT. For example, a Bored Ape has blonde hair, it has blue eyes, it has whatever, and based off the relative score, it assigns a rarity score to that NFT. People have been using that in the space to gauge if an NFT is valuable or not. We're now moving into more complicated ways of appraising NFTs. One way is Upshot, where you're using ML [machine learning] to value that NFT. Another way Genie could be useful here is, we're talking to some NFT as collateral platforms where you could actually buy the debt ticket to that NFT, when it makes sense as a good deal. So you could buy the NFT for maybe half the price, if the loan is underwater and the ticket is on the market.

**MD:** Can we just go through, this is the first time we've introduced NFTs as collateral. Just describe that to me. I own, let's say, an NFT that's worth, theoretically, US \$250,000. How do I use that NFT as collateral? Can you just explain how that might work?

**SG:** Yeah, so there's a few ways NFT as collateral can play out. There's not one solution that fits all. So if we're talking about an NFT that's worth US \$250,000, there's not enough liquidity at the moment to instantly liquidate that NFT, so the structure that would have to be set up is you would have an auction system where you bring your NFT bidders to bid on that NFT. The highest bidder becomes the lender, and if you have a month or whatever time period to pay off that loan, and if you don't pay off that loan, then the highest bidder who became the lender would be able to take your NFT.

**MD:** Got it. Nick, so I think this is a good question for you. There's a comment from Seth here that in order to financialise NFTs, use NFTs as collateral, you're going to need KYC, credit checks, clearing houses. And I think one of the really important things here is since NFTs are represented digitally and this is all on-chain, you can actually remove all of these intermediaries. That's the whole point of what we're doing here. We can represent all of these functions that have traditionally been performed by institutions as programmatic functions that are hardcoded into how these different primitives work. Can you talk a little bit about what that might look like, and why we no longer need these centralised institutions to perform these different functions that historically have really operated in a space where there is a lack of trust or transparency?

**NE:** Sure. I mean, a lot of these protections come with the chain itself. Blockchain as a technology removes a lot of the needs around custody and things like that, that have plagued the traditional art world to date. In that, you remove the need for a lot of those things. And what's nice about everything operating on-chain is that you come in with this sort of baked history for a given wallet, and can potentially be transposed into a given group of wallets. So you begin to be able to build up this history that cannot be faked; that doesn't need this extra trusted party in order to verify, and that it comes inherently with the kind of operating platform in which the assets live, in which the people are interacting with. It's the blockchain comes with a lot of features baked in.

**MD:** Yeah, and I think that's a really hard part for people coming from traditional finance to conceptualise, is all of these traditional intermediaries we might have in a traditional world no longer need to exist. Even questions around authenticity. If an asset is purely digital, the authenticity can be verified on-chain using the original contract under which the NFT was issued. When it comes to physical assets, any time we digitise a physical asset, obviously there is trust required, but I think NFTs, generally, as a primitive – particularly when they're digitally native – remove a lot of that.

Question from Sylvia around trading commodities as NFTs or just financialisation, moving more financial assets on-chain as NFTs. We'd love to hear, guys, what you're seeing or if you're talking to any more traditional financial institutions who are thinking about representing certain assets that they might have issued in the past in a digital way, using NFTs. Floor is open.

**SG:** I haven't heard anything yet. Andy, has Citadel reached out to you?

**AC:** No, no. My DMs are open, Citadel. Do you want to talk? Let me know. Yeah, I haven't seen it too much. I guess I can speak a little bit to, more so actually my time at MakerDAO than what I've been doing previously. But there was some research into some of this stuff. Generally, it wasn't with NFTs though, it was with ERC20 tokens. The challenge, again, is a lot of the... building the right structures for trading these things when you do have to explicitly restrict who can use them, and creating a lot of that infrastructure is pretty challenging, because currently NFTs are all fully open. Anyone, any wallet, can buy anything. They can really do whatever they want with the NFTs, for the most part. And as you have these new pieces of infrastructure that require significantly more structure where, say, you have to do KYC to own this thing because it is a security, or, you know, you can't, if someone were to burn it, that would be really bad and it would cause issues, and you have to build all these either new special marketplaces, or new tooling around these systems. That kind of stuff takes a long time, and as of right now, I'm not super familiar with anyone who's doing that in the NFT space.

**MD:** Yeah, I think the only project I've looked at is Centrifuge, which is trying to find ways to represent real-world assets digitally. But again, I think, challenging space. Nick, we've gotten a lot of questions around market manipulation, effuse valuation models. Can you talk a little bit about where and how bias might show up in

different ways that NFTs are being valued, and what the challenges are around market manipulation? Because obviously we see a lot of market manipulation in the traditional art space. I would love to hear how that shows up for you guys at Upshot.

**NE:** Sure, yeah, that's definitely always an issue, and it's a bit of an arms race. There are always different ways to manipulate markets. People get creative around how they can manipulate markets, and it's kind of our job as the appraisers to build models that account for those biases or modes of manipulation, and build models that weed them out. I think a really popular means of manipulating markets right now is wash trading, and we're protecting against that by placing some standard deviation bounds around trades as they relate to the broader collection to try to identify wash trading programmatically.

I think the other way to limit bias or manipulation in models, or valuation methodologies, is to take into account many different factors. As was mentioned earlier, the primary means of identifying the more valuable assets or NFTs in a collection versus the less valuable ones have been rarity. What we've found empirically is that, generally, the market and different communities have placed too much weight on rarity when pricing NFTs. It is a factor, a fairly significant factor, but what matters much more is order book composition at any given time; the provenance of NFTs in a collection, in the collection at large, is smart money buying into NFTs? Or is it more retail, kind of visual characteristics or aesthetics of NFTs that aren't represented explicitly in metadata, but are seen in the aesthetics of the NFT itself? All of these things are ways to further diversify the input or the parameters of valuation, and I guess try to minimise bias or manipulation as much as possible. But it is an arms race, like I said.

**MD:** Well, what I know as someone who spent a lot of time in markets is, show me a market and I'll show you a market arbitrage or a market manipulation opportunity. And that line is very blurry sometimes, especially in this new frontier. Let's switch gears a bit and look forward to the future. You guys are building tools to fractionalise, to aggregate liquidity, to value NFTs. But what are other types of NFT financial primitives that you think are going to need to be built? A lot of students in the class, they think, are entrepreneurs themselves, are thinking about building things in this space. What are key pieces of NFT infrastructure that you think will need to be built over the coming years that are going to allow for continued financialisation? Would love to hear your thoughts on things you're excited about, things that don't exist yet that you'd like to see, or where you think there's still white space in the NFT market space.

**AC:** You know, I think one of the things that – it's not explicitly a tool that needs to be built to see more financialisation, but more just NFTs in general – is there's a lot of conversation around NFT utility, and eventually NFTs that are generating income based on x, y, and z or some other desirable things about them. Most of that at this point is pretty theoretical. It's not really happening very much, as we mostly have been talking about digital collectibles, where if they are making any income, it's purely just, say, airdrops to that collection, new NFTs that they're able to mint, different things like that; as opposed to more like, this NFT is generating value because there is demand for it.

And so I think that really is one of the most important things that we need to see as we see more financialisation, is a market for these things that isn't purely driven just on speculating and collecting rare pictures of monkeys and CryptoPunks, but like, hey, this digital metaverse land is in a really desirable place, and so I'm able to rent it out for x amount per month. And that just creates a system that becomes, where it becomes, way more interesting and easy to financialise those types of assets. So I think that just the general growth and increase of actual utility, and general infrastructure growth, is really important.

**MD:** Yeah, that's something I'm excited about. I actually own some NFTs in a Roblox derivative that I rent out so people can use my little avatars to go mine coins. It's kind of fun. I'm a digital landlord, who knew? I can't afford land in the real world, but I can own digital land and have digital farmers give me digital tokens. What a life. Andy, Nick, any thoughts from you on infrastructure, tooling around NFT financialisation that you think is going to emerge, or that you'd like to see?

**NE:** Yeah, one I'm really excited about is synthetic exposure to NFTs or NFT synthetics. Right now, if you want to interact with the NFT market, you have to do so by interacting with the assets themselves, or fractionalised shares of those assets, which still require those assets to be held in a specific place. What synthetic NFTs will allow us to do is enter these potentially arbitrarily deep positions into assets that are just synthetically tracking the price movements of a given NFT. I'll be able to point to a price feed of some basket of NFTs that I've curated myself, regardless of who's holding them or where they're being held, and produce an asset that moves based on the price movements of those assets; and that enables, obviously, much more accessibility to NFTs, but also more advanced financial instruments to be built. Things like being able to take positions in both directions of price movements, enter these long and short positions, which is obviously important for building out more robust financial vehicles.

If I wanted to create a market neutral NFT fund today, it would be difficult because I don't have access to very robust or mature vehicles for shorting NFTs. But as synthetic NFTs reach a level of maturity, I'll be able to enter short positions at a far larger level of robustness.

**MD:** Yeah, I think the only way to really do a short today that I found is using prediction markets, but...

**NE:** Yeah, and those are quite illiquid right now.

**MD:** They are. Typically the majority of the liquidity on those trades... I think again for me, sitting in the asset management space, and trading space, synthetics are definitely really interesting: the ability to have exposure, non-directional delta one exposure, is super interesting. Scott, any other thoughts? Could Nick and Andy have given, sort of, their wish list of NFT tooling, NFT infrastructure? But anything?

**SG:** Yeah, I definitely agree with both of them on, first we need actual utility for NFTs and then derivatives as well, because that opens up not only long positions, but also short positions. I think the last thing is just leverage. So, NFT as collateral will allow for more healthy leverage in the space, or maybe unhealthy at some point, creating more leverage.

**MD:** I don't fear unhealthy. I like all leverage.

**SG:** Yeah, and that will just open up more market cap in the space and more room to grow. And it's also very democratic if people have a really deep conviction on an NFT that they want to buy, but they don't have enough liquidity, they can just easily go get a loan to go buy those NFTs, and then maybe connect to that utility where they can then rent that NFT, and then boom, they have a business going. Yeah, NFT as collateral is definitely going to be huge in the year forward.

**MD:** Awesome. And then I think the last question I have, and we'll do this as a rapid-fire round, and then everyone who's in today's chat, we'll open it up to Q&A. But my last question, I guess. If you had a prediction of what a mainstream financial product tied to NFTs might look like, what do you think might materialise in the

coming years?

**AC:** Yeah, so I'll say one that we haven't said yet or haven't talked about yet, but it kind of ties into a couple of different things we've spoken about. I have a feeling something that would be pretty popular, which doesn't really exist right now, is a buy now, pay later system, which generally is probably going to require something like what Nick is building, and some sort of loan system where you can basically have some third party front the cost for you to buy your NFT that you need in the metaverse and you slowly pay them back over time, either with accrued yield on the blockchain or just from you paying it down.

**MD:** Nice, yeah, I think someone in the comments mentioned flash loans, which is kind of an interesting experiment in that space. But I'd love to be able to get a mortgage or a large loan to buy NFTs. I would be buying the most degenerate NFTs only. Nick, Scott, any thoughts from you on what financial products tied to NFTs might look like in the coming years?

**NE:** Yeah, I think one, it's less of a financial product, and I guess more of just an interaction type, is more robust liquidity and market-making in the space, leading to more fluid entrance and exits from NFT positions. You could start to picture a type of interaction similar to Opendoor, but for NFTs, instead of having to go through this eBay-like experience when I want to move out of an NFT position – and having to list it, wait for someone to accept that price, or have bidders come in on my NFT – being able to instantly move in and out of positions because there is, I guess, mature enough market-making and liquidity provision in the NFT space for me to do so. I think that will become much more ubiquitous over the coming months and years, and allow for much nicer UX in the NFT space.

**SG:** Yeah, I'm going to piggyback on Nick here, and that's actually one of the functionalities of Genie. We allow you to list across marketplaces, but then we're also going to be tapping into market-makers so that when you're in the process of listing, a market-maker will give you a real-time quote, kind of like a Google Ads auction, and you'll be able to choose if you want to maybe wait seven days, or maybe you want to take a 5% haircut and liquidate instantly with that market-maker.

**MD:** Yeah, so it's almost like tendering a request for quote across a multitude of different brokers as opposed to tendering individual RFQs.

**SG:** Exactly. Yeah.

**MD:** Very cool. Awesome, well, thank you so much, guys. We went all over the place. We covered a lot. I know there are a lot of questions in the chat. Let's start with one that's career based. A lot of people taking this course want to maybe switch careers or start something in the crypto space. Are you guys hiring? What's the best way to get into the NFT space, and where should people go if they're interested in working in the NFT industry or working at your companies?

**NE:** Yeah, definitely hiring. Hiring a lot of people right now, just come to our website [upshot.xyz](http://upshot.xyz), there's a lot of information there, but hiring a lot of people right now, especially on the engineering front.

**AC:** Yeah, same, [fractional.art](http://fractional.art) hiring a lot of people.

**MD:** Scott, do you want to throw your pitch in there?

**SG:** We're also hiring a really cool team coming from Web2 and also Web3. So, yeah, send your resumes.

**MD:** Yeah, so if you want to work in the NFT space, all three of these teams are hiring. And then there's a lot of great job boards as well, I think, related to NFTs, and great resources. Again, we'll share those on the programme page. Let's talk a little bit about NFT standards. I think one thing we've skirted around but haven't really talked about explicitly, is a question from Sean, is thoughts around the evolution of NFT standards. I think a lot of these financial primitives we're talking about are standards, sort of, in their own right. But what are emerging NFT standards that you see coming? And then Nick, especially since you talked about moving away from the language of NFTs as a category, when it's really a standard, and starting to get more nuanced language around NFTs, what are the things you see being built or being worked on around standards in the NFT space?

**NE:** Sure. Well I think just to give some context right now, there are two primary standards: the 721 [ERC721], which we've talked about primarily, but there's also 1155 [ERC1155], which creates this middle ground between NFTs and fungible assets. In an 1155 standard you can represent an arbitrary number of NFTs, but they also come with a balance or a supply. And so now, these are often seen in gaming right now, but they have a bunch of applications across different financial primitives as well, in that you can represent things that have a supply that's greater than one; so, semi-unique assets. I think as we start to bridge into the world of more analogue financial assets, we'll see standards start to emerge that account for things that relate to regulation, or the legal side of interacting with types of highly-regulated assets in different domiciles or jurisdictions.

Yeah, I think we'll see these sort of soft standards be built on top of NFTs as they relate to the various kinds of verticals that NFTs will start to bridge into. There are going to be specific standards, and there has been some standard exploration as things get into real estate; as things get into insurance. But I think we're still in the early days of what standards are going to look like there, and things are still being worked out as far as specifics are concerned.

**AC:** Yeah, I'll piggyback off of that and say, I think what we'll see generally is, we have this really, really high-level standard of what a non-fungible token is, and we're going to see people start to drill down into standards for different verticals of like, hey, these are the explicit things that a house on the blockchain that is an NFT, these are the particular functions that it should have and the things that it should do. And then that will be very different than what a house in the metaverse looks like, because it has different requirements and different regulatory requirements and all this stuff. So I think we'll start to see these different tracks of standards for different things, and probably a lot of companies and projects that look very similar, but are working in different areas and niches of the metaverse, and of NFTs, all focusing on different verticals.

**SG:** Yeah. I said I'm a bit concerned about NFT standards given that there's not a lot of people working on them; there's no working groups or anything, and that scares me. There's a lot of progress in terms of applications using 721 and 1155. And there's a lot of different verticals of NFTs coming. But I feel like we're not even prepared for the fundamentals of NFT standards, especially if we look cross-chain and then being able to index all these different NFTs, and their different standards, it's going to be a mess.

One EIP that I'm looking forward to is 4400 [ERC4400], which allows you to assign utility to an NFT. For example, if you want your friends to use an NFT rather than just renting it, you would just assign their address to use it. And these are standards that should be in development but are just in the backlog, and haven't been worked on for years.

**MD:** Yeah.

**AC:** I also like that standard.

**SG:** Yeah, that's a good one.

**MD:** Yeah, I think on the standard side, we've tried to convene some people to talk about NFT standards. One I've been really interested in is non-transferable NFTs and making them, credentialling especially, compatible cross-chain, especially best practices on what not to issue as an NFT, a non-transferable NFT. But I do think indexing data, every blockchain has such different metadata associated with the NFT, especially Solana, which has become more and more popular. It's very difficult to index Solana data. Reading a Solana block, the explorer is like a Herculean task. I have no idea how to make sense of anything, so it's going to be interesting to see how that world starts to become more standardised, especially as we see people trying to move NFTs cross-chain.

Let's see. Is there an existing NFT standard website? That's a question Pock asked in private DM. Is there any place people can go to learn about NFT standards? I haven't really thought about that, but it's a good question.

**AC:** Yeah, there actually is. I just wanted to make sure I knew the website. I'll post it in the chat. It's nftstandards.wtf.

**MD:** Scott already posted it, Andy.

**AC:** I'm too slow.

**MD:** He outran you.

**SG:** Yeah, and that is the person to go to about NFT standards. But she doesn't have a large group of people behind her.

**MD:** Oh, amazing. OK, so that's a cool idea for a project for people who are in the course if you want to spend time on that. OK. Dynamic, Sean has a question around dynamic NFTs. I guess this is NFTs that sort of evolve over time, things like generative NFTs. What's possible there? Do you guys have any thoughts on generative or continuously evolving NFTs?

**SG:** Yeah, I think non-fungible assets constantly evolve. Whether it's identities like your passport photo, it's not the same when you're 10 or when you're 50 years old; also real estate, if there's renovations you have built in, you need to be able to show that in the metadata. So dynamic NFTs are the future and we'll need to be able to index those.

**NE:** Yeah. Oh, sorry. Go ahead, Andy. Alright, I guess I'll just jump in real quick. Yeah, I think dynamic NFTs is a way to represent reputation as well. I think reputation is going to be a much larger part of how different primitives are built in the crypto space, and dynamic NFTs become this low-hanging fruit, or this feasible way to tokenise reputation and how it evolves over time.

**AC:** Yeah, so I have a different type of dynamic entity that I'm more interested in personally, and what I really think is super interesting is on-chain metadata NFTs, which is essentially for when, instead of storing the metadata for the NFT on Arweave or IPFS or something, you store it all on the native blockchain that it is a part of. What's really interesting here is you can have the metadata update over time based on characteristics of the blockchain itself, whether that's different interactions you've taken in a game that you're playing, or ways you've interacted with the protocol. I think that stuff is really interesting where you can have this – the metadata also be this way to display the history of an NFT, or its transactions, or its current state – not based on external input to the system saying, hey, this is updated, but just based on reading and understanding what's happened over the last, however many blocks, or something like that.

**MD:** Thanks guys. We'll do one more question. Minjay has asked this question twice, so let's talk about it. They said NFT off-chain metadata is stored in IPFS via pinning services like Pinata, if the Pinata server goes down, isn't that the same as a centralised server in terms of security? How do NFT companies think about storing and backing up their metadata safely? Thoughts on some of the infrastructure-related issues; and I think this isn't just limited to file storage. We also see this with data, like when The Graph goes down, and indexing data is difficult to pull. We also see it when the layer-1 chain goes down. We've definitely had some layer-1 issues with consistency and service levels. So, what are some of the considerations from a security perspective when it comes to the relative immaturity of some of the underlying infrastructure here, and some of the intermittent nature of accessibility of some of these chains?

**AC:** Yeah, so that kind of goes back to, that's another reason the on-chain metadata is cool, because it can't go anywhere. I think as far as IPFS in particular, yes, the pinning service could go down – I mean, generally they're pretty robust – but also anyone, the benefit that it has there still is, anyone can pin a particular metadata; set of metadata. And so if you have an NFT that you own and you really, really don't trust Pinata or something, you are not solely reliant on them. You could also host that server yourself. You could pay your friend to also pin that data. You're not just stuck relying on them. We're also seeing some interesting blockchains that are working on stuff like this. Arweave and Filecoin are two of the big ones in the adding pinning metadata, whether it's to IPFS or to their own native chain, as a core functionality of what they're doing. That's a space that I'm not super... I don't have a crazy depth of depth of knowledge in, but it's pretty interesting.

**MD:** Thanks Andy. Cool, well, we're about at the end of time, so thanks to everyone for joining today. I hope you found this to be informative, insightful. NFTs are a continuously evolving space. When we first put the course curriculum together last summer, NFTs were a teeny tiny market, no one was really talking about NFTs, and here we are nine months later, NFTs are a massive market and it seems like all we can talk about is NFTs. So I'm really grateful to Nick, Andy, and Scott for joining us this morning.

# 1.8 Case Study: Venezuela's National Cryptocurrency – The Petro - Can a State-Backed Crypto Succeed on Crypto Terms?

## 1.8 Case Study: Venezuela's National Cryptocurrency – The Petro

### Overview

In February 2018, the Venezuelan government, led by President Nicolás Maduro, launched its national cryptocurrency: the petromoneda (petro). At the time, Venezuela was mired in political and economic upheaval. The collapse of its mismanaged oil industry, coupled with falling oil prices in 2014, led the government to frantically print money, paving the way for runaway hyperinflation, severe food shortages, and crumbling infrastructure (BBC, 2020).

### Introducing Venezuela's National Cryptocurrency: The Petro

The petro (symbol: PTR) was intended to act as an alternative medium of exchange to the country's currencies—first the bolívar fuerte (strong bolívar) and later its replacement, the bolívar soberano (sovereign bolívar)—after both had seen their value decimated in the face of hyperinflation.

Ahead of the petro's launch, the Venezuelan government painted a brilliant picture: As the world's first sovereign cryptocurrency, the petro would combat the crippling hyperinflation that Venezuelans had endured for more than a decade and lead to the country's monetary sovereignty. The crypto was to be backed by Venezuela's oil and gas reserves, pegging the petro to a valued commodity. Importantly, the petro would not only raise capital from foreign investors to overcome US and EU sanctions but also function as a payment platform to circumvent the international financial system that enforced the sanctions.

But could the petro, backed by the Maduro government, gain enough traction to pull the Venezuelan economy out of its tailspin and, as the original white paper stated, act as an "instrument for Venezuela's economic stability and financial independence" (Gobierno Bolivariano de Venezuela, 2018)?

### Crypto Versus Superman

For the launch of the petro, a total of 100 million tokens were to be issued, each valued at around US \$60, pegged to the price of a barrel of oil. The public was invited to register to purchase petros with Russian rubles or cryptocurrencies, such as Bitcoin. On the first day of the pre-sale, President Maduro declared in a televised address, "Today, a cryptocurrency is being born that can take on Superman" (Reuters Staff, 2018). Maduro claimed—but presented no evidence—that US \$735 million was raised on the first day from more than 87,000 investors in 127 countries, including

Russia, Mexico, and China (2018).

Chaos surrounded the petro's launch, as problems abounded on the pre-sale website, and scammers launched fraudulent websites to take advantage of the confusion. Further, although the petro was meant to shore up the bolívar fuerte (and vice versa), the bolívar fuerte declined so precipitously over the next six months that the government knocked five zeros off the currency and introduced the bolívar soberano in August 2018. The Venezuelan government promoted the bolívar soberano as being pegged to the petro in an effort to raise the value of the nation's fiat currency (Robinson, 2018). However, bolívar soberanos continued their free-fall; while US \$1 was worth 40,000 bolívares in late 2019, that same dollar was worth around four million bolívares by September 2021 (YCharts, n.d.).

## A State-Backed Experiment

As the value of the bolívar has deteriorated, the Venezuelan petro has languished both as an investment for foreigners and as a spending mechanism for the nation's citizens. While the government has made the use of petros mandatory in certain instances—the payment of state pensions and paying for new passports and renewals, for example—experts believe that the few people using the petro are most likely “[...] close to the Maduro regime or otherwise able to take advantage of Venezuela's corruption to make money” (Chainalysis Team, 2020). One reason for this claim is the fact that the petro is frequently traded on Criptolago, the Venezuelan cryptocurrency exchange led by a staunch ally of Maduro, and “most Venezuelans would want to avoid a platform that could be monitored by [a] government” that “is infamous. . . for retroactively declaring certain activities illegal and prosecuting those who have taken them” (Chainalysis Team, 2020). Moreover, 75% of the transfers on the platform averaged around US \$1000—over a thousand times higher than the average citizen's daily wage of US \$0.72. The young creator of the petro, Gabriel Jiménez, noted that “the petro is being misused as a political weapon by the government” and expressed regret over his involvement (Erazo, 2021).

Meanwhile, every day, Venezuelans have turned to alternative cryptocurrencies, including Bitcoin, Ether, and other highly traded coins, to conduct daily commerce and avoid hyperinflation rates that by 2019 had surged to 10,000,000% (Sanchez, 2019). Venezuela ranks third in the world for cryptocurrency use on LocalBitcoin, the preferred peer-to-peer (P2P) exchange mechanism for Venezuelans, as citizens accept payments from abroad and invest to protect their savings (Chainalysis Team, 2020). Scaled for the number of internet users and purchasing power parity per capita, the country ranks second. Venezuelans who have fled the country also use cryptocurrency to send funds back home, as family members cannot rely on bank accounts or bolívares. They have also turned to the use of the US dollar, with Maduro himself proclaiming, “This process which they call dollarisation can be useful for the recovery and for unleashing the country's productive forces and for the functioning of the economy. It is an escape valve. Thank God it exists” (Long, 2019).

As an experiment in creating a cryptocurrency that is able to contain hyperinflation and evade US sanctions, the petro has largely failed. Critics have pointed to the irony of its state-backed nature, especially as one of the regularly stated appeals of Bitcoin is that no single entity controls it and that the entire system is transparent, open, and instils trustless confidence in its users. As economist Eswar S. Prasad noted, “Like any other currency, [the petro] is only as strong and trusted as the government that stands behind it” (Prasad, 2021, p. 262). In October 2021, Venezuela, in a fresh bid to combat inflation, launched a new currency: the digital bolívar. In the process, the government cut off

six zeros from the existing currency and introduced new paper notes into circulation. As of May 2022, the digital component has not yet been launched.

## Guest Video: The Challenges of the Petro

In this video, guest speaker Federico Spagnoli, Regional President of Prudential Financial and Emerging Markets, pinpoints why Venezuela's cryptocurrency, the petro, has struggled to gain traction.



Another example that we notice of trying to use cryptocurrency as part of the legal currency in Venezuela, which in a way has a number of similarities when compared to El Salvador, lack of a strong local currency, a shrinking GDP, millions of Venezuelans leaving the country because of a populist political system. But was the same populist government that was actually trying to propose this idea of petro which was more like a stable cryptocurrency. They didn't choose one of the most popular cryptocurrencies like Bitcoins.

So the challenge with petro was twofold. Number 1 was back to the oil reserves that Venezuela has, and as we all know that those numbers can be manipulated, especially when you are dealing with a government with very poor reputation in global markets. So that was why they are a problem. Then they had another challenge, which was the lack of infrastructure to actually allow most citizens to get access to that type of cryptocurrencies.

What is interesting is that Venezuela is ranked as one of the top countries when it comes to use of cryptocurrencies. Why? Because of the conditions that I mentioned before. Local citizen they don't trust in the bolivar, the local currency, and they had much more trust in cryptocurrency that can be traded digitally.

We are seeing similar examples in Africa where a country like Nigeria, cryptocurrencies are getting really, really popular and they are ranked at the top. If you look at the top 10 countries of high use of cryptocurrencies, most of them are actually emerging economies with very weak local currencies. So clearly, we are seeing the value that cryptocurrencies are adding to these emerging economies.

## Programme Director Video: The Caribbean Sand Dollar

In this video, Meltem Demirors explains another important use case to understand: the Caribbean Sand Dollar.



The second use case I want to talk about is a slightly different one, and this is the use case of the Caribbean Sand Dollar. Now, the Caribbean is a region that is made up of a variety of different countries and territories that are all operating their own economies, and to some degree use the dollar as their primary currency, even though some of these nations and territories may have their own local currencies.

Because these island states, all have a lot of economic interconnectivity, they pioneered a new project called the Sand Dollar, which was an attempt to create regional currency that would allow these island states to transact with one another and to begin utilizing a common currency for

commerce within the region.

This would also allow the Caribbean region to keep more of the wealth created through tourism, through exports and other activities within the region instead of putting it into the US dollar. And so the Sand Dollar is a great example of a way that smaller nations can come together to use this technology to create shared money technology, that allows them to have one fabric for money movement in the region, to make it really simple from a technology perspective to integrate with that money as a protocol, and to allow entrepreneurs and innovators in the region to build on top of that money protocol as a type of technology.

So this is an interesting example and one I think we'll see much more of the future, where nation states can work together to implement their own regional standards for how money might operate in their own region.

Now, what I really want to highlight with these two use cases is a really important element to grasp in this course. The separation of money and state is something that has not been effectively implemented since the advent of Bitcoin. But in my belief, it is one of the most exciting experiments in our lifetime.

The separation of money in state allows us for the first time to create global communities that transcend the physical borders of a nation state. No longer does it matter what stamp is in your passport or what color its pages are, anyone anywhere has the choice to participate in the Bitcoin network.

There are no gatekeepers, there are no officials, there are no authorities, there is only code an open source online community and the ability for anyone anywhere with an internet connection to run this code and participate in the Bitcoin network. And that is a truly democratizing and exciting aspect of where the future of money is going.

## Case Analysis

Having read this case, consider the following questions:

- Was Venezuela's implementation of its petro cryptocurrency successful? What was the primary reason for its success or failure?
- What steps should a country consider to launch its own cryptocurrency?
- Besides bitcoin, what other use cases are achieving, or close to achieving, the separation of money and state?

## References

To deliver the highest quality content, we collate information from many leading sources. We include references to attribute works to their original authors. Some of the sources are freely available, and some are not. Access to referenced articles may require a purchase.

The following sources were last accessed on 15 March, 2022.

BBC. (2021, 12 August). Venezuela crisis: How the political situation escalated. <https://www.bbc.com/news/world-latin-america-36319877>

Chainalysis Team. (2020, 27 August). Hyperinflation and Sanctions Evasion: What On-chain Data Tells Us About Venezuelans' Trust in Cryptocurrency. *Chainalysis*. <https://blog.chainalysis.com/reports/venezuela-cryptocurrency-market-2020>

Erazo, F. (2021, 29 April). Venezuelan Programmer who Created the Petro Token Regrets Participating in the Project – Works on an Alternative Token. *Bitcoin.com*. <https://news.bitcoin.com/venezuelan-programmer-who-created-the-petro-token-regrets-participating-in-the-project-works-on-an-alternative-token>.

Gobierno Bolivariano de Venezuela. (2018). Petro [White paper]. <https://www.allcryptowhitepapers.com/wp-content/uploads/2018/05/Petro-PetroDollar-XPD-whitepaper.pdf>

McSweeney, M. (2020, 20 November). Crypto firms work with Venezuela's government-in-exile to disburse funds to health care workers. *The Block*. <https://www.theblockcrypto.com/linked/85319/crypto-firms-venezuela-guaido-coronavirus>

Millard, P., Hoffman, C., Gertz, M., & Lin, J.C.F. (2019, 16 February). A Timeline of Venezuela's Economic Rise and Fall. *Bloomberg*. <https://www.bloomberg.com/graphics/2019-venezuela-key-events>

Robinson, T. (2018, 31 August). The Venezuelan Petro: Sanctions, Scams and Smokescreens. *Elliptic*. <https://www.elliptic.co/blog/venezuelan-petro-sanctions-scams-smokescreens>

Sanchez, V. (2019, 3 August). Venezuela hyperinflation hits 10 million percent. 'Shock therapy' may be only chance to undo the economic damage. *CNBC*. <https://www.cnbc.com/2019/08/02/venezuela-inflation-at-10-million-percent-its-time-for-shock-therapy.html>

Team Circle. (2020, November 20). Circle Partners with Bolivarian Republic of Venezuela and Airtm to Deliver Aid to Venezuelans Using USDC. *Circle*. <https://www.circle.com/blog/circle-partners-with-bolivarian-republic-of-venezuela-and-airtm-to-deliver-aid-to-venezuelans-using-usdc>

YCharts. (n.d.). US Dollar to Venezuelan Bolivar Exchange Rate. [https://ycharts.com/indicators/us\\_dollar\\_to\\_venezuelan\\_bolivar\\_exchange\\_rate](https://ycharts.com/indicators/us_dollar_to_venezuelan_bolivar_exchange_rate)



Module 2:

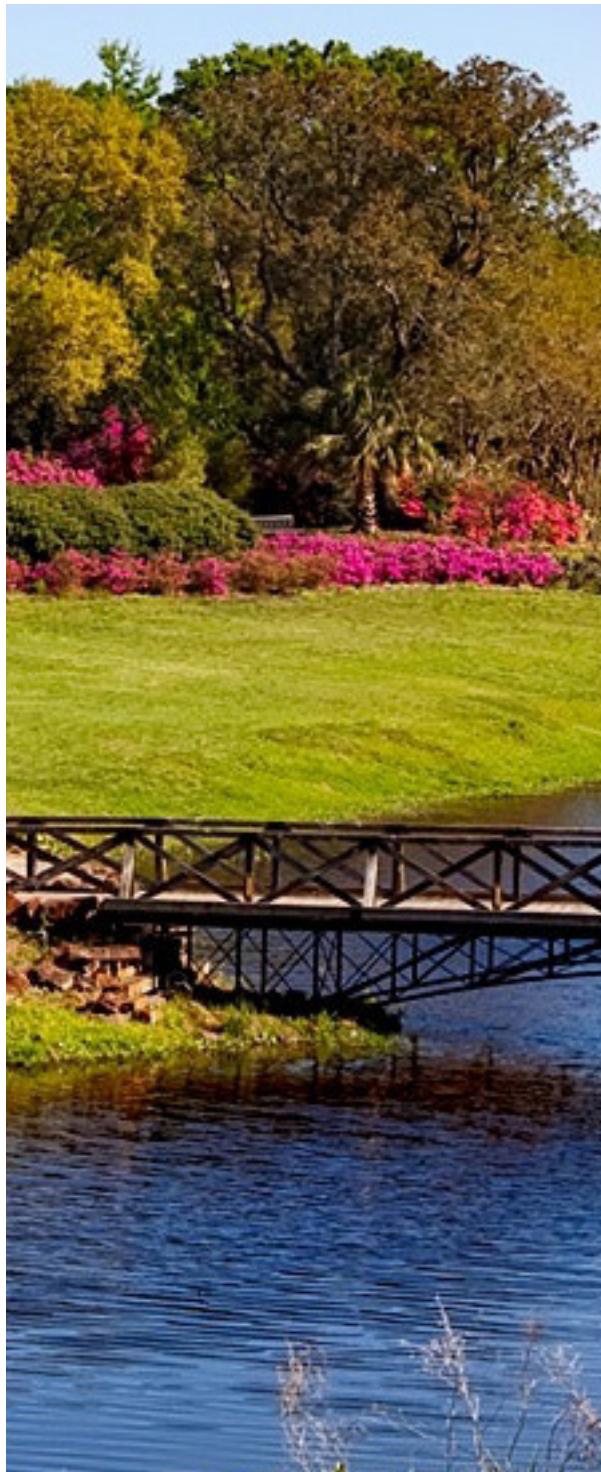
# Opportunity: Use Cases Across Industries

---

Oxford Blockchain Strategy Programme  
2022

# Oxford Blockchain Strategy Programme

## Module 2: Opportunity: Use Cases Across Industries



### Table Of Contents

<b>2.1 About Module 2</b>	<b>3</b>
2.1.1 Overview of Module 2	3
<b>2.2 Digital Scarcity</b>	<b>6</b>
2.2.1 Overview	6
2.2.2 Use Case 1: Bitcoin and Ethereum as Verifiably Scarce Assets	8
2.2.3 Use Case 2: Digital Scarcity Across Metaverses (Gaming and Art)	8
2.2.4 Key Takeaways and References	13
<b>2.3 Payment Rails</b>	<b>17</b>
2.3.1 Introduction to Payment Rails	17
2.3.2 Payment Rail Architecture	18
2.3.3 The Differences Between Payment Rail Layers	19
2.3.4 Problems with Traditional Payment Rails	21
2.3.5 Blockchain Payment Rails	22
2.3.6 Use Case 1: Placing Fiat Currencies on Public Blockchains (USDC and Tether)	24
2.3.7 Use Case 2: Placing Fiat Currencies on Private Blockchains (CBDCs)	26
2.3.8 Use Case 3: cLabs, Decentralised Cross Border Mobile Payments, and Stablecoin Issuance	30
2.3.9 Key Takeaways, References, and Further Exploration	32
<b>2.4 Distributed Ledgers</b>	<b>37</b>
2.4.1 Distributed Ledgers	37
2.4.2 Distributed Ledger for Diamond Authentication	38
2.4.3 Distributed Ledger for Verifying Collateral	40
2.4.4 Distributed Ledger for Indexing the World's Blockchain Data	44
2.4.5 Tokenisation Distributed Ledger	46
2.4.6 Key Takeaways, References, and Additional Resources	49
<b>2.5 What Makes a Use Case Successful?</b>	<b>53</b>
2.5.1 Introduction	53
2.5.2 Ease of Use	56
2.5.3 Interoperability	58
2.5.4 Shared Governance	60
2.5.5 Network Effects	68
2.5.6 Key Takeaways, References, Additional Resources	70
<b>2.6 Determining Suitability for a Use Case</b>	<b>74</b>
2.6.1 Overview	74
2.6.2 Framework for Assessing a Company's Need for a Blockchain-Based Solution	76
2.6.3 Six Questions	77
2.6.4 Key Takeaways, References, Additional Resources	78

# 2.1 About Module 2

## 2.1.1 Overview of Module 2

### Overview

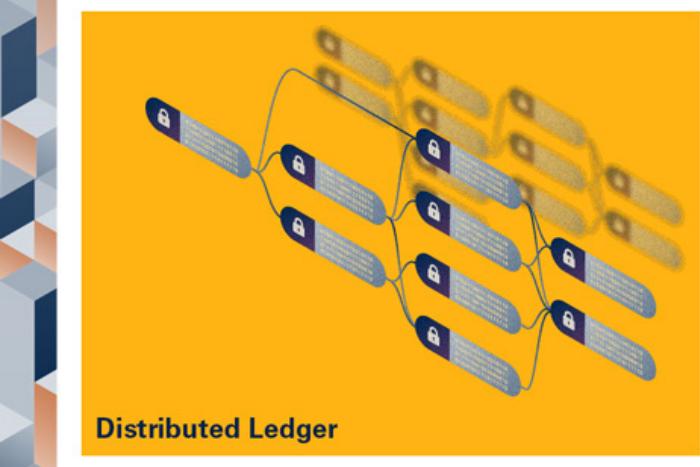
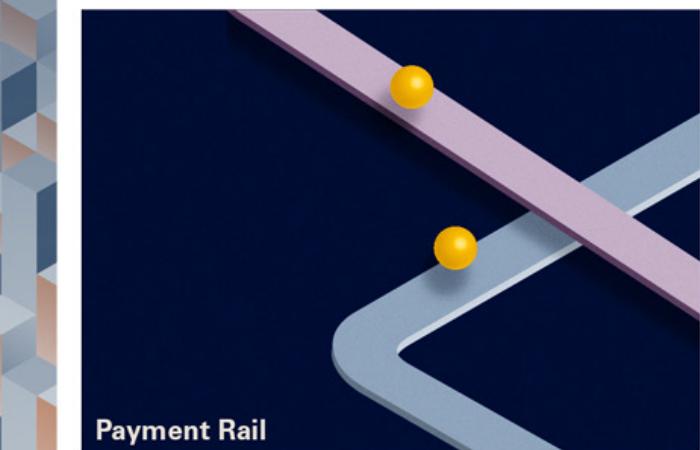
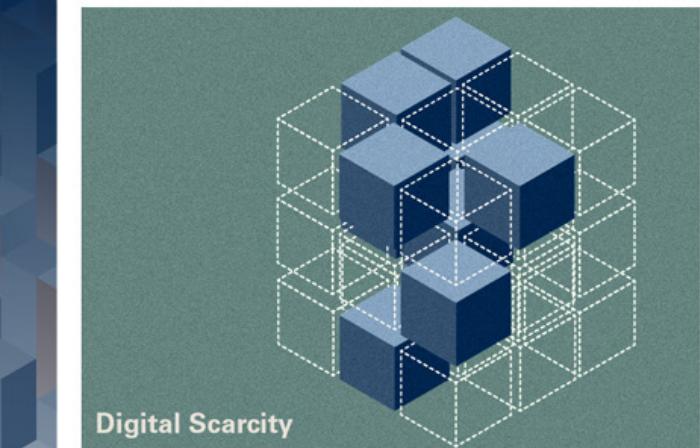
Welcome to Module 2 of the Blockchain Strategy Programme!

The influx of creative developers, entrepreneurs, and investors in the blockchain ecosystem has led to the rapid growth of new applications for blockchain technology. In Module 2, we will dive deeper into applications for blockchain technology in a variety of industries and learn how companies are blending new and traditional business models to monetise their blockchain solutions.

We will examine three major areas of blockchain use:

- **Digital scarcity:** Programming digital assets to have a fixed or variable supply, which enables consumers of those assets to ascribe value to them.
- **Payment rail:** Making payments and transferring money across borders in ways that are faster, cheaper and more transparent.
- **Distributed ledger:** Determining the origin, ownership, methods of production, transportation, and storage of tokenised physical assets or digitally native assets and making these details verifiable by all stakeholders involved.

### Three Major Areas of Blockchain Use



## Learning Outcomes

By the end of this module, you will be able to:

- Recognise the types of use cases blockchain technology enables.
- Describe the three main ways in which organisations are using blockchain technology: to create digital scarcity, as a payment rail, or, as a distributed ledger.
- Compare different business models of blockchain use cases.
- Evaluate whether a use case is suitable for a blockchain.

## Vocabulary

In each section, you will learn several new terms that are associated with blockchain technology. Develop a strategy to easily access the terms and their meanings as you move through this programme, employing memorisation techniques so that the terms become second nature to you.

## Graded Assignments

You will complete individual and group assignments, which count towards your completion of the programme. This week, you will:

- Meet with your group to determine a single use case the group will explore throughout the rest of the programme.
- Complete a quiz on the module's content and key takeaways.
- Reflect on what you have learnt by applying it to your personal or professional experiences.

You must submit all graded assignments in Module 2 by **21 June 2022, 23:59 UTC**. (Try the [Time Zone Converter](#) to get your local time.)

## Additional Activities

In each module, we present additional activities related to the core learning. This week, you will:

- Share with the class your favorite application of blockchain technology, and describe how the organisation is using blockchain technology.

## Time Commitment

Plan to spend seven to ten hours on Module 2 this week. As there is a lot of reading material and video content, you might want to divide your work into several sessions. The module is broken up into sections by theme, giving you potential breakpoints.

Make sure you plan time to meet with your group, and to complete the assignments.

## 2.2 Digital Scarcity

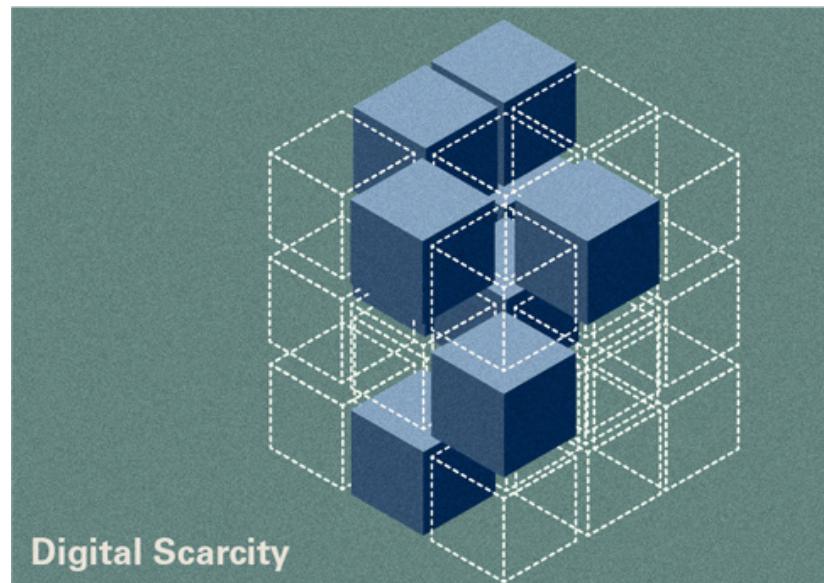
### 2.2.1 Overview

#### Overview

In this section, we explore how blockchain technology can be used to create scarcity amongst digital assets.

As we learned in Module 1, when there is no physical token corresponding to entries in a digital ledger, there is a risk of double spending.

Blockchains solve the double-spend problem by providing a distributed ledger in which multiple parties must perform a set of difficult computations under a PoW or PoS consensus mechanism in order to come to an agreement on the current state of the ledger (that is, who sent how much to whom, and how much exists in each person's wallet after each transaction).



In solving the double-spend problem, blockchains offer a method for attaining scarcity in a digital environment, thereby enabling digital assets to be perceivably valuable in the same way that physical assets have historically been valued based on physically imposed limitations.

**Note:** The double-spend problem has also been solved through a centralised clearing counterparty, in which a central and trusted third party verifies transactions (CFI, n.d.).

Value, according to Oxford Learner's Dictionary, is "how much something is worth in money or other goods for which it can be exchanged" (n.d.).

#### Verifying Scarcity

The price of an asset is a function of its scarcity relative to its demand. In other words, price depends on how much of the asset exists relative to how many people want to acquire it.

The degree to which an in-demand asset can maintain its scarcity is also the degree to which it can maintain its price. The current supply of an asset and the resources companies require to source it over time determines its scarcity.

Blockchain technology can be an effective solution for verifying the scarcity of assets that exist in a digital environment. Blockchains can enable users to view an immutable and transparent ledger that relies on programmable consensus (that is, consensus mechanisms) to verify the quantity and ownership status of tokens, and the process (that is, resource requirements) for altering its supply over time. In a digital world, the scarcity of cryptocurrencies is programmatically established from inception and reinforced through consensus mechanisms that confirm the amount of resources (or “work”) necessary to produce more of the asset.

## Vocabulary Check

This section introduces the following terms:

- [censorship-resistance](#)
- [digital asset](#)
- [digitally native asset](#)
- [ERC-20 token standard](#)
- [ERC-721 token standard](#)
- [fiat currency](#)
- [halving](#)
- [hashrate](#)
- [meatspace](#)
- [metaverse](#)
- [mining](#)
- [non-fungible token \(NFT\)](#)
- [permissionless blockchain platform](#)
- [post-scarcity](#)
- [programmable consensus](#)
- [scarcity](#)

## **2.2.2 Use Case 1: Bitcoin and Ethereum as Verifiably Scarce Assets**

### **Quick Fact**

There are approximately 18.8 million bitcoin in circulation today, out of a total of 21 million allowed in the system. Every 10 minutes, the system rewards miners who validate transactions with 6.25 new bitcoin. The 6.25 newly mined bitcoins join the circulating supply. Every four years, an event known as “the halving” occurs, and the bitcoin rewards decrease by half. In 2012, the reward was 25 BTC; in 2016, it was 12.5 BTC; in 2020, it was 6.25 BTC, and in 2024 it will be 3.125 BTC (CMC Markets, n.d.).

### **Use Case 1: Bitcoin and Ethereum as Verifiably Scarce Assets**

Due to the halving rates and the speed at which miners currently source bitcoin, the entire 21 million units will not be in circulation until 2140. For bitcoin, the consensus amongst a decentralised group of miners is vital for verifying the true scarcity of the network’s native asset.

Unlike bitcoin with its 21 million fixed supply, Ether has no explicit supply cap. The Ethereum blockchain rewards miners with approximately 13,000 new Ether each day, which equates to an annual growth rate of 3.77% per year (ICRYPEX, n.d.). Due to recent updates made to the Ethereum network under the Ethereum Improvement Proposal 1559 (or EIP-1559), this growth rate will decrease each year through the burning of excess supply earned through miner fees (Cryptopedia, 2021).

Bitcoin and Ether are both digitally scarce assets created on a blockchain and programmed to have a limited or controlled supply.

## **2.2.3 Use Case 2: Digital Scarcity Across Metaverses (Gaming and Art)**

### **Use Case 2: Digital Scarcity Across Metaverses (Gaming and Art)**

The metaverse describes a virtual and expansive universe built on augmented reality, virtual reality, and internet infrastructure. It is predicted that there will be 3.07 billion active video gamers by 2030, based on a 5.6% growth rate per year (Newzoo, 2020).

Consider popular video games such as the Sims, World of Warcraft, and Fortnite—what comes to mind? Is it that each features a virtual world with the ability to shape environments and create custom characters? In these gaming ecosystems, developers structure markets and economies to work around the creation and consumption of digital assets. The needs of individuals—who depend on these digital assets to achieve specific milestones or shape the environment to suit their desire within a game—determine the “value” of the in-game assets.

Blockchain technology enables tokens, digital art, and gaming accessories to be programmed to have a fixed supply just as bitcoin does. Once a program is deployed with specifications around the supply and issuance rate of a digital asset, these rules become immutable and therefore almost impossible to overturn.

Consensus mechanisms such as PoW and PoS are used to facilitate the issuance of new digital assets while rewarding miners for correctly validating transactions and keeping the network secure.

Attempting to alter the supply of NFTs or tokens after the transaction has been confirmed would require reversing the transaction which could be done only via a successful 51% attack, where the expenses involved would likely be higher than the potential reward. This constraint is what keeps the scarcity of digital assets intact.

## Guest Video: NFTs and the Art Market

Digitally native assets are alternative forms of expression that most popularly come in NFTs.

In this guest speaker video, Christophe Spaenjers, an Associate Professor of Finance at HEC Paris, explains what NFTs are and how they relate to the art market.



So what is an NFT? An NFT is a non-fungible token, or NFT stands for non-fungible token. You can think of it as an electronic identifier that links to a digital object or links to the metadata associated with a digital object. And a digital object, in the context of today's discussion, we can think about a digital artwork, right? So the token—you can think of it as a certificate that links to a digital object.

And so the digital—or these certificates which link to these digital objects—they can be traded themselves. Their transactions and their ownership are recorded on the blockchain, which you can think of as an electronic ledger, as a secure electronic ledger. So the NFTs can then be bought and sold just like you can buy and sell other types of assets. Now, what makes NFTs different from other artworks is that if you own an NFT, it's not so clear that you really own the underlying artwork. All you can say is that you own a link to or a certificate that relates to a digital artwork, right?

So what are you really owning? You're owning a certificate. And that gives you bragging rights maybe or a sense of patronage in the sense that you may think that you're supporting an artist. And you, of course, you have the ability to resell the token. But it's different from ownership in the traditional way or any meaningful way, right? You're not really owning the artwork, because the artwork will still be enjoyed and downloaded by thousands or millions of other people on the web. The artwork doesn't disappear from other places on the internet just because you've bought the NFT.

## Non-Fungible Tokens (NFTs)

Unlike the ERC-20 token standard, which creators use to produce indistinguishable tokens to trade for other tokens, the ERC-721 token standard allows creators to issue tokens that each have a unique identifier code. Whenever an NFT is “minted” (meaning a new ERC-721 token is created), it is the only token on that blockchain that has its code and can be distinguished from all other NFTs and ERC-721s on the network, hence the term “non-fungible”.

Creators of NFTs can use them to represent digital artwork, music files, collectables or tickets as “one of a kind” items on a blockchain. Through the same methods of programmable consensus that

a blockchain system relies on to verify the quantity of an item, an NFT issuer can prove that only a certain number of a particular item exists. For example, a buyer who wishes to purchase what an artist claims is a limited edition piece of digital art can verify this claim by looking on the blockchain and seeing how many NFTs have been minted to represent each piece of art.

Creators can also tie NFTs to physical world assets like a piece of property or a company. However, in these cases, the issuer (an individual, company or organisation) is not able to create any new value. Instead, it simply represents the transference of value from the physical world to the blockchain, which makes the tokenisation of physical assets a distributed ledger use case.

## Value of Digitally Scarce Assets

Cryptocurrencies, tokens and NFTs are units of fixed or variable data points represented on a distributed and immutable ledger. Those who elect to be part of a cryptocurrency community ascribe values to these digital assets.

It is important to distinguish between the utility of blockchain technology in verifying scarcity amongst digital assets and the purpose or perceived value of those assets. The rise of digitally native assets formed on blockchains has reignited the debate around what it means for something to have value. The subjective theory of value, which Carl Menger, the founder of the Austrian School of Economics, developed alongside other economists and thinkers, argues that “the value of an object is not fixed by the number of resources and the hours of labour that went into creating it but is variable according to its context and the perspective of its users” (Menger, as quoted in Kagan, 2021). In essence, the price of a product is determined by how scarce and useful it is to the buyer or seller.

With the help of blockchain technology, people can now verify the supply of digital assets that they perceive as valuable and connect with like-minded individuals and communities, however niche, who share the same sense of value.

## Guest Video: The State of Crypto Adoption in Africa

In this video, Nelly Chatue-Diop, the Co-Founder & CEO of Ejara, a fintech company that allows people in Africa to invest in cryptocurrencies, explains how some people in Africa hedge against inflation by using stablecoins and adopting cryptocurrency.



I would think that when it comes to—in West Africa, in general, you have to differentiate between the countries, like Nigeria or Ghana, that have a high volatility currency, like a high inflationary currency. Like in Nigeria, it's almost 13% per year. In Ghana, it's 10% per year. So it has been eating up the savings of people.

And people have started to realise that, hey, I mean, I shouldn't hold that kind of cash anymore. I should invest into stablecoins. And I have many friends in those countries that whenever they receive their salaries or their income, they convert it into stablecoins. And then they spend it along as they need to buy a computer, to pay for rent, to buy food. When it comes to francophone zone, our

currency, the CFA franc, is backed to euro. So it's kind of stable.

But you have to remember that 20 years, 25 years ago, there is a devaluation. Actually, it was 1994 that happened, where the value of the money dwindled by half overnight. So people still remember that, and they still are in need to control their own wealth. They still want to protect it. And also, because of capital controls, having access to all those things they see on Amazon, to pay for Netflix, to pay for all the things they want to get access to, and even to buy some investment product, it's still a hurdle.

That's why people are starting to adopt crypto, because imagine, a young developer in West Africa that wants to receive his payments from a company in Silicon Valley or in France. Receiving it in crypto is way easier than even thinking of opening a bank account with all the fees involved with the 40 intermediaries banks that can do the transfer with high fees, right?

And people that are doing e-commerce also in Africa, they see that they can receive those payments in crypto. And then they can also buy goods in Bitcoin whenever they want, instead of trying to figure out how to get access to renminbi when they want to buy in China or to lira when they want to buy in Turkey. So that's why I think that crypto and stablecoins are here to stay and that Africa will be the battleground for mainstream adoption.

So usually, when people have, I will say, a lot of savings, they buy some lands. They buy real estate. But they also buy some cattles. You know, that's what we are up against. And I definitely think that investing in Bitcoin or in stablecoin is maybe a little bit easier

to under than when you want to travel, to bring all your cattle with you. So this is kind of the thing. And also, obviously, some goals. Yes, people are diversifying into commodities they can think of. And cattle has been one thing I've seen across Cameroon, Nigeria, Senegal, and the likes.

And it's funny because when I discussing with people on the ground—I have this 70-year-old customer of Ejara. And the way he reframed what Bitcoin is, he told me, "So it's like I'm buying a land on internet, but it's a digital land, and it will appreciate in value. And then I could transfer it to my kids. Is that what it is?"

And I thought it was really, really smart to frame it that way. And that in that moment, he completely unlocked what it was and what it could mean for him, for his family, for his family protection. And he was like, wow, that is great because I can buy it with a small amount, like 10 euros, whereas to buy a land, it's kind of much more complex. And it's also illiquid.

## Guest Video: NFTs, Gaming, and Digital Art

In this next guest speaker video, Marguerite deCourcelle, the CEO of Blockade Games, Inc., explains the subjective value of NFTs—gaming and digital art—and discusses her blockchain-powered video game. Blockade Games is one of the earliest NFT gaming companies in the blockchain space. The company powers its games through the blockchain and registers in-game assets as NFTs, which users can capture and trade within a games ecosystem.



What I saw in those processes of creating these puzzle trails were that people were very excited to walk along with the opportunity to possibly win something valuable. But it wasn't guaranteed. And what we can do now with non fungible tokens is, we can capture the actual experience of the journey for a player, be it, is it a key that unlocks your access to the experience?

Then, as you move through the experience, the metadata that's attached now to the token as you progress-- all of this can be captured through apps, through the decentralised systems that we're building on top of the watching technology now today, and with the new standards of tokens.

I'm very excited about what's possible with digital media being tokenised across the board. It changes so much of what we know for even concepts like the internet and e-commerce.

So, Neon District, the way it's designed is that you have the game application, which is actually a centralised application. But all of the assets are decentralised. So as the assets interact with the application, the application pushes updates. It has permission to write to the tokens. So it pushes updates to the tokens, and then the tokens then are all verified across the network as being valid, and can be transferred and traded on the peer-to-peer marketplaces.

But the game company is the authority over the state of the tokens, essentially. And we have immutable and mutable data associated with each. What's neat about that is you can do things like have a character, which, as it levels up through the game and becomes more specialised, you can unlock features of your token.

Which is-- back in 2018 when we were doing this, you had something like a CryptoKitty. Which, based on its DNA and breeding, it became more degenerate over time, actually. That's how it was designed. Which, in my mind, was a negative experience.

So as a game designer, I want to produce an experience where you have this zero state asset that is not valuable at all. So our goal was to onboard people with as little friction as possible, give them these seemingly valueless assets. But then, once in your hands, you have the ability to make it something unique and cool through your game, your skill, and your strategy. And then how you play with your assets combined together-- similar to Magic the Gathering-- means how you're going to win in the game.

So, the goal-- the very, very large, big picture goal for this-- is how do we unlock the global economy of people around the world that do not have any money, they don't have a bank account, they don't have crypto. How do they get to onboard and participate in this new economy we've created?

And free to play gaming-- people that can create or demonstrate skill and earn value through that experience, and then be able to trade for their first crypto without having to have a bank account or any of those first pay walled experiences, is the opportunity for us to really onboard a whole new generation of creatives around the world that have never participated.

## Services and Business Models

A variety of services have emerged from the ability to create digitally scarce assets, including centralised and decentralised exchanges that enable users to trade and invest digital assets on a blockchain, platforms that enable users to borrow or lend assets, and custodial services (for example, crypto wallets) for users to securely store and transfer their assets.

Business models for these services include:

- Collecting transaction fees from the trading of digital assets
- Lending or staking assets to earn interest
- Providing custodial services (wallets)
- Generating revenue from price appreciation of underlying digital assets

An example of a company that collects transaction fees and provides custodial services is Robinhood, a company that is opening access to financial services and offers cryptocurrency trading through its app. In July 2021, Robinhood went public on the Nasdaq at a share price of US \$38. The company is also launching a cryptocurrency wallet to allow its investors to send, receive and move cryptocurrencies through their app. This new addition is being implemented because cryptocurrency makes up a large part of its revenue (Fitzgerald, 2021). The revenue from cryptocurrency trading fees reached US \$233 million in 2021, which is a 50% increase from the year before, but they also lost US \$502 million compared to a profit of US \$58 million a year before. This loss may be attributed to an emergency funding round in 2020 (Griffith, 2021).

Coinbase on the other hand is the largest cryptocurrency exchange in the US. They listed on the Nasdaq in 2021 and were the first cryptocurrency company to go public (Field, 2021). In 2021, their profits reached \$1.6 billion, a 4,900% increase from the year before (Sigalos, 2021).

### 2.2.4 Key Takeaways and References

#### Key Takeaways

Let's review the key points of this section:

1. The immutable, transparent, and secure properties of blockchain technology make it a useful tool for creating scarce digital assets.

2. Using blockchain technology, digital assets can be programmed to have an immutable and fixed supply, which can be helpful for ascribing value to non-physical assets.
3. Cryptocurrencies, tokens, NFTs all represent different forms of digitally scarce assets.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

### 2.2.1 Overview

Corporate Finance Institute. (no date). Double-Spending. <https://corporatefinanceinstitute.com/resources/knowledge/other/double-spending>

Oxford Learner's Dictionaries. (no date). value. *Oxford Learner's Dictionary*. [https://www.oxfordlearnersdictionaries.com/us/definition/english/value\\_1](https://www.oxfordlearnersdictionaries.com/us/definition/english/value_1)

### 2.2.2 Use Case 1: Bitcoin and Ethereum as Verifiably Scarce Assets

CMC Markets. (no date). Bitcoin-halving 2020: what you need to know. <https://wwwcmcmarkets.com/en/learn-cryptocurrencies/bitcoin-halving>

Cryptopedia. EIP-1559: A Proposal to Update Transaction Fees on Ethereum. <https://www.gemini.com/cryptopedia/ethereum-improvement-proposal-ETH-gas-fee>

Godbole, O. (2021, 19 July). Bitcoin Network Sees Fourth Straight Downward Difficulty Adjustment. *CoinDesk*. <https://www.coindesk.com/markets/2021/07/19/bitcoin-network-sees-fourth-straight-downward-difficulty-adjustment>

Hanke, S. (2019, 1 January). Venezuela's Hyperinflation Hits 80,000% Per Year in 2018. *Forbes*. <https://www.forbes.com/sites/stevehanke/2019/01/01/venezuelas-hyperinflation-hits-80000-per-year-in-2018/?sh=100aa6b74572>

ICRYPEX. (no date). Ethereum Additional Info. [https://www.icrypex.com/en/features/products/ethereum/details?\\_cf\\_chl\\_jschl\\_tk\\_=pmd\\_KRZXOyUf\\_RiZ3aD4pCCbCmkBJuPiLzU\\_vADKzAv9zNI-1632321695-0-gqNtZGzNAfujcnBszQiR](https://www.icrypex.com/en/features/products/ethereum/details?_cf_chl_jschl_tk_=pmd_KRZXOyUf_RiZ3aD4pCCbCmkBJuPiLzU_vADKzAv9zNI-1632321695-0-gqNtZGzNAfujcnBszQiR)

Janus, E. (2019). Venezuela Traded Over \$60M in Bitcoin Already in 2019. *Bitcoinist*. <https://bitcoinist.com/venezuela-60-million-bitcoin-2019>

Knoema. (no date). Nigeria — Purchasing power parity conversion factor for gross domestic product. <https://knoema.com/atlas/Nigeria/topics/Economy/Inflation-and-Prices/Purchasing-power-parity>

Lielacher, A. (2021, 20 June). China turns off its miners — does price follow hash rate or hash rate follow price? *Brave New Coin*. <https://bravenewcoin.com/insights/does-hash-rate-follow-price-or-does-price-follow-hash-rate>

Marq. (2020, 19 November). Bitcoin is valuable as it is the best tool to transfer value across Space and Time. *The Nifty Crypto Nomad*. <https://niftycryptonomad.com/bitcoin-is-the-best-tool-to-transfer-value-across-space-and-time>

Mozée, C. (2021, 17 February). 3 reasons why gold prices have struggled lately, according to Bank of America. *Markets Insider*. <https://markets.businessinsider.com/news/stocks/gold-price-struggling-for-3-key-reasons-bofa-2021-2>

Nakamoto, S. (2009, 11 February). Bitcoin open source implementation of P2P currency. *The Foundation for Peer to Peer Alternatives*. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>

Namcios. (2021, 24 August). Africa now has the largest volume of bitcoin peer-to-peer trading worldwide. *Bitcoin Magazine*. <https://bitcoinmagazine.com/markets/bitcoin-largest-volume-peer-to-peer-africa>

Ndukwe, I. (2021, 28 February). Cryptocurrencies: Why Nigeria is a global leader in Bitcoin trade. *British Broadcasting Corporation*. <https://www.bbc.co.uk/news/world-africa-56169917>

O'Neill, A. (2021, 18 May). Inflation rate in Nigeria 2026. *Statista*. <https://www.statista.com/statistics/383132/inflation-rate-in-nigeria>

## 2.2.3 Use Case 2: Value Across Metaverses (Digital Scarcity in Gaming and Art)

Fitzgerald, M. (2021, 3 August). Robinhood surges more than 24%, blows past \$38 IPO price. *CNBC*. <https://www.cnbc.com/2021/08/03/robinhood-surges-10percent-runs-past-38-ipo-price.html>

Fitzgerald, M. (2021, 22 September). Robinhood to launch cryptocurrency wallets as bitcoin becomes a bigger part of business. *CNBC*. <https://www.cnbc.com/2021/09/22/robinhood-to-launch-cryptocurrency-wallets-as-bitcoin-becomes-bigger-part-of-business.html>

Griffith, E. (2021, 18 August). Robinhood's revenue more than doubled even as it lost money last quarter. *The New York Times*. <https://www.nytimes.com/2021/08/18/technology/robinhood-earnings-q2-2021.html>

Kagan, J. (2021, 3 September). Subjective Theory of Value. *Investopedia*. <https://www.investopedia.com/terms/s/subjective-theory-of-value.asp>

Manoylov, M.K. (2021, 22 August). OpenSea is first NFT marketplace to pass \$1 billion in monthly trading volume. *The Block*. <https://www.theblockcrypto.com/linked/115222/opensea-is-first-nft-marketplace-to-pass-1-billion-in-monthly-trading-volume>

Newzoo. (2020). Number of Gamers Worldwide 2021/2022: Demographics, Statistics, and Predictions. *Finances Online*. <https://financesonline.com/number-of-gamers-worldwide>

NonFungible. (no date). Market Overview. <https://nonfungible.com/market/history>

Field, H. (2021, 16 April). Coinbase Becomes First Crypto Company to Go Public, Opening at Valuation Near \$100 Billion. *Morning Brew*. <https://www.morningbrew.com/emerging-tech/stories/2021/04/16/coinbase-becomes-first-crypto-company-go-public-opening-valuation-near-100-billion>

Sigalos, M. (2021, 10 August). Coinbase profits surge following volatile stretch of cryptocurrency trading. *CNBC*. <https://www.cnbc.com/2021/08/10/coinbase-coin-earnings-q2-2021.html>

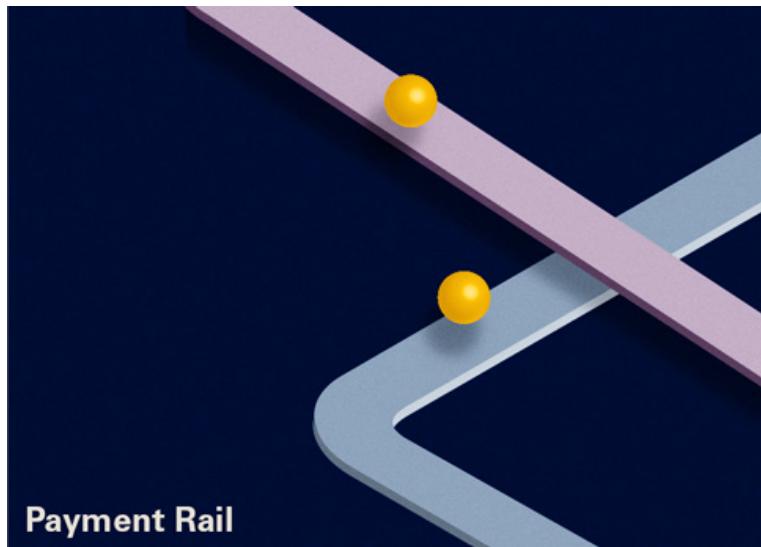
## 2.3 Payment Rails

### 2.3.1 Introduction to Payment Rails

#### Overview

A payment rail is a network or form of digital infrastructure that transfers money from the payer to a payee. Centralised financial institutions have traditionally set up payment rails to facilitate and control the flow of funds between permissioned participants in exchange for a transaction fee.

Our current financial system interconnects different types of payment rails that form a hierarchy. Each layer of the hierarchy provides unique features with the support of the layer beneath it.



#### Vocabulary Check

This section introduces the following terms:

- [algorithmic stablecoin](#)
- [burning](#)
- [card rail](#)
- [central bank digital currency \(CBDC\)](#)
- [decentralised app \(dApp\)](#)
- [decentralised finance \(DeFi\)](#)
- [lightning network](#)
- [micropayment](#)
- [minting](#)
- [negative interest rate](#)

- [negative interest rate policy \(NIRP\)](#)
- [net settlement](#)
- [payment rail](#)
- [pegging](#)
- [programmable money](#)
- [proof of work \(PoW\)](#)
- [sidechain](#)
- [stablecoin](#)
- [tokenisation](#)
- [tokenomics](#)
- [transaction volume](#)

## 2.3.2 Payment Rail Architecture

### Payment Rail Architecture

Popular traditional payment rails include:

- **Real-time gross settlement (RTGS) networks** – Fedwire in the US and TARGET2 and EURO1 in Europe are domestic real-time gross settlement systems.
- **Interbank networks** – Interbank networks such as CHIPS and ACH offer an efficient alternative to the more expensive Fedwire payment system.
  - The Clearing House Interbank Payments System (CHIPS) is another type of funds transfer system that facilitates and processes large interbank transactions in the US. Unlike Fedwire, CHIPS does not settle transactions instantly and with finality. Instead, it batches multiple transactions together and engages in a “net settlement” process.
  - An automated clearing house (ACH) is an electronic network that facilitates transfers of funds. Payroll, direct deposit, tax refunds, consumer bills, tax payments, and many more payment services in the US use ACH transactions.
- **Communication and payment networks** – Communication networks play a significant role in the ability of financial institutions to transfer and settle payments with each other, both domestically

and internationally. The communication network for both ACH and wire transfers is the Society for Worldwide Interbank Financial Telecommunications (SWIFT).

- **Credit card networks** – Companies like Visa, American Express, and Discover operate their own card networks, or card rails, which work by transmitting information about the cardholder's payment request to the merchant bank, then submitting a request to the cardholder's bank for payment. If approved, the bank issues the payment to the merchant's bank account (Scott, 2018). Ultimately, the provider settles card transactions through Fedwire or ACH.
- **C2C or P2P networks** – “Consumer-to-consumer” (C2C) and “peer-to-peer” (P2P) networks include companies like PayPal, Venmo, or Cash App. PayPal, Venmo, and Cash App are fintech applications that connect to the ACH or RTGS networks to settle payments while enabling users to send and receive payments, and store balances, in the app.

### 2.3.3 The Differences Between Payment Rail Layers

#### The Differences Between Payment Rails

The key factors that differentiate payment rails include:

##### Transaction Processing Volume

Transaction volume refers to the monetary value (usually in USD) of transactions that occur between counterparties within a given period.

##### The Necessary Level of Trust

The level of trust necessary for participants to engage in a transaction is a function of the ability of a sender to reverse the transaction if necessary, as well as the ability to verify the transaction. Payment rails like Fedwire, which instantly settle transactions with finality, are built on a high degree of trust between counter-parties—and ensure an equally high degree of certainty in the transaction details. Payment rails such as credit card networks or ACH systems do not offer instant settlement finality, and therefore do not require as high a degree of trust in the process and the reputation of the parties involved. Therefore, these mediums reduce the risk for parties transacting with others in whom they do not have a high degree of trust, as there is a grace period during which their transactions can be reversed.

## Comparison of Payment Rail Types

Payment Rail Type	Example	Transaction Type	Typical Transaction Size	Transaction Frequency	Trust Level required	Instant Settlement Finality	Time to receive payment	Cost
Base Layer	Fedwire	Wire transfer - instant settlement - once confirmed, transactions are irreversible	Large - average transfer value is US \$3.3 million (Fedwire, n.d.).	Low - 727,313 transfers per day in the USA. (265 million per year) (Fedwire, n.d.)	High	Yes	Instant - Takes up to 24 hours for credit transfer from receiving bank to the receiver's bank account	High
Interbank Network	CHIPS - Clearing House Interbank Payments System	Wire Transfer	Large - Average transaction is over US \$3million (Soramäki, et al., 2006).	Low - Settles 345,000 transactions per day (Soramäki, et al., 2006).	Medium	No	Same day (intraday settlement) (Modern Treasury, n.d.)	High
Interbank Network	ACH - Automated Clearing House	Batched - domestic & international	Small to - Transfer limit - US \$2,000 to US \$6,000 per day (Shiffrin, 2021).	High - 26.8 billion payments totalling US \$61.9 trillion in value for 2020 (Nach, 2021).	Medium	No	2-3 business days	Low
Communication Network	SWIFT - The Society for Worldwide Interbank Financial Telecommunications	Primarily facilitates international bank transfers through SWIFT Codes	N/A - SWIFT is a messaging service only - Does not hold funds or debit/credit accounts	N/A	Medium	N/A	2-5 business days	High
Credit Card Network	Visa, MasterCard, Discover, American Express	Card transactions processed by merchant service providers settled via Fedwire or ACH (Herbst-Murphy, 2013).	Very Small - Average card transaction is US \$112 (Shepherd, 2020).	Very High - 468 billion transactions in 2020 (de Best, 2021).	Low	No	1-3 business days	Low
C2C or P2P Networks	Zelle, PayPal, Venmo, and Cash App	Peer-to-peer transfer within the app. Settlement between originating & receiving bank done via ACH or Fedwire	Very Small - Venmo average transaction size = US \$60 (Milena, 2021).	Very High - Total number of transactions in 2020 across PayPal, Cash App, Venmo and Zelle = US \$22 billion (Curry, 2021).	Low	Yes	1-3 business days	Very Low

## 2.3.4 Problems with Traditional Payment Rails

### Traditional Payment Rails

Three problems traditional payments rails lie in the areas of:

- Control and regulation
- Lack of privacy and centralised security risks
- Cost and inefficiency (long settlement time)

#### Control and Regulation

The centralisation of traditional payment rails enables service providers to control who can participate in their services. The dominance of services like PayPal and ACH systems limits the ability of those who are shut out of the banking system to digitally earn, send, or receive money.

#### Lack of Privacy and Security Risks

Hosting customer and financial data on a centralised database can create security risks, as in the case of a breach, all private data could be exposed.

The problems with centralised security infrastructures compound when traditional payment rails force users to share sensitive data to use their systems, leaving them vulnerable to potential identity theft and fraud.

#### Cost and Inefficiency: Long Settlement Times

Centralised payment rails can incur high operating and compliance costs to communicate with one another. As a result, consumers making cross-border payments face higher transfer costs and longer waiting times for payments to settle. The delay is a particular problem for minimum wage workers from developing nations sending remittances back home. The cost of transferring funds from the US, for example, is still as much as 5% of the transaction on average (Norrestad, 2021). The problem has traditionally been that incumbent banks tended not to be incentivised enough to provide cheaper and faster payment services due to the lack of competition, though this is changing with the growing number of fintech players.

## Guest Video: Capital Market Infrastructure

In this video, Yves Messy, Chief Technology Officer at Divvy, talks about the future of capital markets, in which he believes payment rails will no longer be necessary in the fiat context.



I would say the fact that capital market infrastructure itself is being rethought. There's a genuine amount of competition now happening between the likes of the London Stock Exchange, NASDAQ, and protocols like DeFi.

It's interesting to see, if you care about the future of capital markets, which personally, I'm very concerned about, then you need to be aware of that race where you no longer need a broker, you no longer need a settlement entity, you no longer need a payment rail in the field context in order to trade derivative swaps and frankly make them far more composable and lean in a way that's frankly impossible in traditional finance today.

So that capital market infrastructure bit is one that really needs to be included in the curriculum because I think it's a trend that will redefine how trading happens, how settlement happens, and how assets are sold and distributed to retail investors and institutionals.

### 2.3.5 Blockchain Payment Rails

#### Bitcoin: The First Blockchain Payment Rail

Bitcoin, as a cryptocurrency, is also a payment rail. In fact, Satoshi Nakamoto's Bitcoin white paper features the title "Bitcoin: A Peer-to-Peer Electronic Cash System". The title regularly sparks debate in the crypto-blockchain realm, with many believing that bitcoin's true utility is as a means of payment and not a store of value.

Bitcoin fits the definition of a payment rail, yet for a variety of reasons, it is not widely used as such for everyday transactions.

The first reason for the overall lack of adoption is because the network can process only seven transactions per second due to its 10-minute confirmation block times, and average block size of about 1 megabyte (Blockchain, n.d.). The speed of the Bitcoin network pales in comparison to Visa's 24,000 transactions per second.

The problem of slow transaction speeds on the Bitcoin blockchain is not a new phenomenon. Users have been debating the topic since the cryptocurrency's inception. Major disagreements over potential scaling solutions have led to the creation of alternative cryptocurrencies like Bitcoin Cash, which is a fork (a copy on which different changes are made going forward) of the original Bitcoin protocol with an increase in maximum block size to 32MB.

Current solutions to Bitcoin's scalability challenges include the Lightning Network. The Lightning Network's purpose is to expand the Bitcoin blockchain's capacity to process more transactions by creating bidirectional payment channels between counterparties. The payment channels will

process transactions “off-chain” using a smaller network of participating lightning nodes. All off-chain transactions are batched together prior to validation (settling) as one large “on-chain”—back on the main blockchain—transaction.

This setup resembles the relationship between Mastercard and Fedwire. Mastercard processes smaller transactions, which are ultimately settled at the ACH level or at the base settlement layer that is Fedwire.

The second reason bitcoin is not a popular everyday payment system is due to its volatility, and the disincentive for people to spend an asset that has historically appreciated in value at an annual rate of 230% per year (Young, 2021). If bitcoin holders believe that the value of a bitcoin will appreciate more rapidly than other assets, they will hold on to their bitcoin and spend the other instead.

## Blockchain Payment Rails Versus Fedwire

While Fedwire offers instant settlement finality, which requires an assumption of trust between participants, Bitcoin blockchain settlement occurs in degrees, increasing incrementally with each newly validated block to achieve proof of work (PoW) consensus finality (Wandhöfer & Berndsen, 2019).

Blockchains neither create nor eliminate trust. Rather, they convert trust from one form to another. With Fedwire, consumers trust financial institutions to verify transactions. With blockchain, consumers trust the technology itself and have full visibility into transactions (Baur & Van Quaquebeke, 2017).

As the adoption of the Bitcoin blockchain increases, the number of Bitcoin transactions is gradually catching up to Fedwire, which may speak more to Bitcoin’s wider accessibility as a payment network than the more exclusive Fedwire system.

## Blockchain Payment Rails Versus ACH

While the ACH network requires a centralised clearing house to authenticate transactions between parties, Bitcoin’s consensus mechanism, enforced by a group of miners, achieves this function. Each node acts as its own clearing house on the blockchain, working in sync with other nodes across the public, immutable ledger to achieve consensus before recording financial transactions. The result is a system for performing online transactions with instant settlement.

Traditional payment rails require a clearing house to verify transaction details before the actual settlement of funds. The process could take several business days due in part to the number of intermediaries in the clearing and settlement process (merchant, originating bank, ACH, Federal Reserve receiving bank, receiver).

On a blockchain, counterparties in cryptocurrency transactions have access to a public ledger that updates its records at the same time for everyone. When an entity transfers cryptocurrency from one digital wallet to another on the same blockchain, the transfer is incrementally validated and quickly settled.

## **2.3.6 Use Case 1: Placing Fiat Currencies on Public Blockchains (USDC and Tether)**

### **Use Case 1: Placing Fiat Currencies on Public Blockchains (USDC and Tether)**

One important benefit of a Blockchain payment rail is that it enables participants to exchange the value of fiat currencies peer-to-peer without a centralised intermediary. To exchange a fiat currency on a blockchain payment rail, a trader must convert—or “tokenise”—the fiat currency into a stablecoin.

#### **Stablecoins**

Stablecoins are digital representations of fiat currencies on a blockchain. A \$1 stablecoin represents US \$1 of fiat currency. Stablecoins can be backed by fiat currencies, real-world assets, such as commodities like oil, or even other cryptocurrencies.

It is also possible stablecoins are not fully backed; they may still maintain their value because people believe they have a stable value. When stablecoins are not fully backed, when many users try to withdraw USD at one time, they may not be able to retrieve the expected value.

The term “backed by” refers to the underlying asset—of greater or equal value—that acts as collateral to the balance of a particular stablecoin in circulation, which the holder can redeem in the future.

Examples of crypto-collateral backed stablecoins include Dai and Liquidity USD (LUSD). Dai is the first crypto collateral-backed cryptocurrency that developer MakerDAO intends to maintain a stable 1:1 value with the US dollar to reduce crypto volatility and enable decentralised finance (DeFi) capabilities such as borrowing, lending, or trading (Cryptopedia, 2021). The Maker system allows users to collateralise a wide range of crypto assets to “mint” new Dai (Liquidity, n.d.).

LUSD is, according to Liquity’s claims, “a fully backed stablecoin pegged to the US dollar” that Liquidity maintains through an algorithmic monetary policy (Liquidity, n.d.). The Ethereum blockchain’s Ether backs LUSD. Users can draw LUSD against their Ether collateral by paying a one-time borrowing fee as a percentage of the amount drawn, rather than having to pay any interest.

Stablecoins have appropriated the term “fully” backed from traditional finance, where it means fully collateralised with safe or almost safe assets in the same currency. Whether or not that is the case remains a point of contention.

#### **Algorithmic Stablecoins**

Certain types of cryptocurrencies like Ampleforth (AMPL), Fei (FEI), or Empty Set Dollar (ESD) are not backed by any asset but instead achieve price stability algorithmically (these are known as algorithmic stablecoins). Algorithmic stablecoins aim to maintain a peg to the price of a US dollar or other fiat

currencies, cryptocurrencies, or commodities without the use of any underlying collateral. If the price of a stablecoin goes above or below the pegged currency during times of market volatility, the system will use smart contracts to automatically increase or decrease the supply of the stablecoin.

The change in supply creates a scarcity or surplus of the stablecoin, which incentivises market traders to either buy or sell more of the currency until it falls back in line with the pegged asset. Given the volatile nature of the crypto markets, algorithmic stablecoins have not always been successful in maintaining their peg and sometimes have to rely on reserves or alternative sources of funds to prop up their price if there is a lack of incentivisation for traders to purchase the coin at a discount.

## Stablecoins on Blockchains

Stablecoins operate on both private and public blockchains. Two popular stablecoins on the Ethereum blockchain are Tether (USDT) and Coinbase & Circle's USD Coin (USDC).

Tether is the largest stablecoin, with—at the time of writing—a market capitalisation of US \$82.4 billion, and USDC came second with a market cap of US \$51.5 billion (CoinMarketCap, n.d.). According to Tether's claims with regard to crypto reserves breakdown, USDT holds over 75% of its reserve in cash or cash equivalents (Gans, 2021). After that, 12.55% is wrapped up in loans to what Tether claims are “unaffiliated entities,” and 9.96% sits in corporate bonds, funds, and precious metals, with the remaining 1.64% in use for additional investments (Gans, 2021). As De & Hochstein point out, however, “[m]uch remains murky ... in part because the[se numerical proportions] provided by Tether ... make no mention of any independent review by an accounting firm” (2021).

USDC practices full reserve banking, where it lends out only USDC in proportion to a 100% or greater reserve ratio (reserve ratio is the amount of money a bank has in its reserves as a percentage of the amount lent out). The higher the reserve ratio, the less risk the lending institution takes on. The exact makeup of these reserves is also important for calculating risk.

At roughly US \$63 billion in reserves, Tether controls 75% of the stablecoin market (Carfang, 2021). In recent years, this market dominance has come under threat from USDC and other alternative stablecoins that offer various collateral structures appealing to investors with different risk profiles. In January 2021, Tether dipped below 75% market share for the first time, while USDC surpassed 15% in market share (CB Insights, 2021).

The primary use cases for stablecoins include instant payment and settlement of transactions between global participants on a blockchain network and protection against volatility for cryptocurrency traders (Brownworth, 2019). Stablecoins are also used as a store of value by citizens in countries with unstable currencies.

The transparency of blockchain payment rails also enables stablecoin providers to issue loans for margin trading or lend out against crypto-based collateral through smart contracts—alternatively, stablecoins can act as collateral when borrowing other digital assets. Blockchain payment rails strip away many of the physical and operational costs of setting up bank lending services, enabling lending platforms to tout lower banking infrastructure costs, coupled with the use of smart contracts and rising global demand for USDC and Tether when selling their services and annual yields.

## 2.3.7 Use Case 2: Placing Fiat Currencies on Private Blockchains (CBDCs)

### Use Case 2: Placing Fiat Currencies on Private Blockchains (CBDCs)

For fiat currency-providing institutions, governments explore stablecoins as a primary use case of blockchain technology (Moné, 2021). Currently, national central banks are working on a sovereign version of a private stablecoin or cryptocurrency known as central bank digital currency (CBDC). The central banks of individual nations are currently gaining the ability to control and issue their CBDC, which is accessible to individuals and businesses for payments or settling transactions between banks domestically (CB Insights, 2021).

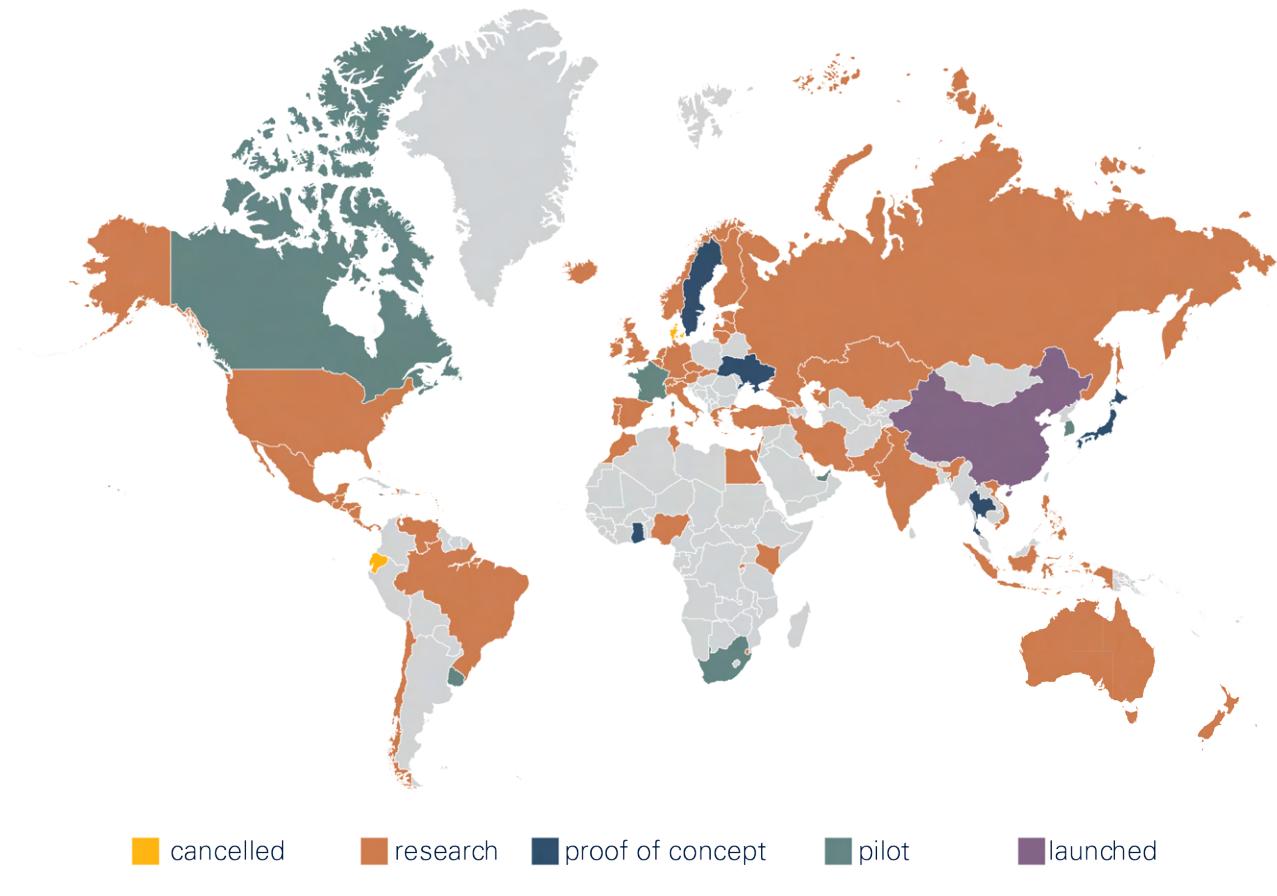
At this point, central banks engaging in CBDC deployments are typically using a private blockchain network consisting of nodes that the central bank operates. CBDC networks may evolve to include commercial banks, regulators, and other regulated payment service providers as node operators which would better leverage the distributed consensus mechanisms that form part of a number of blockchain networks. The storing and distribution of CBDCs occur through digital wallets held by a variety of stakeholders including individual citizens and registered entities on a private permissioned network. By using this private blockchain and digital wallet infrastructure, central banks can establish a direct method for implementing monetary policy, and a distribution channel to debit and credit the accounts of individual citizens, enterprises, and other economic stakeholders.

### Examples of CBDCs

At least 57 central banks are currently exploring CBDCs, with up to 15 that have either launched, piloted, or are in the advanced stages of exploration (CBDC Tracker, 2021).

The following chart compares the leading CBDC projects based on objectives, features, and technologies used (Gross & Kiff, 2021):

## Central Bank Digital Currencies Status



One of the most high profile examples of CBDC adoption comes from China, which launched its Digital Renminbi or e-CNY, during the 2022 Winter Olympic Games in Beijing. This Digital Currency Electronic Payment (DCEP) system will integrate into the country's banking sector and the largest payment services such as AliPay and WeChat (Kharpal, 2021). Before the Beijing Winter Olympics, the DCEP had already been piloted in Shenzhen, Suzhou, Chengdu and the Xiong'an zone near Beijing, with over RMB 20 million (US \$3 Million) distributed amongst early participants to stimulate usage (Zhang, 2021). In February 2022, during the Beijing Winter Olympics, the digital yuan was being used to make payments of 2 million yuan (USD \$315,000) per day (Jones, 2022).

Comparison of Advanced Retail CBDC Explorers					
Jurisdiction (Project Name)	Status	Date of Launch	Objectives	Offline Payments	Technology Providers
The Bahamas (Sand Dollar)	Fully launched	2020 (October)	Payment systems efficiency and resilience, financial inclusion, fighting illicit activities	X	NZIA Limited (NZIA Cortex DLT)
Eastern Caribbean Currency Union (DCash)	Pilot launched (in 4 of the 8 member countries of the currency union)	2021 (March)	Reducing the cost and risks of physical cash management, financial inclusion	X	Bitt (Hyperledger Fabric DLT)
China (e-CNY)	Pilot launched (selected participants)	2020 (April)	Monetary sovereignty, resilience, financial inclusion, cross-border payments	O	Proprietary
Uruguay (e-Peso)	Pilot conducted (6-month pilot in 2017-2018)	2017 (November)	Reducing the costs of physical cash management, digitalisation, fighting illicit activities	X	Roberto Giori Company

## Implications of CBDCs

Blockchain payment rails and CBDCs have the potential to revolutionise both monetary and fiscal policy, creating significant efficiencies in taxation, welfare distribution and coordination of economic activity. Through the concept of “programmable money”, central banks could embed smart contract functionality into digital wallets connected to blockchain payment rails to customise and automate the execution of taxation, stimulus and interest rate policies.

## Flexible Implementation of Fiscal Policies

Whether via a blockchain or not, the ability to manage various payment channels under a single network would enable central banks to distribute stimulus payments directly to citizens’ digital wallets based on select criteria such as income or household size. Similarly, stimulus payments could be made direct to enterprises who offer services in a particular industry.

The use of CBDCs could also reduce tax avoidance and money laundering due to their traceability

and governments' ability to monitor all digital wallets that hold CBDCs (Allen et al., 2020).

There's even potential for a world where CBDC denominates all trading accounts on brokerage services or a shared central bank ledger—an achievable feat that would enable governments to gain complete visibility into the profits and losses of market participants to ensure fair play.

Governments could calculate and deduct taxes from the profitable sale of securities immediately upon exiting a position, eliminating the time and costs of filing and reporting capital gains. Similarly, employers could eliminate the time and costs of withholding and reporting taxable income by simply paying employees in CBDCs, automatically deducting a percentage of an employee's salary and diverting it straight to a nation's tax authority digital wallet account.

## Flexible Implementation of Monetary Policy

Widespread CBDC adoption could enable central banks to customise interest rates between different demographics and industries to incentivise growth or contraction in different sectors of the economy.

For example, a government that aims to incentivise high earners between the ages of 30 and 40 to spend more to stimulate economic growth could simply enforce negative interest rates on the digital wallet accounts of these citizens while simultaneously increasing savings rates on older demographics approaching retirement.

Similarly, central banks could force industries that use environmentally damaging energy sources to borrow from them at higher interest rates with negative-yielding digital wallet accounts, and environmentally friendly companies could receive lower borrowing and higher savings rates.

Because CBDCs are programmable money, governments will have the ability to apply many of the same "tokenomic" models observed on decentralised apps (dApps) and public blockchain networks to coordinate and incentivise activities that produce desirable effects for the economy, and offer more complex financial products with terms enforced through smart contracts.

## Possible Concerns with CBDCs

Like any other technological innovation, blockchain technology has both positives and negatives. While Cryptocurrencies are an example of blockchain technology giving people the freedom to choose an alternative to their existing monetary system, CBDCs enable governments to offer the security and convenience of digital while also being able to impose controls wider-reaching than those of traditional fiat.

So, there could be flaws in the CBDC system, too—its transparency, in the hands of governments or erroneous entities, could enhance the surveillance of money and capital flows. If the world continues towards the removal of physical money and adopts transparent blockchain alternatives, it becomes conceivable that governments could have a clear view of all transactions made by citizens.

With the rapid adoption of technologies worldwide, and the governmental drive for new, tech-enhanced infrastructure, a system in which access to public transportation services, loans or even

housing requires the ability to use a CBDC isn't so hard to imagine. In the wrong hands, power over a system like that could be dangerous, as CBDCs can arbitrarily be made inaccessible to citizens for any reason.

The immutability of blockchains leads to further concerns about the diminished capacity for official records to be expunged or contested and raises ethical questions about the circumstances in which a person's history should or should not be used against them.

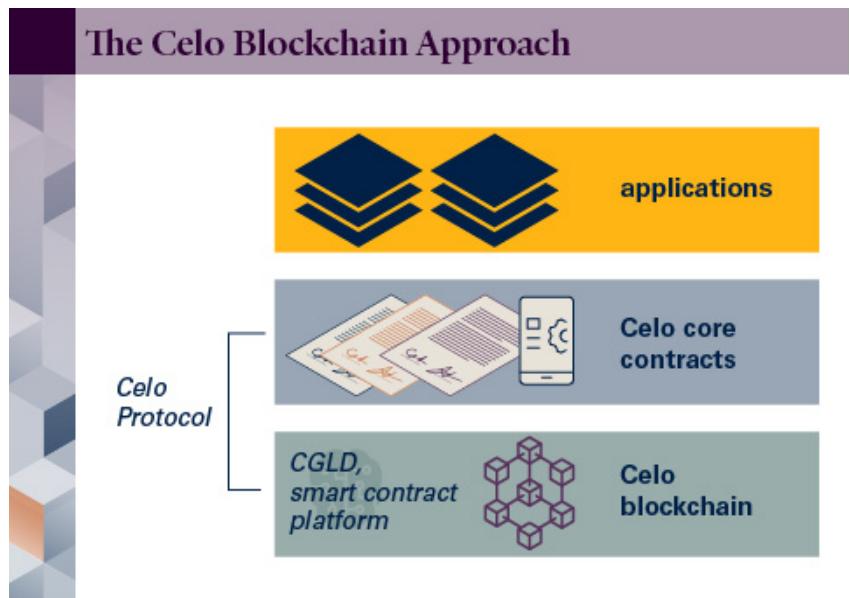
Negative interest rates occur when instead of the capital reserve paying banks to hold reserves, it charges banks for maintaining their reserve balances. The European Central Bank (ECB) has already implemented negative interest rates and the Bank of Japan (BOJ), each of which charges -0.50 and -0.1% on bank reserves, respectively, to stimulate economic growth through consumers and businesses borrowing and spending more (Reuters, 2021).

The side effect of a negative interest rate policy (NIRP) is that it penalises bondholders and retail bank depositors who keep their funds in savings accounts. Under a negative interest rate policy, bondholders pay the bond issuer a net amount at maturity instead of earning a return through interest. At the same time, bank depositors lose the face value of their money in addition to the normal decline in purchasing power caused by inflation. The execution of NIRP could help central banks escape liquidity traps, and decrease fragility. Or it could cause inflation as borrowers are effectively being paid to take on debt.

### 2.3.8 Use Case 3: cLabs, Decentralised Cross Border Mobile Payments, and Stablecoin Issuance

#### Use Case 3: cLabs, Decentralised Cross-Border Mobile Payments, and Stablecoin Issuance

cLabs is a project built on the Celo blockchain to facilitate stablecoin issuance and permissionless cross-border mobile payments. The company's mission is to support financial inclusion in developing countries by solving the challenges of cryptocurrency usability, such as self custody and security, on resource-constrained mobile devices. The Celo blockchain hosts a number of decentralised applications, such as the Celo wallet app, which enables users to manage accounts, exchange and stake digital assets and make secure micropayments using the Celo protocol.



## Guest Video: Financial Inclusion is Core to Celo's Mission

In this video, cLabs' CTO & Co-Founder Marek Olszewski discusses Celo blockchain missions and some of the key projects being built on the network to advance financial inclusion.



Financial inclusion has been really core to Celo's mission right from the get-go, as it has been to the broader crypto community. And it makes sense because, if you think about it, much of crypto is really built around this idea of self-custody and being able to interact with others in a fully decentralised, trustless manner, and that means that in many legal jurisdictions worldwide, people can transact and send assets, custody of these assets in a way that doesn't require a government-recognised ID.

And so this is very, very exciting. I think the challenge, though, has been always around making this really easy to use. Self-custody is very hard, you know. People lose their keys all the time. And then, doing so on mobile devices, especially resource-constrained mobile devices, has also been really, really challenging. And so Celo has really focused on making it just much easier to solve these problems with end-user applications, with mobile end-user applications that effectively allow you to build these lightweight bank account experiences that are just very easy to use but also permissionless and self-custodial.

And when you do that, then suddenly, it just enables a whole slew of just amazing experiences and opportunities that really help advance financial inclusion. And so I can list just a couple of these that are being currently worked on the Celo platform, not by me but by others in the broader ecosystem, that are just really, really exciting. The first is around microwork.

So there's a company called Corsali that has built a platform that allows people to do microwork directly on their smartphones, primarily targeting folks in Kenya. And these folks are able to perform these microtasks and actually get paid after each microtask instantly using a small transaction that goes straight to their self-custodial wallet literally every time they've completed a small task. And this is really compelling because it takes away this fear that you might not get paid, and it also takes away the fear that all of your earnings will be wasted on transaction fees that typically hinder folks in these markets.

And it's been really exciting to see. The community has been growing. It's primarily university students who, especially in these COVID times, are looking for other ways to top up their income. And it's just been really, really rewarding to see this take off and to see people not only earn these funds but then, through another ecosystem company, convert them into M-Pesa to be able to spend them really near instantly, which is just amazing. The second example that I think is also really exciting is around cash transfers.

And so there's been a lot of work in the NGO community moving towards cash transfers as a form of aid. And especially in the last year, we've seen this really take off. And there is one ecosystem organisation called the Grameen Foundation—a very storied organisation—that was able to raise some funds from JP Morgan and then do a big campaign in the Philippines where they were doing unconditional cash transfers to women entrepreneurs who have been disproportionately affected by COVID.

## Use Case 3: cLabs, Decentralised Cross-Border Mobile Payments and Stablecoin Issuance (ctd.)

The project is compatible with Ethereum virtual machines for creating smart contracts, ERC-20 stablecoins, and identity attestations, and for leveraging proof-of-stake consensus mechanisms for governance.

The Celo blockchain also offers a menu of algorithmic stablecoins that track the value of fiat currencies, commodities and natural resources. The platform supports several stablecoins, including the Celo Dollar (cUSD) and Celo Euro (cEUR), which track the US dollar and euro value and are collateralised by a collection of digital assets, including bitcoin and Ether.

Payment Rail - Business Models
Transaction fees from cross-border payments
Providing stablecoin liquidity and charging fees to convert real fiat currency to stablecoins
Stablecoin lending services
Subscription service to operate stablecoin payments network with user accounts and crypto-to-fiat on and off-ramps

### 2.3.9 Key Takeaways, References, and Further Exploration

#### Key Takeaways

Let's review the key points of this section:

1. A payment rail is a digital infrastructure that enables the transfer of money between parties. Traditionally centralised authorities set up payment rails to facilitate and control the flow of funds between permissioned participants in exchange for a transaction fee. Blockchain technology offers a decentralised and permissionless alternative.
2. Ethereum and Bitcoin are also payment rails because they offer a decentralised, digital peer-to-peer payment system. However, companies and individuals are yet to widely adopt Ether and bitcoin—the currencies—for day-to-day transactions.
3. Stablecoins are representations of fiat currencies on either a private or public blockchain.
4. CBDCs or central bank digital currencies are similar to private stablecoins, but they're placed on private central bank-controlled blockchains and are accessible to individuals and businesses for payments or settling transactions.
5. Blockchain technology is merely a tool that people, businesses, and organisations have at their disposal, so each use case will have its own implications and possible concerns.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

### 2.3.2 Payment Rail Architecture

EBA Clearing. (no date). A unique RTGS-equivalent large-value payment system. <https://www.ebaclearing.eu/services/euro1/overview>

European Central Bank. (no date). What is TARGET2? <https://www.ecb.europa.eu/paym/target/target2/html/index.en.html>

Federal Reserve System. (no date). Fedwire Funds Services. [https://www.federalreserve.gov/paymentsystems/fedfunds\\_about.htm](https://www.federalreserve.gov/paymentsystems/fedfunds_about.htm)

Hayes, A. (2021, 24 February). Clearing House Interbank Payments System (CHIPS). *Investopedia*. <https://www.investopedia.com/terms/clearing-house-interbank-payments-system-chips.asp>

Sanction Scanner. (no date). SWIFT Payments and Transaction Screening. <https://sanctionscanner.com/knowledge-base/swift-payments-and-transaction-screening-201>

Scott, G. (2018, 11 June). Payments 101: Credit Card Processing vs. ACH Transfers. *Motile*. <https://paymotile.com/blog/credit-card-processing-vs-ach-payments>

SWIFT. (no date). SWIFT FIN Traffic & Figures. <https://www.swift.com/about-us/discover-swift/fin-traffic-figures>

### 2.3.3 The Differences Between Payment Rails

Curry, D. (2021, 6 May). Venmo Revenue and Usage Statistics (2021). *Business of Apps*. <https://www.businessofapps.com/data/venmo-statistics>

de Best, R. (2021, 9 July). Visa, MasterCard, UnionPay transaction volume worldwide 2014-2020. *Statista*. <https://www.statista.com/statistics/261327/number-of-per-card-credit-card-transactions-worldwide-by-brand-as-of-2011>

Fedwire. (no date). Fedwire Funds Service - Annual Statistics. *The Federal Reserve*. <https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/annual-stats.html>

Herbst-Murphy, S. (2013, October). Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts. *Federal Reserve Bank of Philadelphia*. <https://www.philadelphiahfed.org/-/media/frbp/assets/consumer-finance/discussion-papers/d-2013-october-clearing-settlement.pdf>

Milena. (2021, 21 June). Venmo Statistics. *Balancing Everything*. <https://balancingeverything.com/venmo-statistics>

Modern Treasury. (no date). CHIPS. <https://www.moderntreasury.com/learn/chips>

Nacha. (2021, 4 February). ACH Network Sees Record Growth in 2020 to 26.8 Billion Payments. <https://www.nacha.org/news/ach-network-sees-record-growth-2020-268-billion-payments>

Shepherd, M. (2020, 16 December). Cash vs Credit Card Spending Statistics (2021). <https://www.fundera.com/resources/cash-vs-credit-card-spending-statistics>

Shifrin, M. (2021, 17 June). ACH Transfer Limits at the Top U.S. Banks. *MyBankTracker*. <https://www.mybanktracker.com/news/ach-transfer-limits>

Soramäki, K., Bech, M.L., Arnold, J., Glass, R.J., & Beyeler, W.E. (2006, March). The Topology of Interbank Payment Flows. *Federal Reserve Bank of New York*. [https://www.newyorkfed.org/medialibrary/media/research/staff\\_reports/sr243.pdf](https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr243.pdf)

### 2.3.4 Traditional Payment Rails

Norrestad, F. (2021, 17 May). Average cost of sending remittances from the U.S. 2013-2020. *Statista*. <https://www.statista.com/statistics/962747/average-cost-of-sending-remittances-from-usa> 34

### 2.3.5 Blockchain Payment Rails

Baur, D., & Van Quaquebeke, N. (2017, 15 November). The blockchain does not eliminate the need for trust. *The Conversation*. <https://theconversation.com/the-blockchain-does-not-eliminate-the-need-for-trust-86481>

Bitcoin Mining Insights. (2021, 11 January). How Much Would it Cost to 51% Attack Bitcoin?. *Braiins*. <https://braiins.com/blog/how-much-would-it-cost-to-51-attack-bitcoin>

Blockchain. (no date). Average Block Size (MB). *Blockchain.com*. <https://www.blockchain.com/charts/avg-block-size>

Burtey, N. (2020, 22 July). Lightning as a retail payment system. *Galoy*. <https://medium.com/galoymoney/lightning-as-a-retail-payment-system-part-1-7463c46342ef>

Wandhöfer, R., & Berndsen, R. (2019, June, Volume 7, Number 4). Proof-of-work blockchains and settlement finality: a functional interpretation. *Journal of Financial Market Infrastructures*. <https://www.risk.net/journal-of-financial-market-infrastructures/6813151/proof-of-work-blockchains-and-settlement-finality-a-functional-interpretation>

Young, M. (2021, 15 March). BTC was best-performing asset of past decade by 1,000%. *Coin Telegraph*. <https://cointelegraph.com/news/btc-was-best-performing-asset-of-past-decade-by-900>

### 2.3.6 Use Case 1: Placing Fiat Currencies on Public Blockchains (USDC and Tether)

Brownworth, A. (2019, 25 April). How to move \$1M in USDC. *YouTube*. [https://www.youtube.com/watch?v=Wlf6\\_ukDtsg&ab\\_channel=Circle](https://www.youtube.com/watch?v=Wlf6_ukDtsg&ab_channel=Circle)

Carfang, A. (2021, 5 July). Crypto Stablecoins and Prime Money Market Funds. If it walks like a duck.... *Finextra*. <https://www.finextra.com/blogposting/20557/crypto-stablecoins-and-prime-money-market-funds-if-it-walks-like-a-duck--->

CB Insights. (2021, 16 February). What Are Stablecoins? <https://www.cbinsights.com/research/report/what-are-stablecoins>

CoinMarketCap. (no date) Today's Cryptocurrency Prices by Market Cap. <https://coinmarketcap.com>

Cryptopedia. (2021, 12 March). What is MakerDAO? <https://www.gemini.com/cryptopedia/makerdao-dai-decentralized-autonomous-organization>

De, N., & Hochstein, M. (2021, 13 May). Tether's First Reserve Breakdown Shows Token 49% Backed by Unspecified Commercial Paper. *CoinDesk*. <https://www.coindesk.com/markets/2021/05/13/tethers-first-reserve-breakdown-shows-token-49-backed-by-unspecified-commercial-paper>

Gans, N. (2021, 13 May). Tether (Finally) Releases Breakdown Of Its \$42 Billion In Crypto Reserves. *Forbes*. <https://www.forbes.com/sites/nicholasgans/2021/05/13/tether-releases-breakdown-of-its-reserves/?sh=7755d36a1109>

Liquity. (no date) Interest-free liquidity at your fingertips. <https://www.liquity.org>

### 2.3.7 Use Case 2: Placing Fiat Currencies on Private Blockchains (CBDCs)

Allen, S., Capkun, S., Eyal, I., Fanti, G., Ford, B., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., Prasad, E., Wüst, K., & Zhang, F. (2020, 23 July). Design choices for Central Bank Digital Currency: Policy and technical considerations. *Brookings Institution*. [https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC\\_Final-for-web.pdf](https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf)

CB Insights (2021). What Are Stablecoins? [https://www.cbinsights.com/reports/CB-Insights\\_What\\_Are\\_Stablecoins.pdf](https://www.cbinsights.com/reports/CB-Insights_What_Are_Stablecoins.pdf)

CBDC Tracker. (2021, September). Today's Central Bank Digital Currencies Status. <https://cbdctracker.org>

Gross, J., & Kiff, J. (2021, 27 July). Which jurisdictions head up the retail central bank digital currency league table?. *Jonas Gross*. <https://jonasgross.medium.com/which-jurisdictions-head-up-the-retail-central-bank-digital-currency-league-table-4938a996613f>

Kharpal, A. (2021, 18 April). China may test its digital currency with foreign visitors at the 2022 Beijing Winter Olympics. *CNBC*. <https://www.cnbc.com/2021/04/19/china-may-trial-digital-currency-with-foreign-visitors-at-beijing-olympics.html>

Moné, L. (2021, 6 April). Which Governments are Researching CBDCs Right Now? *ConSensys*. <https://consensys.net/blog/enterprise-blockchain/which-governments-are-using-blockchain-right-now>

Reuters. (2021, 4 February). Explainer: How do negative interest rates work? <https://www.reuters.com/world/europe/how-do-negative-interest-rates-work-2021-02-04>

Zhang, Z. (2021, 12 May). China's Digital Yuan: Development Status and Possible Impact for Businesses. *China Briefing*. <https://www.china-briefing.com/news/chinas-digital-yuan-status-roll-out-impact-businesses>

## Further Exploration

[Is Tether backed by anything?](#)

[Asset Class Returns](#)

[Bitcoin Charts & Data](#)

[Ranking Asset Classes by Historical Returns \(1985-2020\)](#)

[The Blocksize War by Jonathan Bier](#)

## 2.4 Distributed Ledgers

### 2.4.1 Distributed Ledgers

#### Overview

A distributed ledger is a special type of database in which records are replicated across several nodes (computers), which are distributed across locations and institutions. Each node contains a full, identical copy of the database. When the database is updated, the update is replicated on each node, so each copy stays in sync. (The speed of replication depends on the network; there can be latency.) The nodes then use a consensus algorithm to determine the correct record, and the consensus record is then replicated to all nodes.

#### Vocabulary Check

This section introduces the following terms:

- [consortium](#)
- [disintermediate](#)
- [distributed ledger system](#)
- [indexers](#)
- [security token](#)

#### Distributed Ledgers

The ability for multiple network nodes to verify the ownership and transfer of value is potentially useful for solving problems of transparency in different industries, especially those that involve multiple stakeholders operating across different jurisdictions.

The more expansive the network, the more of a challenge it is to create standardisation of products and services, or to account for stakeholders assets and exchanges between individuals and entities using traditional accounting methods. For example:



- Lack of coordination between corporations and their franchises/resellers can lead to different quality standards for products and services offered. Certain participants within the value chain might cut corners or succumb to negligence due to lack of oversight.
- Luxury products could be counterfeited and sold on secondary markets without any way to determine their authenticity.
- Traders seeking access to excess credit in global markets could take advantage of the lack of transparency in the system to hypothecate collateral to multiple lenders without consent, thereby increasing their leverage beyond what is deemed safe.

In all three cases, a distributed ledger's role in verifying and reconciling the authenticity of a product, service, or asset can contribute to maintaining the integrity of these industries as they become more dispersed. The distributed ledger can provide stakeholders with a method for tracking the history and origin of products, services, or assets in a transaction.

Distributed ledgers can help businesses in diverse industries. Examples of the types of problems distributed ledgers can solve include:

- **Cross-border transactions:** By eliminating the need to process transactions through different banks, a distributed ledger reduces efficiencies and costs.
- **Smart contracts:** By storing contracts as code, a distributed ledger can securely automate the execution of agreements reducing time and the need for intermediaries.
- **Secure digital identities:** Storing identity information on a distributed ledger can provide more secure authentication processes and reduce the risk of fraud.
- **Ownership history:** By storing a record of ownership transfers, distributed ledgers can better manage challenges of licensing and ownership.
- **Supply chain management:** By providing a transparent and secure record of provenance, digital ledgers can reduce inefficiencies in supply chains.

In the following lessons, we will explore how distributed ledgers empower commodity producers, brokerage services, issuers of tokenised securities, and others to achieve a synchronised and global view of the assets held and transactions between industry stakeholders.

## 2.4.2 Distributed Ledger for Diamond Authentication

### Distributed Ledger for Diamond Authentication

By now, many consumers are aware of the diamond industry's challenges with the mining, export and sale of "conflict" or "blood" diamonds. In the past 20 years, establishments and institutions have been looking for ways to clamp down on conflict diamond sales, the most notable of which was the establishment of the Kimberley Process in 2003.

The Kimberley Process (KP) is a multilateral trade regime between 56 participants—including members of the European Union, which stand as one nation—in 83 countries that outlines requirements for controlling rough diamond production and trade to remove conflict diamonds from the global supply chain (Kimberley Process, n.d.). The Kimberley Process Certification Scheme (KPCS) establishes safeguards for the shipment of rough diamonds and criteria for certifying that the diamonds are “conflict-free”.

Under the terms of the KPCS, participants must:

- Satisfy “minimum requirements” and establish national legislation, institutions and import/export controls.
- Commit to transparent practices and the exchange of critical statistical data.
- Trade only with fellow members who also satisfy the fundamentals of the agreement.
- Certify shipments as conflict-free and provide the supporting certification.

Distributed ledgers are a natural fit for improving the KPCS. Blockchain technology can serve as the ideal solution to the extent that the current process has costly inefficiencies. This is the basis on which Everledger, a digital transparency company, is developing its blockchain-powered platform to help diamond suppliers, merchants, NGOs, governments, insurers, and clients gain access to a distributed ledger that contains information about the journey of each diamond from the mine to the retail store, in addition to compliance documentation and sustainability credentials (Everledger, n.d.).

On Everledger’s platform, diamond suppliers can share documentation proving compliance and provenance of individual diamonds, which is then given a unique identifier on the blockchain so that all parties can trace its movement and receive precise updates on its whereabouts. Inventory data can be accessible to certain parties using access controls enforced by a private permissioned blockchain.

Through well-defined compliance and sustainability criteria, retailers can leverage supplier data to build a profile of partners in an attempt to protect their brand’s reputation. Regulators can verify compliance claims, catch fraud, and resolve legal disputes using an immutable audit trail. The London-based startup has raised over US \$20 million from the UK Government’s Future Fund and Chinese tech company Tencent (Ledger Insights, 2020).

It has also recently partnered with Rare Carat Inc., an e-commerce platform for buying diamonds and diamond rings, to help its customers gain deeper insight into their diamonds’ origin, manufacturing, and transportation (Dotson, 2021).

## 2.4.3 Distributed Ledger for Verifying Collateral

### The Archegos Capital Case

The 2021 implosion of Archegos Capital Management reveals a stark truth about the ease with which entities can seek an unfair advantage under the guise of opacity in an increasingly complex and fragile financial system (McDowell, 2021). Archegos Capital was a family office managed by Bill Hwang, a relatively unknown trader with a murky history that included accusations of insider trading and a guilty plea of wire fraud (Schatzker et al., 2021).

As a result of excessive risk-taking, Hwang was able to amass a US \$20 billion fortune in eight years by leveraging trades through a financial instrument known as “total return swaps”. Total return swaps (TRS) are a type of derivative contract through which a bank executes a market trade for an asset such as a stock or bond on a client’s behalf (CFI, n.d.).

If the trade makes money, the bank delivers the profits to the client, and if it loses money, the loss becomes a debt owed by the client. Banks secure the swaps through collateral that the client must post and allow the bank to liquidate if the trade goes against them. The client also agrees to pay a set interest rate to the bank throughout the contract’s lifetime.

TRS gave Bill Hwang indirect exposure to the markets, allowing him to conceal his trades from regulatory filings and the full details of his collateral postings from the banks.

Multiple Banks, including Goldman Sachs, Morgan Stanley, Deutsche Bank, Nomura Holdings and Credit Suisse, agreed to lend Archegos the funds needed to participate in these swap contracts despite Hwang’s reputation.

However, the banks did not know that Archegos had been working with the other banks to offer the same assets as collateral for multiple loans, a process known as “rehypothecation”.

Rehypothecation of collateral is a legal and common practice amongst banks and brokers. However, without a transparent account of the value and ownership of the collateral in use, it becomes possible for TRS clients to overextend their credit limits by reusing collateral that other lenders have a right to claim.

A sudden drop in the collateral value or a leveraged trade against the client can result in lenders needing to liquidate the collateral to avoid further losses. If multiple lenders each claim a piece of collateral set for liquidation, it quickly becomes apparent that certain parties are more vulnerable to significant losses than others.

When a series of 5-to-1 levered bets on stocks like ViacomCBS, Discovery and Baidu went against Archegos, the banks contacted the firm with warnings that they would liquidate its collateral unless it posts more margin. At that point, Archegos had to default on its loans and reveal the actual state of the collateral. The banks quickly scrambled to rid their books of the bad debts that would have resulted in billions of dollars in losses and potential negative impact on the broader public markets.

Credit Suisse, Nomura, and Morgan Stanley ultimately took the most significant hit, losing US \$5.5 billion, US \$2.3 billion and US \$911 million, respectively, while Goldman Sachs and Deutsche Bank escaped the fiasco relatively unscathed (Hetzner, 2021). Bill Hwang had to watch his firm, Archegos, implode under the cascade of liquidations, wiping out his entire US \$20 billion net worth within two days (Schatzker et al., 2021).

In this case, problems could have been avoided if the participant institutions had been using a distributed ledger to record the collateral posted by Archegos. While a simple, cloud-based spreadsheet or other centralised database could have just as easily provided the banks with an overview of Archegos' collateral, a blockchain would have provided greater transparency and immutability, whilst making it difficult to tamper with the data. In Module 5, we will examine how to evaluate and articulate a business case using blockchain technology, how to understand the economics of a blockchain project, and how to choose between a traditional, more centralised platform and a blockchain.

## X-Margin

X-Margin has built a solution that it calls the “world’s first distributed clearing house” to help lenders monitor borrowers’ assets in real time. The company uses a feature known as “zero-knowledge proof” cryptography to verify crypto traders’ collateral so that it can be used transparently across multiple trading platforms without the need for a central intermediary while protecting privacy.

Zero-knowledge proof (ZKP) is a method that enables one party (the prover) to prove to another party (the verifier) that they have knowledge of a specific piece of information or that the transaction meets certain conditions without revealing what the information is.

## Guest Video: The X-Margin Use Case

In this video, Darshan Vaidya, the CEO and Founder of X-Margin, explains this use case and uses zero-knowledge technology to verify transactions.



We use a combination of privacy-preserving technology and zero-knowledge proofs to disintermediate credit facilitation for trading firms. Basically, it leverages this really powerful technology that takes away the need to trust someone that does computations or analysis of data. So often, you have trusted or regulated intermediaries that look in on a data set and then provide some sort of information about it, so a credit scoring agency, for example. It basically is someone that’s entrusted to look into this black box and then produce an output that people are like, well, I can rely on that.

The power of zero-knowledge technology is that you can basically do the equivalent of shake that black box and then get something that is cryptographically and mathematically verified without having to trust anyone to do that calculation. And so for a trading perspective, what normally happens when a trading firm wants to access multiple trading venues, you go through this central intermediary.

And they do three main things, which is assess someone's risk and look into that risk and then give them credit to trade across these multiple venues and underwrite that credit because they have a bunch of control over the credit that's being extended. Now what we're doing is that first step is we can do that through this provably unbiased and neutral and accurate calculator that doesn't need anything to trust it.

And it also preserves the privacy of all the trading firm's data so that, again, you don't need to trust that they'll be careful with the data or all of that. So once you can do that, it allows them to access credit from multiple different venues, not just the one. And then on the back of that, you can underwrite it through multiple different underwriters. And so it just opens up a whole world of opportunity for trading firms to access credit and capital efficiency through just this very simple disintermediation of decision-making.

## X-Margin (ctd.)

Some more examples of use cases for ZKPs include a concert attendee that needs to prove to a venue that they are over 18 years old without revealing their exact age, or a loan applicant that needs to prove to a bank that they generate enough income to be approved without revealing exactly how much they earn.

The technology works by encrypting the sensitive details of the prover (the loan applicant) and converting it into a function for which the verifier (the bank) must perform a calculation to confirm that the function is correct. Verifying that the function is correct confirms that the prover's claim that they are over a certain age or make enough money to qualify for a loan is valid.

Clearing and margining are the focal points of X-Margin:

- Clearing is the process in which a central clearing house settles a trade between a buyer and a seller, meaning it transfers the correct funds to the seller and the securities to the buyer according to the transaction details.
- Margining is the process of adding collateral to a derivatives contract to borrow funds to execute a margin trade.

When traders have multiple margin positions across different accounts, they can perform "cross-margining", which is a process that allows the trader to reduce any excess collateral on one account and apply it to another account where the margin requirements to maintain that trading position may be higher. Traders primarily perform this offsetting process to manage risk and avoid unnecessary liquidations of potentially vulnerable positions.

Clearing houses calculate cross-margining by tracking the amount of margin traders apply to each account to manage trade settlements between clearing houses at the end of the trading day. Clearing houses require massive centralised infrastructures to process trillions of dollars in trading volume every year.

X-Margin disintermediates the clearing houses by creating a zero-knowledge proof algorithm that calculates margin risk across various trading accounts and enables more efficient cross-margining

between traders and trading platforms without compromising sensitive transaction details and without the need of a central party.

X-Margin's platform also utilises a distributed ledger to ensure that margin requirements across different accounts are met and that the system tracks all collateral globally.

## Paradigm

Paradigm offers a global liquidity network that automates price negotiation and trade settlements between institutional clients. The company anchors its simple vision to the value of distributed ledger technologies: "trade anything, with anyone, anytime, anywhere, and execute, clear, margin, and settle how you want."

Through the use of a distributed ledger, Paradigm's clients can transact peer-to-peer without any centralised intermediary while accessing a transparent audit trail of communications and transactions to help with regulatory compliance, risk mitigation and fraud prevention.

The company also offers a single access point to on-demand liquidity pools for trading different financial products such as futures, spots and options. One of the unique properties of Paradigm is the separation of the trading settlement processes; trading, which includes conducting peer to peer price negotiations and trade executions, while the final settlement of the trade can be done on an exchange, through a custodian or also peer to peer through a smart contract.

This model enables institutions to have flexibility in how they choose to execute different strategies in order to cut down on time and trading costs.

## Guest Video: The Competition Layers

In this video, Anand Gomes, the Founder of Paradigm, explains their vision of enabling trading of anything with anyone and clearing it anywhere.



We started out with a simple vision—create anything with anyone and clear and settle it anywhere, right? And if you think about what that represents, it's the highest level of competition at both the execution layer, which is you can choose your asset, so there's competition there. You can choose your dealer, meaning you can choose who you want to trade with. So there's competition there.

And then there's also competition in how you want to settle the trade, right? Like I said, in the old world, you didn't have that flexibility. You couldn't choose where you wanted to settle it. The whole market settled in one place.

And so we started out like that. And of course, now, in crypto, what does that mean, right? So it means that, a, like I said, you can choose your asset. Choose who you want to trade with. And you can use a different range of execution protocols—an RFQ, et cetera. We have a few on the platform.

But then you can also choose to clear using a custodian. You can choose to clear using an exchange. You can choose to clear using a smart contract. And we, basically, have a unified clearing module that allows you to do that with, basically, being completely seamless, right? So that was the idea of trade anything with anyone and clear it anywhere.

## 2.4.4 Distributed Ledger for Indexing the World's Blockchain Data

### Distributed Ledger for Indexing the World's Blockchain Data

The Graph is a decentralised protocol that aims to index all of the world's on-chain data to make information about all public blockchain networks accessible to anyone simply by running queries. With a decentralised index of all blockchain data, users can search for transparently sourced, data-driven answers to questions like: "What are the newest (DeFi) projects?" or "What exchanges have the most liquidity?"

Many compare the Graph project to Google, which initially set out to index all data on the web (Jakub, 2021). While Google, Facebook and other Web 2.0 platforms exploit user data for profit, the decentralised Web 3.0 empowers users to own and manage their data.

The Graph leverages distributed ledgers to build indexing and querying tools that facilitate the free exchange of information that is non-exploitative. On the Graph, anyone can build their own APIs containing indexed data called subgraphs. Thousands of subgraphs make up a global graph of all the world's public information, similar to how independent and verified entries make up the Wikipedia resource. Users can organise and transform the data on subgraphs and share it across applications for anyone to run queries just as efficiently as entering a search on Google.

Indexers operate nodes on The Graph Network and stake Graph Tokens (GRT) to provide indexing and query processing services.

Edge & Node, a software development company led by Tegan Kline and Yaniv Tal, are the original developers of the Graph Network. The company is also behind Everest—a project built on the same indexing architecture. It offers a universally shared registry of decentralised projects. Projects registered on the platform cover various categories, including DeFi, education, identity, environment and supply chains.

## Guest Video: Distributed Use Case—The Graph

In this video, Yaniv Tal, Project Lead at Graph Protocol, explains this distributed use case, Web3, and decentralised truth on top of the internet.



The graph is an indexing protocol for organizing and serving blockchain data, making that data easily accessible. My background is in developer tools, and I had started multiple companies and worked in multiple companies, working to make software development more accessible to people. We are in the internet age right now. A lot of what we do, as knowledge workers, as participants in the economy, is participating in information systems.

It's all information.

And right now, the software that we use is owned and controlled by a handful of large tech companies, and those employees end up making decisions that impact all of our lives. And so right now, we're kind of in the process of rebuilding a whole protocol and application stack to change how we build information systems more broadly to make sure that information is verifiable, that we know—that we can start to get towards a new concept of decentralised truth on top of the internet. Let's actually start at the web. So the web is a layer on top of the internet.

It starts with HTTP and a set of standards around building these web pages, which is how we kind of share information, and then people build applications on top of the web. But it is a distinct layer on top of the internet. The web has a client server architecture and has this property that whoever runs the server has complete control and can basically decide to do whatever it wants on the server.

And so with the Web 3, we're moving away from this client server sort of architecture to rebuilding the application stack on top of decentralised networks that nobody controls. And the graph is a core layer in this stack, which similarly to the web is the layer on top of the internet, and with the graph, it's on top of blockchains that's organizing all of this data and serving the data. So all data is relational. It actually forms a graph.

If you think of any of the tools that you use, whether it's spreadsheets and you're linking records to different records, there's no reason to bound data within specific applications. And right now, they are bound to specific applications because that's how we've kind of architected the web to live in these silos. But this shift in how we organize these information systems is going to completely change how we build these applications..

## 2.4.5 Tokenisation Distributed Ledger

### Guest Video: Prudential Considers Blockchain Technology

In this video, Federico Spagnoli, the Regional President of Prudential Financial/Latin America and the Lead for Product Innovation & Ecosystem for all emerging markets, explains how Prudential is considering blockchain technology.



So at Prudential Financial, we are periodically revisiting a number of user cases where we can apply blockchain technology to our business. And again, with this idea of trying to create value to our customers. As part of the PGIM strategy-- PGIM is our asset management arm. It is one of the largest in the country. We have a division referred as PGIM Real Estate where we have a number of funds available to institutional sophisticated investors.

However, we believe that by incorporating the use of blockchain technology, like tokenisation, we will be able to democratise the access of these type of asset management solutions to a variety of investors that today, if they want to join, it will be either too expensive or too complex for them to go with.

And so the tokenisation will allow us to, for example, materially reduce the administrative costs related to these type of transactions. At Prudential, we're also part of a consortia. As we all know, blockchain technology is challenging if you want to do it on your own as one organisation trying to lead with this.

Here, I believe it made much more sense if you create a sort of ecosystem where a number of participants in the industries join forces. There is an initiative in the US called RiskStream which is a focus on an ecosystem trying to improve the level of risk mitigation solutions in the market. And we are using the platform Canopy as a way to develop a number of user cases that we are testing as we speak.

One example that I can give you is the first notice of loss, where pretty much we can take it paperless and really streamline the process. So let me give you an example. In the case of life insurance, in the case of a death benefit, having a blockchain-based solution where the beneficiaries are not required to present a death form in order to get access to their claims benefit. This will be integrated as part of the solution. Just by getting this benefit covered in their policies, automatically, the beneficiaries will get their funds in their accounts without further ado.

### Broader Tokenisation of Assets Using Security Tokens

When we think about how tokenisation is simply the creation of a digital representation of any physical or digital asset on the blockchain, it becomes apparent that there are almost no limits to the assets that can be exchanged using blockchain technology.

Security tokens are tokenised assets issued under a regulatory framework that designates the tokens as registered securities, similar to stocks or bonds, which are registered securities under the regulation of the Securities and Exchange Commission (SEC). Security tokens can either be fungible (that is, a

security token can represent one of the issued shares in a company) or non-fungible (that is, a security token can represent a unique asset).

However, an NFT's classification as a security token must undergo a case-by-case evaluation. It will depend on whether the NFT represents a consumer product with entertainment value or an investment contract.

A startup, TokenSoft provides technology and regulatory infrastructure for the creation and issuance of tokenised assets. The company has a variety of solutions ranging from SEC-registered security token offerings and project token sales to tokenising real estate assets and accessing larger pools of investor liquidity while increasing market transparency.

## Guest Video: The Tokensoft Use Case

In this video, the CEO and Co-Founder of TokenSoft, Mason Borda, explains the TokenSoft use case.



It started in 2018. And so we were sort of the first company that helped blockchain companies comply with securities laws. And so naturally, people wanted to come through and to put hard assets onto the blockchain, and to get them registered.

And for us it began with a little bit of education and outreach with the SEC, just to make sure that they knew how we were thinking about things. We did a lot of work in the background with our lawyers to prepare and figure out what exactly needed to be done to have tokens comply with securities laws on the blockchain. And so step one was education.

And step two was we had to develop a little bit of technology to help these securities comply with the requisite laws while they're transferring on the blockchain. So we developed some technology called ERC-1404, which is a standard that is on the Ethereum blockchain primarily, but can be put to any blockchain. And that helps enforce some of the compliance requirements around transfers for publicly and privately registered—sorry—publicly registered securities, and private securities as well.

## Broader Tokenisation of Assets using Security Tokens (ctd.)

The TokenSoft platform's security tokens include:

- **Investor onboarding:** This reduces the time and cost of paperwork required to onboard new investors into a digital environment.
- **KYC/AML accreditation checks:** These are investor screenings for maintaining regulatory compliance.
- **Multiple payment gateways:** This allows payments to be made in cryptocurrencies, USDC, USDT, and USD wire transfers.

- **Admin dashboard:** This manages the lifecycle of a digital asset, including cap tables, lockups and vesting schedules.
- **Token issuance:** TokenSoft uses Ethereum's ERC-1404 token standard, an open-source standard for security tokens (ERC-1404, n.d.).

The standard enables issuers to identify token holders and maintain a whitelist of wallet addresses while also applying transfer restrictions for public and private offerings.

TokenSoft is blockchain agnostic, which means it can support a range of blockchain networks outside of Ethereum, such as Blockstream Liquid, CommerceBlock, Hyperledger, Corda, and Tezos. Corporate actions such as permission-based issuance of dividends and burning or minting new tokens can all be done on the platform.

The company is also making inroads into the DeFi space with the launch of Wrapped.com, which allows institutions to “wrap” assets like bitcoin into an Ethereum smart contract which entities can use to generate yield or borrow new assets on DeFi protocols (Kuznetsov, 2019).

### Distributed Ledger - Business Models

BaaS (Blockchain as a Service) model - Charge subscription fee for clients to operate on distributed ledger.

Offer real-time analytics services to identify risks and ways to optimise ledger operations.

Earn fees from distributed ledger transactions.

Charge fees to tokenise assets.

## Faculty Video: The Problem with Tokenisation in Respect of Properties

In this guest speaker video, Andrew Baum, Professor of Practice at Saïd Business School, University of Oxford describes the problems with tokenisation with respect to properties.



The problem with tokenisation, particularly in respect of individual properties and splitting them into small pieces, is that it requires several major steps to go from where we are now to where we might want to be in the future. So the first step, for example, involves understanding how blockchain works, believing in it, accepting that it is immutable, not corrupt, not subject to fraud. And all of these issues need to be worked through by investors and by the investment market first thing.

The second thing is that the whole concept of fractionalising units and buildings needs to be accepted. There needs to be a proven demand for small pieces of big buildings. And that's, by no means, evident.

There have been several attempts in the past to split buildings into small pieces. They've usually fallen over through lack of demand. Sometimes they've been unfortunate because they've been launched at times when the market is about to collapse. So there is not that proven market. It may exist, but it's not proven.

And thirdly, there's the whole regulation piece. And it is often an attractive idea to tokenise a piece of art or a racehorse or even a building, thinking that you can stay outside the system, particularly if you're interested in

using cryptocurrency. But the fact is that a tokenised investment in a real estate asset will almost certainly be captured by real estate, by investment regulations. And you'll be talking about some sort of security, which will be regulated. So it doesn't work on that particular ground. It's just the same as anything else.

And then fourth, the fourth issue is that-- and this is the key one-- is that it's technically not possible to tokenise a building by splitting it into small pieces. You can't-- the whole concept is nonsense when you think about it. What you can split into small pieces is a company or a partnership or some sort of legal entity that owns the building.

So again, this idea that you can fractionalise a building is somewhat utopian. What you can do is unitise the vehicle which owns the asset. And again, that takes you back into the traditional world of real estate investment, where you have a REIT company, a property fund the partnership, or so on.

So we have to go through this pain process. If there is a proven demand for units and buildings, we've got to still go through the pain process of setting up a legal entity, getting the entity regulated, and understanding blockchain before we can really jump into this brave new world of tokenised assets.

## Compare Business Models Between Blockchain Use Cases

Blockchains incorporate many of the same business models used by SaaS providers, platforms and financial service companies. The main difference is that through decentralisation, customers, service providers and other stakeholders can benefit from the revenue that accrues to the network, either by owning the blockchain's token or by being a member of a private blockchain consortium.

Here are ways that entities can monetise each blockchain use case:

Compare Business Models Between Blockchain Use Cases		
Digital Scarcity	Payment Rail	Distributed Ledger
Collecting transaction fees from the trading of digitally scarce assets	Transaction fees from cross-border payments	BaaS (Blockchain as a Service) model - Charge subscription fee for clients to operate on distributed ledger
Lending or staking assets to earn interest	Providing stablecoin liquidity and charging fees to convert real fiat currency to stablecoins	Offer real-time analytics services to identify risks and ways to optimise ledger operations
Providing custodial services (wallets)	Stablecoin lending services	Earn fees from distributed ledger transactions
Generating revenue from price appreciation of underlying digital assets	Subscription service to operate stablecoin payments network with user accounts and crypto-to-fiat on and off-ramps	Charging fees to tokenise assets

## 2.4.6 Key Takeaways, References, and Additional Resources

### Key Takeaways

Let's review the key points of this section:

1. Distributed ledgers provide a method for tracking the history and origin of products, services or assets in a transaction.
2. Distributed ledgers offer a feasible solution for diamond authentication because they open up transparency, creating a digital trail back to the source of every diamond.
3. Distributed ledgers can alleviate fraud because of the fact that collateral for example can be recorded digitally, which offers transparency to all the parties involved.
4. Distributed ledgers use cryptography techniques such as zero-knowledge proofs to validate transactions, and clients of companies can interact and transact peer-to-peer without a centralised intermediary while accessing a transparent audit trail of communications and transactions to help with regulatory compliance, risk mitigation, and fraud prevention.

### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

#### 2.4.2 Distributed Ledger for Diamond Authentication

Dotson, K. (2021, 12 January). Everledger and Rare Carat use blockchain to boost transparency in diamond sales. *SiliconANGLE*. <https://siliconangle.com/2021/01/12/everledger-rare-carat-use-blockchain-boost-transparency-diamond-sales>

Everledger. (n.d.). Diamonds. <https://everledger.io/industry-solutions/diamonds>

Kimberley Process. (n.d.). What is the Kimberley Process? <https://www.kimberleyprocess.com/en/what-kp>

Ledger Insights. (2020, 15 July). Blockchain startup Everledger raises \$7m from UK gov, Tencent, updates diamond platform. <https://www.ledgerinsights.com/blockchain-everledger-raises-7m-uk-gov-tencent-diamond>

### **2.4.3 Distributed Ledger for Verifying Collateral**

CFI. (no date). Total Return Swap. *Corporate Finance Institute*. <https://corporatefinanceinstitute.com/resources/knowledge/finance/total-return-swap-trs>

Hetzner, C. (2021, 17 April). Here's how much the big banks have lost so far from the Archegos collapse. *Fortune*. <https://fortune.com/2021/04/27/heres-how-much-big-banks-have-lost-so-far-from-the-archegos-collapse>

McDowell, H. (2021, 16 July). The collapse of Archegos Capital Management. *The Trade*. <https://www.thetradenews.com/the-collapse-of-archegos-capital-management>

Schatzker, E., Natarajan, S., & Burton K. (2021, 8 April). Bill Hwang Had \$20 Billion, Then Lost It All in Two Days. *Bloomberg*. <https://www.bloomberg.com/news/features/2021-04-08/how-bill-hwang-of-archegos-capital-lost-20-billion-in-two-days>

### **2.4.4 Distributed Ledger for Indexing the World's Blockchain Data**

Jakub. (2021, 13 January). The Graph – Google Of Blockchains? *Finematics*. <https://finematics.com/the-graph-explained>

### **2.4.5 Tokenisation Distributed Ledger**

Bank for International Settlements. (2019, 8 November). Statistical release: OTC derivatives statistics at end-June 2019. [https://www.bis.org/publ/otc\\_hy1911.pdf](https://www.bis.org/publ/otc_hy1911.pdf)

Bus, M. (2021, 13 January). Size Matters: Does Crypto Stack Up To Other Asset Classes? *Blockworks*. <https://blockworks.co/size-matters-does-crypto-stack-up-to-other-asset-classes>

Comdex. (2019, 25 April). Commodity Trading: Backbone of the global economy. <https://comdexofficial.medium.com/commodity-trading-backbone-of-the-global-economy-131c78f12989>

ERC-1404. (no date). ERC-1404: An open source standard for security tokens. <https://erc1404.org>

Grossbard, J. (2021, 9 June). 2021 Forex Statistics. *Compare Forex Brokers*. <https://www.compareforexbrokers.com/forex-trading/statistics>

ICMA. (2020, August). Bond market size. *International Capital Market Association*. <https://www.icmagroup.org/Regulatory-Policy-and-Market-Practice/Secondary-Markets/bond-market-size>

Kuznetsov, N. (2019, 26 October). Wrapped Crypto Tokens, Explained. *Cointelegraph*. <https://cointelegraph.com/explained/wrapped-crypto-tokens-explained>

Mitova, T. (2021, 6 August). 19+ AMAZING Stock Market Statistics to Know in 2021. *SpendMeNot*. <https://spendmenot.com/blog/stock-market-statistics>

TBRC. (2021, January). Real Estate Global Market Report 2021: COVID-19 Impact and Recovery to 2030. *BCC Research*. <https://www.bccresearch.com/partners/tbrc-market-briefs/real-estate-global-market-report.html>

Statista Research Department. (2021, 5 August). Art market worldwide - statistics & facts. *Statista*. <https://www.statista.com/topics/1119/art-market>

## Additional Resources

[What are Payment Rails?](#)

## 2.5 What Makes a Use Case Successful?

### 2.5.1 Introduction

#### How Blockchains Accelerate the Rise of the Collaborative Economy

The collaborative economy (or “sharing economy”) is an economic system that encapsulates peer-to-peer, peer-to-organisation, and organisation-to-peer exchanges (Ertz & Boily, 2019). Consumers rely on each other instead of large institutions to meet their wants and needs in such a system.

In recent years, technological advances in artificial intelligence, increasing amounts of generated data, augmented reality, and blockchain technology have enabled a rise in collaborative economic models. Platforms that adopt collaborative economic principles include Airbnb, Craigslist, and Uber—each platform relies on market participants offering and receiving products and services under a common theme or set of rules dictated by a centralised intermediary.

Legal contracts, accounting firms, insurance companies, and clearing houses are examples of intermediaries that traditionally enforce trust within collaborative economies. The use of blockchain technology enables collaborative economic models to operate at scale by cutting out the intermediary and eliminating friction associated with intermediaries.

Blockchains leverage what is typically open-source software to empower market participants to verify and enforce trust through programmable consensus. Following the shift from centralised gatekeepers to open and decentralised networks, some companies have begun embracing shared governance models between stakeholders and creating interoperable systems with other networks to maximise user growth and benefit from network effects.

Successful use cases for blockchain technology have the following traits in common:

- They emphasise ease of use.
- They are highly interoperable.
- They embrace shared governance.
- They employ network effects.

#### Vocabulary Check

This section introduces the following terms:

- [atomic swaps](#)
- [blockchain governance](#)

- [coopetition paradox](#)
- [cross-chain functionality](#)
- [crypto native users](#)
- [interledger protocol \(ILP\)](#)
- [interoperability](#)
- [network effect](#)
- [non-crypto-native users](#)
- [self-amending blockchain](#)
- [shared governance](#)

## Programme Director Video: What Makes a Use Case Successful

In the following video, Meltem Demirors describes what makes a good use case and what doesn't, and discusses the primary considerations to take into account in designing a blockchain technology solution.



Now the odds are if you've heard about blockchain technology, you've heard about a lot of different potential use cases. The blockchain industry has certainly been through its ups and downs. And over the years, I've heard of some great use cases for blockchain technology, like Bitcoin and cryptocurrencies, and also some really not so great use cases for this technology, for example, in tracking supply chains and other sorts of assets.

I want to talk quickly about what actually makes blockchain use cases successful. Now one of the important things to remember is that a blockchain ecosystem has a few key characteristics. At its core, a blockchain is a compute structure and a database in the form of a distributed ledger. What this means is there is an actual computational cost to maintaining a distributed ledger.

In the Bitcoin network, we have proof of work, which requires machines around the world performing complex computation. Other networks, like proof-of-stake, require people to post financial capital to ensure that they tell the truth in staking their assets. There are other forms of consensus as well, like proof-of-history or proof-of-authority, that also provide consensus in new and different ways, but all blockchains have a computational cost.

And so it's really important when selecting a blockchain use case to ensure that the data you're putting on a blockchain has actual value. If the use case, you're deploying can be fulfilled with a managed centralised database, you should probably reconsider the use of a blockchain. Because blockchains have a cost to operate, the data you're securing and the data you're computing with the blockchain should have real economic value to someone who is willing to pay for that transaction cost.

As you look at blockchain use cases, there are a few key characteristics that I think are important to success.

First is ease of use. Second is interoperability. Third is governance, and fourth is network effects. Now let's delve into each of those for just a moment, so you understand what that means.

Let's start with ease of use. When you're thinking about your blockchain use case and the stakeholders who are going to be participating in that use case, it's very important to think about how easy or challenging your solution will be for that end stakeholder. Now that doesn't always just mean technological challenges. That could also mean organisational challenges or structural challenges that would make it challenging for someone to operate your particular solution or product.

Second is interoperability. One of the really important elements of blockchain technologies is that they create open protocols and open-source software ecosystems that allow for extensibility of code through a protocol. Basically, what that means is, with a protocol, anyone can review the source code for that protocol and can utilise it to build on top of. Interoperability allows the interaction of protocols and the movement of assets or information between protocols.

For example, there aren't 10,000 internets. There's one internet with one set of protocols and standards that allow for a variety of different use cases and companies and services to proliferate on top of that global internet architecture. Similarly, I don't believe there will be 10,000 blockchains.

I believe there will be rich and diverse blockchain ecosystems, but they will all interact and interoperate to form one digital economy. So as you're building your use case, it's important to think about how you'll bridge in and out of various existing ecosystems and connect into them. The third consideration is governance.

How is your protocol or your blockchain use case going to be governed? Are there just a small number of participants who make all of the decisions and what happens in your blockchain use case? If the answer to this is yes, you should probably reconsider as to whether or not you need a blockchain, because you most likely don't.

You could probably use a managed database for something like that. But if your use case requires a large number of stakeholders to participate in this network and require some form of decentralised decision making, then that's an important consideration. How will this governance happen? What type of transparency will you enable?

How will decision making around resources in your blockchain use case happen? All of these are important considerations when you think about key stakeholders and how you structure decision-making in your particular use case. Lastly, network effects are really important to think about. And network effects are not just unique to blockchain use cases.

Obviously, the internet was a really important medium that facilitated massive network effects. Before the advent of the internet, the majority communication and marketing was done one-to-one. What the internet did is it allowed us to communicate and market one-to-many for the first time.

I could create one piece of collateral and get it to thousands, if not hundreds of thousands or millions, and now potentially 3 billion people, using this beautiful medium known as the internet. Blockchains also can have network effects. And it's a very important to think about some of the design choices you're making in your use case. If you're building on a proprietary blockchain that doesn't have a lot of interoperability or compatibility with other blockchain solutions, it might be difficult for you to see adoption of your use case, because it requires people utilising a whole new set of infrastructure.

So it's important to think about the network effects of what you're building and how you can leverage some of the existing momentum in blockchain ecosystems in order to increase the likelihood of success for your particular use case. Now when we look at blockchain use cases, we have a history to draw on to tell us and teach us what historically has and hasn't been successful. Cryptocurrencies have by far been the most successful use case of this technology.

And here's why. Cryptocurrencies are about communicating value. And people are willing to pay transaction costs in order to secure value. So, again, it's very important that the use case you're focused on involves some type of value exchange and people who have a willingness to pay for that value to be preserved.

If there's no value involved in the information you're facilitating or if there's no value involved in the use case you're pursuing, then again, you should likely reconsider whether or not it's a suitable use case for blockchain. There's also different models that people are utilising to build blockchain solutions. In the late 2010s, the idea of permissioned blockchains or walled gardens that were controlled by corporates or a small group of entities became very popular.

However, none of these so-called enterprise blockchains have really seen adoption. And here is why. A walled garden or permissioned blockchain is challenging to interoperate and suffers from a lack of network effects. By utilising public open blockchain infrastructure, entrepreneurs are able to tap into a much larger potential audience of users and also leverage some of the existing infrastructure of these blockchains to make it much easier to build their specific solution.

So as you're thinking about how to go about building your blockchain strategy and how to develop your blockchain use case, be very careful in thinking about the actual value that's being communicated and exchanged, who's willing to pay for it, and how it might be funded. Because again, if we are utilising compute and electricity or stake to secure these transactions, it's important that the information you're communicating is valuable to someone who will pay to have it secured.

## 2.5.2 Ease of Use

### Ease of Use

Non-technical and novice users have historically faced barriers to entry in using decentralised applications, setting up digital wallets, and transferring or securing their funds. In addition to the challenge of learning to use new apps, these users have faced negative experiences including lost funds due to forgotten login credentials (Popper, 2021; Ruth, 2021). Moreover, many of the security breaches in crypto have occurred because users were unaware of methods to store their private keys securely, the risks of clicking email links, or how to identify common scams (Powers, 2020). Developers of blockchain application user interfaces have sought to address these risks by developing security measures that protect these users, who are least likely to understand crypto security measures and most likely to fall victim to hacks.

## Appealing to Non-Crypto Native Users

In general, end users belong to one of the following categories:

- **Crypto native users (minority):** Those already interacting with blockchain-native platforms and services like Uniswap or Metamask.
- **Non-crypto native users (majority):** Those who will interact with decentralised applications for the first time with limited to no knowledge of the specific blockchain protocols that underpin them.

To address technical barriers that result in poor user experience, developers can seek to empower the average user to perform actions like making payments and taking or issuing loans without knowing or understanding what blockchain networks they are using to perform each function. This outlook can help companies develop frameworks around how to design consumer-facing blockchain products and services that cater to non-native crypto users.

An example of a blockchain application that achieved mainstream adoption from non-native crypto users is Celo.

### Celo

Valora is a mobile wallet for making global peer-to-peer payments with the support of Celo's Identity protocol. Instead of relying on public key addresses, which some non-native crypto users find confusing, the protocol allows users to send and receive payments using their mobile contact list (Celo Docs, n.d.).

### Guest Video: The Celo Design Process

In this video, cLabs' CTO & Co-Founder Marek Olszewski discusses how this solution came about and the back and forth process that goes into discovering what non-crypto native end users expect in terms of product usability.



Usability is just so important. And one of the things we discovered in these studies is that most people are just really intimidated by publicly derived addresses. They look funny to most people. They're long.

If you tell them that if they make a mistake with one character, the money is lost forever, it's just absolutely terrifying. And so to remedy this, we wanted to build off of an identity system that people knew and trusted today. And the one that overwhelmingly was the most popular were phone numbers.

And so people have phone numbers as identifiers. And they know how to use them. And more importantly, they have contact lists full of their friends and loved ones with all of these phone numbers already on their phones. And so to tap into that amazing social network—I mean it is this huge, massive social network, arguably bigger than Facebook that's also decentralised. We created a decentralised phone verification protocol, which allowed

people to not only securely verify their phone number, but also allowed then others to send payments to those phone numbers. And crucially, even before the recipient has created an account, which you can't do with Bitcoin or Ethereum.

Today, you need to create a publicly derived public address, which then gives you your account address. And you can't receive a payment until you have that. But with phone numbers, you can put the funds in an escrow smart contract. And the funds can automatically be claimed when you verified your phone number. And so we work just incredibly hard to enable this kind of functionality. And a lot of it came through this back and forth while building the mobile application, because we just discovered along the way that these were the things that people were expecting in their end-user experiences.

## 2.5.3 Interoperability

### Interoperability

Interoperability refers to the ability of different computer systems to connect and exchange information with each other without restriction.

To understand interoperability, it can be useful to think of a blockchain network as a giant city that generates millions of dollars in value, which residents exchange at a single location. Interoperable systems are the bridges, ferries, or other means of transport that enable newer and smaller cities to capture value from large areas that are thriving with activity, thereby increasing their competitive advantage and providing residents with the ability to consume a variety of products and services between cities with minimal friction.

As more blockchain networks emerge to solve problems for similar target markets, companies and developers are beginning to create “cross-chain” functionality that enables end users to transfer value and information across different siloed blockchain networks with as little friction as possible. Public and private blockchains have developed “oracles”, which are effectively gateways or bridges used to import external data that can trigger smart contracts.

### Different Approaches to Achieving Interoperability

Developers are using multiple approaches to create interoperability between private and public blockchains. The most common of these approaches include:

- **Atomic swaps** leverage smart contracts to facilitate the exchange of one cryptocurrency for another without the need for a centralised intermediary. An atomic swap can occur between two different blockchains or between a blockchain's on-chain and off-chain channels.
- **Relays** create interoperability by allowing one chain to verify information about a block and events on another chain. ConsenSys's BTC Relay open-source project is the most well-known example

of a relay that allows Ethereum contracts to verify Bitcoin transactions without any intermediaries with a high degree of security (Coleman, 2016). However, this method of achieving interoperability has historically been expensive to operate.

- **Merged consensus** enables two-way interoperable transactions to occur by using a relay chain. This interoperability method is conducted entirely on-chain instead of using side chains or other types of off-chain payment channels (Hammond, 2019). The drawback of a fully on-chain system for interoperability is that it must be built from the base layer of the blockchain and can be difficult to scale. Projects like Cosmos and ETH2.0 are currently utilising merged consensus (Hammond, 2019).
- For financial service providers that focus on private permissioned blockchains, the **interledger protocol (ILP)** offers a “cryptographic escrow” solution that connects blockchain ledgers from multiple banks to facilitate payments across different blockchain payment rails (Interledger Foundation, 2017). Hyperledger Quilt also leverages the interledger protocol to facilitate fiat and crypto payments across different parent networks (Hyperledger, 2017).
- Through the open-source contributions of Fortune 500 companies Accenture and Fujitsu, **Hyperledger Cactus** (formerly known as the Blockchain Integration Framework) has developed its own blockchain integration framework for enabling private permissioned blockchains to exchange information with each other (Klein & Montgomery, 2020; Kuhrt, 2019). Other blockchains that utilise this framework include Corda, Hyperledger Fabric, ConsenSys Quorum, and Hyperledger Sawtooth (Somogyvari & Montgomery, 2021).

## Interoperability in the DeFi Ecosystem

In the DeFi ecosystem, the recent success of new protocols like Solana and Binance Smart Chain have gained users by offering benefits such as lower fees and faster transactions. The Binance Bridge and Solana Wormhole enable users to seamlessly transfer cryptocurrencies from one blockchain network to the next in the same time it takes to transfer tokens within the same network (Cooling, 2021). While these networks compete, the ability to set up cross-chain functionality with the Ethereum network enables them to quickly capture large clusters of liquidity and user traffic from other DeFi-based protocols.

## Private/Public Blockchain Interoperability

Cross-chain functionality is especially critical for private blockchains. Private blockchains build bridges with public and other private blockchain networks to gain and maintain users, maintain updated records, improve user experience and establish a minimum threshold of transparency for stakeholders.

Examples of cross-chain functionality between private and public blockchains include:

- **Public ledger to private ledger:** Using digital assets hosted on DeFi protocols as collateral or showing proof of net worth to access certain traditional banking services (the bank could be part of a consortium on a private ledger that is interoperable with the Ethereum blockchain).
- **Private ledger to private ledger:** Enabling cross-chain verification of consumer data (such as age) between private hospital networks in different jurisdictions using ZKPs. Another example would be enabling cross-chain transfer of voting records from a private blockchain consortium of local governments to a private blockchain consortium of state and national governments to create multiple layers of authentication.
- **Private ledger to public ledger:** Achieving final reconciliation of transaction records of the public interest, such as metrics related to the global distribution of vaccines by a pharmaceutical company. Here, a private blockchain consortium consisting of vaccine manufacturers, distributors and hospitals could leverage cryptocurrency blockchains as a final settlement layer for vaccine distribution data for the public to verify.

Ultimately, cross-chain functionality between blockchain networks enables users to adopt multiple blockchain applications at once and engage in low-friction value transfers between disparate systems.

### 2.5.4 Shared Governance

#### Shared Governance

Blockchain governance centres around the means by which stakeholders achieve control, direction, and coordination within a blockchain network. Operating decentralised systems requires approaches towards governance that would not be applicable under a traditional corporate structure.

The lack of a centralised, hierarchical structure means that system operators must develop new forms of governance around three focal points:

- **Decision rights** are concerned with the rights that enable one to govern.
- **Accountability** capture the degree to which actors can be and are held accountable for their actions.
- **Incentives** highlight what motivates actors to take actions.

## Three Layers of Blockchain Governance

A 2021 research study by Utrecht University introduces a blockchain governance framework that defines the governance of a blockchain as a combination of three layers and six dimensions (Pelt et al., 2020). The layers are:

### Off-Chain Community

As the highest layer, the off-chain community layer is where participants address governance matters that occur in the real world, including methods for engaging with external stakeholders such as regulators, vendors, or the general public. Details about a project's mission and its relationship to the broader community are highlighted here. The Ethereum community and Tezos Foundation are examples of off-chain communities that bridge the real world and the blockchain networks they support.

### Off-Chain Development

The off-chain development layer is where relevant parties address governance matters in the real world that specifically relate to software development. This layer includes the roles and responsibilities of developers in maintaining the protocol, including recruitment, coordination, and organisational structure of development groups.

### On-Chain Protocol

The on-chain protocol layer is where relevant parties address governance matters that occur on the blockchain's underlying protocol. Examples include voting mechanisms, consensus mechanisms, and miner rewards. On-chain protocols are governed by decentralised autonomous organisations (DAOs). DAOs are made up of individuals who are part of and wish to participate in a public blockchain network's governance. These individuals help establish rules for mining rewards, network upgrades and other changes based on voting consensus.

## Six Dimensions of Blockchain Governance

The six dimensions of blockchain governance are:

- 1. Formation and context** – Encompasses a blockchain's background information, such as its purpose, launch style, ideology, and type of license.
- 2. Roles** – Describes the roles represented in each of the three governance layers. Each role exists on a hierarchy, with unique responsibilities and levels of accountability.
- 3. Incentives** – Explores the motivations behind the actions taken by each role based on the incentives present on the three governance layers. Important questions to ask include:

- What are the core motivations of community members?
- How are developers funded?
- Why should people want to operate nodes on the blockchain?

**4. Membership** – Describes how to manage membership and participation for each role. It covers whether the blockchain is open for anyone to participate or whether it requires permissions or certain access rights. Important questions to ask include:

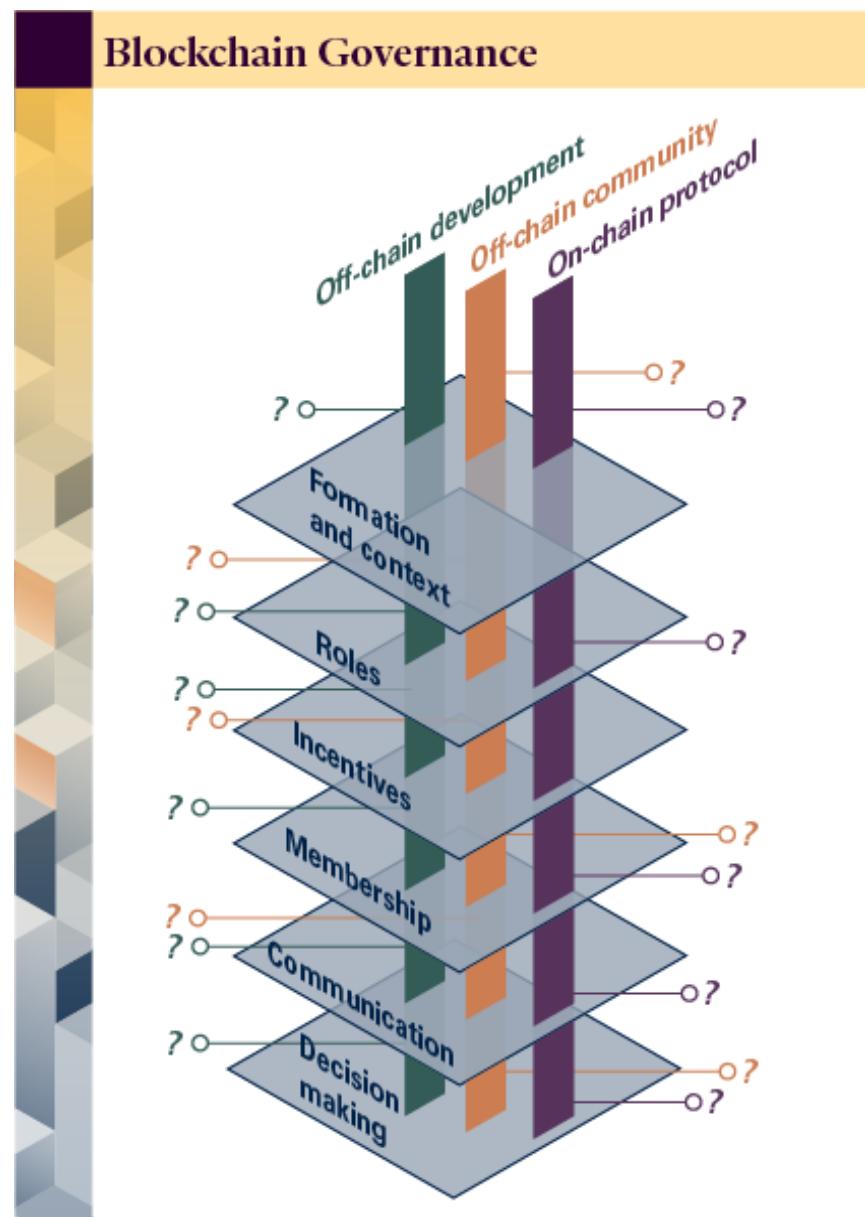
- What is the process for enabling new participants to join the network?
- Should new contributors be able to directly participate in the development process?

**5. Communication** – Covers the formal and informal methods of communication between blockchain stakeholders, including the available tools for communication (including coordination and tracking systems) and open discussion on public forums or in meetings and working groups.

**6. Decision making** – Describes how decisions are made and how consensus is achieved on each of the three layers of governance. It also looks at how the decision-making process is set up, including voting mechanisms, consensus mechanisms, and procedures for conflict resolution.

The six dimensions and three layers overlap with one another and provide guiding questions for how companies should assess their blockchain governance structure along with this framework (images adapted from: van Pelt, et al., 2020):

The blockchain governance framework is most useful for companies as a starting point for evaluating new blockchain projects, as a testing framework to analyse which existing blockchains to join, and as a checklist to confirm that certain aspects of the blockchain's governance have not been forgotten.



# Blockchain Governance Roles

## *Ethereum governance roles*

### **Off-chain development**

token holders  
Ethereum Foundation  
industry organisation  
fellowships  
community figureheads  
online moderators

### **On-chain protocol**

miners      full nodes      lightweight nodes

Off-chain community  
contributors  
maintainers  
EIP editors

## *EOS.IO governance roles*

### **Off-chain development**

token holders  
EOS Alliance  
block producer teams  
Block.one  
online moderators  
voter proxies

Off-chain community  
contributors  
maintainers

### **On-chain protocol**

block producers  
non-producing nodes  
API nodes  
seed nodes

## Governance on the Tezos Blockchain

The Tezos blockchain network, which became accessible upon initial release in 2018, is an open-source, decentralised platform for building dApps. Tezos is similar to Ethereum in its ability to build dApps using smart contracts. However, it distinguishes itself from Ethereum through its on-chain governance, which empowers holders of XTZ—the platform's cryptocurrency—to vote on the network's future direction (Abra, n.d.).

### Guest Video: The Tezos Use Case

In this video, Kathleen Breitman, the Co-Founder and CEO of Tezos, explains the Tezos use case.



Tezos was born out of the observation that Bitcoin lacks a mechanism to upgrade itself. Back in 2013, there were a lot of projects that were launched, Litecoin, the first proposal for Zcash. And they were all proposed as new blockchains, because there was no way for Bitcoin to fold in any new innovations in a coherent way. That's the paradox of having an open system, is that sometimes it's hard to formalise things, like governance.

And so Tezos was basically made to have a formal mechanism to upgrade the protocol without having ambiguous politics around it and, rather, instead, have token holders basically have their views expressed in the polity of the network, explicitly. So that's the origin story.

And then there's a few other things that Tezos wanted to innovate on, so this is all captured in the position paper which is from 2014, so again, 2013-2014. And one of them is basically having a formal governance process—that's probably the most notable—but also having an emphasis on formal methods when creating smart contracts, so an emphasis on security. These things are meant to underpin hundreds of millions of dollars—why not use the same type of rigour that people in Aeronautics use, for example? So basically an emphasis on security in the architecture of the blockchain. So I would say those are two key principles.

## Governance on the Tezos Blockchain

Tezos bills itself as the first “self-amending” blockchain. The platform adapts and adopts new features natively and automatically via its on-chain governance mechanism, which oversees the protocol amendment process, codifying procedures for every cycle of changes. To enable this capability, the developers programmed Tezos blockchain to go through every upgrade proposal and act according to the correlating voting steps—crucially, without a centralised director (Goodman, 2014).

Potential protocol upgrades are proposals from “bakers”, who are frequently developers. The system automatically collects all proposals and then presents them to the bakers, who cast their votes. The vote of a baker represents a wider group of users, and the number of tokens behind the baker's node dictates the strength of their vote. In a digital edition of democracy, community members can move their XTZ tokens into the node of whichever baker's vote aligns with their own ideas for the network's future without transferring ownership of the currency (Breitman, 2021).

For off-chain governance, Tezos set up the Tezos Foundation in Switzerland shortly after its 2017 ICO. The foundation's stated mission is to promote the Tezos protocol through grants and other capital deployment vehicles (Tezos Foundation, 2021).

The Foundation Council oversees Tezos' mission and is responsible for the management and administration of foundation assets. At the time of writing, the council manages 1.2 billion in assets and has issued 62 grants across 27 countries (Tezos Foundation, n.d.). Alongside several other committees, including an executive committee, audit committee, investment committee, technical advisory committee and nomination and remuneration committee, the council defines the foundation's forward movements. The Tezos blockchain's original architects, Arthur and Kathleen Breitman, continue to influence the foundation, with Arthur currently sitting as a foundation council member alongside eight others.

## Private Blockchain Shared Governance Framework

Companies often join a private blockchain network to consolidate resources and share data and infrastructure that can ultimately reduce costs and make business processes more efficient. Private blockchain networks straddle the fence between traditional legal structures and the digital world of blockchains, where "code is law". These networks often include members competing for the same customers or collaborating across industries to achieve some mutual benefit.

An example of competitors coming together can be seen in shipping companies, including CMA CGM and Mediterranean Shipping Company S.A., joining IBM and Maersk's TradeLens platform to share shipping data (Wolfson, 2020). By collaborating on the platform, all members gain real-time insights intended to them in optimising business operations.

International law firm Bird & Bird structured a framework for private blockchains to operate under that encapsulates many of the same principles that the Utrecht University study highlights (Bird & Bird, 2019; Bird & Bird, 2020). According to Bird & Bird, to establish a fair governance model between collaborators and competitors, private blockchains should form through a joint venture (JV) where each member owns a share in the legal entity.

The joint venture's goal is to act as a trustworthy intermediary that establishes specific rules for governance around the data and technology that the network creates and utilises. The venture will typically develop the software that underpins the private blockchain or license this software from service providers like R3 or ConsenSys. The nodes that validate transactions on the private network would be run by the conglomerate in the joint venture and possibly other subcontractors linked to the consortium.

On the application layer of the private blockchain, the joint venture parties have to build the app that connects to the nodes via API and interfaces with end users (consortium members, business value chain stakeholders, customers) whose transactions will be recorded on the blockchain.

Hybrid blockchains that combine public and private blockchain features might allow participants who are not members of the consortium to set up the nodes with limits on their access rights, such as the ability to access certain data about transactions but not to validate the transactions.

This implementation can increase transparency for external stakeholders like users or regulators while maintaining network control and without compromising important private data, such as pharmaceutical companies or food suppliers. Ultimately, the successful implementation of any blockchain solution depends on multiple, often competing, parties collaborating within the same blockchain network and achieving shared governance.

The more participants that exist on a shared ledger, the more the ledger can enable more efficient and transparent sharing of information, leading to cheaper cost structures for all participants. For example, TradeLens shipping partners can pay less for traffic data because they have access to each other's trading routes via a shared ledger, reducing the need for the costly and time-consuming printing of paperwork (TradeLens, 2021).

## Coopetition Paradox

A challenge that must be resolved for members to achieve shared governance is the coopetition paradox (Carson et al., 2018). The coopetition paradox describes how natural competitors must work together to achieve shared governance in a blockchain network while remaining competitive.

While the traditional business environment rewards the creation of competitive advantages and a winner-take-all mentality, successfully operating a blockchain network requires entities to accept a limited share of the pie from the onset. In turn, the value that comes from effective coordination and collaboration to achieve shared governance can ultimately be much larger than what each entity could have attained on its own.

When members operate in fragmented markets, delegating final authority over decisions on how the blockchain's system, data, and investments will be led and managed to an industry body or regulator can reduce disagreement among members. These intermediaries can serve the role of keeping all network members aligned in their strategic goals as the network grows and priorities change.

## Governance and Structuring Considerations in Blockchain Consortia

A recent article by Deloitte highlights four key considerations that organisations make in the early stages of developing a blockchain consortium (Massey et al., 2020):

1. Decision-making authority
  - How do members accurately classify decisions?
  - Which members can make decisions or have decision-making rights?
2. Funding and revenue-sharing
  - Which members are responsible for funding the consortium?

- How are funding commitments distributed between members? Do members who provide greater funding have more voting rights?

### 3. Legal entity structures and risk

- Will there be a separate legal entity established for the consortium? What jurisdiction will this entity be in?
- How are tax liabilities handled between members? Which members are in charge of financial reporting and accounting for the registered legal entity? How does the underlying blockchain technology enforce this?

### 4. Identification and ownership of intellectual property (IP)

- What are the relevant types of IP in the consortium?
- Who owns the IP, and how much is shared?
- How will current consortium members be compensated for the value of IP developed by newer members?

These considerations highlight the planning required to set up a private consortium blockchain. Members are typically involved in business for several years and adjust to governance rules based on changes in the external business environment and internal membership structure. Controlling members of the consortium often seek to establish themselves within their respective industries to help create stability among the group.

## Further Exploration: BIPs & EIPs

The process for proposing new changes to the Bitcoin network is called a Bitcoin Improvement Proposal (or BIP). There are three types of BIPs: Standards Track, Informational, and Process (CoinMarketCap, 2021).

- Standards Track BIPs request changes to the underlying protocol or methods for validating transactions on the Bitcoin blockchain.
- Informational BIPs are created to raise awareness of an issue, but do not request changes.
- Process BIPs request process changes outside of the Bitcoin protocol, such as changes to guidelines or tools (Franco, 2019).

Informational BIPs do not require an in-depth review process, and can be accepted or ignored, much like entries on Wikipedia. Standards Track and Process BIPs require a draft to first be proposed (a process called “triaging”), which can be either accepted, rejected, deferred, or withdrawn. If accepted, it must be considered and requires community consensus in order to pass.

BIPs can be used for making decisions about important issues like hard or soft forks, such as SegWit, which was a soft fork proposed under BIP 141 (Bitcoin Core, 2021).

The Ethereum community utilises standards to keep this protocol interoperable across implementations. Anyone can submit an Ethereum Improvement Proposal (EIP) which is then discussed by community members. The EIP must include the technical specifications and rationale of the proposed changes. The author is expected to build consensus in the proposed improvements.

There are three types of EIPs:

- Standards Track EIP is a broad category that includes changes to the network protocol, block or transaction validity rules, or any modification that affects interoperability of applications using Ethereum.
- A Meta EIP proposes changes to the areas around Ethereum, other than the Ethereum protocol itself. They might include modifications to the procedures or the tools used in development. This is also considered a Process EIP.
- An Informational EIP does not propose changes to the protocol but provides general guidelines or outlines a design issue. This type of EIP does not require consensus (Becze, Jameson, 2015).

The two largest blockchain platforms, Bitcoin and Ethereum, utilise different methods for accepting new proposals but achieve common goals—to protect, enhance, and secure their decentralised networks.

## 2.5.5 Network Effects

### Network Effects

The network effect is a phenomenon whereby larger numbers of users or participants increase a service's value. One example of this is the internet, which was originally a resource of the military and scientists. Eventually, the platform became more accessible to the general population, who swiftly began creating more content, information, and online services. As the amount of content and services scaled, so too did the number of users connecting and communicating with each other—further increasing the amount of content and services.

Blockchains that capture network effects could experience similar gains in user and revenue growth through transaction fees and other business models. However, unlike the internet, where users contribute valuable data on platforms that subsequently own and profit from this data, a blockchain network redistributes the monetary value back to the users who hold the relevant network's token. In theory, empowering individuals through redistribution incentivises user adoption.

If, for example, a public blockchain existed for exchanging exclusive licenses to musical recordings, and had only a small number participants, the blockchain would lack information, and users would have to explore external data sources to verify ownership of works to be able to execute licensing transactions. As more participants join the network and more transactions occur, the network will accumulate more data about music rights ownership, eventually forming a parallel database that can become as robust as the external sources.

The issuance of cryptocurrencies that represent the value of a blockchain network is perhaps the strongest driver of network effects, as it gives users a direct monetary incentive to grow the network. A cryptocurrency holder is essentially a shareholder of the cryptocurrency's respective blockchain network. As more market participants purchase the network's token, the token's price will rise, and so will the collective wealth of all token holders—this incentivises cryptocurrency owners to not only contribute to the network by participating in mining, staking or voting, but also to promote the network to their friends and associates.

## Metcalfe's Law

Metcalfe's Law, a theory by the founder of Ethernet technology, Robert Metcalfe, suggests that a network's value is directly proportional to the square of the number of its nodes (users, in this case). Academic studies on large companies including Facebook, Google, and Tencent have given Metcalfe's opinion empirical support.

Successful blockchain solutions require a large enough number of participants exchanging and verifying information within the same network to accrue sufficient data for the next wave of participants to gain value from the blockchain (Blockchain, n.d.). This means that in theory:

- Twitter's value as an information network for the 100 millionth user is greater than the value was for the 100 thousandth.
- At a hash rate of 136m TH/s, the security of Bitcoin's network is more robust for a buyer today than it was for a buyer in 2013 when the hash rate was just 22 TH/s (Blockchain, n.d.). (Hash rate is the total amount of computational power that is being used to mine and validate transactions on the Bitcoin blockchain. The more miners participate in the network, the greater the hash rate, and the more secure the network.)

Although private, permissioned blockchains have advantages that include increased protection of IP, they cannot capitalise on network effects: These blockchains limit participants, leading to less data accumulating on the blockchain.

The failure of private intranet networks as compared to the internet is an example of this phenomenon. By comparison, the internet's open-source architecture encourages the existence of collaborative communities that freely share knowledge, typically leading websites to publish frequently updated content that has high user ratings and to improve the user experience based on feedback.

To mitigate these challenges, private blockchain networks like HyperLedger and Corda have built interoperable systems that enable cross-chain functionality with other public and private blockchains to retain the benefits of privacy while avoiding the pitfalls of permissioned networks (Hyperledger, 2020; Corda & Skuchain, 2020).

## 2.5.6 Key Takeaways, References, Additional Resources

### Key Takeaways

Let's review the key points of this section:

1. The key characteristics that are important to a blockchain use case success are ease of use, interoperability, shared governance, and network effects.
2. Ease of use can lead to both increased adoption and increased security, as non-technical and novice users interact with the blockchain more easily and developers include mechanisms to protect these users.
3. Interoperability refers to the ability of different computer systems to connect and exchange information with each other without restriction. Cross-chain functionality enables users to transfer value and information across different siloed blockchain networks with as little friction as possible. Approaches include atomic swaps, relays, and merged consensus.
4. Blockchain shared governance centers around the means by which stakeholders achieve control, direction and coordination within a blockchain network. The three layers of blockchain governance are off-chain community, off-chain development, and on-chain protocol. Shared governance also introduces the “coopetition paradox”, in which natural competitors must work together to achieve shared governance in a blockchain network while remaining competitive.
5. The network effect is a phenomenon whereby larger numbers of users or participants increase a service’s value, which then increases the number of participants. Metcalfe’s Law suggests that a network’s value is directly proportional to the square of the number of its nodes. Public blockchains can take advantage of network effects, while private, permissioned blockchains that limit participants generally do not.

### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 15 March, 2022.

#### 2.5.1 Introduction

Ertz, M., & Boily, E. (2019, December). The rise of the digital economy: Thoughts on blockchain technology and cryptocurrencies for the collaborative economy. *International Journal of Innovation Studies*. <https://www.sciencedirect.com/science/article/pii/S2096248719300426>

## 2.5.2 Ease of Use

Celo Docs. (2020, 24 August). Phone Number Privacy. <https://docs.celo.org/celo-codebase/protocol/identity/phone-number-privacy>

Popper, N. (2021, 12 January). Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes. *The New York Times*. <https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html>

Powers, B. (2020, 16 December). New to Bitcoin? Stay Safe and Avoid These Common Scams. *CoinDesk*. <https://www.coindesk.com/learn/2020/12/16/new-to-bitcoin-stay-safe-and-avoid-these-common-scams>

Ruth, C. (2021, 28 April). Blockchain hackers netted over \$100 million in Q1 2021. *Atlas VPN*. <https://atlasvpn.com/blog/blockchain-hackers-netted-over-100-million-in-q1-2021>

Shu, C. (2020, 10 December). Seoul-based payment tech startup CHAI gets \$60 million from Hanwha, SoftBank Ventures Asia. *TechCrunch*. <https://techcrunch.com/2020/12/09/seoul-based-payment-tech-startup-chai-gets-60-million-from-hanwha-softbank-ventures-asia>

Terra. (2019, 12 June). Terra partners with mobile payment app CHAI to service the growing eCommerce market. *Terra Money*. <https://medium.com/terra-money/terra-partners-with-mobile-payment-app-chai-29c593f0a364>

Terra. (2020, 7 April). Questions on Chai. <https://agora.terra.money/t/question-on-chai/220>

## 2.5.3 Interoperability

Coleman, L. (2016, 21 August). BTC Relay Bridges BTC With Ethereum, Allowing BTC Verification For Smart Contracts. *Capital & Celeb News*. <https://www.ccn.com/btc-relay-bridges-btc-with-ethereum-allowing-btc-verification-for-smart-contracts>

Cooling, S. (2021, 9 August). Wormhole 2.0 launches as cross-chain bridge connecting SOL, ETH, BSC, and Terra. *Coin Rivet*. <https://coinrivet.com/solana-wormhole-2-0-launches-multi-chain-upgrade>

Hammond, M. (2019, 9 August). Blockchain Interoperability & Cross-Chain Communication Series. *Matthew Hammond*. <https://medium.com/@mchammond/blockchain-interoperability-319bce3f9105>

Hyperledger. (2017, 16 October). Hyperledger Gets Cozy With Quilt. <https://www.hyperledger.org/blog/2017/10/16/hyperledger-gets-cozy-with-quilt>

Interledger Foundation. (no date). Interledger Protocol (ILP). <https://interledger.org/rfcs/0003-interledger-protocol>

Klein, M., & Montgomery, H. (2020, 13 May). TSC Approves Hyperledger Cactus as New Project. *Hyperledger*. <https://www.hyperledger.org/blog/2020/05/13/tsc-approves-hyperledger-cactus-as-new-project>

Kuhrt, T.A. (2019, 20 November). Accenture Open Sources Blockchain Integration Framework as a Hyperledger Lab. *Hyperledger*. <https://www.hyperledger.org/blog/2019/11/20/accenture-open-sources-blockchain-integration-framework-as-a-hyperledger-lab>

Somogyvari, P., & Montgomery, H. (2021, 31 March). Hyperledger Cactus: On the Road to General Blockchain Integration. *Hyperledger*. <https://www.hyperledger.org/blog/2021/03/31/hyperledger-cactus-on-the-road-to-general-blockchain-integration>

## 2.5.4 Shared Governance

Abra. (2017, 17 December) Tezos: A self-amending decentralized platform. <https://www.abra.com/cryptocurrency/tezos>

Bird & Bird. (2019, 8 February). Blockchain. <https://www.twobirds.com/en/in-focus/blockchain>

Bird & Bird. (2020, 10 July). Bird & Bird & Private Blockchains. <https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf>

Breitman, K. (2021, 13 July). Tezos: Superior Governance and Use Cases. *Cryptopedia*. <https://www.gemini.com/cryptopedia/what-is-tezos-xtz-governance-use-cases>

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018, 19 June). Blockchain beyond the hype: What is the strategic business value? *McKinsey Digital*. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>

CoinMarketCap. (2021, 9 January). Bitcoin Improvement Proposal (BIP). <https://coinmarketcap.com/alexandria/glossary/bitcoin-improvement-proposal-bip>

Franco, A. (2019, 24 June). Bitcoin Improvement Proposal (BIP). *Messari*. <https://messari.io/article/bitcoin-improvement-proposal-bip>

Goodman, L.M. (2014, 2 September). Tezos — a self-amending crypto-ledger White paper. *Tezos*. <https://academy.bit2me.com/wp-content/uploads/2021/04/tezos-whitepaper.pdf>

Massey, R., Prokop, M., Henry, W., Taylor, P., & Simpson, L. (2020, 15 May). Governance and structuring considerations in blockchain consortia. *Deloitte*. <https://www2.deloitte.com/us/en/pages/consulting/articles/blockchain-consortium-governance-considerations-models-standards.html>

Pelt, R.V., Jansen, S., Baars, D., & Overbeek, S. (2020, 9 March). Defining Blockchain Governance: A Framework for Analysis and Comparison. *Information Systems Management*. <https://www.tandfonline.com/doi/pdf/10.1080/10580530.2020.1720046>

Tezos Foundation. (2021, 15 March). Role of the Tezos Foundation. <https://tezos.foundation/about-us>

TradeLens. (2021, 17 June). TradeLens Digital Shipping Platform Adoption Grows in China. <https://www.tradelens.com/post/tradelens-adoption-grows-in-china>

Wolfson, R. (2020, 15 October). Global shipping leaders join IBM and Maersk blockchain platform. *Cointelegraph*. <https://cointelegraph.com/news/global-shipping-leaders-join-ibm-and-maersk-blockchain-platform>

## 2.5.5 Network Effects

Blockchain.com. (no date). Total Hash Rate (TH/s). <https://www.blockchain.com/charts/hash-rate>

Cipolaro, G., & Stevens, R. (2020, November). The Power of Bitcoin's Network Effect. *New York Digital Investment Group LLC*. <https://nydig.com/wp-content/uploads/2020/11/NYDIG-Power-of-Bitcoins-Network-Effect.pdf>

Corda., & Skuchain. (2020, 24 March). Trade Finance, meet Interoperability. *Corda*. <https://www.corda.net/blog/co-authored-by-skuchain>

Hyperledger. (2020, 28 May). Interoperability and Integration Developments in the Hyperledger Community. <https://www.hyperledger.org/blog/2020/05/28/interoperability-and-integration-developments-in-the-hyperledger-community>

Simpplr. (2019, 13 December). 90% of Intranets Fail: 5 Reasons the Intranet Industry Needs a Change. *CMSWire*. <https://www.cmswire.com/digital-workplace/90-of-intranets-fail-5-reasons-the-intranet-industry-needs-a-change>

## Additional Resources

[Tutorial - Blockchain basics: Introduction to distributed ledgers](#)

[Defining Blockchain Governance: A Framework for Analysis and Comparison](#)

## 2.6 Determining Suitability for a Use Case

### 2.6.1 Overview

#### Overview

When evaluating whether a blockchain technology solution is suitable for a business or project, there are important features to consider such as the true meaning of decentralisation, hard forks, soft forks, and public versus permissioned infrastructure. This section introduces a framework which can be used to assess blockchain technology requirements and a company's need for a blockchain-based solution.

#### Programme Director Video: Suitability for Use Case

In the following video, Meltem Demirors explains the suitability criteria when assessing blockchain technology use cases.



Now as you're building your use case, it's really important to remember that this technology is still in its early days. And it will continue to evolve as the overall space continues to evolve and the world continues to change. So as you think about specific features, don't worry if the features you're trying to build today aren't possible quite yet on open public networks.

Something that's really important to remember is there are two types of technology upgrades that can happen with blockchains that can help bridge some of the gaps here. The first is a hard fork. A hard fork is an upgrade to a protocol which is forward compatible but not backwards compatible. What that means is all transactions in the past remain as they are, but all transactions going forward necessitate usage of a new protocol or this new software upgrade.

A soft fork is different. A soft fork is an upgrade to a protocol that is both backwards and forwards compatible, meaning that you can use the new form of the protocol and its upgraded version to push through transactions. But the old code and the old way of running the protocol is still functional. Soft forks and hard forks are two important mechanisms that are utilised to upgrade blockchain protocols but also to enable compatibility and interoperability use cases. And you'll hear about some of these from various experts throughout this programme.

Now another element that you might think about as you're building your use case is data privacy and confidentiality. For example, as I've talked about before with Bitcoin, transactions on the Bitcoin network are not anonymous, but they are pseudonymous. And what this does is it lends a degree of privacy to people who are transacting on the Bitcoin network.

However, all Bitcoin transactions are public domain and can be viewed using a block explorer, which allows you to query the Bitcoin blockchain. If you're deploying a use case where privacy really matters or where something like trade secrets, let's say, are being transferred, then it might be important to include privacy-preserving features in your specific blockchain use case.

In fact, there are a number of cryptocurrency protocols out there today who enable various types of anonymity in order to preserve privacy and transactions. So as you're thinking about some of these trade-offs, it's important to think about whether or not your stakeholders might have concerns about privacy or anonymity that would need to be preserved in order for you to be effective in implementing your use case.

Another thing to think about is public versus permissioned infrastructure. And this is a topic that's really hotly debated in the blockchain space. I want to introduce a concept here known as progressive decentralisation. The word decentralisation gets talked about a lot in the cryptocurrency space, but there's really no quantifiable way to measure decentralisation.

At the protocol level, decentralisation means having multiple reference implementations. It means having multiple developer communities working on the code. It means having a clear and transparent process for protocol upgrades. At the network level, it means having a sufficient number of nodes running the protocol, having those nodes be based in a variety of different geographies, having those nodes be run on a variety of different cloud vendor platforms or bare metal.

And at the currency level, decentralisation could mean having the token of your protocol be held by a really wide number of stakeholders. After all, if only four or five key entities hold 80% of the value in your protocol, is it really that decentralised? So again, decentralisation is not something that you can really quantify, but it's something you can qualify, and you can think about it in a progressive fashion.

Most blockchain use cases and most protocols, for that matter, start out highly centralised. And this is because most protocols have a founding team, a group of individuals behind it, and an early community that helped bootstrap that protocol. But over time, most blockchain projects take steps towards progressive decentralisation. And what this means is they take steps to remove central points of control or central points of vulnerability.

Now one of the last features I want to talk about is probably not the sexiest, but it's very relevant to what we're doing in this programme. It's important to remember that blockchain technology doesn't exist in a vacuum. And at the end of the day, all of us are, I hope, law-abiding citizens and subject to some of the rules and regulations that exist in capital markets and in our relevant jurisdictions today.

It's very important that as you're designing your blockchain use case that you think about compatibility with rules and regulations in their current form. Now, there are certain exogenous variables or variables outside of your product or your use case that will be very difficult to control. And rules and regulations are one.

For example, someone might say, oh, this is a great use case, but rules and regulations will change. I would not bank on that. And as we've seen with regulators around the world, rules are very slow to change, particularly when it comes to capital markets and capital controls. So as you're thinking about your use case, make sure you take into consideration the existing regulatory regime around your specific use case, some of the entrenched interests that have led to those rules and regulations, and the likelihood of those rules and regulations to change in the near future.

I would not count on rules and regulations changing. And in fact, if anything, I would prepare for more scrutiny of blockchain technology, generally as financial regulators around the world are starting to become more and more concerned about potential systemic risk or financial stability issues that could be introduced by wider utilisation of cryptocurrency and blockchain protocols.

## Vocabulary Check

This section introduces the following terms:

- [double ledger accounting](#)
- [medium of exchange](#)
- [store of value](#)
- [unit of account](#)

### 2.6.2 Framework for Assessing a Company's Need for a Blockchain-Based Solution

#### Framework for Assessing a Company's Need for a Blockchain-Based Solution

Analysing current and successful applications can help companies develop a framework for assessing their potential blockchain technology requirements.

Specific criteria should be met for there to be a valid use case for blockchain technology. Knowing when a company does not need blockchain technology is just as important as understanding when it does.

Blockchain technology is most useful when multiple parties rely on an intermediary to establish trust to exchange value (information, money, assets) or verify that certain information is correct and unchangeable. As you learnt in Module 1, blockchains rely on consensus protocols for the network of nodes to agree on the validity of each new transaction before it is uploaded on a permanent ledger.

Examples of use cases where blockchain technology could add significant value to participants include:

- Exchanging money across borders for goods or services for which the quality or origin cannot be easily verified.
- Transporting goods across multiple jurisdictions where details about the methods of production, transportation and storage of those goods must be verifiable by all stakeholders involved.
- Trading, storing and assigning an agreed-upon value to digital assets based on verifiable scarcity.

In each example, blockchain technology (payment rails, distributed ledgers, and digital scarcity, respectively) replaces intermediaries such as banks, lawyers, or governments with a decentralised, secure, transparent and immutable database that all participants in a transaction have access to. Participants such as lenders, suppliers, clients or investors can verify the data about an asset or transaction simultaneously and in real-time.

## 2.6.3 Six Questions

### Six Questions

When evaluating a use case for blockchain technology, you could also ask yourself the six questions in the book *Basic Blockchain: What It Is and How It Will Transform the Way We Work and Live* (Shrier, 2020):

**1. Is the process I am trying to apply a blockchain solution to one that is repeatable or can be automated?**

A repeatable process that requires an intermediary can be costly. If the role of the intermediary can be partially or fully automated by computer code while maintaining the same or a higher level of trust, then transactions can occur at scale, leading to significant improvements for the business. An example of this would be to replace multiple legal contracts written for different parties with a single, smart contract that would automate compliance by storing the parties funds in the smart contract and only releasing them once certain verifiable conditions are met (a loan is repaid, an item is delivered, and so on).

**2. Will this solution be applied only once? Or will it be part of an ongoing process?**

One-time transactions do not warrant the effort of developing a blockchain solution. Companies should only develop a blockchain solution to apply it to a part of the ongoing and integral business, such as tax reporting, supply chain management or payment processing.

**3. Are there multiple stakeholders involved in the process, and is it already easy for you to verify that each participant is acting honestly?**

The more stakeholders involved in the business value chain, the more important it is to consider a blockchain solution. Blockchain technology can help companies mitigate the risk of conflict between multiple parties with different drivers; this is particularly important when stakeholders operate anonymously, do not operate within the same legal jurisdiction, or if the costs of enforcing legal action are higher than the potential losses incurred.

If, however, a company's extended value chain features third parties working in alignment, with strong relationships and a level of interdependency between them, there's no need to implement a decentralised system—centralised alternatives will suffice.

**4. Are multiple parties involved in reconciling the different types of data that accumulate throughout the business value chain?**

One example would be a multinational bank that uses different accounting standards to record transactions in various jurisdictions. Reconciling these transactions from multiple siloed databases can be timely and costly. Additionally, if a central authority performs transaction reconciliation, it can create room for errors or corrupt activities due to a lack of transparency.

Blockchains empower entities to reconcile transactions in real-time. When a transaction is confirmed, it is recorded by all nodes on a shared ledger using the same format and standards. Each node on the network has access to the same data and can reach consensus on the final reconciliation.

### **5. Is something of value being transferred between stakeholders (for example, information, money, assets, and so on)?**

It is important to use blockchains to record the transfer and accounting of valuable elements to justify the costs and effort in implementing a blockchain. The more value exchanged, the more trust is required to maintain the integrity of the data that reflects that value, thus making a blockchain solution more useful.

### **6. Is it essential for all records of transactions between stakeholders to be permanent? Would the ability to revise past transactions have a negative impact on stakeholders?**

The purchase of a house or a second-hand car are two examples of transactions that require an immutable history of prior modifications to accurately assess their present value. If these records can be edited, bad actors can misrepresent the value of the sold items.

Individuals and companies can use these six questions to determine whether a blockchain solution is right for their business. Once these questions have been answered and you believe blockchain technology is likely a good solution for your organisation, you will need to ask more profound questions about functionality, regulations, costs, financing, talent, partnerships and internal stakeholder incentives.

All of the questions and considerations will be examined more closely in Module 5.

## **2.6.4 Key Takeaways, References, Additional Resources**

### **Key Takeaways**

Let's review the key points of this section:

1. Two types of technology upgrades can happen with blockchains to bridge some existing gaps, including a hard fork and a soft fork.
2. A hard fork is an upgrade to the protocol, which means the transactions in the past remain as they are, but the future transactions use the upgrade or new protocol.
3. A soft fork is an upgrade to a protocol that is both backwards and forward compatible.
4. The privacy and confidentiality of entities should be a consideration because the pseudonymous features of blockchain technology allow privacy, but all bitcoin transactions (that is, all transactions on public permissionless networks) are in the public domain on an immutable ledger for all to see.

5. Public versus permissioned infrastructure can make a difference in suitability for a use case because most blockchain technologies and protocols start centralised. Over time, many blockchain projects take steps towards progressive decentralisation to remove central points of control or vulnerability.
6. When designing a blockchain use case, organisations should think about compatibility with rules and regulations in their current form, even though they may change in the future.

## References

### 2.6.3 Six Questions

Shrier, D.L. (2020, January). *Basic Blockchain: What It Is and How It Will Transform The Way We Work and Live*. Robinson.

## Additional Resources

[Architecting Enterprise Blockchain Solutions](#)



**Module 3:**

# Landscape: The Blockchain Ecosystem & Stakeholders

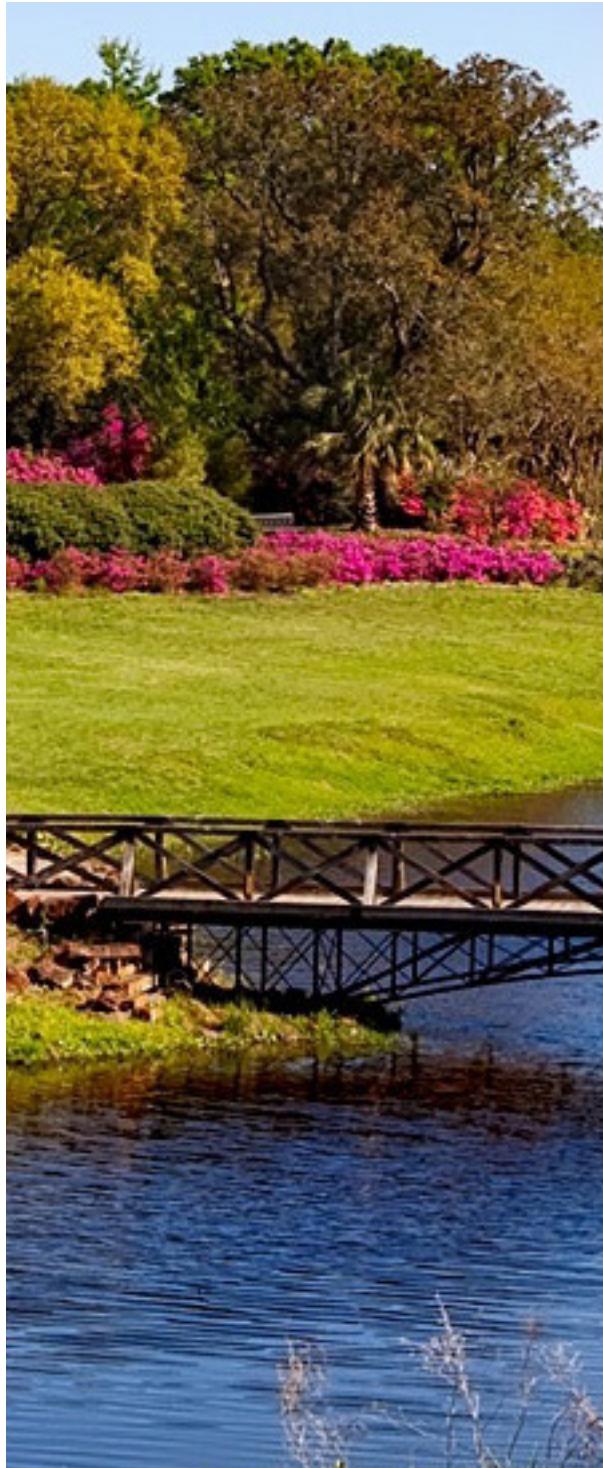
---

**Oxford Blockchain Strategy Programme**  
2022

# Oxford Blockchain Strategy Programme

## Module 3: Landscape: The Blockchain Ecosystem & Stakeholders

### Table Of Contents



<b>3.1 About Module 3</b>	<b>3</b>
3.1.1 Overview of Module 3	3
<b>3.2 The Cryptocurrency and Blockchain Technology Ecosystem</b>	<b>6</b>
3.2.1 The Cryptocurrency and Blockchain Technology Ecosystem	6
3.2.2 Industry Organisations	9
3.2.3 Developers	9
3.2.4 Operators	11
3.2.5 Governing Bodies and Advocates	12
3.2.6 Rounding Out the Ecosystem	12
3.2.7 Key Takeaways, References, and Further Exploration	14
<b>3.3 Internal Stakeholders in the Blockchain Technology Ecosystem</b>	<b>17</b>
3.3.1 Overview of Internal Stakeholders	17
3.3.2 Internal Stakeholders	18
3.3.3 Key Takeaways and References	21
<b>3.4 External Stakeholders: Roles, Incentives, and the Marketplace</b>	<b>22</b>
3.4.1 External Stakeholders: Roles, Incentives, and the Marketplace	22
3.4.2 Competitors	25
3.4.3 Corporations and Enterprises	27
3.4.4 Influencers	28
3.4.5 Venture Capital and Institutional Investors	30
3.4.6 Key Takeaways, References, and Further Exploration	31
<b>3.5 External Stakeholders: The Regulatory Environment</b>	<b>34</b>
3.5.1 External Stakeholders: The Regulatory Environment	34
3.5.2 General Public	35
3.5.3 Policymakers and Governments	37
3.5.4 Academic Institutions	39
3.5.5 Journalists and Media	40
3.5.6 NGOs and Global Institutions	41
3.5.7 Key Takeaways, References, and Further Exploration	45
<b>3.6 Stakeholder Considerations</b>	<b>48</b>
3.6.1 Overview of Stakeholder Considerations	48
3.6.2 Internal and External Stakeholder Considerations	48
3.6.3 Key Takeaways	50
<b>3.7 A Framework to Engage with Stakeholders</b>	<b>52</b>
3.7.1 Overview of a Framework to Engage with Stakeholders	52
3.7.2 Stakeholder Mapping Exercise	53
3.7.3 Developing a Stakeholder Engagement and Communication Plan	54
3.7.4 Key Takeaways	55
<b>3.8 Case Study: LO3 Energy</b>	<b>56</b>
Case Study: LO3 Energy	56

# 3.1 About Module 3

## 3.1.1 Overview of Module 3

### Overview

Welcome to Module 3 of the Blockchain Strategy Programme!

In Module 3, you'll explore the key players in the cryptocurrency and blockchain technology ecosystem, their roles, and their influence in this industry. You'll also identify the most relevant internal stakeholders involved in your project, business, or organisation, as well as the external stakeholders that are key to developing a blockchain technology solution.

You'll study the following concepts in this module:

- The diverse nature of the blockchain and cryptocurrency ecosystem.
- Who the internal, external, and industry stakeholders are, including real-world examples of who they are and the influence they have.
- Important considerations to think about and address when considering and implementing a blockchain technology solution.
- The key elements that make up a framework to engage and communicate with important stakeholders.

Module 3 will prepare you to analyse important internal, external, and industry stakeholders when developing blockchain solutions and help you develop a framework to engage them. By exploring the LO3 Energy case study, you'll learn about the stakeholders that one company engaged with to develop a blockchain-enabled solution.

### Programme Director Video: An Introduction to the Blockchain Technology Ecosystem and Stakeholders

In the following video, Meltem Demirors describes what to expect in this module and walks you through the subjects you will learn about this week.



Welcome back. I'm excited to introduce you to module 3 of the Oxford Blockchain Strategy Programme. In this module, we're doing something really unique. We're going to introduce you to the rich and diverse ecosystem and different stakeholders that are members of the blockchain community.

You'll hear from technologists, entrepreneurs, and corporate innovators who work with a variety of different stakeholders, whether they're their own team members and people internal to their business, the external market, peers, competitors, clients, or institutions, governments, and academia. You'll hear from these entrepreneurs and innovators how they're working to engage with these different types of stakeholders, and how they think about communicating the benefits of their specific use case. I hope you'll leave this module with a better understanding of the blockchain ecosystem and the wide range of different stakeholders that are a part of it.

## Learning Outcomes

By the end of this module, you will be able to:

- Identify the key players in the cryptocurrency and blockchain technology ecosystem.
- Develop a stakeholder engagement and communication strategy for a specific blockchain project.
- Compare the incentives, organisational dynamics, and competitive dynamics between blockchain stakeholders.

## Graded Assignments

You will complete individual and group assignments, which count towards your completion of the programme. This week, you will:

- Complete a quiz on the module's content and key takeaways.
- Reflect on what you have learnt by applying it to your personal or professional experiences.

You must submit all graded assignments in Module 3 by **28 June 2022, 23:59 UTC**. (Try the [Time Zone Converter](#) to get your local time.)

## Additional Activities

In each module, we present additional activities related to the core learning. This week, you will:

- Meet with your group to discuss the stakeholders that are relevant to your blockchain project and assess their influence and interest in it to create an engagement strategy. Start thinking about potential challenges that could impact your blockchain use case.
- Share your thoughts with the class on the LO3 Energy case study, the stakeholders that were essential for a successful launch, and why stakeholder planning and engagement is essential.

## Time Commitment

Plan to spend seven to ten hours on Module 3 this week. As there is much reading material, and many videos, you might want to divide your work into several sessions. The module is broken up into sections by theme, giving you potential break points.

Make sure you plan time to meet with your group, and to complete the assignments.

## 3.2 The Cryptocurrency and Blockchain Technology Ecosystem

### 3.2.1 The Cryptocurrency and Blockchain Technology Ecosystem

#### Quick Fact

The market is no stranger to high growth in the price of cryptocurrencies. However, the growth in the number of new blockchain projects being funded, launched, and adopted each year is also rapid:

- **2018–2021 New Cryptocurrencies**

As of 2021, over 10,000 new cryptocurrencies were in the blockchain ecosystem (CoinMarketCap, n.d.). The number of new coins has roughly doubled every year since 2018 (de Best, 2022). At the same time, the Ethereum network, which serves as the infrastructure layer for most newly launched cryptocurrencies, has grown from 18.4 million unique wallet addresses in 2018 to 182 million at the close of 2021 (Etherscan, n.d.).

- **2020–2021 Total Value Under DeFi Applications**

The total value locked under decentralised finance (DeFi) applications surged from US \$26 billion to a peak of US \$112 billion in 2021 (DeFi Pulse, n.d.).

- **2021 NFT Market Cap**

The combined market capitalisation of the major non-fungible token (NFT) projects increased from US \$330 million to over US \$40 billion in 2021 (CoinGecko, n.d.).

- **2021 Blockchain Startups**

“Venture capitalists invested more than [US] \$33bn into crypto/blockchain startups in 2021, more than all prior years combined” (Thorn, 2021).

#### Vocabulary Check

This section introduces the following terms.

- asset class
- decentralised
- decentralised autonomous organisation (DAO)

- [decentralised finance \(DeFi\)](#)
- [miner](#)
- [mining pool](#)
- [staked tokens](#)
- [token incentive model](#)
- [validators](#)
- [whitepaper](#)

## Overview

The invention of bitcoin introduced the world to a new form of digitally scarce currency, and it popularised the concept of using decentralised and distributed networks to exchange value. Following the introduction of the Bitcoin network, additional cryptocurrencies began to proliferate. Vitalik Buterin created one such cryptocurrency, Ether, and the Ethereum blockchain, which features infrastructure for building and monetising decentralised applications (dApps) in a scalable and censorship-resistant form (Shipp, 2020). Other developers, seeking fast transaction speeds, enhanced privacy, and operability that did not require specialised hardware, adopted different blockchain infrastructures and created more new cryptocurrencies.

## Guest Video: The Future of Work

In the following video, Abbey Titcomb, Community Lead at Radicle, speaks about open-source software, decentralisation, and the future of work.



I really like talking about open-source software in this context, because open-source software—open-source development is actually the first type of commons-based peer production. It was kind of the phenomenon that actually coined that term, because it is people contributing to an open public good in a completely decentralised manner, usually.

And so when we think about the future of work, and when you think about the space that we're building in Web3 decentralised technologies, all these projects are building decentralised tech. And they're doing it purely on the internet. They're doing it purely open-source. And they're doing it in a decentralised manner.

The future of work is definitely online, decentralised, and open source. And I think that Web3 space is really spearheading that movement as we all try to build technology, use that technology to build more technology, and then build ourselves and decentralise ourselves around that technology.

## From Cryptocurrency to Ecosystem

Bitcoin, Ether, and the thousands of cryptocurrencies that have been built on blockchain networks have led to the emergence of a new asset class of similar investment vehicles. Developers, researchers, service providers, and advocates within this new asset class contribute their expertise to form an entire ecosystem around blockchain technology.

### Guest Video: The Ethereum Space

In the following video, Abbey Titcomb, Community Lead at Radicle, speaks about Ethereum's developer community and ecosystem.



The Ethereum space is an incredibly strong developer ecosystem, and it has for a while, regardless of where the market is. And I think that that ecosystem is incredibly important, because these developers are also stewarding a new vision of the web, a new vision of technology. One that is decentralised, open-source, and entirely online. And I think that this is the hedge that blockchains have against—I don't want to say against, but in relation to another, is who's building where?

And I think Ethereum has a ton of baseline primitives, like actual standards, whether it be token standards to organisational primitives, and these are now the toolbox for the decentralised web. And that will continue to grow, and it will continue to be that hub of activity, I think, in the decentralised web.

## Ecosystem Participants

The cryptocurrency and blockchain ecosystem consists of participants serving in one or several of the following roles:

- Developer communities
- Researchers
- Operators
- Governing bodies
- Service providers
- Investors
- Users or consumers
- Regulators
- Advocates

### **3.2.2 Industry Organisations**

#### **Industry Organisations**

The blockchain ecosystem includes industry organisations that help bridge the gap between research, advocacy, and commercialisation of blockchain technology. Through these communities, technology experts, policymakers, and business professionals worldwide can collaborate and exchange ideas to form global industry standards that support the growth, legislation, and adoption of blockchain technology. These groups are primarily member-driven and consist of influential industry leaders in technology, politics, and academia. The key roles in this group include developers, operators, governing bodies, and advocates. Examples of industry organisations include:

- The Blockchain Association
- The Global Blockchain Business Council
- The Blockchain Industry Group
- The American Blockchain & Cryptocurrency Association
- The Association of Cryptocurrency Enterprises & Startups Singapore (ACCESS)
- The International Association for Trusted Blockchain Applications
- Chamber of Digital Commerce

### **3.2.3 Developers**

#### **Developers**

Developers are the architects of the cryptocurrency and blockchain ecosystem. They collaborate in open source communities to develop and upgrade blockchain infrastructures, leveraging a hybrid of skills including knowledge of coding languages like C++, Java, Python, and Solidity and an understanding of open-source software, database architecture, distributed systems, and cryptography.

Developers behind the most popular cryptocurrencies and blockchain networks leverage skills in financial engineering, game theory, economics, and even philosophy. These subjects form the basis for why bitcoin and blockchain technology exist and remain relevant as the ecosystem evolves to propose sophisticated solutions to complex societal problems. Further, the number of blockchain developers is rapidly growing: demand for technical talent in the blockchain ecosystem increased by 517% from 2019 to 2021 (Mearian, 2019).

## Guest Video: Open Source and the Future of Development

In the following video, Abbey Titcomb, Community Lead at Radicle, speaks about open-source communities and the future of development.



It's entirely online. It's decentralised. But I think that there is inherent power in the primitives in the decentralised web space, such as the financial primitives, DeFi. It could be the organisational primitives, like DAOs.

But these tools are giving people the ability to build things together on the internet, whether it be new ways to fund their creation and fund their work, whether it be new ways to create more trust in the way that they collaborate with each other, or if it just gives them more of a way to do this anonymously online. And so it's really powering up what we are able to do when it comes to controlling the means of our production. And that's incredibly important for open-source maintainers and contributors because now they have new paths to fund their work that are outside of the traditional paradigm, which actually limits them in their ability to actually sustain themselves when contributing to an open-source project. And so that's what I think the future is, is that developers are just going to continue being able to use these decentralised tool links, these organisational primitives, DeFi, and crypto to wield and maintain a new form of work that is under their control and on their terms.

## Developer Communities

Developer communities are a natural component of the open-source architecture of blockchains, which operates on a decentralised and flat hierarchical structure. The earliest contributors to the Bitcoin blockchain were able to collaborate and exchange network optimisation ideas and strategies via community forums.

Today, developer communities play an increasingly important role in the creation of new ideas that lead to cutting-edge innovations in blockchain security, scalability, and overall optimisation. As more industry sub-sectors emerge, there has been an increase in new communities that focus on solving unique problems within their own blockchain networks. Engaging with these communities can help companies gain insight into which blockchain networks are thriving and whether their infrastructure is potentially a good fit for adoption in an enterprise or startup.

Decentralised autonomous organisations, or DAOs, are the most common structures for blockchain developer communities to work under. DAOs are not companies, but are instead vehicles set up using smart contracts to manage funds and orchestrate the development of blockchain projects without a formal legal structure. Non-profit foundations that fund research, development, and education efforts often support DAOs and work to spur the networks' growth. Foundations carry influence over the decisions made within a DAO but do not directly govern them.

## Competitive Dynamics Between Developer Communities

Although communities within the same blockchain network are collaborative, there is often fierce competition between networks, particularly those that aim to solve similar problems around blockchain

scalability. This phenomenon is a consequence of the token incentive models that many of the largest blockchains chose to achieve mass adoption.

As users benefit from the price appreciation of their tokens, some grow a strong sense of loyalty to the network—if competing blockchains prove successful, these competing blockchains could threaten financial incentives, which leads to competition among developers and users to ensure the supremacy of their chosen blockchain network. Examples of these dynamics are visible between the Bitcoin and Bitcoin Cash community, the Bitcoin and Ethereum community, Ethereum and Tezos or Cardano, and more recently in the DeFi space between Uniswap, SushiSwap, and Binance Smart Chain.

However, while these competitive attitudes exist within some segments of the blockchain ecosystem, many developers and token holders are blockchain agnostic and work toward building solutions that enable connectivity between networks. Many developers are working on network design projects that connect blockchain networks such as Cosmos, Polkadot, and Thorchain.

### 3.2.4 Operators

#### Operators

Operators in the cryptocurrency and blockchain ecosystem are those who help validate transactions and uphold a network's security. For a proof of work (PoW) blockchain, such as Bitcoin, operators are “miners” who contribute hashing power to solve computational problems in exchange for rewards in the form of coins. For a proof of stake (PoS) blockchain, operators are “validators” who stake their coins to help validate transactions on the network.

As the number of users on the Bitcoin blockchain has grown along with the price of bitcoin, the amount of computing power generally required to earn a reward has increased, leading groups of miners to form “mining pools” wherein the miners combine their computing power and agree to split the bitcoin reward between participants. Most mined bitcoin comes from mining pools, including pools set up by mining companies like Riot Blockchain and Marathon Digital Holdings.

Meanwhile, on a PoS blockchain such as Cardano, the validators lock native tokens into a smart contract which incentivises these validators to only submit “compliant” transactions to the blockchain and to verify that other validators have done the same. The blockchain uses the staked tokens to validate transactions and reward validators based on their proportion of tokens at stake. The system selects these validators randomly.

The core differences between PoW miners and PoS validators are the resources required for members of each group to participate in validating new blocks, and the amount of energy expended in validating new blocks. PoW blockchains require no tokens to participate as a miner, but demand more hardware and significant computational power. PoS blockchains require potential validators to stake their tokens, but have few hardware and computational power demands.

## **3.2.5 Governing Bodies and Advocates**

### **Governing Bodies and Advocates**

Industry organisations also include governing bodies, who establish and enforce rules around blockchain networks, and advocates, who promote blockchain technology.

#### **Governing Bodies**

Governing bodies can take the form of decentralised autonomous organisations (DAOs), which are made up of individuals who participate in the governance of a public blockchain network, or the form of other regulatory institutions, such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) in the US. Participants in DAOs can establish rules for mining protocols and rewards, network upgrades, use of treasury funds, and other changes based on voting consensus. The rules established within and between DAOs ultimately dictate how applications in the blockchain ecosystem interact with the external world.

#### **Advocates**

Journalists and influencers educate the general public about blockchain technology and advocate for its mainstream adoption. In keeping with the underground origins of Bitcoin, early advocacy for cryptocurrency and blockchain adoption was largely driven by subcultures and groups that existed outside of the mainstream, communicating mainly in online forums.

## **3.2.6 Rounding Out the Ecosystem**

### **Rounding Out the Ecosystem**

Also crucial to the blockchain ecosystem are contributors including researchers, service providers, investors, users, and regulators.

#### **Researchers**

Researchers test hypotheses, publish papers on cutting-edge technologies, and conduct experiments. Some of these concepts are developed into real-world products and services that entrepreneurs and investors commercialise. Projects like Filecoin, Zcash, Cardano, and Algorand can trace their origins to academic institutions such as MIT, Berkeley, the University of Oxford, and Stanford.

## **Service Providers**

Service providers are the companies and entrepreneurs who build new products and services on top of existing blockchain infrastructures and include wallet service providers, exchanges, lending platforms, and staking services. Service providers look to leverage blockchain technology to solve critical problems facing users, such as privately securing and storing value or engaging in financial transactions with greater transparency.

## **Investors**

Investors provide funding to service providers, foundations, other legal entities, or DAOs. In some cases, investment can be made using traditional payment rails, such as wire transfers. However, investors can only use digital currencies in many cases. As the industry develops, the size and sophistication of investors—from angel to venture capital investors—funding blockchain projects continuously increases.

There are different types of investors. In general, investors can be long-term investors, short-term investors, flippers, day traders, high-frequency traders, or market makers.

- Long-term investors usually have a time frame of more than five years.
- Short-term investors usually have a time frame of fewer than five years.
- Day traders buy and sell assets daily purely to make a profit.
- Flippers buy assets early, then sell the assets when they're liquid and can be sold easily.
- High-frequency traders usually use automated processes to buy and sell assets very quickly.
- Market makers act as wholesalers and buy and sell assets to satisfy markets.

## **Users or Consumers**

Consumers extract value and utility from service providers through blockchain applications for actions such as lending, borrowing, transacting, speculating, and gaming. In June 2021, the estimated number of global cryptocurrency users reached 221 million, doubling the previous number of 100 million in just four months (Wang, 2021).

## **Regulators**

Financial regulators such as the Securities and Exchange Commission (SEC), Financial Crimes Enforcement Network (FinCEN), and the Commodity Futures Trading Commission (CFTC) establish rules around how users and investors can interact with cryptocurrencies and blockchain service providers.

Many debate the stance of governments on cryptocurrencies as securities and what this means for service providers looking to issue tokens to raise capital or create unique incentive models for users. The CFTC has officially ruled that bitcoin is a commodity (U.S. Commodity Futures Trading Commission, 2019). The CFTC has asserted that Ethereum is also a commodity, though this classification has not been made official (Foxley, 2019).

### 3.2.7 Key Takeaways, References, and Further Exploration

#### Key Takeaways

Let's review the key points of this section:

1. Cryptocurrencies built on blockchain networks have led to the emergence of a new asset class, and the stakeholders related to this asset class contribute in unique ways to form the blockchain technology ecosystem.
2. Industry organisations help bridge the gap between research, advocacy, and commercialisation of blockchain technology. Through these communities, technology experts, policymakers, and business professionals worldwide can collaborate and exchange ideas to form global industry standards that support the growth, legislation, and adoption of blockchain technology.
3. In summary, the different stakeholders and their roles in the ecosystem include:
  - Developers are the architects of the cryptocurrency and blockchain ecosystem. Developer communities play an increasingly important role in the creation of new ideas that lead to cutting-edge innovations in blockchain security, scalability, and overall optimisation.
  - Operators help validate transactions and uphold the network's security. For a PoW blockchain, such as Bitcoin, operators are “miners” who contribute hashing power to solve computational problems in exchange for rewards in the form of coins. For a PoS blockchain, operators are “validators” who stake their coins to help validate transactions on the network.
  - Governing bodies can take the form of decentralised autonomous organisations (DAOs) made up of individuals who participate in the governance of a public blockchain network.
  - Advocates such as journalists and influencers educate the general public about blockchain technology and promote its mainstream adoption.
  - Researchers test hypotheses, publish papers on cutting-edge technologies, and conduct experiments.
  - Service providers are the companies and entrepreneurs who build new products and services on top of existing blockchain infrastructures and leverage blockchain technology to solve critical problems facing users.

- Investors provide funding to service providers, foundations, other legal entities, and DAOs.
- Users or consumers extract value and utility from service providers through blockchain applications for actions such as lending, borrowing, transacting, speculating, and gaming.
- Regulators establish rules around how users and investors can interact with cryptocurrencies and blockchain service providers.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 12 April, 2022.

### 3.2.1 Introduction to the Cryptocurrency and Blockchain Technology Ecosystem

Browne, R. (2021, 22 July). Blockchain start-ups raised a record \$4.4 billion in the second quarter despite the slump in crypto prices. *CNBC*. <https://www.cnbc.com/2021/07/22/blockchain-start-ups-raise-record-funding-despite-crypto-slump.html>

CoinMarketCap. (n.d.). *Cryptos*. <https://coinmarketcap.com>

de Best, R. (2022, 3 January). Quantity of cryptocurrencies as of January 3, 2022. <https://www.statista.com/statistics/863917/number-crypto-coins-tokens>

DeFipulse. (n.d.). Total Value locked (USD) in DeFi. <https://defipulse.com>

Etherscan. (n.d.). Ethereum Unique Addresses Chart. <https://etherscan.io/chart/address>

Shipp, D. (2021, 12 December). Blockchain & Ethereum: Welcome to the Decentralized Internet. *Atomic Object*. <https://spin.atomicobject.com/2020/12/12/blockchain-ethereum-decentralized>

Young, J. (2021, 29 March). NFT Market Rages On: NFTs Market Cap Grow 1,785% In 2021 As Demand Explodes. *Forbes*. <https://www.forbes.com/sites/youngjoseph/2021/03/29/nft-market-rages-on-nfts-market-cap-grow-1785-in-2021-as-demand-explodes>

### 3.2.3 Developers

Marian, L. (2019, 28 February). Demand for blockchain engineers is ‘through the roof’. *Computer World*. <https://www.computerworld.com/article/3345998/demand-for-blockchain-engineers-is-through-the-roof.html>

### **3.2.6 Rounding Out the Ecosystem**

- Foxley, W. (2019, 10 October). CFTC Chairman Confirms Ether Cryptocurrency Is a Commodity. *CoinDesk*. <https://www.coindesk.com/markets/2019/10/10/cftc-chairman-confirms-ether-cryptocurrency-is-a-commodity>
- U.S. Commodity Futures Trading Commission. (2019, December). Bitcoin Basics. [https://www.cftc.gov/sites/default/files/2019-12/oceo\\_bitcoinbasics0218.pdf](https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf)
- Wang, K. (2021, July). Measuring Global Crypto Users: A Study to Measure Market Size Using On-Chain Metrics. *Crypto.com*. [https://crypto.com/images/202107\\_DataReport\\_OnChain\\_Market\\_Sizing.pdf](https://crypto.com/images/202107_DataReport_OnChain_Market_Sizing.pdf)

### **Further Exploration: Companies Using Open-Source Technology and Research**

In the crypto industry, a “whitepaper” is a piece of documentation commonly produced by developers to explain the technical specifications of a blockchain network and token structure. Some people and businesses use open-source technology research and resources to develop their own whitepapers purely to raise money for their own benefit.

The crypto market has seen multiple examples of this practice, whose goal is to take advantage of less experienced retail investors to launch Ponzi-style investment schemes under the veneer of credible research published as whitepapers.

While these practices have been a byproduct of the unrestricted access companies have to capital in a retail-driven and largely unregulated market, the recent increase in regulation and sophistication of investors over time may reduce the appeal of such tactics.

# 3.3 Internal Stakeholders in the Blockchain Technology Ecosystem

## 3.3.1 Overview of Internal Stakeholders

### Overview

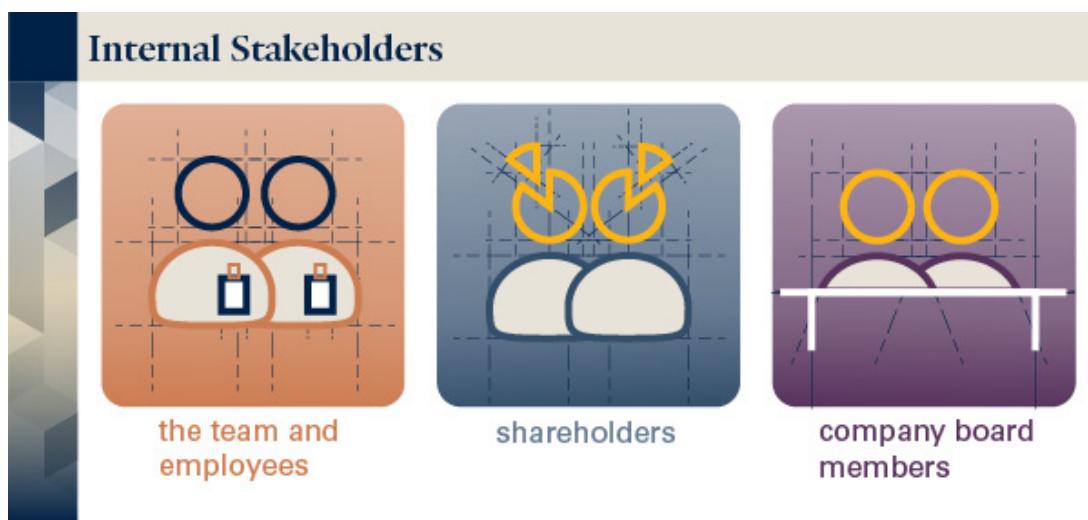
This section explores the role and incentives of internal stakeholders in the blockchain technology ecosystem and the related organisational and competitive dynamics. Because internal stakeholders have direct influence and make key decisions, as you assess the viability of implementing a blockchain technology solution for an organisation, new venture, or project, you'll need to develop a comprehensive understanding of how these stakeholders are involved in the ecosystem and the decision-making processes.

### Internal Stakeholders

Internal stakeholders are the individuals who: have a direct interest in a company, organisation, or product offering; are impacted by decisions made by teams; and can influence any decision in the business or organisation.

Internal stakeholders include:

- The team and employees
- Shareholders
- Company board members



### 3.3.2 Internal Stakeholders

#### Internal Stakeholders

The three main categories of internal stakeholders in the blockchain technology ecosystem which you'll consider when working on a blockchain technology project include team and employees, shareholders, and the company board.

Later in this module, you'll learn to develop a stakeholder engagement and communication strategy based on your analysis of your Capstone project's internal and external stakeholders. As we explore the roles and incentives of internal stakeholders, consider each stakeholder in the context of these key questions:

- Is the primary goal of a blockchain solution to reduce operating costs or increase revenue?
- How do you assimilate a blockchain solution within your existing technology infrastructure?
- What are your intellectual property rights, and how do you protect them?
- What are the immediate costs associated with implementing a blockchain solution?
  - How will you finance the development and maintenance of your blockchain solution?
- How much of this solution will be outsourced to vendors versus developed internally?
- What will be your legal structure? (Joint venture/consortium? Foundation?)
- To what extent does a blockchain solution cannibalise parts of your existing business model?
  - Which internal stakeholders will be affected as a result?
- What are the talent gaps within your organisation that you must fill to develop and operate a blockchain solution?
- Which internal stakeholders can contribute the most value (in terms of knowledge, relationships, or skills) to the implementation of your solution?
- Which internal stakeholders have the most influence on your ability to implement a blockchain solution?

When engaging with and getting buy-in from internal stakeholders that influence a blockchain technology project, it is important to understand each group's objectives. The considerations you'll have to make will depend on which stakeholder you're focusing on. For example, the concerns of employees are different from those of shareholders. Employees may fear losing their jobs by embracing new technology, whereas shareholders may fear financial loss.

The table below shows the key roles within each of these internal stakeholder groups and summarises their objectives (Kolmer, 2021; Indeed Editorial Team, 2021; Barlow, 2016; Perry, 2020).

Internal Stakeholders	Key Roles	Summary of Objectives
<p>Team and employees</p> 	<p>Executives and management</p>	<ul style="list-style-type: none"> <li>Develop strategic objectives for the overall business and relay them to other internal stakeholders (shareholders, company board, employees, product development, sales and marketing, customer support, and operations).</li> <li>Set organisation up for success through fundraising and talent acquisition.</li> <li>Engage with external stakeholders to promote organisational interests.</li> </ul>
	<p>Financial operations</p>	<ul style="list-style-type: none"> <li>Assign and approve budgets for marketing, sales, and product teams.</li> <li>Forecast expenses and revenue for strategic objectives.</li> <li>Manage accounts and ensure regulatory compliance (perform risk assessments).</li> </ul>
	<p>Legal</p>	<ul style="list-style-type: none"> <li>Outline rules and regulations for new products and services.</li> <li>Ensure compliance in company formation and operations.</li> <li>Formulate and review contracts and protect intellectual property.</li> </ul>
	<p>Product development</p>	<ul style="list-style-type: none"> <li>Create a product roadmap to address the organisation's strategic objectives within a set time frame.</li> <li>Organise and assign tasks to engineers, designers, and other product development stakeholders.</li> </ul>

Internal Stakeholders	Key Roles	Summary of Objectives
<p>Team and employees</p> 	Sales and marketing	<ul style="list-style-type: none"> <li>Achieve product-market fit.</li> <li>Identify user pain points to communicate with product and marketing teams.</li> <li>Convey value proposition to prospective customers and achieve sales targets.</li> </ul>
	Customer success/support	<ul style="list-style-type: none"> <li>Onboard customers and provide support.</li> <li>Minimise churn rate.</li> <li>Identify customer needs and challenges and relay these to other internal stakeholders.</li> </ul>
<p>Shareholders</p> 	Founders and owners, angel investors, venture capitalists, stockholders, M&A shareholders	<ul style="list-style-type: none"> <li>Invest in the company with varying degrees of influence and control.</li> <li>Respond to incentives.</li> <li>Influence outcomes within the company.</li> </ul>
<p>Company board</p> 	Chairperson, Vice Chairperson, Treasurer, Secretary	<ul style="list-style-type: none"> <li>Recruit, advise, and support executive team and company.</li> <li>Leverage industry expertise and relationships to build strategic partner relationships.</li> <li>Establish an internal system of governance.</li> <li>Protect the interests of investors.</li> <li>Vote on key issues such as CEO position or M&amp;A approvals.</li> <li>Provide direction for the company that leads to positive outcomes for shareholders.</li> </ul>

### 3.3.3 Key Takeaways and References

#### Key Takeaways

Let's review the key points of this section:

1. There are two categories of stakeholders in a tech venture. The first is internal, meaning anyone with a direct interest in the company or product. This would be the team and employees, shareholders, and the company board. External stakeholders indirectly influence the company but are not directly involved, and include competitors, regulators, and the broader community.
2. The team and employees are responsible for setting and executing strategic initiatives and daily operations, including financial and legal processes, product development, and sales and marketing.
3. Shareholders are responsible for achieving a positive return on investment and can advise and influence the organisation, though they have varying degrees of influence and control.
4. The company board is responsible for protecting the interests of investors, advising the executive team, setting strategic partnerships, and voting on key issues.

#### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 12 April, 2022.

#### 3.3.2 Internal Stakeholders

Barlow, J. (2016, 13 March). What are a Board Member's Responsibilities? *BoardEffect, LLC*. <https://www.boardeffect.com/blog/board-member-responsibilities>

Perry, J. (2021, 10 December). Board Member Responsibilities & Roles: A Nonprofit's Guide. *Boardable*. <https://boardable.com/blog/board-member-responsibilities>

Indeed Editorial Team. (2021, 18 March). A Guide To Executive Business Titles. *Indeed*. <https://www.indeed.com/career-advice/resumes-cover-letters/executive-business-position-titles>

Kolmer, C. (2021, 11 January). Corporate Titles: Examples and what they mean. *Zippia*. <https://www.zippia.com/advice/corporate-title>

# 3.4 External Stakeholders: Roles, Incentives, and the Marketplace

## 3.4.1 External Stakeholders: Roles, Incentives, and the Marketplace

### Overview

The next two sections explore the external stakeholders in the blockchain technology ecosystem, their roles and incentives, the associated organisational and competitive dynamics, and the differentiation between emergent sectors of this industry. As you assess the viability of implementing a blockchain technology solution, you will need to understand the external stakeholders you will partner with, compete against, and provide with services.

### Vocabulary Check

This section introduces the following terms.

- [enterprise blockchain](#)
- [permissioned blockchain platform](#)

### Overview of External Stakeholders

External stakeholders are parties who are not part of your business, project, or organisation, but who influence and are affected by decisions indirectly. They represent part of the broader business environment, which includes customers, competitors, regulators, intermediaries, and potential investors. When you create and pitch a blockchain technology project, external stakeholders present an important set of needs and potential roadblocks to the project's success.

External stakeholders include:

- Competitors
- Corporations and enterprises
- Influencers
- Venture capital and institutional investors
- Industry regulators

- General public
- Governments and policymakers
- Academic institutions
- Journalists and media
- NGOs and other global institutions



When exploring external stakeholders in more detail and the influence they have on projects and the ecosystem, keep in mind that later in this module, you'll be evaluating them as part of your Capstone project in preparation for developing a blockchain solution.

To adequately prepare for engaging external stakeholders, consider these strategies:

- Identify strategic partnerships with influencers or industry communities to support funding, development, or marketing needs.
- Assess the regulatory climate and identify key policymakers.
- Understand the competitive landscape and identify market leaders in each sector.

## Guest Video: Overview of Coinbase's Stakeholders

In the following guest speaker video, Emilie Choi, President and Chief Operating Officer at Coinbase, gives an overview of Coinbase's stakeholders.



The first and most important constituents that we have are our customers. And we have three different segments of customers. So the foundation of the business is built on this retail consumer brokerage model, where we have a number, 50 million-plus accounts.

Those customers typically have come in to buy or sell Bitcoin. And then over time, we think about them as having a profile in the crypto economy that we want to expose them to more and more features such as staking. We want to expose them, to your point, to more and more assets. Maybe they start with Bitcoin and then they get into Ethereum.

And then we have a bunch of cool things. We have the urn offering, which allows you to learn more and more about other cryptocurrencies. And then after you go through a small course, that cryptocurrency will be deposited in your account.

The second leg of the business on the customer front is the institutional customers. And we started building out that business about two years ago. We had zero assets under custody. And now we have many, many, many billions of assets under custody that we're holding and protecting on behalf of our institutional customers.

The institutional customers are going to be a more conservative set by nature. And so they're going to want very strong custody. And then they're going to want to be able to do things with those assets that they park with us. They might want to trade. And they might also want to be able to do things with those assets such as lend and borrow and things like that like a typical prime brokerage.

The third group of customers that we have are developers. We acquired a company called Bison Trails in the past year. And we just believe that there's a very large opportunity for developers to be able to nimbly build on blockchain infrastructure. And so we have a set of developer tools and infrastructure tools for those developers.

So we have those three customer sets. In terms of other constituents, the way that I think about it is the crypto

ecosystem is so robust, we have a role to play in many different parts of it. So on the venture side, we booted ventures up about 3 and 1/2 years ago. And we have now invested in over 150 startups in this space.

The reason we do that is multifold. One is that they are going to be really interesting companies in the space that are doing things that are slightly outside of our core and strategic. And we want to make sure that we make bets on them and have some optionality, even if we don't want to play that game as a principle today.

We also have a number of other constituents that you can imagine. Those include partners. For example. We have payments and banking partners. The value proposition of Coinbase is a fiat to crypto bridge in many cases.

And so those banking and payment partnerships allow all sorts of people around the world to be able to access Coinbase and to be able to use money between fiat and crypto. And then there's vendors that we use. And then finally, as you pointed out earlier, we work very closely with regulators to figure out how we can help proactively shape the face of regulation across the world.

### 3.4.2 Competitors

#### Competitors

The competitive landscape for companies developing blockchain-based solutions varies by industry, sector, use case, and target audience (for example, users who are currently active within the blockchain ecosystem versus users who are not). Competitors include enterprise blockchain companies and blockchain startups.

#### Enterprise Blockchain Companies

This category includes companies that offer “blockchain as a service” (or BaaS) solutions to traditional companies, such as small and medium-sized enterprises (SMEs). The main competitors in this category include Hyperledger (developed by the Linux Foundation, which IBM supports), ConsenSys Quorum (a partnership formed from ConsenSys’s acquisition of JPMorgan’s “Quorum” blockchain), and Corda (developed by R3).

Enterprise blockchain service providers are differentiated by industry focus (such as general, finance, and supply chain), governance model, ledger type, use of a cryptocurrency within their network, consensus algorithm, and smart contract functionality (HFS Research, 2018):

	Hyperledger Fabric	R3 Corda	ConsenSys Quorum
<b>Industry focus</b>	Cross-industry	Financial services	Cross-industry
<b>Governance</b>	Linux Foundation	R3 Consortium	Ethereum developers & JPMorgan Chase
<b>Ledger type</b>	Permissioned	Permissioned	Permissioned
<b>Cryptocurrency</b>	None	None	None
<b>Consensus algorithm</b>	Pluggable framework	Pluggable framework	Majority voting
<b>Smart contract functionality</b>	Yes	Yes	Yes

Enterprise blockchains enable companies to set up private consortiums with specific partners they wish to transact with in a more distributed, transparent, and secure manner. These services can also form bridges to public blockchains like Ethereum so that companies can utilise features on the Ethereum network (like smart contracts) without compromising their privacy.

For example, Hyperledger Burrow is designed to be a permissioned Ethereum smart-contract blockchain node that executes smart contract code and manages transactions on the Ethereum blockchain.

## Blockchain-Focused Startups

This category of competitors in the blockchain ecosystem includes blockchain networks, blockchain-focused startups, and traditional companies that have spun off new businesses to capture users within and outside the crypto and blockchain ecosystem.

The competitive landscape for blockchain startups is based on the following emerging sectors of the industry:

- dApp infrastructure
- Financial services (CeFi, DeFi, payments, institutional digital asset infrastructure, asset tokenization, and stablecoins)
- Metaverse (art, gaming, and NFTs)
- Data analytics, compliance, and security
- Decentralised cloud computing and storage
- Privacy
- Interoperability
- Insurance

- Oracles
- Wallets
- Prediction markets
- Advertising

Capital flows drive competition amongst blockchain-focused startups into the industry. Blockchain startups successfully managed to raise over US \$6 billion in 2021 and an estimated US \$19 billion during the 2017–18 ICO boom (Liu, 2020, 2021). This funding provides startups with the capital to develop and market their solutions to capture market share and grow their ecosystems to benefit from network effects.

### **3.4.3 Corporations and Enterprises**

#### **Corporations and Enterprises**

Corporations and enterprises such as IBM, Ernst & Young, Oracle, and Amazon are major blockchain technology service providers. Other corporations, like Ant Group, Boeing, Maersk, Walmart, and Cargill, are already partnering with private enterprise blockchains to improve the transparency and efficiency of transactions within their supply chains and operational networks (Castillo, 2021). Companies that support enterprise blockchain services include Hyperledger (Linux Foundation), ConsenSys Quorum, Corda, Enterprise Ethereum Alliance, Hedera Hashgraph, and Oracle Blockchain.

Corporations including Apple, Meta, and Google have explored blockchain technology to reduce operating costs, increase market share, or develop new business models on decentralised networks. The following organisations also use blockchain technology.

- **Ant Group, a spinoff from Alibaba (blockchain partners: Hyperledger and ConsenSys Quorum)**

Ant Group has developed over 50 blockchain applications on its custom blockchain network, Ant Chain. The organisation also recently launched OpenChain, a network with 6,000 SMEs, which leverages smart contracts and other blockchain applications to lower operating costs.

- **Boeing (blockchain partners: Go Direct and Hyperledger Fabric)**

Through its venture arm, HorizonX, the aircraft manufacturer is funding SkyGrid, an air traffic control system that leverages blockchain technology to track and communicate with drones.

- **A.P. Moller - Maersk (blockchain partners: TradeLens, Hyperledger Fabric, and IBM Blockchain)**

In 2018, shipping and logistics company A.P. Moller - Maersk launched TradeLens in partnership with Hyperledger Fabric and IBM Blockchain. Since then, TradeLens has onboarded around 50% of all container ships globally to the network. The network processed one billion shipments, 30 million containers, and 14 million documents in 2020.

- **Walmart (blockchain partner: Hyperledger Fabric)**

Walmart has partnered with Hyperledger Fabric to enable food traceability on the blockchain. The retail giant can trace up to 500 items, including vegetables, seafood, meat, and coffee, to detect contamination or other food safety issues. The company's solution has aided the FDA in six investigations involving food safety, providing detailed accounts of the source of contamination within an hour of inquiry.

- **Cargill (blockchain partners: ConsenSys Quorum and Hyperledger Grid)**

Cargill is leveraging blockchain technology to gain more transparency into the transportation of its grain and oilseed products worldwide. The company has also worked with Hyperledger to create an immutable record of its turkey supply chain through the US Thanksgiving period in late November.

### 3.4.4 Influencers

#### Influencers

Influencers play key roles in being advocates, participants in governing bodies, service providers, and investors. Influencers consist of famous entrepreneurs, early adopters, developers, journalists, and media personalities who advocate for the adoption of cryptocurrencies and blockchain technology.

Influence in the cryptocurrency and blockchain ecosystem is gained by building successful businesses, generating viral memes, or becoming subject matter experts in the space and sharing unique insights on platforms like Twitter and YouTube. Most influencers maintain a direct stake in the ecosystem through their ownership of cryptocurrencies or operation of blockchain-based businesses, which further incentivises them to educate the general public about the value of blockchain technology.

## Notable Influencers



### **3.4.5 Venture Capital and Institutional Investors**

#### **Venture Capital and Institutional Investors**

This group of stakeholders includes investors and advocates such as Coinbase Ventures, Galaxy Digital, and a16z. The growing adoption of blockchain technology has attracted institutional investors looking to fund startups and protocols in the space.

Institutional investors allocate capital to early-stage projects with hopes of achieving substantial returns from an emerging industry and disruptive technology. Their primary goal is to fund projects that benefit from network effects, global distribution, exponential growth, and high margins. According to a 2020 venture capital (VC) report published by Cointelegraph, 942 venture capitalists have invested in over 2,700 private equity deals involving startups and companies in the blockchain space since 2012 (Hays et al., 2021).

Blockchain technology is also disrupting how VCs make investments. Funds that traditionally invested in debt or equity are now taking more creative approaches to allocate capital into this space, from purchasing equity and convertible notes to non-equity tokens and Simple Agreement for Future Tokens (SAFT) agreements. The emergence of cryptocurrencies as a separate asset class is changing the way investors approach capital allocation, both from the buy side (in purchasing securities) and from the sell side (in issuing securities) (Hays et al., 2021).

Blockchain startups that capture network effects can realise gains in user growth and revenue growth through transaction fees and the appreciation of the network's tokens. Unlike the internet, where most of the value that users create accrues on the platforms of individual companies like Google or Facebook, a larger share of the monetary value that blockchain networks create is distributed back to the users who hold the network's tokens, thereby creating even greater incentives for user adoption.

The potential to own shares or tokens in projects that are capable of capturing billions of users on a global scale with instant revenue-generating capacity and the ability to benefit from network effects is the primary reason for the explosion in the growth of crypto-focused VC funds and capital flows into the blockchain ecosystem.

#### **Infrastructure for Institutional Adoption of Digital Assets**

Institutions investing in cryptocurrencies require special considerations around custody, security, and the actual purchasing of large quantities of digital assets. Prior to 2017, institutional investors found it difficult to allocate capital towards cryptocurrencies because the market caps were too small to absorb hundreds of millions of dollars without having a significant impact on prices. Furthermore, the lack of known custodial providers meant that institutions would have to manage the storage and security of millions of dollars in cryptocurrencies themselves, using less secure digital wallets geared towards retail customers.

As the market capitalisation of all cryptocurrencies surpasses US \$1.5 trillion (CoinMarketCap, 2021), institutions from hedge funds, mutual funds, and pension funds to university endowments and insurance companies are slowly gaining exposure to the digital asset space. A variety of custodial and brokerage firms around the world service these institutions.

According to The Block Research, 115 companies are building out institutional infrastructures for digital assets. To date, these companies have raised a combined total of approximately US \$2.1 billion (Dantoni, 2020).

Digital asset infrastructure companies operate primarily in North America, Europe, and Asia, where high net worth individuals and institutions cluster. Firms provide a spectrum of products and services to garner more capital or achieve higher trading volumes than their competitors. These products and services include custody, market making, providing spot liquidity, brokerage, lending, derivatives, clearing/settlement, trade execution, and securitisation/tokenisation.

### 3.4.6 Key Takeaways, References, and Further Exploration

#### Key Takeaways

Let's review the key points of this section:

1. Some blockchain companies sell their services to partners, including enterprises and startups. Enterprise blockchain companies enable companies to set up private blockchains with specific partners for more distributed, transparent, and secure transactions. They also serve as a bridge to public blockchains. Blockchain startups include blockchain networks, blockchain-focused startups, and traditional companies that have started new blockchain businesses.
2. Major corporations are getting involved in blockchain either as service providers or by partnering with private enterprise blockchains to improve transparency and efficiency of transactions within their supply chains and operational networks. Large corporations like Apple and Google are exploring blockchain as a way to reduce operating costs.
3. Influencers advocate for the adoption of cryptocurrencies and blockchain. Influence in cryptocurrency and blockchain is earned by building successful businesses, making memes, or sharing expertise on social media.
4. Institutional investors invest in early-stage projects with the hopes to capitalise on network effects, global distribution, exponential growth, and high margins, with high returns. Blockchain is also allowing VCs to take creative approaches to allocate capital, expanding to agreements for tokens.
5. Companies are building infrastructures around transactions and the security of large digital assets. As the market cap grows, more traditional funds are exposed to digital assets. The companies working to create that infrastructure have raised approximately US \$2.1 billion to date.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 12 April, 2022.

### 3.4.2 Competitors

HFS Research. (2018, 16 March). The top 5 enterprise blockchain platforms you need to know about. [https://www.hfsresearch.com/blockchain/top-5-blockchain-platforms\\_031618](https://www.hfsresearch.com/blockchain/top-5-blockchain-platforms_031618)

Liu, S. (2021, 10 May). Level of blockchain startup venture-capital funding worldwide 2016-2021. *Statista*. <https://www.statista.com/statistics/621207/worldwide-blockchain-startup-financing-history>

Liu, S. (2020, 30 November). Blockchain ICO projects: funds raised worldwide 2017-2019. *Statista*. <https://www.statista.com/statistics/804748/worldwide-amount-cryptocurrency-ico-projects>

### 3.4.3 Corporations and Enterprises

del Castillo, M. (2021, 2 February). Blockchain 50 2021. *Forbes*. <https://www.forbes.com/sites/michaeldelcastillo/2021/02/02/blockchain-50>

### 3.4.5 Venture Capital and Institutional Investors

Coinmarketcap. (2021). Global Cryptocurrency Charts Total Cryptocurrency Market Cap. <https://coinmarketcap.com/charts>

Dantoni, J. (2020, 12 May). Mapping the Institutional Digital Asset Infrastructure space. *The Block Research*. <https://www.theblockresearch.com/mapping-the-institutional-digital-asset-infrastructure-space-64661>

Hays, D., Elkov, D., Rosenberg, H., Malkhasyan, N., & Kravchenko, I. (2021). Blockchain Venture Capital Report. *Cointelegraph*. <https://mercuryredstone.com/wp-content/uploads/2021/04/Cointelegraph-consulting-venture-capital-report.pdf>

## Further Exploration

A distinguishing factor amongst blockchain networks is Layer 1 (L1) and Layer 2 (L2) solutions. L1s are base layer networks like Bitcoin, Ethereum, Stellar, Solana, and Cardano.

L1s like Bitcoin and Ethereum, which both run PoW consensus mechanisms, are generally more decentralised and secure; however, they take longer and it can become expensive to process

transactions during times of network congestion. Ethereum experiences this through an increase in “gas” fees, which make it more costly to trade tokens and NFTs or deploy smart contracts. Similarly, it can take several hours to get the necessary number of confirmations to receive a transaction on the Bitcoin network.

Developers build L2s on top of L1s as a solution to this scalability problem. They enable several smaller transactions to be processed on a “sidechain” (think of this as a separate blockchain that has fewer nodes and can confirm transactions more quickly), then batched together and confirmed as one transaction on the main L1 chain. Examples of L2s include Polygon, Arbitrum, Optimism for Ethereum, and Lightning Network for Bitcoin.

L2s seek to remove the computational burden from L1s while providing the bare minimum transaction data back to the L1 network. The selling feature is completing faster transactions while still inheriting the security of the L1 network.

Competing blockchains like Solana and Cardano operate their networks under variations of the PoS consensus mechanism to achieve scalability at L1 without needing to build L2 solutions.

# 3.5 External Stakeholders: The Regulatory Environment

## 3.5.1 External Stakeholders: The Regulatory Environment

### Overview

This section explores additional external stakeholders, focusing on industry regulators, the general public, policymakers and governments, academic institutions, journalists and media, and NGOs and global institutions.

### Vocabulary Check

This section introduces the following terms.

- [anti-money laundering \(AML\)](#)
- [cryptocurrency gain](#)
- [know your customer/client \(KYC\)](#)

### Industry Regulators

This stakeholder group includes regulators such as the SEC, CFTC, and FINRA. The fast pace of innovation in the cryptocurrency and blockchain ecosystem is forcing regulatory bodies to quickly adapt new rulings around issues such as:

- The classification of tokens as securities or utilities
- Tax reporting on cryptocurrency gains
- Know your customer/client (KYC) and anti-money laundering (AML) compliance on unregulated exchanges

The current global regulatory environment is fragmented into different jurisdictions where authorities enforce tax and compliance laws with varying degrees of severity. In the US, for example, the main regulatory bodies in charge of regulating the cryptocurrency and blockchain industry include:

- **Securities and Exchange Commission (SEC):** The SEC operates to protect investors, support capital formation, and maintain a fair and orderly securities market.
- **Commodity Futures Trading Commission (CFTC):** The CFTC regulates US commodity, futures, and options markets. It aims to protect investors against market manipulation and fraud while promoting fair and efficient markets.

- **Financial Industry Regulatory Authority (FINRA):** FINRA is responsible for writing and enforcing the rules under which registered brokers and broker-dealers in the US operate.
- **Financial Crimes Enforcement Network (FinCEN):** FinCEN investigates and enforces actions against persons involved in money laundering and other financial crimes. FinCEN operates both domestically and internationally as a branch of the US Department of the Treasury.
- **US Department of the Treasury (USDT):** The USDT is an office of the United States government responsible for the issuance of Treasury bonds, bills, and notes. Government departments that operate under the USDT include the Internal Revenue Service (IRS), the US Mint, and the Alcohol and Tobacco Tax and Trade Bureau (TTB).
- **The Office of the Comptroller of the Currency (OCC):** The OCC is responsible for regulating, chartering, and supervising national banks, federal branches, and foreign banking agencies in the US.
- **Internal Revenue Service (IRS):** The IRS is a US government agency responsible for the collection of taxes and enforcement of tax laws.
- **US Department of Justice (DOJ):** The DOJ is the nation's federal law enforcement agency and is tasked with enforcing the law, including prosecuting financial crimes. The DOJ is authorised to launch probes and take action to prevent crimes and fraud related to cryptocurrencies.

#### **International regulatory bodies include:**

- Group of Twenty (G20)
- International Monetary Fund (IMF)
- Bank of International Settlements (BIS)
- International Organization of Securities Commissions (IOSCO)

### **3.5.2 General Public**

#### **General Public**

The general public refers to the users of blockchain technology, who are either “crypto native users” or “non-crypto native users”. Crypto native users are those who frequently transact with cryptocurrencies, participate in self-custody, and use decentralised applications (or dApps). Non-crypto native users are those who do not use any dApps, do not own any crypto, or only own crypto as passive investors.

The general public can be broadly classified into four groups:

- **Passive crypto owners** primarily own small allocations of BTC and ETH through mainstream custodial services like Coinbase and do not actively follow market or industry news.
- **Active crypto owners** use crypto-native services like Uniswap and Metamask, own multiple coins, participate in self-custody, and follow the industry closely. Primary use cases centre around trading, investing, earning mining and staking rewards, liquidity providers (LPs), payments, and gaming.
- **Non-crypto owners** have access to the internet and to basic financial services. They mostly hear about crypto through mainstream sources like CNBC or Bloomberg and are primarily from developed nations with access to financial services. These users generally view cryptocurrencies as a tool for speculation and do not always know about the underlying properties of blockchain technology.
- **The underbanked** include those who have limited to no access to traditional financial services, such as the 1.7 billion adults globally who do not have a bank account (Findex, 2017). Because accessing blockchain networks requires only a smartphone, expanding mobile phone services have increased access to cryptocurrencies among this population (Fries, 2021). Crypto users in this group exist primarily in developing countries where use cases for crypto are centred around remittances, circumventing capital controls, and providing a hedge against inflation.

These distinctions are not absolute, as many people fall under multiple classifications. The purpose of segmenting the general public in this way is to help formulate distinct approaches to messaging and product design that can improve the adoption of blockchain technology.

## Cryptocurrency Adoption

Overall, the broad consensus amongst influencers, companies, and entrepreneurs in the blockchain space is that increased simplification of the core concepts of blockchain technology, and a more intuitive user experience for blockchain applications, are both essential to achieving mass adoption by the general public. For blockchain to follow the same path of adoption as the internet, the general public needs to be able to seamlessly perform actions like making payments, taking or issuing loans, and storing or exchanging value without needing to know or understand what blockchain networks they are using to perform each function. This level of intuitive design has enabled the mass adoption of the internet through email services, search engines, video streaming sites, and social media platforms, all of which sit on top of Transmission Control Protocol/Internet Protocol (TCP/IP) and Hypertext Transfer Protocol (HTTP), some of the building blocks of the internet.

The names of service providers like Yahoo, Google, YouTube, Facebook, and Twitter may always remain present. However, the interoperability of these services enables the general public to have the experience of using one internet, which is an experience that many developers and entrepreneurs in the blockchain system are trying to replicate to spur greater user adoption.

Accessibility also plays a significant role in user adoption of cryptocurrencies. The open access of public blockchain networks like Bitcoin and Ethereum, in addition to the infrastructure built by services like Coinbase and Cash App, has enabled cryptocurrencies to be adopted all over the world.

The top geographies for the general public's crypto adoption in 2021 include (Chainalysis, 2020):

- Ukraine
- Russia
- Venezuela
- China
- Kenya
- United States
- South Africa
- Nigeria
- Colombia
- Vietnam

### **3.5.3 Policymakers and Governments**

#### **Policymakers and Governments**

Policymakers and governments play an important role in the continued success of the cryptocurrency and blockchain industry. While regulations have generally struggled to catch up to the speed of innovation in this space, there is a growing focus amongst policymakers to develop new regulatory frameworks for participants in the blockchain ecosystem.

Businesses in the cryptocurrency and blockchain ecosystem must find a way to succeed while maintaining regulatory compliance. One way to achieve this is by being aware of the policymakers shaping cryptocurrency regulations, as well as countries and states that are most welcoming to blockchain companies.

#### **Regulatory-Friendly Governments and Nations**

Seeing the potential to revitalise local economies and generate significant tax revenues, many state and national governments have sought to establish crypto-friendly regulations to incentivise blockchain companies to set up operations in their jurisdiction.

Features of governments that are friendly towards cryptocurrency businesses might include:

- Transparent regulations and guidance
- Legislation that permits access to the banking system
- Policymakers that are open to technological innovation

## **El Salvador**

In June 2021, El Salvador became the first country to accept bitcoin as legal tender. President Nayib Bukele put forward the proposal, pitched as an “effort to boost financial inclusion in a country where only 30% of citizens have access to financial services” (De, 2021).

## **Antigua and Barbuda**

The Caribbean island created a regulatory framework called the Digital Assets Business Bill 2020 to regulate crypto companies that establish operations on the island and provide protection for both exchanges and their customers. FTX, one of the most popular crypto exchanges in the world, is incorporated in Antigua and Barbuda (FTX, 2021).

## **Switzerland**

Switzerland was one of the first countries to feature clear regulatory guidelines for launching ICOs, published by the Swiss Financial Market Supervisory Authority (FINMA). It is the home of many blockchain foundations, such as the Ethereum and Tezos Foundation. Switzerland also offers favourable tax laws for ICO investors and issuers (Böhi et al., 2017).

## **Malta**

In 2018, Malta’s government signed the Malta Digital Innovation Authority (MDIA) Act, the Innovative Technology Arrangements and Services (ITAS) Act, and the Virtual Financial Assets (VFA) Act into law to provide a regulatory framework for businesses and investors to adopt blockchain technology (Library of Congress, 2018).

## **Estonia**

In 2017 Estonia gave cryptocurrency exchanges and companies seeking to launch ICOs legal status to operate, leading many entrepreneurs to register crypto-related companies in the Northern European nation. While the country has recently faced some setbacks in its attempts to create a regulatory-friendly environment for cryptocurrency businesses, the government has still explored initiatives to use blockchain technology to create digital identities and healthcare services (Evans, 2020).

## Singapore

Cryptocurrency trading is legal in Singapore, but the country does not accept cryptocurrencies as legal tender. In 2017, the Monetary Authority of Singapore (MAS) clarified that it would not regulate virtual currencies but would regulate digital payments tokens (DPT) that are classified as securities. In 2020, the Payment Services Act 2019 (PSA) came into effect. This law requires crypto exchanges and businesses to have an MAS licence to operate. MAS is seeking to introduce stronger AML and commodities future trading (CFT) standards going forward (ComplyAdvantage, 2021).

## Japan

Cryptocurrencies have been recognised as a legally accepted means of payment in Japan since 2017 under the Payment Services Act (PSA) (Comply Advantage, 2020).

## Regulatory-Friendly US States

While the US does not have clear federal laws around cryptocurrencies and blockchain businesses, America's global influence on cryptocurrency regulation is still profound: the US dollar is heavily used in the crypto ecosystem via stablecoins, and the country has the largest capital market in the world. Despite the lack of federal regulation, however, several individual states have made significant strides in developing a regulatory framework for individuals and entrepreneurs in the blockchain ecosystem, including Wyoming, Colorado, Ohio, Texas, California, Nevada, and Florida. For example, the state of Wyoming passed a law to recognise decentralised autonomous organisations as legal entities, enabling individuals to register DAOs much like they would LLCs. In 2020, the Ohio Senate introduced House Bill 220, which would enable official state bodies to use blockchain tech in their operations (McSweeney, 2021).

### 3.5.4 Academic Institutions

#### Academic Institutions

Academic research plays an important role in creating the initial hypotheses and concepts that eventually transition into code on blockchains. As blockchain networks continue to grow in adoption, the need increases to conduct new research to optimise blockchain scalability and security. Additionally, universities are beginning to launch more blockchain courses to satisfy demand from students looking to enter this fast-growing industry. Examples of partnerships between blockchain networks and universities to promote blockchain research and education include the Algorand Foundation, the Ethereum Foundation, the Blockchain Education Alliance, and MIT's Digital Currency Initiative. Non-academic research organisations include the Blockchain Research Institute.

### **3.5.5 Journalists and Media**

#### **Journalists and Media**

Examples of stakeholders among journalists and the media include CoinDesk, the Block, CNBC, and Bloomberg. The crypto media landscape has grown considerably, facilitated by the emergence of new and successful cryptocurrencies and blockchain startups. Crypto media outlets consist of online news publishers, podcasts, YouTube channels, researcher publications, and mainstream channels. The primary incentive of crypto media outlets is to spread the latest information about current events while also providing industry analysis and education on topics within the cryptocurrency and blockchain ecosystem. Many industry influencers establish their positions as media members, leveraging self-publishing platforms like Twitter, YouTube, Medium, and Substack to provide unique insights into the crypto markets and analysis of new developments in the space.

#### **Insights on Crypto Twitter**

Crypto Twitter is recognised as one of the main sources of major news and information from the crypto and blockchain ecosystem. While this sector of the Twittersphere is relatively small, it includes a vibrant subculture of influencers, researchers, traders, and investors who engage in extensive debates about topics ranging from the merits of different blockchains and protocols (Bitcoin versus Ethereum, Ethereum versus Cardano, Uniswap versus Sushiswap) to the future of the ecosystem as a whole and the best path to mainstream adoption. Other topics that are prominent on Crypto Twitter include the sharing of price targets, breaking news about new projects and current events, and “leaking alpha”: a practice in which industry insiders and influences offer unique insights into the market.

#### **Competitive Dynamics**

Cryptocurrency media is not exempt from the business model challenges that traditional media companies face. The use of ad-based revenue models can sometimes create incentives for news outlets to publish sensational headlines and misrepresentations of the truth to drive traffic. Despite these flaws, crypto media consumers benefit from the ability to acquire the information directly from the source (such as developers and company founders) and a variety of small and large independent outlets that share their views. Newsworthy information about startups or blockchain networks generally comes from the bottom up, with developers sharing updates about their projects via Twitter, Telegram, Discord, and other forums.

Additionally, because the ecosystem is primarily retail-driven and relatively new, it is difficult for any media outlet to establish a shared information monopoly. When claims made by crypto media outlets are contested, the sources themselves, in addition to reputable influencers and individual publishers, are generally willing to share facts on Twitter, Discord, or Telegram that support or disprove these claims, creating an added layer of information dissemination.

## Crypto Media Versus Mainstream Media

In recent years, mainstream media outlets like CNBC and Bloomberg have increased their coverage of the cryptocurrency markets. Some of this coverage focuses on the price of bitcoin, new concerns around regulations, and influential figures in the investing world.

CoinDesk, the largest crypto media outlet, with more than 11.5 million global readers, reported that 64% of its readers are between the ages of 18 and 34 (CoinDesk, 2018). Around 41% of the site's readers have an average annual household income of over US \$100,000. By contrast, the median age of Bloomberg viewers is 48 years old, with an average annual household income of US \$148,000 (National Media Spots, n.d.a.). For CNBC, the median age of viewers is 57 years old, with an average annual household income of US \$160,000 (National Media Spots, n.d.b.). This same demographic (45–65) represents about 16% of CoinDesk's readers (CoinDesk, 2018).

Insights on media audience demographics present an opportunity for crypto advocates to pinpoint key media outlets where the largest gaps in coverage and knowledge exist and make efforts to be featured more prominently on those outlets to educate the general public.

## Guest Video: Media Perception

In this video, Matt Brown, Vice President of Corporate Development at LO3 Energy, gives his perspective on the media's perception of crypto and how it's changing.



As far as media perception of crypto goes, I have seen a material shift just in the—seemingly, the recognition of inevitability is starting to creep in versus what I would classify as a more critical, sceptical, dismissive set of undertones that dominated the previous cycles. We're not at that full acknowledgment. But just the volume of coverage in, I would say, more neutral lights versus sceptical is indicative that they themselves acknowledge their audience cares and that this is not going away anytime soon.

### 3.5.6 NGOs and Global Institutions

#### NGOs and Global Institutions

This stakeholder group consists of non-governmental organisations (NGOs) such as the United Nations (UN), the United Nations International Children's Education Fund (UNICEF), Oxfam, and the Human Rights Foundation, and foundations in the blockchain industry, such as Ethereum, MakerDAO, and Tezos. Blockchain technology has the potential to enhance the way NGOs operate around the world.

Some of the immediate benefits of NGOs adopting blockchain include:

- Direct distribution and accountability of charitable funds donated to beneficiaries.

- Increased transparency and verification of at-risk populations through the use of digital identities.
- More transparent supply chains that efficiently deliver resources to populations affected by a crisis.

## Guest Video: Stakeholders in the Ethereum Foundation

In this video, Aya Miyaguchi, Executive Director of the Ethereum Foundation, talks about the Ethereum Foundation's stakeholders.



To define the Ethereum ecosystem is not easy because it's always growing and changing. But first, there are people working together on the protocol itself, protocol of Ethereum, and proposing new ideas, doing research and development, including pooling, security work, and other tests. And they're also application developers innovating like in all types of ways using the technology itself. And also the team, there are people trying to break systems and end up hardening them, or also there are whole industries along security. And the largest group by far these days are the millions of users taking part in using those applications, can be students, can be businesses, nonprofits, and governments.

They're all now exploring how they can make the most out of what's being built. And in this, the Ethereum Foundation's mission is to support and maintain the health of ecosystems. So naturally, the Ethereum Foundation needs to engage with all types of players. We support research and development of the protocol layer and other public goods funding, often coordinating together with external teams, universities, and organisations in the ecosystem. We also support some specific projects and applications that can be good experiments or that would be great examples of how we can bring a positive impact to the world.

And with this, we have teams that support the funding and all the coordination around either proactively or by receiving applications. There's also a team targeting emerging economies called team experience, as I simply believe the next billion users of these team are there, and 15 just started the same Foundation Fellowship programme this year to work with changemakers whose projects have high potential to set examples for others, including those in developed countries.

And the important thing is that the Ethereum Foundation filled the gap where no one else would. And it maintains the health of the ecosystems. We do not have to step in if things are working organically well, or in a healthy way. So with this, the stakeholders we engage with are meant to change all the time too. How do I see the role had shifted and also is going to shift, is—well I believe it is going to shift, keep shifting depending on how the ecosystem grows. And the healthier ecosystem, the less the Ethereum Foundation is needed is how we believe.

And we've changed a lot already, and it's still healthy to have an ecosystem-first nonprofit like us in the industry, but we don't want to be the only group serving this purpose. So we've been encouraging others to join. And it's been great to see other DAOers/DOAs and funders popping up this year to join us to do the supporting role. So we just want to make sure that someone stays focused on why we got involved in this first place and building out the technology without bias towards enterprise or other interests.

## Notable NGOs and Global Institutions

Here are some of the notable NGOs that are leveraging blockchain technology, as well as some projects these organisations have begun:

### The United Nations

- Providing blockchain solutions to distribute funds in Syria
- Using unique checkout methods to manage the World Food Program (WFP)
- Tracking the supply chains of pig farmers in Papua New Guinea
- Exploring blockchain solutions for Nepalese workers stationed in the UAE
- Launching an Innovation Network

### The United Nations International Children's Education Fund (UNICEF)

- Launching a cryptocurrency fund to receive, hold, and disburse donations of cryptocurrencies and a venture fund

### Oxfam International

- Partnering with ConsenSys and Australian fintech company Sempo to launch the UnBlocked Cash project (UBC), a cash transfer solution powered by blockchain technology

### Blockchain Foundations and DAOs

- Ethereum Foundation donating US \$150,000 worth of bitcoin and Ether to UNICEF for a project that connects schools in different countries to the internet

### Guest Video: The Bitcoin Developer Fund

In this video, Alex Gladstein, Chief Strategy Officer at the Human Rights Foundation, discusses the Human Rights Foundation and the Bitcoin Developer Fund.



So far, Bitcoin has, essentially, a model of financing its growth that's sort of like a patronage model. There is no pre-mine or pre-farm. It's not like Satoshi set aside a bunch of Bitcoin at the beginning to fund development.

It has been done at the beginning by people who essentially were volunteers who were just excited by the project. And more recently, in the modern era of Bitcoin, it's usually been funded

by corporations who are incentivised for different reasons, to want to give back to Bitcoin and make it a more robust system.

So, typically, corporations exchanges, et cetera, have basically underwritten salaries for developers. We at HRF would like to see more human rights groups, non-profits, universities, colleges get involved in this process of doing Bitcoin research, research and implementation.

So MIT, of course, has the DCI, which is like the pioneer when it comes to universities and colleges. And we want to see more of that. There's just very little when we actually think about how far we are in Bitcoin, how valuable it is, how many people use it around the world. The academic world is lost completely when it comes to their potential role in supporting research and development on Bitcoin.

But also, the non-profit world. I mean, I'd love to see Amnesty International get involved. I'd hope that they can start to understand that this is such a powerful tool for the oppressed and for the vulnerable, and maybe they want to take a role in supporting the network, helping it grow stronger, helping it grow more resilient, helping Bitcoin become a better tool for the human rights activists.

So that's what we're doing at HRF. We are looking at devs increasingly around the world in different places. Our latest round of gifts included devs who are from Korea, India, and Nigeria, as well as from the Arab world. And we're giving them gifts, no strings attached, as sort of recognition for their work, to support what they're doing.

And what are they doing? Some of them are working on making it easier to run a full node in Bitcoin so that the network becomes more robust. Some of them are making are making it easier to do multi-signatures so that you can store your funds more securely.

Some of them are working on apps that allow people who have not great technology or internet access to use Bitcoin a little more easily. Some are using it to make the app ecosystem more privacy protecting. Some of them are using the funds to make these apps more usable. Because honestly, a couple of years ago, Bitcoin wasn't very usable. But now, it's getting there. I mean, the user design is great these days.

So we want to keep pushing that forward. We also want to do more in terms of advocacy, education. So we're funding some translation of Bitcoin works into many different languages. And doing things like privacy newsletters, awareness.

So we just want to do what we can as a nonprofit to try and give back to the people who are improving the ability of Bitcoin, to be that human rights tool that many people are realising it is.

### 3.5.7 Key Takeaways, References, and Further Exploration

#### Key Takeaways

Let's review the key points of this section:

1. The fast pace of innovation in the cryptocurrency and blockchain ecosystem is forcing regulatory bodies to quickly create new rulings on things like taxes and securities to keep up.
2. The general public, who are the users of blockchain technology, are either passive crypto owners, active crypto owners, non-crypto owners, or underbanked persons with limited to no access to the internet or basic financial services.
3. For crypto blockchain to be as widely adopted as the internet, the general public needs to be able to do things like make payments or exchange value without deep technical knowledge.
4. While the US has not written new regulations specifically for crypto, in recent years it has clarified that many existing regulations apply to cryptocurrencies, as demonstrated by the US Securities and Exchange Commission (SEC) position that existing security laws apply to digital assets. Other agencies have issued advisories concerning cryptocurrencies. For example, the US Office of Foreign Assets Control (OFAC) has warned of the sanctions risks of facilitating ransomware payments using cryptocurrencies (Boucher et al., 2021).
5. Due to the financial potential of cryptocurrencies, some nations and states are establishing crypto-friendly regulations like lower business taxes, transparent regulations and guidance, legislation that permits necessary access to the banking system, and policymakers that are open to technological innovation to incentivise blockchain companies to establish themselves locally.
6. Blockchain and cryptocurrencies are not immune from regulatory and geopolitical complexities, especially regarding subjects like taxation and privacy.
7. Academic institutions support the blockchain ecosystem through research and education of the next generation of blockchain developers.
8. Crypto Twitter is an important source of cryptocurrency information. Crypto media outlets also spread information and analyse the industry, while influencers share their expertise on social media or self-publishing platforms. Although disinformation can be spread on Twitter and other platforms, reputable influencers and individual publishers are generally willing to engage on social media to support or disprove claims, creating an added layer of information dissemination.
9. NGOs can benefit from blockchain technologies through direct distribution and accountability of charitable funds donated to beneficiaries, increased transparency and verification of at-risk populations through digital identities, and more transparent supply chains to efficiently deliver resources to populations affected by a crisis.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 19 March, 2022.

### 3.5.2 General Public

Chainalysis. (September, 2020). The 2020 Geography of Cryptocurrency Report. <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Geography-of-Crypto.pdf>

Fries, T. (2021, 23 September). Africa's crypto market has grown by \$105.6 billion in the last year. *World Economic Forum*. <https://www.weforum.org/agenda/2021/09/what-are-the-implications-of-widespread-cryptocurrency-adoption-in-africa>

The World Bank. (2017). The Unbanked. [https://globalindex.worldbank.org/sites/globalindex/files/chapters/2017%20Findex%20full%20report\\_chapter2.pdf](https://globalindex.worldbank.org/sites/globalindex/files/chapters/2017%20Findex%20full%20report_chapter2.pdf)

### 3.5.3 Policymakers and Governments

Böhi, R., Wenger, D., & Wandel, S.A. (2017, 27 December). Switzerland: Taxation Of Initial Coin Offerings In Switzerland. *Mondaq*. <https://www.mondaq.com/tax-authorities/659078/taxation-of-initial-coin-offerings-in-switzerland>

Comply Advantage. (2020). Cryptocurrency Regulations in Japan. <https://complyadvantage.com/knowledgebase/crypto-regulations/cryptocurrency-regulations-japan>

Comply Advantage. (2021). Cryptocurrency Regulations in Singapore. <https://complyadvantage.com/knowledgebase/crypto-regulations/cryptocurrency-regulations-singapore>

De, N. (2021, 9 June). It's Official: El Salvador's Legislature Votes to Adopt Bitcoin as Legal Tender. *CoinDesk*. <https://www.coindesk.com/its-official-el-salvadors-legislature-votes-to-adopt-bitcoin-as-legal-tender>

Evans, C. (2020, 27 June). The Great Estonian Exodus — Crypto Firms Are Leaving Estonia. *Cointelegraph*. <https://cointelegraph.com/news/the-great-estonian-exodus-crypto-firms-are-leaving-estonia>

FTX. (2021). FTX Terms of Service. <https://help.ftx.com/hc/en-us/articles/360024788391-FTX-Terms-of-Service>

Hills, B., & Feikert-Ahalt, C. (2018, 31 August). Malta: Government Passes Three Laws to Encourage Blockchain Technology. *Library of Congress*. <https://www.loc.gov/law/foreign-news/article/malta-government-passes-three-laws-to-encourage-blockchain-technology>

McSweeney, M. (2021, 24 April). Wyoming ‘DAO law’ to go into effect in July after receiving final approval. *The Block Crypto*. <https://www.theblockcrypto.com/linked/102813/wyoming-dao-law-to-go-into-effect-in-july-after-receiving-final-approval>

### 3.5.5 Journalists and Media

CoinDesk. (2018, February). Audience Profile. <https://media.coindesk.com/uploads/2018/03/CoinDesk-Audience-One-Sheet.pdf>

National Media Spots. (n.d.a.). Bloomberg Television - Network Profile. <https://www.nationalmediaspots.com/network-demographics/Bloomberg.pdf>

National Media Spots. (n.d.b.). CNBC - Network Profile. <https://www.nationalmediaspots.com/network-demographics/CNBC.pdf>

## Further Exploration

[Gitcoin Grants - Quadratic Funding](#)

[Blockchain Research Institute](#)

[The Blockchain Association](#)

[Global Blockchain Business Council \(GBBC\)](#)

[Blockchain Industry Group](#)

[American Blockchain & Cryptocurrency Association \(ABCA\)](#)

[Association of Crypto Currency Enterprises and Start-ups Singapore \(ACCESS\)](#)

[International Association for Trusted Blockchain Applications \(INATBA\)](#)

[Malta: Government Passes Three Laws to Encourage Blockchain Technology](#)

[Cryptocurrency Regulation and Enforcement at the US Federal and State Levels](#)

[Decoding Crypto: Are There Regulations in the U.S. For Cryptocurrency?](#)

# 3.6 Stakeholder Considerations

## 3.6.1 Overview of Stakeholder Considerations

### Overview

In developing an engagement strategy and communications plan for a blockchain project, it is important to consider key factors that affect the stakeholders and the project itself.

This section explores these considerations in the context of internal and external stakeholders and highlights the key considerations to make during the preparation and development of a blockchain technology solution. Keep in mind what you just learnt about the roles and incentives of each type of stakeholder that you might engage with. These considerations also form an important part of the stakeholder engagement framework that you take away at the end of this module.

## 3.6.2 Internal and External Stakeholder Considerations

### Internal and External Stakeholder Considerations

Creating a list of the stakeholders that impact your blockchain technology project and answering the questions below helps you develop a strategy for engaging and communicating with stakeholders. An effective strategy includes internal, external, and industry stakeholders.

### Internal Stakeholder Considerations

In the context of the internal stakeholders and your blockchain project, answer the following questions:

1. What is the primary goal of your blockchain technology solution?
2. How will you assimilate a blockchain solution within any existing technology infrastructure?
3. Is it appropriate to utilise a public permissionless network (for example, Bitcoin or Ethereum), a distributed network with select participants, or a privately controlled network?
  - If you opt for a public permissionless network, will you be building and launching your own?
  - If not, which existing network will you build on (Bitcoin, Ethereum, Stellar, or a different network)?
4. How much of your solution will be outsourced to vendors versus developed internally?

5. What are the talent gaps within your organisation, business, or project that you must fill to develop and operate this blockchain solution?
6. Which internal stakeholders can contribute the most value (in terms of knowledge, relationships, or skills) to the implementation of your solution?
7. Which internal stakeholders have the most influence on your ability to implement a blockchain solution?

## External Stakeholder Considerations

In the context of the external stakeholders and your existing blockchain project, answer the following questions:

1. Which institutions and/or industry communities could you partner with to conduct the following:
  - Research
  - Receiving consultation on solution viability
  - Establishing frameworks for blockchain governance and industry standards
  - Creating advocacy
  - Achieving regulatory clarity and approval
  - Raising funds
  - Acquiring users
2. Which criteria should you use to evaluate enterprise blockchain service providers?
3. What framework should you use to determine the most suitable network technology and deployment configuration?
4. What framework should you use to distinguish competitors from potential partners?
  - Who are your competitors in this space?
  - Whom should you partner with to share governance?
5. Who are the regulatory authorities that you need to engage with to garner support?
  - What relevant causes are participants in the ecosystem already lobbying for? How can you support them?

6. How could you assimilate a blockchain solution within your existing institutional, regulatory, social, economic, and physical systems?
7. How could you leverage influencers in this space to advance your goals?
8. Which blockchain business models and consortiums already exist in your groups' combined industries? Is it more beneficial to replicate them or join them?

The next section shows you how to create stakeholder mapping exercises, which is an important part of the framework for engaging stakeholders.

### 3.6.3 Key Takeaways

#### Key Takeaways

Let's review the key points of this section:

1. In developing an engagement strategy and communications plan for a blockchain project, it is important to consider key factors that affect the stakeholders and the project itself.
2. Internal, external, and industry stakeholders need to be considered carefully and strategically in the following ways:
  - By identifying strategic partnerships with complementary offerings, influencers, and industry communities to support funding, development, functional, or marketing needs.
  - By assessing the regulatory climate and identifying key policymakers.
  - By understanding the competitive landscape and identifying market leaders in each sector.
3. In summary, the key considerations and questions to address when creating your strategy fall into the following categories:
  - Goals of the blockchain solution
  - Talent and outsourcing
  - Current infrastructure
  - Regulatory authorities
  - Type of blockchain
  - Existing institutional, regulatory, social, economic and physical systems

- Type of business model
- Your competitors
- Potential partners
- Service providers
- Influencers in the industry
- Stakeholders who can contribute the most value to the implementation of the solution and who have the most influence
- Network technology and deployment configuration

## 3.7 A Framework to Engage with Stakeholders

### 3.7.1 Overview of a Framework to Engage with Stakeholders

#### Overview

Now that you have learnt about the internal and external stakeholders involved in the development and implementation of your blockchain technology solution, we'll dive into the strategies and frameworks for engaging with each type of stakeholder. You can apply this framework to any blockchain project. The goal is to map each stakeholder to their level of interest and influence on implementing a blockchain solution by using the stakeholder mapping exercise.

The table below shows the categories of internal and external stakeholders.

Internal Stakeholders	External Stakeholders
<b>Team and employees</b> <ul style="list-style-type: none"><li>• Executives and management</li><li>• Financial operations</li><li>• Legal and compliance</li><li>• Product development</li><li>• Sales and marketing</li><li>• Customer support or success</li></ul>	<ul style="list-style-type: none"><li>• Industry communities</li><li>• Competitors</li><li>• Corporations and enterprises</li><li>• Influencers</li><li>• Venture capital (VC) and financial investors</li><li>• Industry regulators</li><li>• General public</li><li>• Governments and policymakers</li><li>• Academic institutions</li><li>• Journalists &amp; media</li><li>• Non-profit organisations (NGOs) &amp; other global institutions</li></ul>
<b>Shareholders</b> <ul style="list-style-type: none"><li>• Founders and owners</li><li>• Angel investors</li><li>• Venture capitalists</li><li>• Stockholders</li><li>• Mergers and Acquisitions (M&amp;A) shareholders</li></ul>	
<b>Company board</b> <ul style="list-style-type: none"><li>• Chairman</li><li>• Vice-Chairman</li><li>• Treasurer</li><li>• Secretary</li></ul>	

### 3.7.2 Stakeholder Mapping Exercise

#### Stakeholder Mapping Exercise

A stakeholder mapping exercise is a process of prioritising internal and external stakeholders according to their level of influence, interest, and participation in a project.

There are four main categories of stakeholders in terms of their influence on a blockchain project:

- High influence and low interest
- High influence and high interest
- Low influence and low interest
- Low influence and high interest

Each category above is associated with a particular approach to engaging these stakeholders. The four approaches are:

- Keep satisfied
- Key players
- Monitor
- Keep informed



Each stakeholder category can be put in order of priority for engagement:

- **High influence and low interest → Keep Satisfied**
  - These stakeholders should be kept satisfied because of their high influence. However, you should not engage with them too frequently, as they do not express explicit interest in your project.
- **High influence and high interest → Key Players**
  - These are the most important stakeholders to prioritise and keep happy as you progress with your project.

- **Low influence and low interest → Monitor**
  - These stakeholders should be monitored, but do not communicate too frequently.
- **Low influence and high interest → Keep informed**
  - Stakeholders with low influence but high interest should be kept in the loop and informed about your project, as they could convert into high influence stakeholders later.

Think about where you would place the internal and stakeholders relevant to your blockchain project in relation to the diagram above.

### 3.7.3 Developing a Stakeholder Engagement and Communication Plan

#### Developing a Stakeholder Engagement and Communication Plan

Once each stakeholder is mapped according to their level of influence and interest, you'll need to strategically assess the best way to engage each stakeholder to garner their support. A stakeholder engagement and communication plan enables you and your team to more effectively allocate time and resources towards those who have the most impact on your project's needs. It also provides you with a formulaic process for developing and executing a go-to-market strategy. You can stay one step ahead of the market by anticipating the needs of your stakeholders and identifying the most effective communication vehicles based on prior information.

The initial questions and considerations you should answer include:

- What is each stakeholder's motivation?
- What are their priorities, and how best can you align your project and messaging to fit those priorities—or, at the very least, not conflict with them?
- How receptive will stakeholders be to your project? How should you manage stakeholders who have a positive or negative response?

### 3.7.4 Key Takeaways

#### Key Takeaways

Let's review the key points of this section:

1. A stakeholder mapping exercise is a process of prioritising internal and external stakeholders according to their level of influence, interest, and participation in a project to develop a stakeholder engagement and communication plan.
2. Each stakeholder category can be put in order of priority for engaging with them:
  - High influence and high interest are “Key Players” who are the most important stakeholders to prioritise and keep happy as you progress with your project.
  - High influence and low interest are “Keep Satisfied” stakeholders who should be kept satisfied because of their high influence. However, they should not be engaged too frequently, as they have not expressed interest in your project.
  - Low influence and high interest are at the “Monitor” level. They are stakeholders with low influence but high interest. They should be monitored for feedback and kept informed about your project, as they could convert into high influence stakeholders later.
  - Low influence and low interest are “Keep informed” stakeholders who should be kept informed, but not too frequently.
3. Once you have ranked your stakeholders according to their level of interest and influence, you can attempt to understand what you will need to engage them based on the content and collateral that applies to them.

## 3.8 Case Study: LO3 Energy

### Case Study: LO3 Energy

A 2018 research report by Mary C. Lacity at the University of Arkansas assesses the strategies of three organisations as they develop blockchain solutions for different target industries. The study aims to evaluate how each entity was addressing known managerial challenges in the areas of:

1. **Standards:** How are organisations defining standards for access rights, data structures, and allowable transactions for their blockchain solutions, given that no single blockchain standard has yet emerged?
2. **Regulations:** How are organisations ensuring blockchain applications will comply with regulations, given that regulators worldwide are struggling to adapt laws because of the newness of the technology?
3. **Shared governance:** Given that, in many deployment configurations, no single organisation owns or controls a blockchain network, how will the blockchain solution be governed?
4. **Viable ecosystem:** How will organisations attract a critical mass of adopters of a blockchain solution beyond the core originators?

Each challenge requires a unique approach towards defining and engaging stakeholders. This section will focus on just one of the organisations: a startup called LO3 Energy.

LO3 Energy, a private US-based company, has built a technology platform to create peer-to-peer markets and enable residents in different parts of the world to buy and sell the energy they produce locally.

The firm launched its pilot project, the Brooklyn Microgrid, in 2016, to enable New York residents to trade renewable energy across a microgrid leveraging the Ethereum blockchain for transparent and secure transactions. Since then, the company has expanded its peer-to-peer energy trading operations to different locations, including Texas, Vermont, Australia, and Japan. Most recently, LO3 Energy completed a US \$11 million Series B funding round to scale commercial applications of its innovative local energy platform (Ledger Insights, 2021).

In the process of launching LO3 Energy, founder Lawrence Orsini had to engage with multiple stakeholders, including local communities, manufacturers, developers, regulators, and institutions.

### Hardware Manufacturers

The platform that LO3 built to buy and sell locally produced energy is called “Exergy”. LO3 partnered with industrial manufacturing company Siemens to help build physical grids that would enable locally generated power to be routed to different locations when needed.

## Software Development

LO3's proof of concept was built on the Ethereum blockchain, though the company would later investigate alternative networks in search of faster transaction speeds.

## Local Communities

To have a successful launch, LO3 had to create an engagement plan for local communities. Orsini recognised that LO3's value proposition would resonate strongly with New York residents who had experienced severe power outages during the floods caused by Hurricane Sandy in 2012, when over 800,000 residents and businesses experienced power outages that lasted several days. At the time, residents were unable to rely on solar panels to generate their own power because the utility grids that connected to the panels had also failed. Orsini believed memories of this incident would motivate residents to support a peer-to-peer marketplace for trading locally produced energy.

The Brooklyn Microgrid project ran its first live test of the Microgrid in 2016 in a residential neighborhood on President Street in Brooklyn. The high concentration of solar adopters and residents interested in green technology made this the ideal location to run a test.

The test was conducted to prove that smart meters could record electricity from solar panels and store the data on a blockchain, where it would be accessible to "prosumers" (neighbours with solar panels) and consumers to trade power with each other.

## Regulators

To comply with state regulations, LO3 became a licensed utility provider. The team also worked closely with regulators in New York and met with the US Federal Energy Regulatory Commission to ensure that they were adhering to all applicable policies. As LO3 expanded operations, educating and engaging with regulators became a repeated process throughout other jurisdictions in the US, countries like Australia, and parts of Europe.

## Guest Video: Convincing Community Stakeholders and Investors

In this video, Matt Brown, Vice President of Corporate Development at LO3 Energy, describes how the company engages with stakeholders to get buy-in.



In terms of the other stakeholders, the community engagement is a macro theme that we do focus on in terms of keeping value in the communities. Ultimately, that's a bit easier than convincing some of the other commercial counterparties required in the sense that, typically, even in the context of some of the regulatory changes that have happened over the last couple of years, the transactions that can occur in these local models, typically, offer a discount to the participants.

And so one of the major issues in the energy space in getting residential customers in particular engaged is people care about green. They care about the environment and climate. But ultimately it comes down to economics.

And that has been tried and true for decades. No different now. So we typically focus on, ideally, a win-win economic situation for both the asset owners or the prosumers and the consumers, ideally getting a premium for their exports in the case of the solar owners and buying at a discount. So that is really a key, let's say, criteria for defining, let's say, the contours of a project.

Getting the commercial incumbents, really, our customers, our partners, engaged is a harder process in the sense that you need to align commercial incentives for them via transaction fees or subscription fee opportunities, ways that they can maintain their margin in an evolving relationship with their customers. These entities are conservative, not typically classified as innovative, progressive entities. So you've got a multi-stakeholder process even inside these large organisations where you're engaging with the innovation team or the customer solutions team who see the value in these types of solutions.

But getting buy-in from the billing organisation, getting buy-in from the security and the IT folks, getting buy-in from the requisite executives, these are long sales cycles, long engagement that requires the same level of education and kind of information sharing to even get started. And those—I think we are seeing much more maturity in those processes in the last year or two relative to our first couple of years, when the market was quite early.

Investors—we are a venture backed organisation. We've had good success in aligning with strategic corporate investors. So in the Series A for the company Siemens and Centrica out of the UK, Shell Ventures led our Series B earlier this year. And the alignment with their own product development and sort of evolution of their own business models, we are an interesting potential part of those pictures.

Financial investors are a bit of a different story, in that, yes, this is a new market, yes, it potentially has some big upside, there's still a lot of reticence on the part of your traditional financial VCs to invest in models that are looking to disrupt or move the utility space because of the pain from this clean tech 1.0 cycle a decade ago and some of the correct and valid criticisms about the challenges in selling to utilities, working with them.

The pace at which these markets evolve typically does not align with return profiles for these early stage financial investors. So kind of threading the needle between highly disruptive, a model that can scale globally, and showing path to near-term revenue while projecting the long term kind of disruptive, high TAM is what we've been trying to do.

## Case Analysis

Having read the LO3 Energy case analysis, consider using the following key questions as discussion points for a class discussion in the Riff platform:

- Which stakeholders were essential to the successful launch of the LO3 project, and to which categories did they belong?
- Identify the situations in this case study where stakeholder planning and engagement were essential. Why were these moments so important?
- Which stakeholders were most critical in LO3 Energy addressing each of the four managerial challenges?

## References

### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 12 April, 2022.

Lacity, M. (2018, September). Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality. *MIS Quarterly Executive*, Volume 17 : Issue 3. <https://static1.squarespace.com/Blockchains2018.pdf>

Ledger Insights. (2021, 12 March). Shell leads \$11 million Series B for renewables blockchain startup LO3 Energy. <https://www.ledgerinsights.com/shell-leads-11-million-renewable-energy-blockchain-startup-lo3>

### Further Exploration

Read the full LO3 case study [here](#), and then return for discussion in the Riff platform.



**Module 4:**

# Challenges - Legal, Regulatory, ESG, and Organisational Considerations

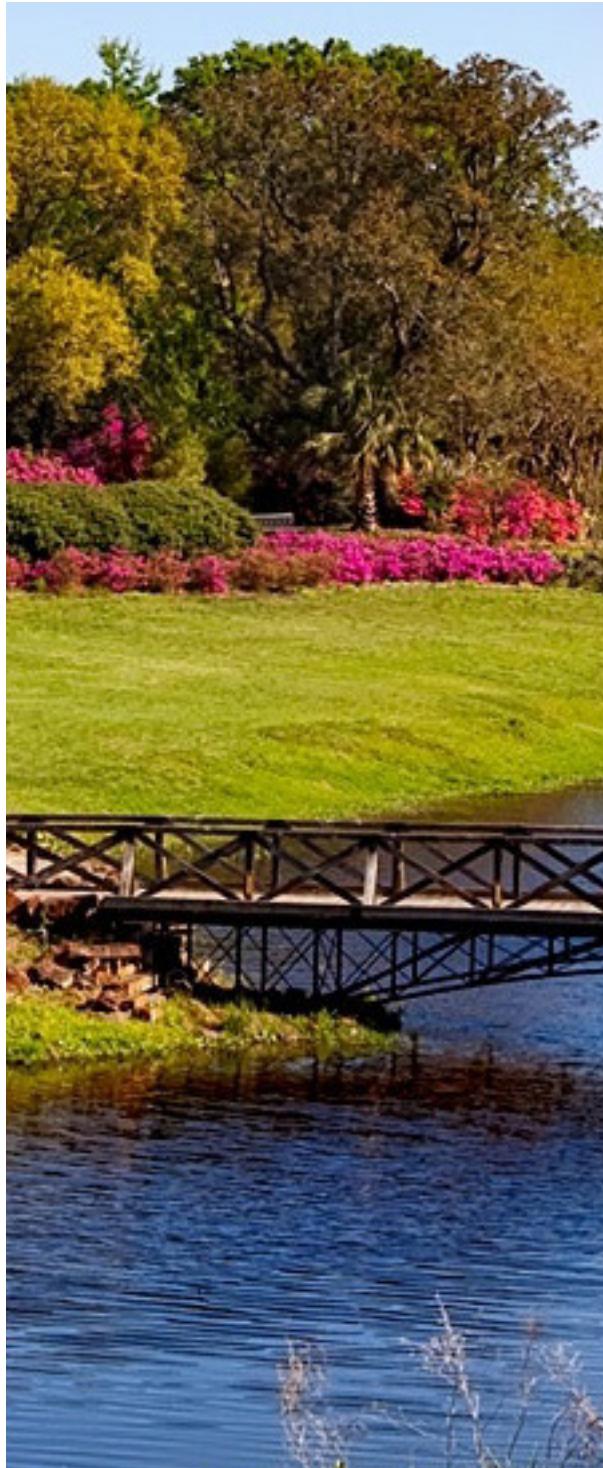
---

**Oxford Blockchain Strategy Programme**  
2022

# Oxford Blockchain Strategy Programme

## Challenges - Legal, Regulatory, ESG, and Organisational Considerations

### Table Of Contents



<b>4.1 About Module 4</b>	<b>3</b>
4.1.1 Overview of Module 4	3
<b>4.2 Blockchain Technology and Decentralised Authority</b>	<b>6</b>
4.2.1 Overview of Blockchain Technology and Decentralised Authority	6
4.2.2 Digital Space and Meatspace	8
4.2.3 Informal Versus Formal Rule Structures	10
4.2.4 Key Takeaways and References	13
<b>4.3 Legal Statuses and Challenges</b>	<b>15</b>
4.3.1 Overview of Legal Statuses and Challenges	15
4.3.2 Is Code Law? Blockchain Technology Meets the Courtroom	15
4.3.3 Case Study: Uniswap Licenses Code to Discourage Copycats	17
4.3.4 Jurisdictional Issues	18
4.3.5 Other Legal Considerations	20
4.3.6 Cryptocurrency Crime Analysis	26
4.3.7 Key Takeaways, References, and Further Exploration	32
<b>4.4 The Regulatory Environment</b>	<b>36</b>
4.4.1 Overview of the Regulatory Environment	36
4.4.2 Regulations and Industry Principles	37
4.4.3 Regulations Around the World: China and the EU	39
4.4.4 Regulations Around the World: The UK and US	44
4.4.5 Regulatory Arbitrage and Domicile Choice	49
4.4.6 Case Study: BitLicense—New York's Regulatory Initiative for Virtual Currency	51
4.4.7 Regulatory Acronyms, Key Takeaways, References, and Further Exploration	53
<b>4.5 Environmental, Social, and Governance (ESG) Standards</b>	<b>59</b>
4.5.1 ESG Overview	59
4.5.2 Environmental Challenges	61
4.5.3 Case Study: Tokensoft Offers the World's First Carbon-Neutral Bitcoin	63
4.5.4 Social Challenges	64
4.5.5 Governance Challenges	69
4.5.6 Addressing ESG Concerns	70
4.5.7 Key Takeaways, References, and Further Exploration	72
<b>4.6 Organisational Considerations</b>	<b>75</b>
4.6.1 Overview of Organisational Considerations	75
4.6.2 Organisational Structures and <i>The Nature of the Firm</i>	75
4.6.3 The Blockchain Platform's Advantages Over the Traditional Platform	77
4.6.4 Other Organisational Challenges	80
4.6.5 Key Takeaways, References, and Further Exploration	83
<b>4.7 Challenges Framework</b>	<b>85</b>
4.7.1 Overview of Challenges Framework	85
4.7.2 Endogenous and Exogenous Variables	86
4.7.3 Regulatory, Legal, and ESG Challenges	86
4.7.4 Timescale Considerations	87
4.7.5 Key Takeaways	88
<b>4.8 Case Study - BitMEX and Know Your Customer, Anti-Money Laundering</b>	<b>89</b>
4.8.1 Overview of BitMEX	89
4.8.2 What Is Next for BitMEX?	92
4.8.3 Key Takeaways, References, and Further Exploration	93

# 4.1 About Module 4

## 4.1.1 Overview of Module 4

### Overview

Welcome to Module 4 of the Blockchain Strategy Programme!

In Module 4, you will examine organisational considerations related to decentralised authority and its challenges in the legal, regulatory, and environmental, social, and governance (ESG) areas of a blockchain project. Through this exploration, you will discover the dynamics of platform strategies and learn how to frame your blockchain project by addressing these considerations.

You'll study the following concepts in this module:

- Decentralised authority in blockchain technology, how it differs from distributed ledger technology concepts, and how it is different from traditional hierarchical structures.
- The Presidio Principles and their importance in developing a blockchain organisation.
- Legal incompatibilities of blockchain technology with current jurisdictional law.
- Regulatory industry principles and specific regulatory efforts in Europe and the UK, the US, and China.
- Environmental, social, and governance (ESG) issues and considerations in the blockchain ecosystem.
- How to utilise blockchain platform strategies to develop an ideal organisational structure.

### Programme Director Video: Introduction to the Challenges of Implementing a Blockchain Strategy

In the following video, Meltem Demirors provides an overview of the challenges and considerations in formulating a blockchain strategy.



Welcome to module four of the Oxford Blockchain Strategy Programme. Over the last few weeks, you've heard a lot about the benefits and opportunities of blockchain technology. This week, you'll learn about some of the unique challenges that exist when attempting to utilise this novel and new technology to solve problems in new ways.

Now, as we go into this module, I want to outline a concept for you. Historically, rules and regulations in our world have been defined by physical perimeter. The borders of nation-states define the rules which we're subject to, and that worked well over the last few centuries of human industry. However, as our

world becomes increasingly digitised and interconnected, regulators around the world are struggling to grapple with how to deal with a global borderless digital technology in the context of rules and lawmaking that have historically been defined by physical location. After all, how do you regulate something like the internet?

In this module, we'll walk through a variety of different challenges, including laws, regulation, and more, but we'll also talk about some of the unique considerations around internal organisational rules, culture, and how you might build an organisational structure that makes you more effective at developing and deploying a blockchain strategy. You'll hear from a variety of innovators and entrepreneurs who themselves have dealt with these challenges. And hopefully take away some exciting new insights as to how you can build your use case in a way to help you overcome some of these challenges.

## Learning Outcomes

By the end of this module, you will be able to:

- Explore the historical perspective on centralised authority and its incompatibility with an increasingly decentralised world with a specific focus on technology.
- Identify Ronald Coase's *Nature of the Firm*'s relevance to the blockchain ecosystem, specifically with an organisational frame of reference
- Recognise how securities, data, privacy, antitrust, and tax laws impact the use of blockchain technology.
- Examine the blockchain regulatory landscape around the world.
- Assess the legal, regulatory, and ESG challenges in blockchain strategies.
- Frame your blockchain project with a perspective on blockchain platform strategies and an understanding of the spectrum of organisational structures.

## Graded Assignments

You will complete individual and group assignments, which count towards your completion of the programme. This week, you will:

- Meet with your group to craft a plan to address ESG concerns and the legal, regulatory, and organisational challenges that affect your blockchain technology use case.
- Complete a quiz on the module's content and key takeaways.
- Reflect on what you have learnt by applying it to your personal or professional experiences.

You must submit all graded assignments in Module 4 by **5 July 2022, 23:59 UTC**. (Try the [Time Zone Converter](#) to get your local time.)

## **Additional Activities**

In each module, we present additional activities related to the core learning. This week, you will:

- Share your thoughts with the class on the BitMEX case study and the lessons you can learn from the company's mistakes as well as the challenges to address upfront when developing a block-chain solution.

## **Time Commitment**

Plan to spend seven to ten hours on Module 4 this week. As there is a lot of reading material and video content, you might want to divide your work into several sessions. The module is broken up into sections by theme, giving you potential break points.

Make sure you plan time to meet with your group, and to complete the assignments.

# 4.2 Blockchain Technology and Decentralised Authority

## 4.2.1 Overview of Blockchain Technology and Decentralised Authority

### Overview

Examining the blockchain ecosystem requires understanding the history and evolution of organisations, starting with the growth of centralised legal, regulatory, and governance authority in the last century—and the emergence of more decentralised systems that are more common in the blockchain ecosystem.

In this module we reference the terms *decentralised* and *distributed*. Both are relevant to blockchain technology concepts; people may use them interchangeably in some cases. For the purposes of this section, *decentralised* relates to topics about authority and governance, while *distributed* relates to protocols and network processes.

### Vocabulary Check

This section introduces the following terms:

- [Presidio Principles](#)
- [self-regulatory organisation](#)

### Bureaucratic Theory

German sociologist Max Weber believed that bureaucracies were the ideal organisational form. During the Industrial Revolution at the turn of the 20th century, Weber's research concluded that the ideal organisational structure was rooted in rules, policies, and procedures, which led to process efficiencies, division of labour, and structured authority (Mulder, 2017).

### The Principles of Scientific Management

Frederick Taylor, a mechanical engineer, supported Weber's conclusions in his 1911 book, *The Principles of Scientific Management*, which defines the role of worker training, hiring, wage incentives, and standards in successful organisations (1911).

### The Nature of the Firm

Ronald Coase wrote *The Nature of the Firm* in 1937 as an economic theory that attempts to discover why firms came into existence. Coase focused on the transaction costs incurred in producing goods

and services. He concluded that transactions are less costly when conducted within the firm, as compared to between independent individuals.

One reason for this would be certain hierarchical and central authorities establishing a rule of order within the firm. Within the firm, leaders give orders, while labourers follow directives from management and, in return, receive a fixed wage. Outside the firm, the labour contractor can negotiate their price. As a result, goods and services created by labour outside the firm cost more to create given the negotiation, coordination, and commitment formalisation required. Other factors that can enable a firm to produce more cheaply include its ability to purchase materials and supplies more cheaply due to purchasing power, other labour needs, and purchasing power of contracted labour from within the firm due to repeat work.

Coase's work provides a base theory for why firms exist and earned him the Nobel Prize in Economics in 1991.

## Theory X and Theory Y

In the 1950s, MIT management professor Douglas McGregor introduced his Theory X, the view that workers wanted to be managed and have financial security, and Theory Y, that workers wanted to be involved with problem-solving and self-direction (Lawter et al., 2015). McGregor's Theory Y provides some of the frameworks for the introduction of decentralised organisations and the power given to employees to participate in decision-making processes.

## The Open Source Software Movement

The open source software movement helped make decentralised authority and organisations more familiar to those working in technology. In 1985, Richard Stallman founded the Free Software Foundation to support the free software movement. Stallman's vision was that software users should have the most freedom possible, not just to use software, but to change it and redistribute it. This freedom necessitated communities of developers who worked through cooperation, not a hierarchy (GNU Operating System, n.d.).

Another notable event in open source history was Eric S. Raymond's publication of *The Cathedral and the Bazaar* in 1997. Building upon Stallman's work and inspired by the success of the Linux operating system, Raymond wrote about the advantages in creativity and efficiency of cooperative networks (bazaars), as opposed to hierarchical organisations (cathedrals), for creating software. He emphasised the importance of peer review in ensuring quality and blamed proprietary (secret) technology for the poor quality of many software products. Raymond's work was influential in Netscape, an early internet browser, becoming an open-source system (Raymond, 1998). The decade following *The Cathedral and the Bazaar* saw the increasing dominance of Linux in server operating systems, and the growth of large-scale open-source projects such as WordPress, new open-source developer tools such as Python, and the growth of GitHub as a platform for enabling open-source development.

## The Revolt of the Public

In his 2018 book, *The Revolt of the Public*, Martin Gurri foresees the dissemination of information through increasing digital means as the public's power to enact change:

My thesis, again, is a simple one. The information technologies of the twenty-first century have enabled the public, composed of amateurs, people from nowhere, to break the power of the political hierarchies of the industrial age.

## Bitcoin and Decentralised Authority

Building on ideas of the open source software movement, Bitcoin was established as a decentralised financial system that could offer its users a community approach to governance and operations. Unlike many traditional organisations, Bitcoin does not have a central authority that controls decisions and resources. Rather, Bitcoin governance is similar to the internet governance, following the Request for Comments (RFC) format that was established in 1969 for the Advanced Research Projects Agency Network (ARPANET) (Nabilou, 2021).

However, Bitcoin governance differs from internet governance in key ways. In particular, stakeholders in the ecosystem—developers, miners, and currency users—are motivated to maintain the Bitcoin network because the digitally scarce asset—bitcoin—is embedded in the system. Miners have an incentive to behave cooperatively to secure and govern the network, or they risk losing compensation. These incentive mechanisms that are built into the Bitcoin network encourage active, cooperative participation in governance (Nabilou, 2021).

Many other cryptocurrencies have followed bitcoin to market, inspiring the formation of decentralised autonomous organisations (DAOs). In Module 6, we will learn more about this structure and its rise and future in the cryptocurrency ecosystem.

In recent news, a study by the National Bureau of Economic Research found that bitcoin is still concentrated in a few hands, which contradicts one of its original objectives: Just 10,000 individual investors own one-third of all bitcoin in circulation. The top 1,000 individual investors own three million bitcoin. The study also found that the top 10% of miners control 90% of the mining capacity and that 0.1% (i.e. ~50) of bitcoin miners control 50% of the mining capacity. This concentration makes bitcoin susceptible to a 51% attack, in which miners could collude to take control of a majority of the network (Graffeo, 2021).

### 4.2.2 Digital Space and Meatspace

#### Digital Space and Meatspace

The Oxford English Dictionary defines “meatspace” as “the physical world, as opposed to cyberspace or a virtual environment” (Lexico, 2021).

The term meatspace refers to the physical world, in which tangible objects exist and humans participate in face-to-face gatherings. Information in meatspace is transmitted through physical artefacts, such as books and other print media, and in-person events, such as speeches or concerts.

Digital space is an evolution of meatspace and represents virtual information, or binary representations communicated digitally via the internet, intranets, or other digitised means. In some representations, humans interact with digital information similarly to how they interact with physical representations of information, such as through e-books. In other representations, such as augmented or virtual reality, human interactions are mediated and transformed by technologies.

Digital space fosters the development of broad-based communities that don't always rely on geographic proximity or centralised authorities for development and governance. The rise of online communities, in particular, has enabled groups to form at a prodigious scale and uncommon speed.

Most companies today operate in hybrid modes, combining digital space and meatspace to optimise business outcomes, whether those organisations are hierarchical or democratic, distributed, or concentrated..

## Guest Video: Digital Space Compared to Meatspace

In the following video, Priyanka Desai, Vice President of Operations at OpenLaw, discusses how much of what is being built in the digital space complements corporations, the firm, and meatspace in general.



Digital organisations are obviously a little bit different than what you would find in meatspace. So meatspace—you have your C corps, you have these, like, mega corporations that exist all over, of course. Like, they have employees and members from all over the world that might work for this larger organisation and its mission. I think with the beauty of DAO and how they operate—it's entirely member-directed and member-managed. So in many ways, there is very little to no bureaucracy. It's very flexible. People can come and go as they please.

Anyone can actually rage quit, as we affectionately call it, or leave the DAO whenever they feel like. Perhaps, like, the mission or mandate of the DAO has changed, or they're not happy, or they just are ready for something new. So there's a lot of modularity, flexibility and freedom to come and go. The way decisions are made are entirely democratically governed. Or let's say if you want to change the fundamental governance of this digital organisation, any individual could propose and write out a—like, depending on what the complexity of the proposal is, they can talk it through with other members, put something up, put it up for a one week vote.

Should it pass, that gets incorporated in the governance document. And so you just, from there, can completely iterate on how the organisation from then on out is governed through these internet communities effectively. Beyond that, there's also the ability to pool your capital and make investments together. So beyond just governing as a community, you can also invest together. And that's a little bit different than, I think, what you see in meatspace world.

You can decide to allocate capital to different digital assets or really anything else that the DAO would like to do. And as I noted earlier, if you're not necessarily—if you're an individual part of one of these DAOs, you're not

necessarily happy with the way things are going, you're more than welcome to leave or sell your interests and move on. And the great thing about the DAO is that open laws put together is because it does actually interact with meatspace just enough, i.e. it's a Delaware incorporated company, everyone's liabilities limited. There is some organisation and touch points to the real world, despite it all being governed and being extremely internet native.

### 4.2.3 Informal Versus Formal Rule Structures

#### Informal Versus Formal Rule Structures

As an ecosystem in its infancy, the blockchain network is establishing industry rules on an ongoing basis to keep pace with its development. Within the young organisations operating in this ecosystem, fast development cycles have sometimes favoured an informal or more flexible organisational structure.

When developing a blockchain strategy, it is important to establish and adhere to ways of working to guide the project's development and, likewise, a governance structure that describes how it will function once deployed.

Some examples of rules-based organisations are as follows:

- In Module 2, we learnt that **shared governance structures** are a means by which stakeholders achieve control, direction and coordination within a blockchain network. Operating decentralised systems requires unique approaches towards governance that would otherwise not be applicable under a traditional corporate structure. Decision rights, accountability, and incentives are three focal points of the governance framework's design.
- A **self-regulatory organisation (SRO)** offers a member-based organisational structure where members establish and agree to follow principles and rules, with penalisation for failing to do so. While the SRO itself is the central authority of the organisation, they are still subject to government rules and regulations. In certain circumstances, the SRO must also register with a government agency, such as US financial SROs must do with the SEC.
- A **blockchain consortium** brings together members of the industry who have a shared vision or goal. The consortium establishes rules to provide operating guidelines, and they may be less stringent than those of an SRO.

Whether an organisation aligns with one of these structures or functions within its own guidelines or not, most will voluntarily operate within industry standards.

#### Presidio Principles

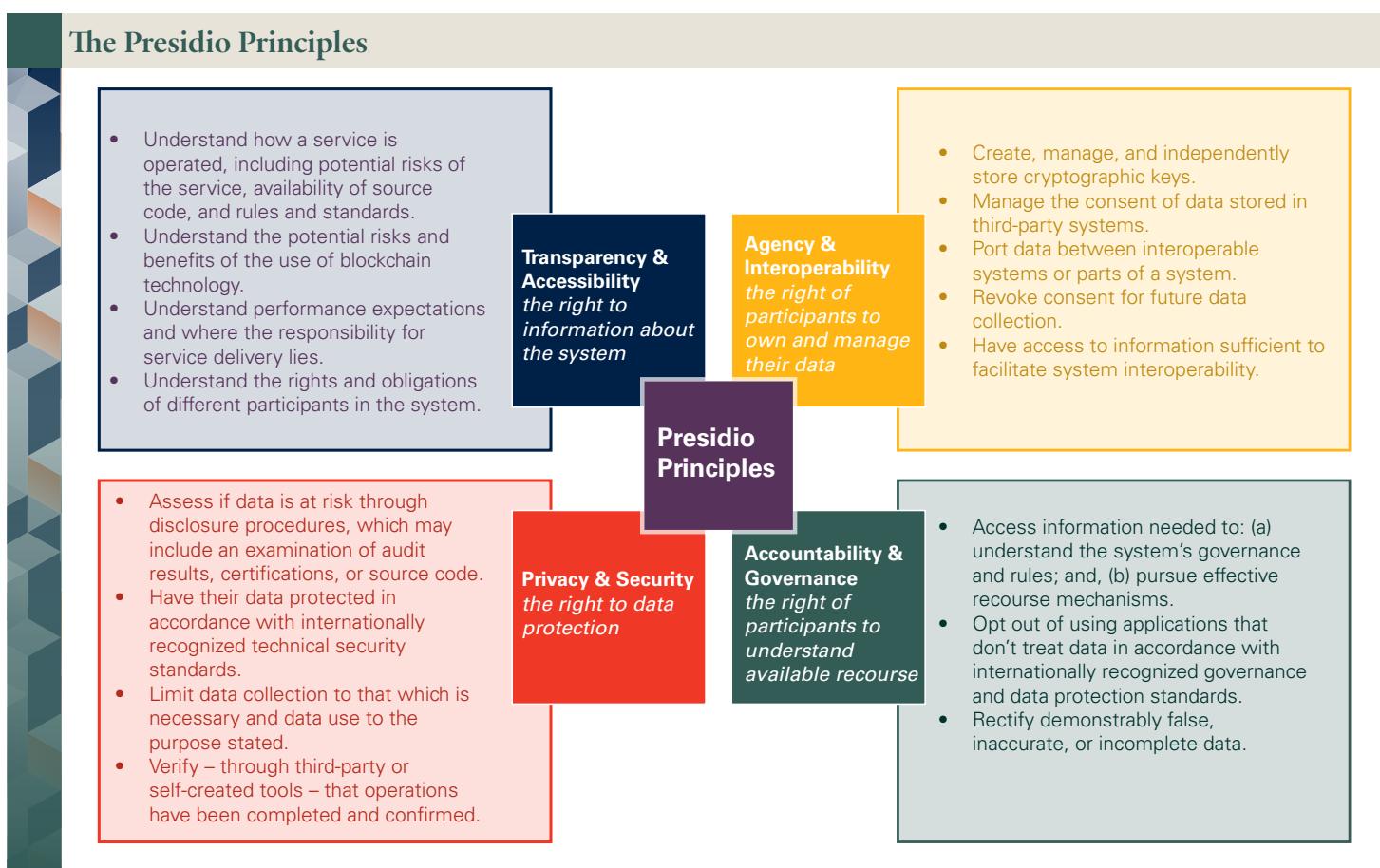
In 2020, the World Economic Forum's Global Blockchain Council introduced its Presidio Principles as a set of foundational values for those building with blockchain technology and decentralised infrastructures. They established four pillars as guidelines for preserving the rights of participants in an organisation's platform:

1. Transparency & Accessibility: the right to information about the system.
2. Agency & Interoperability: the right of participants to own and manage their data.
3. Privacy & Security: the right to data protection.
4. Accountability & Governance: the right to understand available recourse.

In the Preamble to the four pillars, the council introduces its vision for responsible blockchain development:

Blockchain technology, a pillar of the Fourth Industrial Revolution, can not only unlock radical improvements across the public and private sectors, but also enable new business and governance models that help enhance security, accountability, and transparency for people worldwide. However, innovation that progresses without sufficient consideration for governance and user protection often leads to undesirable outcomes for individuals, companies and organizations, and society at large.

The four pillars are described in further detail below (World Economic Forum, 2020):



## **Transparency and accessibility (the right to information about the system)**

- Understand how a service is operated, including potential risks of the service, availability of source code, and rules and standards.
- Understand the potential risks and benefits of the use of blockchain technology.
- Understand performance expectations and where the responsibility for service delivery lies.
- Understand the rights and obligations of different participants in the system.

## **Agency and interoperability (the right of participants to own and manage their data)**

- Create, manage, and independently store cryptographic keys.
- Manage the consent of data stored in third-party systems.
- Port data between interoperable systems or parts of a system.
- Revoke consent for future data collection.
- Have access to information sufficient to facilitate system interoperability.

## **Accountability and governance (the right of participants to understand available recourse)**

- Access information needed to: (a) understand the system's governance and rules, and (b) pursue effective recourse mechanisms.
- Opt out of using applications that don't treat data in accordance with internationally recognised governance and data protection standards.
- Rectify demonstrably false, inaccurate, or incomplete data.

## **Privacy and security (the right to data protection)**

- Assess if data is at risk through disclosure procedures, which may include an examination of audit results, certifications, or source code.
- Have their data protected in accordance with internationally recognised technical security standards.
- Limit data collection to that which is necessary and data use to the purpose stated.
- Verify—through third-party or self-created tools—that operations have been completed and confirmed.

While these guidelines are common sense in principle, they provide a larger benefit to the entire

blockchain ecosystem. The pillars establish a consensus that is broad enough for international usage, but specific to the nuances of blockchain development.

The primary takeaway from the Presidio Principles is to create a system that is not predatory, does not farm or sell data, and is not antithetical to the main benefits of blockchain platforms. Consider these principles as you continue through this module and explore the other challenges of your blockchain project. In the absence of law, you could adhere to the Presidio Principles.

#### 4.2.4 Key Takeaways and References

##### Key Takeaways

Let's review the key points of this section:

1. Since the early 1900s, many organisations have followed a bureaucratic model, with firms built on hierarchies. As information is more broadly disseminated through the power of technology, the public can enact change and disrupt these hierarchies.
2. Digital space is an evolution of meatspace and represents virtual information. Most companies today operate in hybrid modes, combining digital space and meatspace in order to optimise business outcomes.
3. The blockchain ecosystem is in its infancy and developing quickly. Rules cannot keep pace with the rate of innovation, so organisations favour informal or more flexible rules or principles that guide development, protect participants, and set a vision without being overly prescriptive or handling every nuance.

##### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 19 April, 2022.

##### 4.2.1 Overview of Blockchain Technology and Decentralised Authority

Coase, R.H. (1937, November). *The Nature of the Firm*. Blackwell Publishing.

The GNU Operating System (no date). <https://www.gnu.org/gnu/gnu.en.html>

Grafeo, E. (2021, 25 October). Bitcoin Is Still Concentrated in Few Hands, Study Finds. *Bloomberg*. <https://www.bloomberg.com/news/articles/2021-10-25/bitcoin-still-concentrated-in-few-hands-study-finds>

Gurri, M. (2018, November). *The Revolt of the Public and the Crisis of Authority in the New Millennium*. Stripe Press.

Lawter, L., Kopelman, R.J., & Prottas, D.J. (2015). McGregor's Theory X/Y and Job Performance: A Multilevel, Multi-source Analysis. *Journal of Managerial Issues*, 27 (1–4), 84-101. [https://digitalcommons.sacredheart.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1419&context=wcob\\_fac](https://digitalcommons.sacredheart.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1419&context=wcob_fac)

Mulder, P. (2017, 18 April). Bureaucratic Theory by Max Weber. *Toolshero*. <https://www.toolshero.com/management/bureaucratic-theory-weber>

Nabilou, H. (2021). Bitcoin Governance as a Decentralized Financial Market Infrastructure. *Stanford Journal of Blockchain Law & Policy*. <https://stanford-jblp.pubpub.org/pub/bitcoin-governance>

Raymond, Eric (2000, September). *The Cathedral and the Bazaar*. <http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/index.html>

Taylor, F.W. (1911). *The Principles of Scientific Management*. Harper & Brothers.

#### **4.2.2 Digital Space and Meatspace**

Lexico. (no date). Definition of meatspace in English. *Lexico*. <https://www.lexico.com/en/definition/meatspace>

#### **4.2.3 Informal Versus Formal Rule Structures**

World Economic Forum. (2020, May). Presidio Principles: Foundational Values for a Decentralized Future. [https://www3.weforum.org/docs/WEF\\_Presidio\\_Principles\\_2020.pdf](https://www3.weforum.org/docs/WEF_Presidio_Principles_2020.pdf)

# 4.3 Legal Statuses and Challenges

## 4.3.1 Overview of Legal Statuses and Challenges

### Overview

This section will explore the legal and jurisdictional issues that the blockchain industry is starting to face and provide some insights into one domain of legal and regulatory activity, crypto crime, and how crypto crime affects the entire industry. With the fast-paced growth and relative newness of the blockchain ecosystem, there is little legal precedent for cases involving the use of blockchain technology.

### Vocabulary Check

This section introduces the following terms.

- [block explorer](#)
- [crypto dust](#)
- [eclipse attack](#)
- [General Data Protection Regulation \(GDPR\)](#)
- [hack](#)
- [oracle](#)
- [Ponzi scheme](#)
- [ransomware attack](#)
- [third-party doctrine](#)

## 4.3.2 Is Code Law? Blockchain Technology Meets the Courtroom

### Code Is Law

The concept that “code is law” was introduced by law professor Lawrence Lessig in his 1999 book *Code and Other Laws of Cyberspace*. In summary, Lessig writes that in the digital age, technology is used to enforce regulations. Software and algorithms govern interactions and communications online. Furthermore, while traditional law just stipulates rules and consequences if they are broken, code enforces what people can and cannot do at the time they are doing it. Therefore, code, which implements the choices of its creators, is not neutral; code is political, in that it allows and prohibits specific actions (Hassan & De Filippi, 2017).

The advent of blockchain technology and smart contracts is enabling code-based rules to guarantee that transactions will always execute as planned. Furthermore, as smart contracts are enforced through a distributed network, they cannot be disabled or bypassed by a single participant. In this sense, the law that participants must follow emerges from code (Hassan & De Filippi, 2017).

## Blockchain Technology and Case Law

Consider Coase's theory of why and even how firms exist: because individual transactions are too costly. This also lays the foundation for the nature of contracts in firms: that the individual transactions are too costly to record. The firm, then, exists as a legal structure, a formal umbrella for the series of transactions that occur within it.

When issues and disagreements arise within the firm or between firms, the courts become involved, make rulings, and establish case law. Over the last 100 years, modern jurisdictional case law has been structured around firms. These precedents are often difficult to apply to blockchain technology, where new types of legal, organisational structures exist, and "code is law".

New case law is now being established pertaining to the way business is conducted in the blockchain ecosystem. There are several key considerations:

- How do laws get written into and executed by code?
- Can peer-to-peer transactions be adjudicated without a legal intermediary, such as with the use of formally established decentralised autonomous organisations (DAOs)?
- Are participants allowed to be anonymous or pseudonymous?

Hierarchical and centralised decision-making bodies need not be in conflict with decentralised processes designed to distribute work and expedite transactions. However, legal frameworks are still evolving to formalise how those transactions come to pass.

## Guest Speaker Video: New Models of Organising Beyond Traditional Structures

In the following video, Priyanka Desai, Vice President of Operations at OpenLaw, utilises Coase's theory as the basis for discussing new models of organising and the traditional concepts that may carry over.



That's really where I think these decentralized organizations come in, and that's what we as open law have used a protocol to really focus in on coats, nature of the firm. I think we've all read pretty deeply and looked into deeply as far as what it means to actually be a firm, what it means to be a corporation, how people actually interact with one another, how decisions get made.

There is like some baseline human elements going into that. How many people does it take to be hyper effective? What about subcommittees making decisions on behalf of this larger group? I mean, I think some of those elements actually are going to carry with us and won't go away in the digital world.

But I think much of what's being built is a complement to a lot of that theory, and it extends it in a way. As I kind of noted earlier, when you have this flat structure where people from all over the world, different time zones can just kind of coordinate through the internet, things and decisions can be made a lot faster.

You have this hive mind approach. It's almost like a collective consciousness. Like in many ways, I do think that the world has some sort of collective consciousness. If you can harness that in an internet community, which frankly, we saw in web 2 to a little bit like on Reddit and other Web2 communities, there is a little bit of an alignment with people.

Sometimes they think about the same thing at the same time and talk about it. And so if you can actually productively align that ad like some sort of governance structure and banking tied to it, that's a pretty powerful organization. And beyond the benefits of organizing online, being able to do the governance and the efficiencies there. I think the operational efficiency are actually pretty stark, too. You know, having investments that are all internet native, getting tokens in return, all the accounting is done on blockchain.

You know, in many ways, I think the operational efficiencies alone with the digital organizations versus I think meat space is pretty tremendous as well.

### 4.3.3 Case Study: Uniswap Licenses Code to Discourage Copycats

#### Case Study: Uniswap Licenses Code to Discourage Copycats

In 2021 March, the automated market maker Uniswap released its platform upgrade known as Uniswap v3, which included updates to its core programming and supporting smart contracts. The Uniswap v3 Core launched under a new license, the Business Source License 1.1, that differs from the traditional open source software license used in prior versions. As you may recall from section 4.2.1, open source software users typically have license not just to use the software, but to change it and redistribute it. The new Uniswap v3 license provides for a more limited open source software usage. It grants anyone the right to copy, modify, and generally use the work in non-production use cases only. Further, the license invokes a Change Date, after which anyone is granted the same rights for production use cases. The Change Date for Uniswap v3 Core is listed as "The earlier of 2023-04-01 or a date specified at v3-core-license-date.uniswap.eth" (Uniswap, 2021).

The Change Date effectively places a two-year time delay for any production use of the Uniswap v3 code. In fact, Uniswap launched v1 and v2 under the GNU General Public License, which states in part (GNU, 2007):

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

Uniswap's departure from general open source code licensing may signal the company's intent to take violators to court. With more than 200 DeFi apps in the company's marketplace and the market cap of its UNI coins frequently ranking in the top ten of all cryptocurrencies, Uniswap has a lot to protect.

One of the company's main competitors, SushiSwap, released its SUSHI token in August 2020, along with a copy of the Uniswap software. Referred to as "vampire mining", this was a clear attempt by SushiSwap to entice liquidity away from Uniswap and into the new SushiSwap ecosystem. It was after this manoeuvre that Uniswap released its UNI token (Foxley, 2021).

Uniswap highlighted the v3 changes in a blog post on the release date in March and dedicated a section of the blog to this new license. While stating that the ecosystem should be the first to enjoy the rights to its own codebase, Uniswap pointed out the option for its governance to accelerate the Change Date and grant exemptions to the license at any time. The company also clarified that this license does not apply to integrations such as libraries, interfaces, software developer kits, and wallets (Uniswap, 2021).

Read the full text of the [Uniswap v3 Core license](#) here.

#### 4.3.4 Jurisdictional Issues

##### Jurisdictional Issues

Because of the speed at which cryptocurrencies have come into and out of the markets, and the rapid pace of blockchain adoption across industries, legal and regulatory systems lag behind. There is an effort underway by governments to bridge that gap and assume some control over the methods and outcomes introduced with this technology.

There is at least one legal scholar who believes that existing laws are incompatible with the fundamental precepts of blockchain. Edmund Schuster, Associate Professor of Corporate Law at the London School of Economics, believes reconciliation is impossible between existing legal frameworks and distributed ledger technology. He cautions a steady approach to this new age of digital asset technology. His in-depth analysis of the subject centres on the principle that the lack of a hierarchical structure in a decentralised system presents a mismatch between it and the rule of law.

##### The Mismatch with the Judicial System

In a paper titled "Cloud Crypto Land", published in November 2018, Schuster details the mismatch between decentralised blockchain technology and the judicial system (Schuster, 2020). In a follow-up interview for the Business Scholarship Podcast, he reaffirms his position that any fixes to the mismatch are either suboptimal to decentralised systems' nature or require an upheaval in the rule of law (Schuster, 2021):

- 1. Change the laws to be favourable to the decentralised nature of blockchain platforms.** In a traditional financial environment, a plaintiff could successfully argue that the financial transaction they made was not legitimate due to them making it under duress. With adequate proof and a favourable judgement, this transaction could be reversed. This same transaction made in a blockchain environment could also be argued in court. However, a judge's or jury's ruling in favour of

the plaintiff would be outside the scope of the decentralised platform. Laws would need to be in place to address the specifics of how this would work in a blockchain environment.

Thus, if the laws were changed to accommodate the same transaction dispute from above, and the transaction could be reversed, would that platform still be decentralised? Mr Schuster holds that it would not, and that negates the primary purpose of blockchain technology—its decentralised and autonomous basis of existence.

**2. Give the judicial system the ability to correct the record.** This is similar to the resolution proposed above and involves redefining how correcting a record would work.

**3. Through the Choice of Law clause,** one “anchor” jurisdiction rules that a blockchain system is acceptable and legal, and other jurisdictions follow suit to rule similarly. Ultimately, legislation may pass that will codify new laws into a state’s or country’s statutory record. However, there are private international laws already established to protect against the need to import another country’s laws that would be incompatible with their own legal system.

## Pursuing a Use Case

According to Schuster, the hype surrounding the evolving nature of this industry tends to obscure the factual analysis of a business’s decision whether or not to pursue a use case for implementing a blockchain solution. The following questions demonstrate his point:

- Would the cost of implementing and operating the new blockchain technology outweigh the cost of operating the current infrastructure?
- If all decision-makers agree that the current infrastructure needs to or should be replaced, is blockchain technology the best solution? From a cost perspective? From a legal perspective?

Slow and thoughtful consideration should be the focus of any business wanting to analyse whether or not to adopt a blockchain technology use case (Schuster, 2021). You will learn more about analysing your blockchain use case in Module 5.

## Guest Video: Are Blockchain Technologies Compatible with the Legal System?

In the following video, Professor Edmund Schuster provides clarification on the jurisdictional challenges of blockchain technologies.



Blockchain technology is obviously a very wide field and there are a lot of different types of technologies, different protocols, different systems that are being summarised under this term. Part of my research looks at how these technologies are compatible with the legal system, and a core question here is the fundamental compatibility of blockchain technology and the rule of law.

The problem here is that, if you look at truly decentralised systems, the prime design goal, in a way, is to eradicate any sort of hierarchy. Everyone is an equal participant in the system. Obviously, that will be subject to certain facts about the participants, how much compute power does that participant have or, perhaps, in a proof of stake system, how big of an exposure to the crypto asset does the person have. Nevertheless, the absence of hierarchy for public blockchains really is one of the fundamental features here.

Now, what is the rule of law? I argue in my research that the rule of law and acceptance of the rule of law necessarily implies the acceptance of a hierarchy, and this hierarchy is very simple. The hierarchy is that the law is above its subjects in the sense that everyone has to obey the law and we also have, at least in democratic societies, that democratic process by which and through which laws are implemented, decided upon, and enforced.

So the fundamental conflict here between, at least, public blockchains and the law is simply that you can't fully decentralise, you can't fully eradicate hierarchies and, at the same time, accept the superiority, the sovereignty of the law, accept the rule of law as such, because the rule of law is necessarily something that can change over time where the opinions of some people count more than the opinions of others, and so on. And so one fundamental problem and a potential clash is always that the law will sometimes not allow certain transactions to happen, even if these transactions happen according to the rules of a specific protocol, the rules of a smart contract, a transfer of assets, using the right private keys confirmed by the right amount of nodes. All of that may have sufficed for the technological side—so according to the protocol, a transaction will have happened—but the legal system may still say, well, that doesn't work, doesn't count.

I think the easiest example is that there are certain agreements that we never enforce in the law. Of course, if you are looking at a public blockchain system, if somebody puts a gun to my head and makes me use my private keys to transfer crypto assets, then according to the rules of that system, a transfer will have happened. And so one fundamental problem, one fundamental clash here is how do you deal with this situation? How do you deal with a situation where a transaction is valid under protocol rules, but clearly invalid under legal rules?

### 4.3.5 Other Legal Considerations

#### Other Legal Considerations

When developing a blockchain project, it is important to pay close attention to relevant laws that have been enacted or are under legislative consideration. Data, privacy, securities, tax, and antitrust are all areas of focus in the digital space and could have unique impacts on blockchain use cases.

#### Data and Privacy Laws

Satoshi Nakamoto highlighted privacy in the Bitcoin white paper as a major factor in the cryptocurrency's development, and that has been one of the Bitcoin network's primary attractions since its launch in 2009 (Nakamoto, 2009). The use of public keys to transact the currency while maintaining the privacy behind it with private keys was, and is currently, the belief system that promotes anonymity among its users. However, high-profile criminal cases and more sophisticated blockchain analytics tools have improved the traceability of transactions and shown a certain amount of transparency in them. For example, the investigation into the US Colonial Pipeline ransomware attack demonstrated that bitcoin transactions are not as hard to track as once believed (Perlroth et al., 2021).

In addition, privacy is not necessarily compatible with the immutable, distributed ledger system of a public blockchain platform. The transactions are encrypted, yet they are permanently stored on multiple nodes that are widely distributed. Previous transactions from a specific digital wallet address are all discoverable by anyone with knowledge of how to use a block explorer that provides access to all transactions on a particular blockchain platform using a public key. Private or permissioned blockchains provide an alternative solution in certain use cases, such as the Maersk/IBM TradeLens logistics tracking system where multiple parties become stakeholders, or in a closed supply chain use case like those utilised in the food supply.

Still, the architecture of a public blockchain platform, like the Bitcoin and Ethereum platforms, has motivated other data privacy laws and regulations globally. This increased scrutiny in data and privacy protection highlights the importance of understanding and staying current with the laws enacted in places where a blockchain organisation conducts its business. The following are notable occurrences in Europe, the US, and China.

1. Considered by the **European Union** to be the toughest privacy and security law in the world, the General Data Protection Regulation (GDPR) came into effect on 25 May 2018. It is designed to protect EU citizens' personal data and imposes obligations with strict penalties onto organisations anywhere in the world who collect such data (GDPR.EU, 2021).

The GDPR has been central to numerous privacy-related investigations and court cases. One high-profile case, the Schrems II judgement against Facebook, determined that Facebook's transfer of EU citizens' data to the US invalidated the Privacy Shield—the legal mechanism used by many companies making EU-US data transfers. Similarly, the European Court of Justice determined that the US government's ongoing surveillance practices were incompatible with EU data protection regulations (Savova, 2020).

2. The **United States** National Conference of State Legislatures reports that, as of 14 February 2020, 32 US state governments require, by statute, that state government agencies have security measures in place to ensure the security of the data they hold (National Conference of State Legislatures, 2020).

In another example, James Harper filed a lawsuit in 2020 against the Internal Revenue Service (IRS) in the United States, claiming overreach by the IRS when it requested vast amounts of records from the Coinbase exchange to determine if the plaintiff had under-reported his tax liability in 2019. The request was based on the volume of Harper's cryptocurrency transactions. The lawsuit alleges the IRS violated due process for Harper by seizing his financial information from Coinbase without first providing him notice and an opportunity to challenge it.

The case is still pending. The Department of Justice, representing the IRS, filed a motion to dismiss in early 2021, and Harper's legal team filed a motion to reject the DOJ's motion. The lawsuit's outcome could profoundly affect US privacy laws and, specifically, the third-party doctrine, which provides no reasonable expectation of privacy when individuals give their information to a third party. The third-party doctrine was articulated in two US Supreme Court cases in the 1970s (Powers, 2021).

In 2021, the penetration of consumers' data by third parties is so prevalent that a court case like Harper's could set some precedent for how data privacy will be treated going forward in the US.

- 3. China** issued a draft Data Security Law in June 2020 which addresses data collection, storage, processing, use, provision, trading, and public disclosure of data by any organisation, domestic or abroad. It seeks to ensure data is protected and lawfully utilised. Compliance with the law is supervised by the Cyberspace Administration of China (CAC) and loosely specifies that regulators should have the ability to enforce it outside of China (International Trade Administration, 2020).

Organisations conducting business multi-nationally must understand data security laws in all jurisdictions. As each country has a different framework for its regulatory processes, including penalties for violations, making a dedicated effort early in a project's business development strategy can help ensure adherence to these laws.

## Guest Video: The Importance of Data Privacy Laws in Blockchain Technology

In the following video, Mimi Zou, Director of Studies in Law, Regent's Park College, Oxford, discusses the importance of data privacy laws in blockchain technology.



So data privacy laws really have a very important role when it comes to the further development of blockchain technology. So as we know, blockchain technologies are being developed and used for registries and repositories for public records. And I think it's because of blockchains' tamper resistance and its strengths in being able to very quickly and efficiently verify the authenticity and the integrity of the data.

So that's a fantastic thing in terms of data protection and privacy. We can ensure that the data is recorded and there's minimal risk in terms of corruption to the data. We can see that also this data—the blockchain technology is being used in terms of recording and storing data that includes personal data and sensitive personal data, including health records.

And so, I think that raises obviously a lot of potential issues for data protection. Because obviously, depending on the type of blockchain that's used, there's also the problem of the transparency of blockchain, even though blockchain can promise anonymity. But it's also transparent in terms of the data that is there.

And if you're a really brilliant hacker, it may be possible to basically link bits of information—the personal information to individuals, however anonymised it is. I really don't believe that there is truly anonymous data out there. So I think that's something just to be mindful of as we really use these blockchain technologies for record keeping. There's going to be a lot of issues arising from a personal data privacy perspective.

Of course, strong data privacy laws like the GDPR I think can be a good thing in terms of at least incentivising developers to really come up with very strong techniques for anonymisation just to make the compliance obligations arising from these privacy laws related to personal data. So I do believe it is necessary to have strong data privacy protection that will only help the further development of blockchain.

Now, there's obviously problems in terms of how the use of these blockchain technologies will comply with such legislation. So in the GDPR, which really is the gold standard for data protection around the world, there are

concepts like data controllers. Now, the very nature of blockchain technology makes it really hard to identify who takes responsibility for the obligations of a data controller under the GDPR. Right?

And also, on the GDPR a really key right is the data subject's ability to access data that's held about them, or to have that data erased—the right to be forgotten. Now, that's going to be quite hard in the context of blockchain when you think about the element of permanence, that once something is recorded on the chain, that's the whole point. Right? You really can't erase it. I mean really very narrow situations when you try and go back on a transaction. But the whole point is that that transaction is recorded. It's there. It's really, really hard to alter it.

So I think there's going to be some regulatory challenges. But they're not impossible to overcome. And that takes innovation. That takes creative thinking and very much working with policymakers to ensure that the exploitation of this amazing technology is done in a way that respects and protects personal privacy. And that can only be a good thing for the development of blockchain.

## Securities Laws

How cryptocurrencies are classified is becoming an issue governments must wrestle with. Any blockchain project with an underlying crypto asset should consider and closely follow developments in securities laws. For example, in the US in the summer of 2021, the Chairman of the Securities and Exchange Commission (SEC) began putting certain crypto exchanges on notice that one or more of their services did not comply with SEC regulations. Specifically, the SEC Chairman, Jay Clayton, has stated that bitcoin is not a security, because it doesn't pass the Howey Test.

In a more proactive example, Germany passed a law in December 2020 that legalises the use of blockchain technology in the securities sector, and legislators relaxed a rule that required the use of paper certificates in these transactions and instead allow for the use of a blockchain-based register (Kaaru, 2020).

It can be easy to miss new opportunities, as in the case of the new German law, or information about penalties or fines, as in the case of the SEC.

## Antitrust Laws

In the abstract of his paper titled "Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox", Thibault Schrepel, Assistant Professor of Antitrust at Utrecht University and Affiliate Professor at Stanford University, describes the blockchain antitrust paradox by contrasting the decentralised nature of blockchain with the centralised foundation of antitrust laws and saying that antitrust is still needed in blockchain use cases. He cites the internet as a recent example of the relevancy of antitrust laws in modern technology and states that the speed in applying the law to that industry was an integral solution. The immutable, decentralised, and anonymous nature of blockchain creates the conundrum of how to detect anti-competitive activities and apply antitrust laws to them. Schrebel suggests "regulatory infiltration", and a "law is code" approach as new methodologies for regulations to stay relevant to the innovations brought by blockchain technology (Schrebel, 2018).

Blockchain organisations should consider their potential role in anti-competitive activities and take

actions to avoid such occurrences. As regulations and case law develop in this area, a conservative approach is warranted.

Since 2018, blockchain technologies have evolved, and there are many more participants in the industry. Still, there are a rare few antitrust cases to lean on in this budding ecosystem. The first case came about in December 2018 (notably after Schrepel's paper was published). United American Corporation (UAC), a diversified technology company, sued Bitmain, Inc., the largest bitcoin mining pool at the time, and other high-profile stakeholders. To summarise, the case alleges collusion by the defendants to manipulate the Bitcoin cash market, resulting in it becoming centralised. UAC further claimed that the scheme resulted in a global capitalisation meltdown and created more than US \$4 billion in losses to US bitcoin holders (Williams, 2021).

In Miami, Florida, a US federal court dismissed the original complaint and allowed the plaintiff to amend the motion. This amended motion was also dismissed under Federal Rule of Civil Procedure in March 2021, noting that the allegations did not plausibly suggest the transgressions listed in the filing. The judge entered and ordered a final judgment on 8 April 2021 to close this case (Williams, 2021).

In his analysis of the blockchain antitrust paradox, Schrepel concludes, “Antitrust law as we know it must die and be reborn. If not, it soon will be illegitimate” (Schrepel, 2018).

## Tax Laws

The tax implications of a blockchain strategy will depend on the project's stated purpose and local and national tax laws. If the use case is for supply chain economics, data storage, or some non-token based function, tax effects will be as relevant for the overall business.

On the other hand, if a value transfer is involved, it must be determined how to treat the digital asset that is being transferred. As explained by Jarick Poulson and Rob Massey from Deloitte and published by the World Economic Forum, one common determination is to recognise and define an asset's digital representation of value (DRV): “Understanding the asset's character, basis tracking, sourcing and expense and revenue recognition will determine how it will be classified for tax purposes” (Poulson & Massey, 2020).

To define the asset's DRV, consider the following (Poulson & Massey, 2020):

- Determine if the DRV is used in a permissioned, or limited, platform or on a permissionless, or open, platform like cryptocurrencies. A closed loop DRV will less likely be treated as property.
- Consider the platform's participants and how they interact with the platform. Do they come in through an external source? Or can anyone transact with the platform? Both are indications of an open platform.
- Does the DRV have value outside the platform? This may require tax considerations. An example might include a promotional certificate that can be redeemed in exchange for something of value.
- Would the DRV be affected by legal ramifications such as a bankruptcy? In what way? Answers to these questions will help determine tax implications.

- Are there adequate controls in place to store, audit, and manage the DRV?

Based on the answers to the questions, companies should consider the DRV's tax implications for the following three categories:

- 1. Income tax treatment.** This will factor in the relationship between the transferor of the DRV and the DRV's recipient. In promotional situations, sales revenues could be affected. Rewarding employees or contractors may be deemed a compensatory transfer.
- 2. Indirect taxes.** If the DRV transfer is not deemed a sale, there could be indirect taxes such as sales and use tax and value-added tax.
- 3. Information reporting.** This type of reporting may be required and will depend on several factors:
  - Is income fixed and determinable at the time of transfer?
  - Is there cash value in the DRV?
  - Is the DRV transferable?
  - Does value transferred exceed minimum thresholds for reporting requirements?

Planning for what a DRV represents is recommended in a project's planning phase. Following the digital asset through the project's life cycle will help determine its classification and subsequent tax implications. Ideally, tax planning should precede legal agreements and transactions (Poulson & Massey, 2020).

## Summary

Some business considerations for participating in a blockchain use case involve evaluating the design, participants, and function from an antitrust perspective.

- Is the blockchain public or private?
- Does the blockchain include your competitors?
- What information is stored on the blockchain?
- Do changes to the blockchain increase antitrust risk?
- Are competitors excluded from the blockchain or conditioned to avoid anti-competitive conduct?

Even though the blockchain space is evolving, it is beneficial to understand antitrust laws for general business purposes and how those may apply to a blockchain project.

## 4.3.6 Cryptocurrency Crime Analysis

### Cryptocurrency Crime Analysis

This section explores cryptocurrency crime perspectives, notorious financial and technology crimes involving cryptocurrency and blockchain, such as Silk Road, and famous “attacks” such as the DAO attack.

#### Quick Fact

Ransomware attacks saw a 311% increase in 2020, the highest of any crypto crime category. This type of attack involves attackers hacking into a computer or network of computers to block usage and access to data until a ransom payment is made. High-profile corporate ransomware attacks have plagued the news cycles in 2021, and the primary method of ransom payments has been bitcoin. As a testament to law enforcement efforts worldwide, in June 2021, the FBI retrieved US \$2.3 million of the US \$4.3 million seized by DarkSide during a ransomware attack on the Colonial Pipeline organisation in the US (Sonnenmaker, 2021).

### Crypto Crime Perspective

Much of the journalistic reporting of crypto crime has centred around criminal enterprises and the darknet. With time and the emergence of cryptocurrency success stories, the overall low crime rate as a percentage of crypto volume has offered a fresh perspective. Also, crypto crime rates remain in balance with legacy financial crime rates, which remain the primary access point for financial crimes (Chainalysis, 2021).

Blockchain-oriented crimes are new criminal territory and have created challenges for law enforcement as cryptocurrencies do not move through centralised and regulated entities. However, the public nature of blockchain's ledgers is not optimal for criminal activity. In fact, they provide a forensic investigative tool for law enforcement and intelligence agencies.

### Guest Video: Blockchain's Security Weaknesses

In the following video, Yaya Fanusie, Founder and Chief Strategist at Cryptocurrency AML Strategies, describes security weaknesses associated with the growth in cryptocurrencies.



My name is Yaya Fennessy, and I spent several years in government in my previous life, I actually was an analyst at the CIA where I focused on economic and also counterterrorism issues.

But when I left government the US government several years ago, I started working in the National Economic security think tank space, and I started doing research on how illicit actors might use cryptocurrencies and blockchain technology. So basically, the National Security implications of cryptocurrencies and blockchain tech is my research area.

As crypto is growing so much, the biggest weaknesses relating to national security and also illicit finance are pretty much that. There's such a low barrier to entry for anyone to get involved in crypto, to get it to, to access crypto, to even develop a sort of blockchain venture.

So what does this mean? This means that, because pretty much anyone can, for example, anyone could create a token, you know, almost anyone, right? It's very easy, right? You don't need to be a central bank, obviously. So the fact that you have this system that is software that anyone can participate in. It also means that you're going to have an ecosystem built around it that does not always build in security measures, right?

You can have people that have exchanges that are real lax. So they don't have really good cybersecurity or you have exchanges that have been developed or they don't really put in the anti-money laundering and know your customer guidelines or requirements before people use those exchanges, those services.

So that's a vulnerability because it means now you can have somebody, for example, sign up on an exchange. They could say they could sign up for an account and say that their name is Mickey mouse, and they live on 13 13 Mockingbird Lane and then go ahead and get crypto if that exchange does not sort of follow the anti-money laundering rules.

So the fact that there's this low barrier to entry is good in some ways, but it can be exploited. It's a vulnerability, and it allows for some of the illicit activity, some of the fraud that we see that you do see in the blockchain ecosystem, unfortunately.

## Crypto Crime Perspective (ctd.)

As is evidenced by the Silk Road darknet market that existed from 2011 to 2013, cryptocurrency crime has existed since the earliest days of cryptocurrency itself. Through enterprises like Silk Road, criminals have capitalised on the pseudonymity associated with cryptocurrencies, although the transactions themselves are traceable since they are mainly conducted on public blockchains. Criminals learn how to exploit vulnerabilities and take advantage of the low barrier to entry in crypto exchanges.

An example of a traced transaction involved the US Department of Justice (DOJ) seizing US \$1 billion in bitcoin in November 2020. The seizure was related to the Silk Road marketplace and was the result of an investigation by the Criminal Investigation Division of the IRS and the US Attorney's Office for the Northern District of California. They identified Individual X as the individual who hacked into the Silk Road blockchain in 2013 and moved some funds out. Silk Road's founder, convicted felon Ross Ulbricht, identified Individual X at the time of the theft in 2013.

The IRS used a third-party Bitcoin network analysis company to interpret Silk Road transactions. This company was able to identify 54 transactions that were not involved in any illegal transactions of the criminal enterprise and, therefore, deduced that they were stolen from Silk Road. Individual X forfeited the contents of their digital wallet as part of an undisclosed deal with the DOJ (Daily Hodl Staff, 2020).

Crypto crimes can fall into one of two primary categories:

**1. Financial** crimes involve the use of cryptocurrencies in the commission of the crime. Examples include:

- A **crypto dusting attack** involves an attacker intentionally sending digital currency to unsuspecting digital wallets in an attempt to steal their privacy by de-anonymising them. Dust refers to trace amounts of crypto and is often the result of leftover crypto from a trade—the negligible remainder.
- A **digital wallet attack** happens by direct phishing attacks, taking possession of lost or stolen wallets, or hacking/stealing someone's seed phase.
- **Fraud** through an initial coin offering scam happens when a token issuer makes false claims and deliberately sets up a fraudulent system to entice investors into a fake ICO.
- **Money laundering** occurs when the flow of fiat currency or cryptocurrency is masked through corrupt or unregulated cryptocurrency exchanges, ICOs, or privacy coins with additional layers of anonymity.
- A **Ponzi scheme** involves a fraudster setting up a fake crypto enterprise with a false background and statistics to lure investors, who may not be educated in how cryptocurrency investing works. A Ponzi scheme is like a pyramid scheme that rewards its earliest investors, but a Ponzi scheme invokes a false business enterprise.

## 2. Technology

crimes occur when attackers look for and find vulnerabilities within a network.

Examples include:

- An **eclipse attack** occurs when a hacker fools an active node into validating false transactions, blocking the node from knowing legitimate ones.
- A **51% attack** involves an attacker attempting to gain more than half the computing power in a particular network, thereby allowing them to change/reverse previous records.
- In **smart contract exploitation**, an attacker exploits a vulnerability within a smart contract for their own financial gain, typically by stealing other people's cryptocurrency.

Dusting has other meanings outside of dusting attacks (Cryptopedia Staff, 2021):

- An organisation could advertise by sending out messages in the crypto dust, similar to an email blast.
- A network could be spammed by large amounts of dust that would clog it and slow it down.
- Criminals may dust their “dirty” money around to multiple wallets to elude authorities.
- Legal authorities might dust multiple wallets of a suspected crime ring to try and establish identity.
- Analytics firms use dusting to study crypto dust for data purposes.
- Dusting is a way to test a network’s throughput capabilities.

## Notorious Cryptocurrency Crimes

**Silk Road.** The infamous black market platform was regarded as the first darknet market. Silk Road hosted money laundering activities and illegal drug transactions. In 2013 the US Federal Bureau of Investigations (FBI) shut it down, seizing more than 144,000 bitcoins. Its founder, Ross Ulbricht, was sentenced to life in prison (Frankenfield, 2021).

**Mt. Gox attack.** Mt. Gox was the first major crypto exchange, and handled over 70% of all bitcoin transactions shortly after it was founded in 2010. After two smaller attacks in 2011, another hack occurred on the Mt. Gox exchange in 2014 and resulted in the theft of over 850,000 bitcoins, worth US \$460 million at the time. In 2021, the theft was worth over US \$43 billion based on BTC's price of \$50,670 on 3 September (CoinMarketCap, 2021). This attack took place before the invention of hardware wallets (Ledger, 2019).

**The DAO hack.** The DAO was a decentralised autonomous organisation (DAO) that launched on the Ethereum blockchain on 30 April 2016. Through a token sale, it raised 12.7M ETH, valued then at US \$150 million. On 18 June 2016, a hacker drained 3.7M ETH from the DAO smart contract, which was valued then at US \$70 million. Although the intentions were nefarious in this attack, this hack mainly exploited two vulnerabilities in the smart contract. The ETH hard fork resulted from this situation.

**Ethereum Classic attack.** The first 51% attack occurred in January 2019, lasted for three days, and amounted to US \$1.1 million in losses. There were several subsequent attacks in the summer of 2020, and the digital coin (symbol: ETC) was delisted or suspended from multiple exchanges until it could become more stabilised (Voell, 2020).

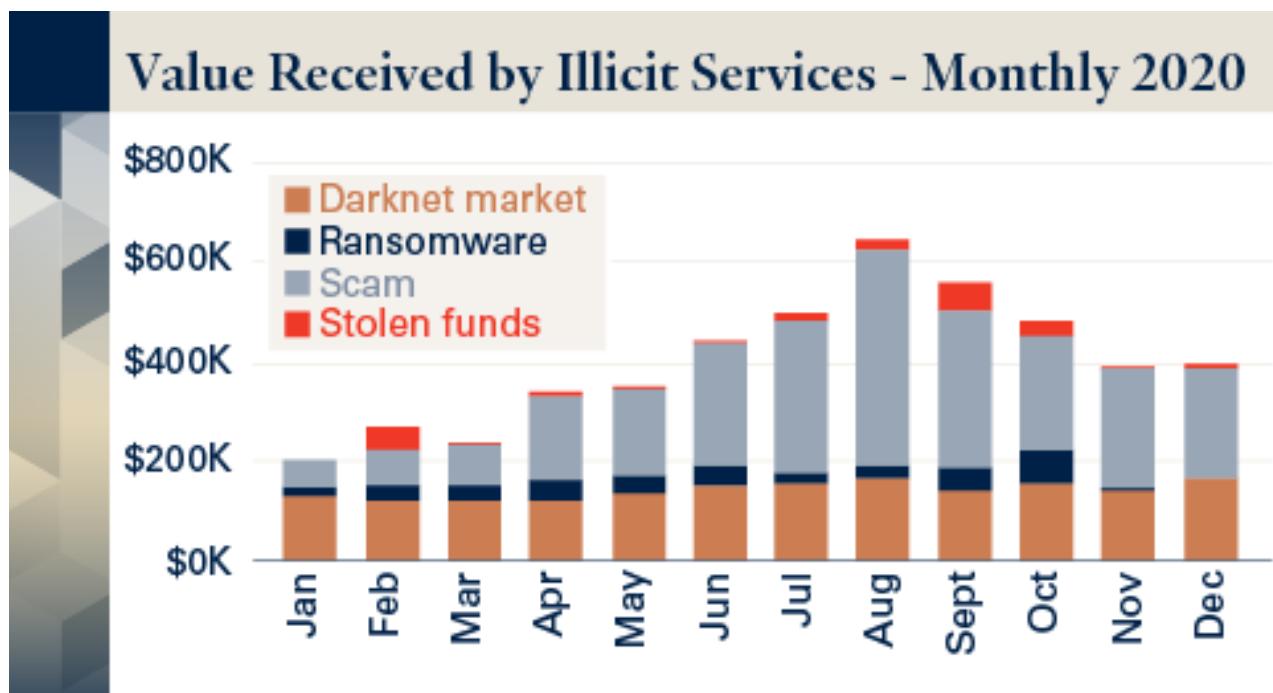
**Onecoin.** This Ponzi scheme ran from 2014 to 2019 and defrauded investors of US \$5.8 billion. The scheme marketed Onecoin as a “Bitcoin Killer” and operated as a multi-level marketing system that compensated members with cash when they brought in new investors. There was no actual blockchain, and the coins were worthless (Sergeenkov, 2021).

## Cryptocurrency Crime Reporting

Chainalysis and CipherTrace are both industry-leading blockchain forensics companies. As holders of some of the world’s largest datasets of blockchain metadata, they share reputable and often-cited viewpoints on the status of crime in the blockchain ecosystem (Marrinan, 2021).

Each company issued a 2021 crypto crime report, and each company noted the low overall crime rate in 2020—0.34% according to Chainalysis and 0.50% according to CipherTrace (CipherTrace, 2021). Their reasons for this low rate point to an overall increase in economic activity that exponentially offset the crime rates. Chainalysis reports that in 2020, scams accounted for 54% of crypto-related crime, representing approximately US \$2.6 billion worth of cryptocurrency (Insights, 2021). This majority was similar to 2019, although that year’s figures were somewhat skewed by the large PlusToken Ponzi scheme which alone accounted for US \$2 billion taken from millions of victims. Darknet markets represented the second-largest category again, accounting for US \$1.7 billion worth of cryptocurrency, a 30% increase over 2019.

Ransomware increased 311% in 2020. Although the US \$350 million amount stolen is far less than that of the scams and darknet crimes, the trend is alarming. With many more people working from home in 2020 due to the Covid-19 pandemic, increased systems vulnerabilities were likely contributors to this increase.



(Chainalysis Inc, 2021).

## Practice Due Diligence

Sometimes, what seems like a cryptocurrency theft is an oversight or lack of due diligence on one or both parties involved in a transaction. Smart contracts provide a good example of this type of vulnerability. There may be a flaw in the contract that goes undetected until a triggered event or profit-seeking attacker exposes it. Each party involved in the contract must assume their own due diligence. If a contract is poorly written and cryptocurrency funds are not dispersed correctly, that alone does not indicate fraud nor any other crime.

## Audit

Consider a formal audit for deploying a smart contract, especially one that has multiple complexities. Smart contract auditing firms exist for this very reason. An audit group may be a unit of a larger organisation, or it may exist solely for this narrow purpose. Some will handle the full scope of writing, auditing, and deploying smart contracts as a third-party provider.

Some important areas to consider auditing include the following, as outlined by Deloitte in its block-chain auditing guide titled, An internal auditor's guide to auditing blockchain (2021):

- **Governance framework** to establish appropriate oversight and controls.
- **Change management process** to establish protocols for code management, permissions (for a permissioned platform), legacy system interfaces, policies and procedures.
- **IT security** to address and analyse the consensus mechanism, system scalability, and data confidentiality.
- **Smart contracts** to ensure network layer controls, review of automation code, and effectiveness of contract enforcement.
- **Blockchain data integrity** to confirm data is effectively controlled to prevent attacks; data transfer, storage, and retrieval is efficient; and transaction immutability is sound.

Smart contract code audit assessments would consider the following:

- Can the code be accessed or modified by avoiding network security measures?
- Is the code comprehensive enough to encompass the specific details of triggered events?
- Are tokens handled correctly within the contract?

Another factor to enhance your project's state of readiness is to utilise tested platforms and systems—ones that have existed for some time and offer the results of their own third party audits. In other words, expect to be hacked and take diligent steps to scrutinise your internal and external partners.

## Insurance

Is insurance a good solution for the safety and soundness of smart contracts? There are insurance options available, and a review of those alongside audit considerations would be worthwhile. In fact, the discovery process itself may produce valuable results. For example, an insurance organisation will likely perform some level of smart contract auditing before the organisation insures the smart contract. Therefore, this process would further strengthen that contract.

Insurance coverage comes in the following forms:

- Protocol protection to cover failures in the protocol a user invests in.
- Custodial protection to cover hacks and frozen funds on exchanges or custodial wallets.
- Yield token protection to cover protocol failures on yield-bearing tokens.

Organisations like **Nexus Mutual** offer a membership-based coverage pool that is similar in concept to a life insurance mutual. Nexus Mutual's membership decides if and how claims are paid, and that is supported by the execution of smart contracts (Nexus Mutual, n.d.).

A peer-to-peer insurance market fits with the peer-to-peer nature of DeFi. A user can provide coverage similar to how they would provide liquidity with tokens. Likewise, a user can request coverage to hedge on a crypto asset like they would borrow funds on a decentralised exchange.

The insurance market is a budding participant in the blockchain ecosystem. There have been enough past examples of hacks, exploitations, and other protocol failures for some precedent in terms of how insurance coverage might work, and businesses are entering this quickly evolving space.

### 4.3.7 Key Takeaways, References, and Further Exploration

#### Key Takeaways

Let's review the key points of this section:

1. While there is some legal precedent for native cryptocurrency use cases, very little case law addresses real-world blockchain applications. Aside from case law, blockchain also touches data laws, security laws, privacy laws, antitrust laws, and tax laws.
2. With the fast-growing cryptocurrency industry, crimes have also increased at a fast pace. There are analytical tools available to understand where and how crimes occur, specifically through crypto forensics firms. As you pursue your blockchain strategy, consult the resources available here and your local law enforcement agencies.
3. Crypto crime rates continue to lag behind legacy financial crimes, though there is likely under-reporting of crimes. The hackers and fraudsters are adept at contriving new methods of theft and work hard to stay ahead of being caught in the act.

#### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 19 April, 2022.

#### 4.3.2 Is Code Law? Blockchain Technology Meets the Courtroom

Hassan, S., & De Filippi, P. (2017). The Expansion of Algorithmic Governance: From Code is Law to Law is Code. *OpenAddition Journals*. <https://journals.openedition.org/factsreports/4518>

#### 4.3.3 Case Study: Uniswap Licenses Code to Discourage Copycats

Foxley, W. (2021, 23 March). Uniswap V3 Introduces New License to Spoil Future SUSHIs. *CoinDesk*. <https://www.coindesk.com/tech/2021/03/23/uniswap-v3-introduces-new-license-to-spoil-future-sushis>

GNU Operating System. (2007, 29 June). GNU General Public License. <https://www.gnu.org/licenses/gpl-3.0.en.html>

Uniswap. (2021, 23 March). Introducing Uniswap V3. *Uniswap Blog*. <https://uniswap.org/blog/>

Uniswap/v3-core. (2021, 21 March). v3-core/LICENSE. GitHub. <https://github.com/Uniswap/v3-core/blob/main/LICENSE>

#### 4.3.4 Jurisdictional Issues

Schuster, E. (2018, 21 November). Cloud Crypto Land. *Modern Law Review*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3476678](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3476678)

Schuster, E. (2021, 18 March). Ep.98 - Edmund Schuster on Blockchain Hype. *Business Scholarship Podcast*. <https://vurbl.com/listen/ep98-edmund-schuster-on-blockchain-hype-7Uuj67e6qOI>

#### 4.3.5 Other Legal Considerations

GDPR.EU. (2021). General Protection Data Regulation (GDPR). <https://gdpr.eu/tag/gdpr>

International Trade Administration. (2020, October 29). China's Data Security Law. <https://www.trade.gov/market-intelligence/chinas-data-security-law>

Kaaru, S. (2020, 21 December). Germany passes law legalizing electronic securities on blockchain. Coingeek. <https://coingeek.com/germany-passes-law-legalizing-electronic-securities-on-blockchain>

Nakamoto, S. (2009). Bitcoin open source implementation of P2P currency. *P2P Foundation*. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>

National Conference of State Legislatures. (2020, 14 February). Data Security Laws | State Government. <https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx>

Perlroth, N., Griffith, E., and Benner, K. (2021, 9 June). Pipeline Investigation Upends Idea That Bitcoin Is Untraceable. *The New York Times*. <https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html>

Poulson, J., & Massey, R. (2021, 16 July). Key tax considerations when using blockchain for value transfers. *World Economic Forum*. <https://www.weforum.org/agenda/2020/07/key-tax-considerations-when-using-blockchain-for-value-transfers>

Powers, B. (2021, 14 September). How a Lawsuit Against the IRS Is Trying to Expand Privacy for Crypto Users. *CoinDesk*. <https://www.coindesk.com/lawsuit-irs-expand-privacy-for-crypto-users>

Savova, V. (2020, 13 September). Privacy laws might prove to be a blessing in disguise for crypto. *National Crowdfunding & Fintech Association*. <https://ncfacanada.org/privacy-laws-might-prove-to-be-a-blessing-in-disguise-for-crypto>

Schrepel, T. (2018, 25 June). Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox. *Georgetown Law Review*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3193576](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193576)

Williams, K. (2021, 26 September). United American Corp. v. Bitmain, Inc. (1:18-cv-25106). *Court Listener*. <https://www.courtlistener.com/docket/8382061/united-american-corp-v-bitmain-inc>

#### 4.3.6 Cryptocurrency Crime Analysis

Chainalysis. (2021, January). The Chainalysis 2021 Crypto Crime Report. <https://go.chainalysis.com/2021-Crypto-Crime-Report.html> (download required).

CipherTrace. (2021, 28 January). Cryptocurrency Crime and Anti-Money Laundering Report, February 2021. <https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report>

CoinMarketCap. (2021). Bitcoin Overview. *CoinMarketCap*. <https://coinmarketcap.com/currencies/bitcoin>

Cryptopedia Staff. (2021, 30 May). What Is a Crypto Dusting Attack? *Cryptopedia*. <https://www.gemini.com/cryptopedia/crypto-dusting-attack-bitcoin>

Daily Hodl Staff. (2020, 6 November). DOJ Filing Sheds Light on \$1,000,000,000 Bitcoin Transactions Linked to Silk Road. *The Daily Hodl*. <https://dailyhodl.com/2020/11/06/us-justice-department-trying-to-seize-1000000000-in-bitcoin-linked-to-silk-road>

Deloitte. (2021). An internal auditor's guide to auditing blockchain. *Deloitte*. <https://www2.deloitte.com/us/en/pages/risk/articles/internal-auditing-guide-to-blockchain.html>

Frankenfield, J. (2021, 14 May). Silk Road (Website). *Investopedia*. <https://www.investopedia.com/terms/s/silk-road.asp>

Insights. (2021, 19 January 19). Crypto Crime Summarized: Scams and Darknet Markets Dominated 2020 by Revenue, But Ransomware Is the Bigger Story. *Chainalysis*. <https://blog.chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets>

Ledger. (2019, 18 February). Hack Flashback: The Mt.Gox Hack - the Most Iconic Exchange Hack. <https://www.ledger.com/hack-flashback-the-mt-gox-hack-the-most-iconic-exchange-hack>

Marrinan, P. (2021, 29 March). Crypto-crime & caveats. *Thomson Reuters*. <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/crypto-crime-caveats>

Nexus Mutual. (n.d.). Get covered against smart contract failure & exchange hacks. *Nexus Mutual*. <https://nexusmutual.io>

Sergeenkov, A. (2021, 22 June). 5 of the Biggest Crypto Ponzi Schemes. *CoinMarketCap*. <https://coinmarketcap.com/alexandria/article/5-of-the-biggest-crypto-ponzi-schemes>

Sonnemaker, T. (2021, 7 June). The FBI recovered a huge chunk of the Colonial Pipeline ransom by secretly gaining access to DarkSide's bitcoin wallet password. *Business Insider*. <https://www.businessinsider.com/fbi-used-hackers-bitcoin-password-to-recover-colonial-pipeline-ransom-2021-6>

Voell, Z. (2020, 29 August). Ethereum Classic Hit by Third 51% Attack in a Month. *CoinDesk*. <https://www.coindesk.com/ethereum-classic-blockchain-subject-to-yet-another-51-attack>

## Further Exploration

[Blockchain use case: protecting intellectual property and blockchain patents](#)

[Code Is Law](#)

[Ripple case seen as precedent for cryptocurrency regulation](#)

[United American Corporation vs. Bitmain, Inc., et al.](#)

[JDSUPRA website \(An explanation of the Howey Test and cryptocurrencies\)](#)

# 4.4 The Regulatory Environment

## 4.4.1 Overview of the Regulatory Environment

### Quick Fact

A “regulatory sandbox” is a space for technology innovators, developers, regulators, and consumer and market representatives to come together and collaborate on experimental technologies, rules, and regulations. The children’s adage to “play nice with others in the sandbox” is the concept behind a regulatory sandbox, as it encourages participation and safe development practices.

### Overview

In Module 3, you learnt about cryptocurrency and blockchain industry regulators and their roles in monitoring activity and enforcing regulations. Now, let’s take a look at how some of these agencies around the world have responded to increased investor participation and the pressure to make room for more widespread adoption of blockchain technology and cryptocurrency investment.

Note that most of the established regulatory framework exists only for crypto native projects. Regulations are now emerging for innovative blockchain use cases that may or may not have an underlying token or currency.

(Note that the law, discussed in relation to blockchain in the last section, generally means statutes written by legislatures. Regulations, on the other hand, are standards put in place by administrative agencies that are intended to enforce the law.)

### Vocabulary Check

This section introduces the following terms.

- [anti-money laundering \(AML\)](#)
- [Bitcoin Exchange Traded Fund \(ETF\)](#)
- [principles-based regulation](#)
- [regulatory arbitrage](#)
- [rules-based regulation](#)

## Guest Video: Coinbase Accepts Regulatory Attention

In the following video, Emilie Choi, President and Chief Operating Officer of Coinbase, discusses how the organisation embraces regulatory participation.



The cool thing about Coinbase is that Brian and Fred are co-founders, leaned in to regulatory and compliance fairly early. And that was a bit of an unintuitive thing to do back in the day, just given the roots and ethos of crypto. But I think they recognised that, when you touch people's money, you're going to be regulated whether you like it or not.

And so, it's much better to work with regulators to figure out the right solution to serve those customers in the right compliant way, rather than try to do something too crazy. And so, we always try to straddle that and figure out the right balance. And the way that we do that is we try to help let regulators understand the value of crypto. And so, we just—we're building out a policy function.

We just hired a wonderful person from Goldman Sachs, who's going to be heading up the policy function here. And we continue—I think that the thing that I would say about regulation, right now, is there's definitely an education foundation that needs to be lead with a bunch of different regulators across the world to make sure that they understand the benefits of crypto.

One example of this, for example—I think there's a bunch of misunderstandings about crypto being used for nefarious things, like money laundering. We actually published a fact check blog on this. And it turns out that crypto is actually less used than cash for money laundering. And so, there's some of these myths that we have to just prove out with facts, and then, continue to pave the path for crypto to be a force worldwide.

The challenge is that these things create seismic shifts. And those are scary to a lot of people, right? And so, this is part of the thing with the regulators, is that we want to make sure regulators understand the great properties that crypto brings to the table, some of the myths that exist, and make sure that we're working together and not trying to stifle innovation.

We're seeing a ton of activity and really, really robust future-looking technologies being developed out of Asia, for example. The US government needs to get on board and understand the goodness of these applications before a bunch of that innovation goes offshore, I think. So it's really just an education that, I think, is the biggest challenge, making sure that we help bring people along on that journey.

### 4.4.2 Regulations and Industry Principles

#### Regulations and Industry Principles

Innovators and regulators generally all realise the importance of balancing regulations with innovation in the blockchain ecosystem. Concepts and projects need space to incubate and develop, while regulatory rails become necessary at some point in the development process.

The self-regulatory organisation (SRO) provides an innovative approach to the challenge of balancing innovation and regulations. As we learnt in section 4.2.4, Informal Versus Formal Rule Structures, an

SRO involves members establishing the principles and rules of their organisation's structure. The SRO may also be required to register with a government agency.

## Guest Video: Regulations Play Catch Up to Innovation

In the following video, Eva Kaili, a Member of the European Parliament, discusses how regulation lags behind innovation in blockchain technology.



Regulation plays now—and I think we always, in this case, blockchain—but I think it will always play catch-up with innovation. If we should be faster or if it's better that we are a bit late so that we can understand the extent of the disruption and the positive disruption possibilities. So I think judging from like how we reacted it with blockchain. First, we had innovative business models that are emerging and scaling very fast and then the regulators that follow with like a monitoring approach.

Let's wait and see, this was the response of Kragi when I asked him in 2015, what is his take for Bitcoin. And then we had, as we do now, at this point the legislative initiatives to frame the ecosystems. I think I would say these are the three stages.

And we have policymakers and regulators that they are trying to have a framework to address the developments in the responsible way. We have also the bigger organisations trying to do the same, like the World Economic Forum publicising a policy toolkit. We have the OECD trying to—the forum for blockchain—trying also to form a toolbox for regulators in different member states. And the World Economic Forum is also trying to have a tool kit for decentralised finance to assist governments and to properly address this phenomenon.

But to do so we have to rethink everything, and this takes time. So I would say at least regulation that would set new standards to market participants and expand the basic approach to protect capital and also clearly redefine treatment of the assets that are not covered by the existing financial services regulations.

And I think there should be a safe and proportionate regulatory framework to support that we have innovation, fair competition. So I think the compass of everything we do is to maintain an adequate balance between safeguarding the positive blockchain-based financial innovations in terms of greater efficiency and broader inclusiveness and also to limit the potential of these applications to be misused, in terms of money laundering and terrorist financing, which is actually possible.

#### 4.4.3 Regulations Around the World: China and the EU

##### Guest Video: The Importance of Regulations in Blockchain Technology

In the following video, Mimi Zou, Director of Studies in Law, Regent's Park College, Oxford, discusses the importance of regulations in blockchain technology.



So I think, when I look at the different countries that are involved in blockchain initiatives, I think every country really tried and strives to become leaders or become on the top of the league table, when it comes to innovation in the blockchain ecosystem. And this is not just in the developed world, but also in developing countries.

Like there are countries in Africa, Latin America, Asia that are really trying to adopt and develop new ways of using blockchain technology. And we see just a wide range of initiatives in the public and private sector in many different countries to apply this new technology in different settings, be it land registries or voting.

Now, in terms of-- from my perspective as a lawyer, I do think that having a strong legal and regulatory framework for blockchain governance will put countries ahead of the game. So I think often we associate regulation with stifling innovation. Now, in my view-- and there's a lot of literature out there on regulatory theory-- is that regulation doesn't necessarily stifle innovation.

You can have very careful design and selection of particular regulatory approaches that actually promote innovation, that promote competition in the market. So we shouldn't see regulation of blockchain as a bad thing. In fact, it can be-- in fact, it's necessary, actually. We see countries like Malta, like Singapore, like Switzerland that have developed very strong frameworks that promotes the use and application of blockchain technologies.

And they are among, certainly, the leading countries in promoting innovation in this sphere. Of course, you also have on the extreme China that is pretty much banning all types of cryptocurrency, Bitcoin activities, of course, developing its own digital currency, but at the same time, having a very pro blockchain policy environment. So perhaps, in terms of, regulation, it doesn't matter, if you're very pro blockchain-- or actually, most country, I think, are very pro blockchain.

But in terms of cryptocurrency, that may not make a big difference in the overall ecosystem. But in terms of, the use and application of blockchain services, I think having a regulatory environment that really promotes this-- I think it will be conducive for a country to really innovate. Now, I also think that countries with a dynamic startup environment is also very important for the innovation of blockchain technologies.

So countries that really actively encourage new companies to start and scale and really pump money into that ecosystem, I think those countries will also see innovation in the sphere and not coming just from the big players, like Microsoft and IBM. So we're really going to see really grass up-- a grassroots, ground up innovation from universities, from kids who are really just 20-year-olds who just started their own companies. That's where we're going to see some innovation.

## Guest Video: China's Guidance on Use of Blockchain

In the following video, Mimi Zou provides an overview of the regulatory guidance provided by the Supreme People's Court in China.



So when we're talking about legal precedence or guidelines, I just want to say, technically speaking, we don't have a system of precedence in Chinese legal system. So it's not like the common law that we're perhaps familiar with in the UK, and the Commonwealth, and the US.

So in the Chinese legal system, it's not really precedent or case law, but the Supreme People's Court, which is the top court of the Chinese legal system, does issue regulatory guidance for lower courts. And in China there's, about 3,500 lower courts underneath the Supreme People's Court. So it has issued, in terms of specifically related to blockchain, owing in the context of the use of blockchain in online litigation in Chinese courts. So in 2018, the Supreme People's Court already recognized the authenticity of evidence that is recorded on blockchain in the context of online litigation.

Now recently, in May 2021, Supreme People's Court has further issued a regulation that provides more detailed rules about the use of blockchain evidence in online litigation across all courts in China, not just the internet courts that were specifically set up by the Chinese courts to resolve internet disputes. Now we're seeing, really, online litigation across many courts in China. And so the Supreme People's Court has laid down these rules, and particularly noting the rollout of blockchain technology in the courts as a efficient and effective way of recording trial evidence.

## China

The US Library of Congress describes China's cryptocurrency regulatory framework with the focus on cryptocurrencies not being recognised as legal tender in China. The banking system does not acceptor provide services for cryptocurrencies. The government has declared ICOs as illegal, restricted the main business of crypto trading platforms, and taken strong measures to discourage bitcoin mining. The government states that these measures are geared towards investor protection and financial risk prevention (Library of Congress, 2020). While China has not passed any legislation regarding cryptocurrencies, regulations are prevalent.

Notably, China's central bank, the People's Bank of China, has banned all crypto activity as of 24 September, 2021. The following timeline demonstrates the central government's steady pressure to assert control over crypto activity (Library of Congress, 2020):

Date	Regulatory Activity
3 December, 2013	Banks and payment institutions are banned from dealing in bitcoin, directly or indirectly.
4 September, 2017	ICO rules were issued that banned all initial coin offerings.
15 September, 2017	Senior executives of cryptocurrency trading platforms were summoned for “chats” with the Beijing Internet Finance Risk Working Group, ordered to cease new client registration, and given a deadline when all platforms would cease trading cryptocurrency.
January 2018	The Leading Group of Internet Financial Risks Remediation asked local governments to discourage bitcoin mining and cease giving preferential terms for miners such as favourable electricity prices, taxes, or land use. In addition, localities had to submit regular reports of mining operations in their jurisdictions and encourage bitcoin miners to cease operations.
6 July, 2018	Chinese authorities identified 88 virtual currency trading platforms and 85 ICO platforms that withdrew from the market. Bitcoin traded with the Chinese yuan dropped from 90% of global bitcoin trading to under 1%.
21 May, 2021	China's State Council stated that it would tighten bitcoin trading and mining restrictions, which was the first time bitcoin mining was officially targeted (Heavens, 2021).
24 September, 2021	China's central bank declared all cryptocurrency-related transactions illegal and banned foreign exchanges from providing crypto services to residents (Nagarajan, 2021).

## Bitcoin Mining in China

Until 2021, bitcoin mining was prevalent in China. In Module 1, we reviewed the top four countries with the highest bitcoin mining hash rates. In April 2020, China had the highest bitcoin mining hash rate at 65%, followed by the United States at 7.24%, then Russia at 6.9% (Nash, 2020). In certain provinces, bitcoin mining transitioned to a hydropower electrical supply, which substantially lowered the carbon footprint from mining. However, by March 2021, China's mining hash rate had dropped to 46% (CBECI, 2021). Since the government's crackdown, China's mining exodus has resulted in significant hash rate gains in the US, Russia, Iran, and Kazakhstan.

## The European Union

The European Union (EU) is a political and economic union made up of 27 member states. Its executive branch, the European Commission, strongly supports rules for blockchain-based activities for cohesion among its members and has adopted a comprehensive legislative package of rules regulating crypto assets with the primary focus of ensuring consumer and investor protections. The package creates a legal framework for the development of innovative crypto products and services (European Commission, 2021).

At a Global Crypto Regulation panel discussion on 23 June 2021, with Dawn Stump, US Commodities and Futures Trading Commission (CFTC) Commissioner, and the moderator Jason Brett from Forbes,

Peter Kerstens gave his perspective on the motivation of the EU to pursue regulatory measures for crypto assets. Kerstens advises on technological innovation, digital transformation and cybersecurity at the European Commission's Directorate-General for Financial Stability, Financial Services, and Capital Markets Union. He stated there were four primary reasons for the EU to move forward with establishing a regulatory framework (Kerstens et al., 2021):

- Strong requests by market participants for legal clarity and regulation.
- Obvious market failures such as fraudulent crypto schemes that made it hard for consumers to distinguish those from legitimate opportunities.
- The EU's desire to enable responsible innovation within a legal framework.
- National regulations from individual member states, which had created a segmented market within the EU.

With the implementation of a regulatory framework, issuers could issue assets unencumbered throughout the EU, and service providers could operate throughout the EU (Kerstens et al., 2021).

The European Union is proactive in using blockchain technologies to create trust between parties and establish a “gold standard” in Europe that embraces European values and ideals in its legal and regulatory framework. The comprehensive strategy includes:

- Building a pan-European public services blockchain
- Promoting legal certainty in blockchain use cases
- Increasing funding for research and innovation
- Promoting blockchain for sustainability

The following entities work with the private sector, academia, and the blockchain community to promote responsible blockchain development (European Commission, 2021):

- **The International Association of Trusted Blockchain Applications (INATBA):** INATBA is a public/private partnership designed to bring EU countries together with the private sector and other stakeholders like academia to further the blockchain ecosystem in Europe. INATBA promotes the interoperability of blockchain technologies and good governance and acts as an interlocutor of governments and international bodies.
- **The European Blockchain Observatory and Forum:** The EU Blockchain Observatory and Forum is a European Parliament-funded pilot project, which aims to pool expertise to identify and monitor blockchain initiatives and trends globally to create a comprehensive, publicly available source of blockchain knowledge that supports the blockchain ecosystem within the EU.

## Guest Video: European Parliament Legislation Update

In the following video, Eva Kaili, a Member of the European Parliament (MEP), provides a mid-year 2021 update on the status of this legislation.



So the crypto assets, the MiCA file is ongoing and also the DLT pilot regime has just passed the European parliament's discussions, and now I think it's entering the trialogue basically. Crypto assets are the major applications that we have of blockchain technology and finance, and Econ committee has voted the compromise text for the DLT.

We will basically, let's say, lead the way also for the MiCA file. And the brief presentation of these proposals, if it could be brief, I would say that crypto assets that bear characteristics of transferable securities, they fall within the scope of EU financial framework, but the application of this framework is not always straightforward, and then the DLT might inhibit.

So then we have the DLT pilot regime that provides also for certain exemptions from the EU legislation where we want to test the issuance, the recording, the trading, and the settlement of taxable securities that fall under the scope of the MiFID II on DLT. So it's technical, but people that they have dealt with DLT and MiCA, they understand the two different approaches we have.

So most crypto assets, they fall outside the scope of EU financial services legislation. So they are not subject to provisions on consumer and investor protection and market integrity. And also to do that, we have different national regimes that could create fragmentation, so that's why we have a uniform and competitive effort for the—with the MiCA file.

So the MiCA file would cover all the assets that do not fall under MiFID and they are generally outside the existing EU financial services legislation—for example, the utility tokens and the payment tokens and also some stable coins, the ART and the EMT, the asset-referenced tokens and the EMANATE (MN8) tokens.

It would also not just regulate the tokens themselves but also the crypto assets service providers and what services they can offer. I think this is quite important, because if there's going to be legal certainty and clarity of what we can achieve in Europe, and I think it would bring some uniformity, some harmonisations, and it would replace the existing national frameworks.

And hopefully, it will safeguard the financial stability and the orderly monetary policy that could—the challenges could arise from the stable coins as we saw with the DM a few months ago. And the same time, we would try to address the AML.

And two things for the DLT since we understood that it covers transferable security characteristics of tokens under the scope of the MiFID II, these will allow not just the licenced already about different structures but also new entrants to be licenced in the first, I would say, EU wide experimentation for five years. There would be some time to enter, some time to exit. There will be a very strong position of the ESMA. So I'd say also for the first time we will have a center of European authority that will have a responsibility of who is entering and exiting.

And we will already have, for example, the issuance of bonds on DLT even by the EIB, the European Investment Bank. So this will become possible. And whoever wants to enter, they will have to apply for a licence or permission of DLT, the MFT or the SSS—the multilateral credit facility or the security settlement system. And there will be several exceptions, of course, since this is a pilot that we want to test the technology. So quite complicated, and then I still said that we need to discuss further for defined MFTs.

## 4.4.4 Regulations Around the World: The UK and US

### The United Kingdom

The UK launched the Cryptoassets Taskforce in March 2018 to outline and provide guidance on commitments related to crypto-assets and distributed ledger technology. The task force's focus is to:

- Maintain the UK's international reputation as a safe and transparent place to do business in financial services.
- Ensure high regulatory standards in financial markets.
- Guard against threats to financial stability that could emerge in the future.
- Allow those innovators in the financial sector that play by the rules to thrive.

The Taskforce, created by the Chancellor of the Exchequer, comprises HM Treasury, the Financial Conduct Authority (FCA), and the Bank of England. After a period of study and consultation with stakeholders, the Taskforce published its Final Report in October 2018. The report laid out the UK's policy and regulatory approach to crypto-assets and distributed ledger technology and set the path forward for crypto regulation in the UK.

The Final Report concluded that distributed ledger technology could potentially deliver significant benefits in financial services and other sectors and that all three authorities on the task force would continue to support its development (Cryptoassets Taskforce, 2018).

The UK does not regulate most crypto assets and services. However, the following rules have been established by the FCA and provide some regulatory framework:

- Cryptoasset registration was established in January 2020 and is a requirement for businesses to register with the FCA. The registration will allow the FCA to supervise how crypto-asset businesses manage the risk of money laundering and counter-terrorist financing.
- Bitcoin and other cryptocurrencies are considered exchange tokens, and the UK only regulates them for anti-money laundering purposes.
- Security tokens fall into the regulated assets category and affect tokens that provide ownership rights, repayment of a specific sum of money, and entitlement to a share of future profits.
- Crypto-derivatives sales are banned for retail customers due to concerns over volatility and valuation of the underlying crypto assets.

The UK allows ICOs and the use of stablecoins to make payments. Stablecoins are typically pegged to a fiat currency for value stabilisation. They are a more conservative and less volatile crypto asset. The UK government is currently analysing the use of stablecoins that are used for payment and services and that would, therefore, become a regulated activity (Financial Conduct Authority, 2021).

The regulating authorities of the United Kingdom are (Cryptoassets Taskforce, 2018):

- **HM Treasury:** Her Majesty's Treasury is the government's economic and finance ministry that develops financial services policy. It supports the financial services sector in achieving stability and efficiency through growth, businesses, and consumers. The ministry fosters healthy competition and promotes improving consumer outcomes.
- **The Financial Conduct Authority (FCA):** The FCA is the UK's financial services and markets regulator that oversees the conduct for 58,000 financial services firms and is the prudential regulator (risk control and capital adequacy) for 18,000 of those firms. The authority strives for consumer protection, financial market protection, and healthy competition.
- **The Bank of England:** The Bank of England is the UK's central bank, with the Prudential Regulation Authority (PRA) as its regulatory arm. The bank's primary objective is to maintain monetary and financial stability. The PRA oversees its regulated financial firms' safety and soundness practices.

## The United States

On 22 June 2021, Congresswoman Maxine Waters (D-CA), Chairwoman of the House Committee on Financial Services, announced a Digital Assets Working Group that will work with experts and government officials to learn about digital assets—the challenges, risks, and innovation opportunities. The group will work to advance legislation favourable to digital assets oversight and responsible activities, specifically cryptocurrency regulation, the use of blockchain technology, and the possible development of a US central bank digital currency (US House Committee on Financial Services, 2021).

Separately, the US Senate passed the United States Innovation and Competition Act of 2021 (S. 1260) on 12 May 2021. The bill has many components and works to strengthen the United States' leadership in critical technologies (Congress, 2021).

## Securities and Exchange Commission

The Securities and Exchange Commission (SEC) is the most prominent regulatory agency in the US that has scrutinised cryptocurrencies and, by extension, their underlying blockchain technologies. As an agency of the federal government, two of the SEC's primary responsibilities include protecting investors and maintaining fair and orderly functioning of the securities markets. Two of the SEC's primary areas of focus in blockchain involve DeFi and Bitcoin ETFs:

- **Decentralised Finance (DeFi):** In the summer of 2021, the SEC began announcing charges and potential violations of securities law in the DeFi sector. This included charges against top executives and their company for “unregistered sales of more than US \$30 million of securities . . . and for misleading investors” (SEC, 2021). It also included notification to a major exchange about a potential lawsuit over the organisation’s Lend product and instructions to not bring the product to market. With this move, the SEC is likely establishing that it considers crypto lending a securities offering (Avan-Nomayo, 2021).

- **Bitcoin ETFs:** The SEC has shown persistent resistance to the mainstream adoption of cryptocurrencies as tradable investment vehicles. More specifically, a number of large investment banks have applied to the SEC for approval to establish bitcoin exchange-traded funds (ETFs). As of September 2021, all of these applications have been rejected.

By establishing bitcoin ETFs, the investment banks want to offer bitcoin exposure to traditional investors via existing retail trading apps. The investors would not need to purchase bitcoin directly and go through the process of establishing a digital wallet or an account on a crypto exchange. Instead, they would invest in this fund through their broker.

Some of the SEC's concerns are visible in an application for the VanEck Bitcoin Trust, where a decision has been delayed twice. Nate DiCamillo at CoinDesk noted, "The SEC asked for public comment on their applications, and they also asked interested parties to answer questions about how susceptible the ETF would be to market manipulation and whether or not the regulatory landscape has changed significantly since the first time bitcoin ETF applications had garnered popular attention in 2016" (2021).

How much will the market need to improve for the SEC to favour bitcoin ETF approval? The SEC continues to have concerns over fraud and manipulation. Moreover, the organisation does not have surveillance and controls in place to adequately protect investors. However, Gary Gensler was appointed as the SEC chair in April 2021. As a crypto advocate, Gensler is expected to lower the resistance to approving bitcoin ETFs, although this is not a certain outcome of his tenure (De, 2021).

## In the News

On Tuesday, 19 October, 2021, the first bitcoin ETF began trading. The ProShares Bitcoin Strategy ETF, ticker symbol "BITO", opened at \$40 a share and finished the day up 5%. More bitcoin ETFs are expected to follow ProShares (La Monica, 2021).

## Guest Video: Securities Compliance With Tokensoft's Mapping Process

In the following video, Mason Borda, CEO and Co-Founder of Tokensoft, provides an overview of Tokensoft's protocol that provides securities compliance through its mapping process. The protocol aims to be proactive in helping its users stay compliant with securities regulations.



When putting these securities onto the blockchain in the traditional finance world there's a software that's been developed to track and manage everything from a compliance perspective, from an accounting perspective. Now that we're putting these securities on the blockchain we also have to make sure they comply with the same rules and can engage in the same accounting sort of reporting and activities. And so our role is sort of to provide the mapping in between the blockchain and the existing regulations and securities laws or commodities laws or whatever they may be that are out there and to ensure that the blockchain can and the tokens transfer on the blockchain can comply with those regulations.

## Commodities and Futures Trading Commission

While the SEC monitors and protects investors in the securities markets, the Commodity Futures Trading Commission (CFTC or the Commission) monitors and protects investors in the derivatives markets. A derivative is “a contract between two or more parties whose value is based on an agreed-upon underlying financial asset (like a security) or set of assets (like an index)” (Chen, 2021). The CFTC is also an independent agency of the US federal government.

The Commission has not formally defined virtual currency, or digital asset, through regulation, but the Commission and the federal courts have found virtual currencies to be commodities under the Commodity Exchange Act (CEA), which regulates the trading of commodity futures in the US and establishes the statutory framework under which the CFTC operates. A commodity is a basic good used in commerce that is interchangeable with other goods of the same type.

In the same panel discussion on 23 June 2021 with Peter Kerstens, Advisor to the European Union, CFTC Commissioner Dawn Stump gave her perspective on the timing for regulatory agencies to become involved with the crypto markets, saying, “It’s important to allow the markets to develop a little first before regulations are put in place” (Stump, 2021). Stump outlined some proactive steps that could be taken in the meantime, including:

- Regulatory agencies could help innovation on the front end by providing guidelines.
- Innovators could be more proactive in involving regulators and working together to decrease illicit activity.
- Interested parties could look to the upcoming electronic order book in trading, but temper opportunity with skepticism.
- Innovators and developers could provide the CFTC with new information about changes in digital assets as soon as the information becomes available.

The CFTC acknowledged the rise in prominence of digital assets, and included in its oversight is the monitoring of bitcoin futures markets. In addition, the agency has made attempts to be proactive with its communications, and has issued primers, backgrounders, and interpretive guidance on the following related topics:

- Virtual currencies (CFTC, 2017)
- Self-certified contracts for Bitcoin products (CFTC, 2017)
- Oversight of and approach to virtual currency futures (CFTC, 2018)
- Smart contracts (CFTC, 2018)
- Actual delivery for digital assets (CFTC, 2020)

The CFTC's Division of Enforcement has been active in its oversight and enforcement efforts. In the first four months of 2021, the organisation investigated and prosecuted the following digital assets violations, representing US \$628 million in fraudulent activities (CFTC, 2021):

Date	Regulatory Activity
20 April, 2021	The CFTC orders a Florida man and his company to pay over US \$397,000 in connection with a digital assets solicitation scheme.
8 April, 2021	A federal court orders a Nevada company and its owner to pay more than US \$32 million for a cryptocurrency fraud and misappropriation scheme.
26 March, 2021	A federal court orders a UK man to pay more than US \$572 million for operating a fraudulent bitcoin trading scheme.
19 March, 2021	The CFTC orders Coinbase Inc. to pay US \$6.5 million for false, misleading, or inaccurate reporting and wash trading.
5 March, 2021	The CFTC charges two individuals with a multi-million dollar digital asset pump-and-dump scheme (US \$2 million).
26 January, 2021	The CFTC charges a New York man in multi-million dollar digital asset Ponzi scheme involving Bitcoin and Ether (US \$5 million).

## FINRA

The Financial Industry Regulatory Authority (FINRA) is a non-governmental self-regulated organisation that writes and enforces the rules governing registered brokers in the US. FINRA takes the position that the cryptocurrency markets are volatile and risky. The organisation provides investor guidance and references to other agencies, such as the SEC and the CFTC, and regularly issues investor alerts. FINRA issues proposed rule changes to the SEC, such as Regulatory Notice 20-23, issued July 9, 2020, that states, "FINRA encourages firms to notify FINRA if they engage in activities related to digital assets" (FINRA, 2020).

In January 2017, FINRA issued "Distributed Ledger Technology: Implications of Blockchain for the Securities Industry", a 22-page document that gives an in-depth review of some key applications being explored in the securities industry, the potential impact of the technology, and key implementation and regulatory considerations for broker-dealers. The report is also known as FINRA's Blockchain Report (FINRA, 2017).

The US Treasury, the Federal Reserve Bank, and the Financial Crimes Enforcement Network (FinCEN) all have a stake in the digital assets space. Each has similar positions to encourage the proactive development of a sound legal and regulatory framework around cryptocurrencies and blockchain technology.

## 4.4.5 Regulatory Arbitrage and Domicile Choice

### Regulatory Arbitrage and Domicile Choice

Regulatory arbitrage is the practice of avoiding regulatory violations by using loopholes in current regulations, restructuring a transaction to accommodate the regulations, and re-engineering the financial terms of a transaction to fit into the regulations. This is often done to take advantage of tax havens and weak points in the regulatory framework. Examples of regulatory arbitrage include:

- A business forms as a partnership to avoid taxation as a corporation.
- A financial organisation limits its products or services to avoid classification as an investment company.
- A business sets up its operations in the US state of Delaware because that state does not impose a sales tax.

Domicile choice is a form of regulatory arbitrage that involves operating or basing a business in another location that has more favourable laws and regulations, thereby circumventing the laws in the founder's current location. The Cayman Islands, for instance, offers tax advantages to businesses, as the government there does not require paying taxes on revenue earned outside the territory (Hayes, 2021).

As blockchain technology continues to outpace the legal and regulatory systems, it is common for unscrupulous businesses to employ regulatory arbitrage, including domicile choice, to take advantage of a looser set of regulations and laws. Money laundering and terrorist financing are two of the most common cryptocurrency crimes that utilise regulatory arbitrage to further their criminal activities.

With cryptocurrency transactions favouring cross-border payments, establishing international standards to regulate digital assets has become increasingly important. Anti-money laundering (AML) and combating the financing of terrorism (CFT) have become a focus for governments, both domestically and internationally.

In its crypto assets report dated April 2020, the European Parliament addressed key developments, regulatory concerns, and responses. The Parliament dedicated a section of the report to calling for international cooperation and rulemaking to address AML and CFT activity. The report noted that regulatory arbitrage is a common practice of criminals and terrorists and pointed out the need to strengthen regulations and develop some consistencies with other nations to deter such activity. The report concluded by noting strong efforts are being made toward common regulations in an intergovernmental policy-making body, the Financial Action Task Force (FATF).

Formed in 1989 by the G7 (Group of Seven), the FATF is the global money laundering and terrorist financing watchdog. By strengthening its standards and addressing new risks, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in the areas of money laundering and terrorist financing. The task force currently has 39 members and many more observer organisations (Houben & Snyers, 2020).

At the FATF's June 2021 Plenary held in Paris, France, two of the eight strategic initiatives were related to AML and CFT and to virtual assets or virtual assets service providers (VASPs), aka crypto companies. One of the initiatives focused on combating AML and CFT and the required policies and practices needed to successfully leverage technology-based solutions in this effort.

The other initiative focused on the revised standards on virtual assets and VASPs. FATF conducted a second 12-month review of these standards' implementation and concluded that 58 of the 128 reporting jurisdictions had implemented the revised standards. However, as of later in 2021, the majority of jurisdictions have not implemented the FATF's travel rule, which requires the collection and disclosure of personal data for transactions that exceed US \$1,000 or €1,000. The travel rule requires that this data "travel" with the transaction between VASPs.

The FATF remains concerned that the low implementation rate of the travel rule indicates a lack of global safeguards against money laundering and terrorist financing, as misuse of virtual assets through jurisdictional arbitrage remains a threat. The FATF monitors countries to ensure they implement the FATF standards fully and effectively, holding them accountable for not complying (FATF, 2021).

## Principles-Based Regulations Versus Rules-Based Regulations

In his book *Basic Blockchain*, David Shrier, CEO of Esme Learning Solutions, explains the differences between the two types of regulations and how they may or may not be applicable to blockchain technology. He concludes that rules-based regulations are not well-suited for most blockchain applications as they require strict compliance to the stated rules and do not allow for a more nimble, innovative approach. His full statements on both types of regulations are as follows (Shrier, 2020):

With **principles-based regulation**, rules are articulated in broad strokes so that their interpretation is somewhat flexible. The overall goals of the regulation are patent. How it gets applied, both by the companies and by the regulators, becomes more of a dialogue between the parties and an application of art rather than science. Principles-based regulation allows for a more flexible framework that can be adapted to different circumstances and different levels of regulatory competition. When innovation strikes, as with blockchain, innovative companies engage in a practice known as 'domicile shopping' as they seek out the optimal regulatory regimen to propel growth. In blockchain, small and nimble countries like Mauritius, Bermuda, Barbados and Malta have enjoyed outsized rewards by showing regulatory flexibility, both in adapting existing regulations to new technology and in promoting new pro-innovation regulation. Principles-based regulation also requires sophisticated regulators and compliance professionals at companies to navigate this interpretive path..

**Rules-based regulation** sets out remarkably clear activities that must take place in order to achieve compliance. The individual rules are apparent, but creating a generalisable framework that can apply broadly and that ties to regulatory goals is a more arduous task. How can regulators stitch together a patchwork quilt of highly specific rules that ensure outcomes like greater financial inclusion or financial stability? Rules-based regulatory systems are easier to understand, insofar as a market participant follows a checklist to make sure he or she is in compliance, but very slow and prone to inertia when faced with innovation. Blockchain is still in an evolutionary phase, and its various derivations and the business ecosystems surrounding it are changing rapidly. Rules-based systems are ill-suited to engage with blockchain.

## 4.4.6 Case Study: BitLicense—New York’s Regulatory Initiative for Virtual Currency

### Case Study: BitLicense—New York’s Regulatory Initiative for Virtual Currency

In 2015, New York’s Department of Financial Services (NYDFS) issued virtual currency regulation 23 NYCRR Part 200 under the New York Financial Services law. It is known as the BitLicense regulation, and it was introduced as a consumer protection mechanism to give New Yorkers safe access to virtual currency marketplaces. Consumers can buy, sell, or trade cryptocurrencies without a license.

A BitLicense is for businesses that want to offer cryptocurrency transmission, exchange services, and digital asset management. The DFS held public hearings in November 2013 and released the details of BitLicense in July 2014. Initially, ten crypto companies ceased all activities in the state in protest of perceived unfair legislation.

As of May 6, 2021, 29 entities hold either a BitLicense—a virtual currency license—or a limited purpose trust charter issued and regulated by the DFS. The limited purpose trust charter allows a business to conduct fiduciary activities such as custodial or depositor services and is granted by the DFS under New York banking law.

A 2015 DFS press release provided further insight into the rationale behind this regulation and tied it directly to the Mt.Gox collapse. The release stated that the NYDFS initiated a process for accepting charter virtual currency exchange applications under existing New York banking law in March 2014, noting those exchanges must also meet the NYDFS BitLicense regulatory framework that was not finalised until June 2015 (Anderson, 2015).

Circle Internet Financial, Inc., a global payments company, was granted the first BitLicense in September 2015, and Paxos Trust Co., LLC received the first limited purpose trust charter in May 2015.

The following is a full list of regulated entities in New York and their specific licensures (Department of Financial Services, Regulated Entities, 2021):

Entity	Licensure	Date Granted
Paxos Trust Company, LLC	Limited purpose trust charter	2015-05
Circle Internet Financial, Inc.	Virtual currency and money transmitter licenses	2015-09
Gemini Trust Company, LLC	Limited purpose trust charter	2015-10
XRP II LLC (Ripple)	Virtual currency license	2016-06
Coinbase, Inc.	Virtual currency and money transmitter licenses	2017-01
Genesis Global Trading, Inc.	Virtual currency license	2018-05
Square, Inc.	Virtual currency and money transmitter licenses	2018-06
Xapo, Inc.	Virtual currency license	2018-06
Bitpay, Inc.	Virtual currency license	2018-07
Coinbase Custody Trust	Limited purpose trust charter	2018-10

Entity	Licensure	Date Granted
Bitflyer	Virtual currency license	2018-11
Coinsource	Virtual currency license	2018-11
NYDIG Execution LLC	Virtual currency and money transmitter licenses	2018-11
NYDIG Trust Company LLC	Limited purpose trust charter	2018-11
Cottonwood Vending	Virtual currency license	2019-01
LibertyX/Moon Inc.	Virtual currency license	2019-01
Robinhood Crypto	Virtual currency and money transmitter licenses	2019-01
Bitstamp USA, Inc.	Virtual currency license	2019-04
Seed Digital Commodity Market, LLC	Virtual currency license	2019-07
Zero Hash LLC	Virtual currency and money transmitter licenses	2019-07
Bakkt Trust Company LLC	Limited purpose trust charter	2019-08
Fidelity Digital Asset Services, LLC	Limited purpose trust charter	2019-11
SoFi Digital Assets	Virtual currency and money transmitter licenses	2019-11
Eris Clearing, LLC	Virtual currency and money transmitter licenses	2020-05
PayPal, Inc.	Conditional virtual currency and money transmitter licenses	2020-10
GMO-Z.com Trust Company, Inc.	Limited purpose trust charter	2020-12
Bakkt Marketplace, LLC	Virtual currency and money transmitter licenses	2021-03
BitGo New York Trust Company LLC	Limited purpose trust charter	2021-03
Standard Custody & Trust Company, LLC	Limited purpose trust charter	2021-05

The application process for a BitLicense is arduous. The process involves an initial fee of US \$5,000 in addition to a 30-page application, a four-page checklist of required documents, and a 44-page regulations checklist, among other requirements. However, once approved, businesses receive protection from unnecessary lawsuits and fraudulent investors. In addition, they receive special permission for the following:

- Transmitting digital currency
- Storing or taking custody of digital currency
- Buying and selling virtual currency, including exchanging virtual currencies for fiat currencies
- Operating a virtual currency trading exchange
- Issuing a virtual currency
- Use any of the coins on the Greenlist which are pre-approved by the state for such use

While it was considered stifling and unjust initially, the BitLicense framework does promote legal and regulated cryptocurrency activities. In particular, it exists to protect investors and eliminate illicit activities as much as possible (Adejumo, 2021).

## Guest Video: Regulatory Considerations

In the following video, Federico Spagnoli, Regional President, Prudential Financial/Latin America, reviews the four steps needed to achieve some level of regulation.



So the lag between regulation and the level of innovation behind blockchain technology is difficult to estimate. But it is significant as the structure of these three-letter technology process in that it challenges traditional approaches to regulation and governance. The adoption of enterprise or private blockchains, as we all know, have become much more dominant in recent years. And therefore, traditional government and regulation mechanisms allow to deal with that. The greater adoption of public and permissioned DLTs is what is going to make the situation much more complex.

Just a few considerations for us to think about, as we think about the definition of governance or regulatory frameworks for blockchains. Number one, it's not possible to regulate blockchains themselves. What we can do is to try to regulate their underlying use cases. This should be done in collaboration with regulators from various jurisdictions, as well as all other stakeholders.

There is no clear combination of governance mechanism for blockchains. It will involve a mixture of regulatory levers, which will need to be pulled in order to find the right balance. And last, one of the major dilemmas in regulation of blockchains is that, in one hand, regulation is important to protect users, and data privacy, security. But in the other hand, if you put too much regulation, too many constraints, you are affecting and constraining the ability to innovate, which is what blockchain technology gives us the possibility to do.

### 4.4.7 Regulatory Acronyms, Key Takeaways, References, and Further Exploration

#### Regulatory Acronyms

OSC	Ontario Securities Commission (Canada)
CRA	Canada Revenue Agency
PBOC	People's Bank of China
CAC	Cyberspace Administration of China
MIIT	Ministry of Industry and Information Technology (China)
SAIC	State Administration for Industry and Commerce (China)
CBIRC	China Banking and Insurance Regulatory Commission
CSRC	China Securities Regulatory Commission
EU	European Union

EC	European Commission, the executive branch of the EU
PSA	Payment Services Act (Japan)
FIEA	Financial Instruments and Exchange Act (Japan)
FCA	Financial Conduct Authority (UK)
CFTC	Commodities and Futures Trading Commission (US)
CEA	Commodity Exchange Act (US)
SEC	Securities and Exchange Commission (US)
FINRA	Financial Industry Regulatory Authority (US)
FinCEN	Financial Crimes Enforcement Network (US)
FATF	Financial Action Task Force (G7, Group of Seven)
DFS	Department of Financial Services (New York, US)

## Key Takeaways

Throughout the world, many different regulatory bodies set rules for cryptocurrencies and blockchain technologies. Some key takeaways in the current regulatory environment are as follows:

1. To a great extent, regulations are established only when there is enough traction and history with particular blockchain innovations. This can be a good position to encourage innovation. Conversely, it can hamper activity by stifling innovation. A good example of this is the amount of time it has taken the United States to contemplate the regulatory status of bitcoin and whether a bitcoin ETF will be approved by the SEC.
2. The EU has taken a more pragmatic approach with its regulatory stance out of its need to coordinate member countries' crypto activities. Some countries, like China, already have stricter laws regulating cryptocurrency activities, and many countries have taken a stance against criminal money laundering and terrorist funding through cryptocurrencies.
3. Blockchain technology is developing more quickly than the legal and regulatory systems to support it, so regulatory arbitrage taking advantage of looser regulations and laws, including domicile choice, is common. Money laundering and terrorist financing are two of the most common cryptocurrency crimes that utilise regulatory arbitrage.
4. Because the technology is changing so rapidly, experts recommend a principles-based approach over a rules-based approach to adapt to the technology and its applications as they develop.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 19 April, 2022.

### 4.4.3 Regulations Around the World: China and the EU

CBECI. (2021, 15 July). Bitcoin Mining Map. Cambridge Bitcoin Electricity Consumption Index. [https://cbeci.org/mining\\_map](https://cbeci.org/mining_map)

European Commission. (2021, 25 June). Legal and regulatory framework for blockchain. *European Commission*. <https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy>

Kerstens, P., Stump, D., & Brett, J. (2021, 23 June). *Global Crypto Regulation Panel* [Conference session]. Shining a Light on Digital Asset Markets Conference. New York City, NY, United States.

Nash, H. (2020, September). Adoption rate of emerging technologies in organizations worldwide as of 2020, by scale. *Statista*. <https://www.statista.com/statistics/661164/worldwide-cio-survey-operational-priorities>

U.S. Library of Congress. (2020, 30 December). Regulation of Cryptocurrency: Canada. *Library of Congress Law*. <https://www.loc.gov/law/help/cryptocurrency/canada.php>

### 4.4.4 Regulations Around the World: The UK and US

Adejumo, O. (2021, 25 April). Crypto Regulation: Everything You Need to Know about BitLicense. *Coinspeaker*. <https://www.coinspeaker.com/guides/crypto-regulation-everything-bitlicense>

Allison, I. (2021, 16 June). Banks Edge Closer to Ethereum 2.0 Staking. *CoinDesk*. <https://www.coindesk.com/banks-edge-closer-to-ethereum-2-0-staking>

Anderson, M. (2015, 5 October). NYDFS Grants Charter to “Gemini” Bitcoin Exchange Founded by Cameron and Tyler Winklevoss. *Department of Financial Services*. [https://www.dfs.ny.gov/reports\\_and\\_publications/press\\_releases/pr1802131](https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1802131)

Avan-Nomayo, O. (2021, 12 September). Regulatory and privacy concerns trail SEC’s threat to Coinbase. *Cointelegraph*. <https://cointelegraph.com/news/regulatory-and-privacy-concerns-trail-sec-s-threat-to-coinbase>

Bastiaan, D. (2018, 30 March). Crypto Nation Switzerland: A Glimpse Into the Swiss Blockchain Ecosystem. *BlockImmo on Medium*. <https://medium.com/blockimmo/crypto-nation-switzerland-a-glimpse-into-the-swiss-blockchain-ecosystem-8de03068e0a3>

Brett, J. (2021, 22 April). U.S. House Passes Bill To Create First Crypto Task Force on Digital Assets. *Forbes*. <https://www.forbes.com/sites/jasonbrett/2021/04/22/us-house-passes-bill-to-create-first-crypto-task-force-on-digital-assets>

CFTC. (2017, 17 October). A CFTC Primer on Virtual Currencies. U.S. Commodity *Future Trading Commission*. [https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc\\_primercurrencies100417.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf)

CFTC. (2017, December). CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products. *U.S. Commodity Future Trading Commission*. [https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/bitcoin\\_factsheet120117.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/bitcoin_factsheet120117.pdf)

CFTC. (2018, 27 November). A Primer on Smart Contracts. *U.S. Commodity Future Trading Commission and LabCFTC*. [https://www.cftc.gov/sites/default/files/2018-11/LabCFTC\\_PrimerSmartContracts112718\\_0.pdf](https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718_0.pdf)

CFTC. (2018, 4 January). CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets. *U.S. Commodity Future Trading Commission*. [https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder\\_virtualcurrency01.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf)

CFTC. (2020, 24 March). CFTC Issues Final Interpretive Guidance on Actual Delivery for Digital Assets. *U.S. Commodity Future Trading Commission*. <https://www.cftc.gov/PressRoom/PressReleases/8139-20>

CFTC. (2021, 15 June). CFTC Enforcement Actions. *U.S. Commodity Future Trading Commission*. <https://www.cftc.gov/LawRegulation/EnforcementActions/index.htm>

Chen, J. (2021, June 8). Derivative. *Investopedia*. <https://www.investopedia.com/ask/answers/12/derivative.asp>

Congress. (2021, 12 May). S.1260 - United States Innovation and Competition Act of 2021. *Congress*. Gov. <https://www.congress.gov/bill/117th-congress/senate-bill/1260>

Cryptoassets Taskforce. (2018, October). Cryptoassets Taskforce: Final Report. *Cryptoassets Taskforce*. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/752070/cryptoassets\\_taskforce\\_final\\_report\\_final\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf)

De, N. (2021, 16 February). State of Crypto: Will 2021 Finally Be the Year of the Bitcoin ETF? *CoinDesk*. <https://www.coindesk.com/bitcoin-etf-2021>

DiCamillo, N. (2021, 16 June). SEC Again Delays VanEck Bitcoin ETF Decision. *CoinDesk*. <https://www.coindesk.com/sec-again-delays-vaneck-bitcoin-etf-decision>

Financial Conduct Authority. (2021, 18 June). Cryptoassets. *Financial Conduct Authority*. <https://www.fca.org.uk/consumers/cryptoassets>

FINRA. (2020, 9 July). Regulatory Notice 20-23 FINRA Encourages Firms to Notify FINRA if They Engage in Activities Related to Digital Assets. *FINRA*. <https://www.finra.org/rules-guidance/notices/20-23>

FINRA. (2017, January). Distributed Ledger Technology: Implications of Blockchain for the Securities Industry. *FINRA*. [https://www.finra.org/sites/default/files/FINRA\\_Blockchain\\_Report.pdf](https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf)

FINRA. (2017, 6 December). Anti-Money Laundering (AML) Compliance Program. *FINRA*. <https://www.finra.org/rules-guidance/guidance/reports/2017-report-exam-findings/anti-money-laundering-aml-compliance-program>

Heavens, A. (2021, 21 May). China vows to crack down on bitcoin mining, trading activities. *Reuters*. <https://www.reuters.com/technology/china-says-it-will-crack-down-bitcoin-mining-trading-activities-2021-05-21>

La Monica, P. (2021, 19 October). The first bitcoin ETF finally begins trading. *CNN*. <https://www.cnn.com/2021/10/19/investing/bitcoin-etf-proshares-bito/index.html>

Nagarajan, S. (2021, 24 September). China declares all crypto-related transactions illegal and forbids overseas exchanges from serving its citizens. *Markets Insider*. <https://markets.businessinsider.com/news/currencies/china-crypto-bans-cryptocurrency-transactions-forbids-foreign-exchanges-service-citizens-2021-9>

SEC. (2021). SEC Charges Decentralized Finance Lender and Top Executives for Raising \$30 Million Through Fraudulent Offerings. *SEC.gov*. <https://www.sec.gov/news/press-release/2021-145>

Stump, D., Kerstens, P., & Brett, J. (2021, 23 June). *Global Crypto Regulation Panel* [Conference session]. Shining a Light on Digital Asset Markets Conference. New York City, NY, United States.

U.S. House Committee on Financial Services. (2021, 16 June). Press Release: Waters Announces Digital Assets Working Group. *U.S. House Committee on Financial Services*. <https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=408014>

#### 4.4.5 Regulatory Arbitrage and Domicile Choice

Financial Action Task Force. (2021). FATF Plenary, June 20-25, 2021. Financial Action Task Force. <https://www.fatf-gafi.org/home>

Hayes, A. (2021, 26 April). Regulatory Arbitrage. *Investopedia*. <https://www.investopedia.com/terms/r/regulatory-arbitrage.asp>

Houben, R., & Snyers, A. (2020, April). Crypto-assets - Key developments, regulatory concerns and responses. *Policy Department for Economic, Scientific and Quality of Life Policies*. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL\\_STU\(2020\)648779\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf)

Shrier, D. (2020, 9 January). *Basic Blockchain: What It Is and How It Will Transform the Way We Work and Live*. Robinson.

#### **4.4.6 Case Study: BitLicense—New York’s Regulatory Initiative for Virtual Currency**

Adejumo, O. (2021, 25 April). Crypto Regulation: Everything You Need to Know about BitLicense. *Coinspeaker*. <https://www.coinspeaker.com/guides/crypto-regulation-everything-bitlicense>

Anderson, M. (2015, 5 October). NYDFS Grants Charter to “Gemini” Bitcoin Exchange Founded by Cameron and Tyler Winklevoss. *Department of Financial Services*. [https://www.dfs.ny.gov/reports\\_and\\_publications/press\\_releases/pr1510051](https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1510051)

The Federal Reserve. (1997, September). Know Your Customer Section 601.0. *Bank Secrecy Act Manual*. [https://www.federalreserve.gov/boarddocs/SupManual/bsa/bsa\\_p5.pdf](https://www.federalreserve.gov/boarddocs/SupManual/bsa/bsa_p5.pdf)

#### **Further Exploration**

[The Final Report of the UK’s Cryptoassets Taskforce](#)

[The FATF Recommendations](#)

# 4.5 Environmental, Social, and Governance (ESG) Standards

## 4.5.1 ESG Overview

### Overview

Environmental, social, and governance (ESG) standards have become essential criteria for implementing a sound business strategy. Investors will scrutinise an organisation's ESG standards when considering whether or not to support a blockchain project. Sustainability reporting is becoming a normalised subset of traditional corporate governance as well as within blockchain organisations.

The Bitcoin protocol, which has taken the brunt of the criticism about environmental issues in the blockchain ecosystem, has seen significant efforts to address ESG issues within its ecosystem. The Bitcoin Mining Council, for example, was formed when North American bitcoin miners voluntarily convened in May 2021 to discuss energy usage related to bitcoin mining. The group decided an open forum would be beneficial to promote transparency, share best practices, and educate the public on the benefits of bitcoin and bitcoin mining (Bitcoin Mining Council, 2021). It is open to all bitcoin miners and will work to provide transparency in mining's energy usage.

The major blockchain platforms have some form of organisation around ESG issues, whether through their own efforts or the voluntary efforts of users in their ecosystem.

In analysing a blockchain project's ESG challenges, we will examine the exogenous and endogenous factors presented with each ESG sector:

- **Exogenous** factors represent external variables that affect the project, but that are independent of the organisation.
- **Endogenous** factors represent internal variables within the organisation that directly affect the project and any interactions with it.

### Vocabulary Check

This section introduces the following terms.

- [carbon credit](#)
- [censorship resistance](#)
- [endogenous](#)
- [exogenous](#)

## Programme Director Video: Environmental, Social, and Corporate Governance Challenges

In this video, Meltem Demirors describes Bitcoin and ESG challenges.



Now, if you've opened a newspaper any time in the last few months, you've probably read the acronym ESG, which stands for Environment, Social Equity, and Governance. And as we talk about blockchain technology and cryptocurrencies, it's important to understand the ESG framing for this technology.

Now, let's start with the E, since it's one of the most widely discussed aspects of fluctuating technology. E stands for environmental impact. And as we know, there are many different types of environmental impact that result from different types of industries.

One of the primary criticisms levied against Bitcoin and other cryptocurrencies that utilise a proof-of-work consensus mechanism is that they are damaging to the environment due to the amount of electricity that they consume. Now, I want to counter this with some facts and by highlighting a few important considerations. First and foremost, based on research that has been done throughout the industry and by independent academic bodies, the Bitcoin network's energy usage comes primarily from renewable energy. In the United States, roughly 19% of the energy grid, as a whole, is powered by renewables. In Europe, that number is closer to 22%. And in China, that number is closer to 30%.

Now, based on the latest research, the Bitcoin network is powered by over 70% renewable energy, which would make it almost three times greener than Europe's energy consumption as a whole. It's very important to separate sources of energy from uses of energy. Now, any technology will use energy. Your phone uses energy. Your TV is using energy. Your microwave uses energy. But that doesn't make TVs, or phones, or microphones bad. What does matter is our sources of energy.

And unfortunately, sources of energy are complex and heavily regulated. In the United States, the decommissioning of nuclear power plants and a lack of investment in renewable sources of energy has meant that the share of renewables contributed to our power structure has been low. Other economies are investing heavily in putting renewables on the grid. But unfortunately, one industry alone cannot influence the sources of energy being contributed to the grid.

One really unique thing that is happening, though, is the Bitcoin industry can help put more renewables on the grid by making it economically feasible to develop certain types of renewables that may not be economically sustainable to develop without Bitcoin mining. One great example of this is hydropower plants. There's recently a hydropower plant in Kentucky that was due to be decommissioned, but a Bitcoin mining facility co-located at this power plant and now uses 100% renewable hydroelectric power. And as a result, this hydroelectric power plant is able to stay on the grid. There are countless other stories of places where Bitcoin can be utilised to finance renewable energy infrastructure development, especially in emerging economies.

So it's important to remember that when we look at Bitcoin's energy usage or the energy usage, really, of any of blockchain protocol, the story is much more nuanced than a headline you might read in a newspaper. And it's also important to remember the incentives that are at play here.

Let's also talk about the S and the G, which I think are often overlooked because, after all, it's ESG, not just E. On the S and the G, cryptocurrencies really shine. On a social equity perspective, Bitcoin is really exceptional because the Bitcoin network cannot be discriminatory in nature. Financial services have long struggled with exclusion, financial redlining, and other practices that enforce systemic racism and other types of exclusion.

In fact, the most prevalent form of violence in our world today is financial violence, in the form of financial sanctions and financial exclusion. After all, if I have the misfortune of being born in a state like Iran or Venezuela, why should I be excluded from the financial system as a result? Bitcoin, by its very permission-less nature, cannot exclude any one entity from participating in economic activity on the Bitcoin network. Now, specific companies can and will be regulated on the basis of the jurisdictions in which they operate. But the Bitcoin protocol and the Bitcoin network, itself, are global, decentralised, and permission-less in nature, much like the internet. It functions like a global financial utility. And this provides significant opportunity for more social equity.

For example, recently in Nigeria, the Nigerian Feminist Coalition was able to use Bitcoin to raise funds during the Ends SARS movement, which sought to end police abuse of individuals in Nigeria. Similarly, in other parts of the world, Bitcoin has been used to defend free speech and to preserve the ability for journalists and activists to transact and have privacy. So it's very important to remember that, from a social equity perspective, cryptocurrency is a blockchain technology can go a long way in enabling and facilitating more financial equity in our global financial system.

From a G, or governance perspective, Bitcoin and cryptocurrencies also really shine when compared to the traditional financial system. Bitcoin is really unique from other cryptocurrencies because there is no one central entity that controls Bitcoin. It's important to remember that many blockchain protocols are still highly centralised, from a governance perspective, and have a core group of individuals who are responsible for decision making around what happens in the protocol and what happens to the resources that belong to a protocol, particularly financial resources.

However, from a financial transparency perspective, the benefits of blockchain technology and distributed ledgers that are public in nature is that any and all economic activity on these networks is public domain. So for example, a wallet that is set up to govern community funds can actually be tracked in real-time. It can have a multi-sig, or a multi-signer agreement, where multiple stakeholders have to sign off on use of funds. There could even be a proxy voting mechanism where stakeholders in the protocol participate in governance decisions around what happens in that protocol.

And these are a few examples of why I believe the ESG argument today is incomplete and lacks specificity and nuance. So please remember, when you're presented with commentary around the ESG profile of Bitcoin and other cryptocurrencies, that facts matter more than feelings. And if we look at the facts, I do believe that cryptocurrencies and blockchain technologies are some of the greatest ways to enable more ESG-friendly investment and more ESG-friendly development in our world today.

## 4.5.2 Environmental Challenges

### Environmental Challenges

With the rise in acceptance and usage of the Bitcoin platform, there has been an increasing focus on the environmental effects of the proof-of-work (PoW) protocol. The growing focus is primarily due to

the large amounts of energy required to run mining nodes around the world. Concentrations of these mining pools have been pushed out of China for this main reason, for example.

It is worth noting that the high energy needs of the PoW protocol are part of the Bitcoin platform by design and increase its security. The energy expenses needed to carry out a 51% attack are high enough to make it an uneconomical undertaking. Therefore one can not meaningfully reduce the energy used by the Bitcoin network while maintaining its underlying security.

## Faculty Video: The Environmental Challenges and Costs of Blockchains

In the following video, Professor Bill Roscoe discusses the environmental issues of public and private blockchains, and how PoW systems consume high amounts of energy. Professor Bill Roscoe leads the Blockchain Research Centre at the University College Oxford and has released a number of research papers, such as “Digital Civilisation: Manifesto for a trustworthy, well regulated world” and “The Greening of Blockchain Mining”.



Let's look at some of the problems with blockchain. I think the one probably most people know about is the fact that some blockchains waste energy. There are two main classes of blockchains. There are so-called public blockchains and there are ones who access to whom is controlled by a sort of exclusive membership, at least at the level of who's allowed to control them.

There's no real energy wastage problem with the second of these classes, but at the same time, they lack many of the attractive qualities of the public blockchains. And so people are very attracted to public blockchains because they somehow represent an independent notion of trust developed by wide collaboration and interaction. The trouble is that the first and by far the best known method of creating a public blockchain is via a concept known as proof of work.

Proof of work is a really elegant solution to problems. The trouble is that blockchains and blockchains based upon it became so popular, and the tokens in them became so valuable, that it has caused this absurd amount of energy being wasted in doing them. So just to give you an example, the best known blockchain is called, I think we all know of Bitcoin. And essentially, proof of work means that everybody takes part in a lottery to create the next block and gather their reward, so they gain from creating the next block. So they take part in a lottery by performing a simple calculation, a relatively simple calculation at any rate.

But the absurd quality is, that roughly speaking,  $10^{24}$  such operations, 10 to the 24 lottery tickets in a sense, have to be bought before one will win. And this simply uses an absurd amount of electricity. And at the same time, it actually more or less totally destroys the Democratic ideals of the blockchain, because only people with very specialised machinery and very cheap electricity can afford to do it.

So it's a brilliant idea, which is very strong in many ways in the security front, but which has been disastrous. And I don't think anybody would seriously think that blockchains should take over any important role in society if they carry on wasting energy on anything like that scale.

## 4.5.3 Case Study: Tokensoft Offers the World's First Carbon-Neutral Bitcoin

### Case Study: Tokensoft Offers the World's First Carbon-Neutral Bitcoin

The Tokensoft Protocol has partnered with MOSS.Earth to offer carbon offsets for purchasers of its wrapped bitcoin, eBTC. The process works in the following way (Wrapped, 2021):

eBTC is a wrapped asset created by a ratio of Wrapped Bitcoin on Celo (cBTC) and MOSS.Earth Carbon Credits (MCO2). The ratio for full BTC carbon offsetting is 2 MCO2 per BTC. The MCO2 is equivalent to one Amazon forest conservation project carbon credit, or one ton of certified avoided emission of one ton of CO2. The acquisition and burning (retirement) of 2 MCO2 currently costs **only the equivalent of \$40 per year**.

### Guest Video: Carbon Neutral Bitcoin Token

In the following video, Mason Borda, CEO of Tokensoft, explains the project in further detail.



The energy efficiency of Bitcoin has come under a microscope, especially with Elon Musk's tweets. And so we decided to help launch a carbon-neutral version of Bitcoin. And what that means is users can bring their Bitcoin to our platform. And they can create the carbon-neutral version by inserting their own Bitcoin. And by burning the requisite amount of carbon credits.

And there are sort of two components there. There's the carbon emissions that occurred historically with Bitcoin. And so when users come into the platform, they burn about \$40 in carbon credits to account for that. And then on an annual basis about \$20 in carbon credits is burned to account for the ongoing emissions of securing that Bitcoin.

And so we're set to launch this on Celo, which is also a carbon-neutral blockchain. And this should be available by the end of the month.

### Other Potential Positive Impacts of Blockchain Technology

The World Economic Forum offers other methods where blockchain could have positive impacts as for environmental challenges (Herweijer & Swanborough, 2018):

- **Sustainable finance** through blockchain platforms that offer access to capital from a wider investor group that intends to invest in environmental causes.
- **Supply chains** that offer transparency, immutability, traceability, and other efficiencies that demand less on the environment.
- **Resource management** improvements and sustainability when transitioned to a decentralised system.

- **Disaster preparedness and humanitarian relief** through a shared, permissioned blockchain that provides coordination and trust in services.
- **Monitored sustainability efforts and circular economies** created and incentivised through blockchain-based materials and natural resources management systems

Consider the environmental aspects of your blockchain project:

Exogenous and Endogenous Environmental Challenges	
Exogenous (independent)	Endogenous (able to be controlled)
Are you able to research the blockchain technology you are considering to understand whether it is favourable or unfavourable to the environment?	Are you able to control your overhead requirements to limit environmental impacts?
Are there sufficient energy resources for the size of your project and its demand on energy?	Will your blockchain project result in excess waste or pollution?
Is your project reliant on weather patterns?	Is your project sustainable with a goal to be carbon neutral?
Other exogenous considerations	Other endogenous considerations

#### 4.5.4 Social Challenges

### Social Challenges

In blockchain projects, there are increased pressures to operate in a socially responsible manner. Social considerations for an organisation's construct include:

1. Equity, social justice, and censorship resistance
2. Population served and accessibility
3. Distributed workforce
4. Community reinvestment/philanthropy

These considerations are described below.

#### 1. Equity, Social Justice, and Censorship Resistance

Inclusion and justice have become hallmarks of public blockchain platforms. In addition, blockchains' public and decentralised networks offer another benefit that databases involving intermediaries cannot: censorship resistance. With its public accessibility, anyone, regardless of their persona, can participate. In addition, the immutability and distributed nature of the ledger system provide further levels of censorship resistance.

## Case Study: Solana Labs' Censorship-Resistant Platform

Solana Labs launched its blockchain platform as Loom in early 2018. Renamed Solana, the Proof-of-History protocol provides a timestamp mechanism to create trust between computers. The Solana staking program maximises decentralisation and censorship resistance based on its fast transaction capabilities (Solana, 2021).

### Recent News About Solana:

- [SOL price tumbles as Solana goes through DoS attack](#)
- [Solana Blockchain Network Facing “Intermittent Instability”](#)

### Guest Video: Censorship Resistance

In the following video, Anatoly Yakovenko, CEO of Solana Labs, discusses Solana's censorship-resistant platform.



The interesting thing about smart contract's platforms is this idea of censorship resistance. It's kind of what is the difference between a database and a blockchain. And a lot of functions you can do with a database, but the key difference is censorship resistance.

And to give you an example of what that is when you go through all the hoops to get your computer hooked up to a market at the New York Stock Exchange, they literally give you an ethernet cable that's exactly the same length as everyone else's. And that's to guarantee fair access from your machine to the market, and also for all the other participants to guarantee that no one else can get ahead of them.

And that fair access, that's really what censorship resistance is, is this idea that if we have an open platform that there isn't some way for anybody to trick it or to take advantage of your information ahead of you, if it's truly fair and open.

## 2. Population Served and Accessibility

A blockchain platform can provide access and services to individuals who might otherwise not have financial resources through anonymity and decentralisation.

- Through the Celo protocol, the **Kenyan Microwork** programme demonstrates that a mobile phone is a primary tool used to perform work, get paid, and convert or transfer funds (Alexander, 2021).
- **Bitnation** provides digital identity documentation services to refugees that allow host nations to verify their identities (Allison, 2016).
- The **United Nations World Food Programme** (WFP) supplied Syrian refugees with cryptographically unique food coupons representing an undisclosed number of Jordanian dinars sent to dozens of shops in five refugee camps across the nation (del Castillo, 2017).

## Case Study: Blockchain Empowers Refugees

In addition to the above-referenced use cases, blockchain can assist refugees in the form of funds deposited to a wallet for their use when resettled or if needed to send cross-border payments. Fiat currency in a traditional mobile wallet is typically not accessible and will not suffice in many, if not most, refugee crises. A digital wallet, where all one has to do is remember a 16-word seed phrase, can be pre-loaded by aid organisations and virtually handed off to a refugee, who can then transport the digital currency with them.

### Guest Video: Bitcoin as Private Property

In the following video, Alex Gladstein, Chief Strategy Officer at the Human Rights Foundation, explains this concept in further detail.



Bitcoin is the real private property. Like, anyone can actually, with a handful of words, control their own financial destiny. They can write those words down. They can memorise those words. You can cross the border with a billion dollars in your head or with \$20 in your head.

But the point is, you can then recreate that wallet with a seed phrase when you get to Canada, when you get to Germany, wherever you're going, and then you can spend that Bitcoin and get something else in return for it.

So it allows, yes, people who are fleeing violence, war, repression, to bring their wealth with them when, historically, this was never possible before. Like usually, when refugees leave, it's not like they can bring all their stuff with them, or oh, we'll take a few months to liquidate all of our property into cash and bring it. No, that's not how it works.

And whatever they're carrying usually gets stolen from them. So this idea that you can put your wealth onto your phone, or you can memorise it, or have it on like a small USB key, whatever you prefer to do, or send it abroad.

I mean, from before you leave and go on your harrowing journey, with internet access, you can send that Bitcoin, perhaps to a loved one who's already abroad. I mean, there's just many things that you can do now that weren't possible before. So this is a big, big way that the power balance is changing between individuals and governments.

## 3. Distributed Workforce

Decentralised organisations offer opportunities for work that are often not available in hierarchical firms. A distributed or decentralised workforce is different from a remote workforce in that there is no centralised core. This model offers accessibility to workers and potential efficiencies for the organisation. Out of necessity, the Covid-19 pandemic contributed to an increase in this type of work.

## Case Study: Edge & Node

Edge & Node is a software development company behind the Graph protocol, which utilises a decentralised workforce focused on human coordination. According to the Graph's founder, Yaniv Tal (Kline, 2021):

Instead of growing into a giant corporation like tech companies of the past, we're excited to work closely with many independent crypto teams all over the world and leverage protocols and decentralized technologies to scale across organizational boundaries and work on improving collaboration and redefining the future of work.

## Guest Video: Decentralised Protocol Participation, Part 2

In the following video, Tegan Kline, Co-Founder and Business Lead at Edge & Node, discusses decentralised protocol participation.



With the launch of two protocols, they're both utility tokens where people are purchasing those tokens to use and those networks. Not only are people able to just buy in to be able to hold stake in that protocol, but also to be able to use that ecosystem. And so within the graph, there are many different participants.

And with the blockchain space and these protocols, that revenue no longer needs to go to a centralised company, and it can instead go peer to peer in the ecosystem. And so within the graph, there are delegators, indexers, and curators that can all earn GRT for the work that they're doing for that protocol. And I think that's very powerful.

I come from traditional finance and investment banking. As an analyst, you have to work 100-hour weeks. You are paid the lowest out of anyone within that bank, and you're working the most.

And then you have to work for five years before you can work your way up that totem pole. And I don't think that's how this system should be. I don't think people should have to work hard and not receive compensation commensurate to the value they're bringing.

And I think within the crypto space it's really powerful, because people are compensated based on the value that they're bringing. It brings a lot more opportunity a lot sooner because of this. So within protocols, you no longer have to work for just a centralised company. You can work for many different ideas across the entire ecosystem. For example, you can be a delegator in the graph network, helping to secure that network, helping indexers to have a larger amount stake on different subgraphs, but you could also be a liquidity provider within Uniswap.

There are many different roles that you can take on as opposed to having to work a 9 to 5 just to be able of feed your family. And as Yaniv mentioned, that really brings a lot of opportunity to creatives who have had to put that creative side of themselves on a shelf so that they can make money for themselves and their families. And so I'm really excited about the future of work.

## 4. Community Reinvestment/Philanthropy

There is an increase in nonprofit organisations in the blockchain ecosystem. Many of them have been formed to manage the assets and provide governance for the blockchain protocols themselves. Many blockchain organisations operate with a nonprofit foundation to manage assets and provide governance. Through this process, there are opportunities to give back to the communities that supported the organisations' growth or whose needs align with the platform's needs. Blockchain platforms offer general philanthropic opportunities as well.

### Case Study: The World Bank's Bond-i Issuance

In 2018, the World Bank issued the Kangaroo bond through its new Bond-i platform—its first global blockchain bond using distributed ledger technology. The effort initially raised AUD \$110 million, and through the platform's broader reach, the World Bank was able to raise an additional AUD \$50 million in 2019. The Aaa/AAA bond issued through the International Bank for Reconstruction and Development (IBRD) came in August 2020. Capital raised from the bond issuance was used in accordance with the World Bank's focus to end extreme poverty and promote shared prosperity.

According to the World Bank, the Bond-i initiative is part of a wider strategic focus, which will see the institution harness the potential of disruptive technologies to hopefully develop solutions that benefit its clients. The World Bank established its blockchain innovation lab in 2017 with the intention of using it for global poverty reduction projects; the lab is a hub of innovation and opens the door to developing blockchain use cases in areas such as "land administration, supply chain management, health, education, cross-border payments, and carbon market trading" (The World Bank, 2019).

At the direction of the World Bank, the Central Bank of Australia (CBA) arranged the bond, and the blockchain platform was designed and developed through the CBA Innovation Lab's Blockchain Centre of Excellence in coordination with the World Bank's lab. Microsoft conducted an independent review of the platform's architecture, security, and resilience (The World Bank, 2019).

Consider the social aspects of your blockchain project when completing the following table:

Exogenous and Endogenous Social Challenges	
Exogenous (independent)	Endogenous (able to be controlled)
Does your project reach a socially desirable customer base?	Do your organisation's working conditions show high regard for your employees?
Do your suppliers hold the same values as your organisation?	Does your organisation have a community investment policy?
Are there competitive influences that negatively affect your project?	Are all stakeholders' interests taken into consideration?
Other exogenous considerations	Other endogenous considerations

## 4.5.5 Governance Challenges

### Governance Challenges

An organisation's governance structure may present challenges at certain milestones in a blockchain project's growth cycle. Consideration and a cautious approach to governance decisions in the project planning phase will help avoid or address challenges that may arise. Following is an example of an early challenge involving the Maersk use case we learnt about in Module 2.

### Case Study: Maersk/IBM TradeLens Platform

The IBM/Maersk TradeLens blockchain platform and the signing of two competitors in 2020—Mediterranean Shipping Company S.A. and CMA CGM—represents a private blockchain shared governance framework. That major competitors joined forces to power a blockchain solution to benefit them all was a major business achievement.

Maersk and IBM were hopeful that this partnership with Maersk competitors would form in early 2018. However, there was strong pushback from would-be partners, and the only one to sign on at that time was Pacific International Lines, a mid-level carrier. The TradeLens project's value proposition depended on other large carriers joining and running full blockchain nodes on the network, since large shippers utilise the wider network for their cargo shipments.

Maersk had signed over 100 other partners outside the carrier lines, including port authorities, freight forwarding and logistics companies, and customs authorities. However, other potential carrier partners were concerned about joining the project and not being on equal footing in the governance framework. Maersk and IBM would own the IP rights to the project, and that point created a hurdle that took two years to overcome. There was some discussion about forming an industry advisory board to create neutrality, and TradeLens promoted the project as a collaboration effort. However, IP rights were seemingly the main obstacle to more partnerships initially (Allison, 2018).

In the two years between its initial launch in 2018 and the CMA CGM and Mediterranean Shipping Company S.A. signings in 2020, TradeLens tracked 30 million container shipments, approximately 8% of worldwide shipping volume (Wolfson, 2020). With this new partnership, TradeLens now tracks nearly 50% of the world's ocean container cargo, representing over 11 million of the 25 million total 20-foot equivalent units (TEUs) shipped annually (Statista Research Department, 2021).

Consider governance challenges in your blockchain project when considering the following table:

Exogenous and Endogenous Governance Challenges	
Exogenous (independent)	Endogenous (able to be controlled)
Do regulatory controls influence your organisation's governance?	Does your leadership team or board reflect a diverse and representative group?
Are there competitive influences that negatively affect your governance procedures?	Is your compliance function well-established and forward-looking?
Does your physical location impact your ability to incorporate good governance practices?	Are stakeholders given opportunities to engage with leadership?
Other exogenous considerations	Other endogenous considerations

## 4.5.6 Addressing ESG Concerns

### Addressing ESG Concerns

Identifying ESG challenges is a significant step in the development of a blockchain project. Addressing those challenges and establishing a plan to implement an ESG policy are important next steps in this process. Developers do not need to address every possible challenge right away. However, the acknowledgement of each is an essential component of a long-term sustainable ESG strategy—a healthy addition to an overall organisational business strategy.

Organisations can take several steps to implement an ESG policy. Many major accounting and ESG specialist firms or organisations provide guides and services to help with the process. These include software programs, training, and outsourced services. The steps to implement a policy include the following:

1. Identify and outline the organisation's position on ESG and consider developing a specific mission statement for it.
2. Determine a set of published standards by an accredited body to guide the process—one that is appropriate for the organisation. For example:
  - GSSB - Global Sustainability Standards Board
  - SASB - Sustainability Accounting Standards Board
  - TCFD - Task Force on Climate-Related Financial Disclosures
  - WEF - World Economic Forum
3. Formulate the ESG policy.
  - Include dedicated personnel to oversee the ESG programme.
  - Establish metrics that companies can routinely measure.
4. Revisit and update the ESG programme regularly.

## Guest Video: Bitcoin's Positive Global Impact

In the following video, Alex Gladstein offers his perspective on bitcoin's humanitarian relief benefits.



I guess I would draw a distinction between two kinds of digital currencies that will have dramatic implications for human rights. One would be Bitcoin, and the other one would be central bank digital currencies. I believe that Bitcoin has tremendous positive implications for civil liberties and human rights worldwide and that reality is already unfolding for many, many people and that central bank digital currencies, which are being born today and will be implemented and rolled out over the coming decade, most likely, will have tremendous negative implications for civil liberties and human rights. So it really depends on the way you built these systems.

Bitcoin is decentralised. It has no single point of failure, no single point of control. It is something that the users control, not corporations or governments. And it gives people the ability to check the power of the authorities that tend to control them.

Central bank digital currencies, on the other hand, are a means of magnifying state control and magnifying the way that authorities can kind of micromanage the population, can force spending, do negative interest rates, confiscate money, blacklist people they don't like.

So as we kind of go deeper into the coming decade, there will be a lot of thought and debate, and research put into these two potential paths. And what I'd like to do is draw the human rights community's attention to Bitcoin and what it can do and what it is doing around the world.

It is basically creating this parallel economy. We have the existing fiat system. We have the banking system. We have this corporate fintech system. And by extension, we're going to have the central bank digital currencies. That's like one path we're going to go down.

But this gives us this parallel track where we can now, in a peer-to-peer way, send, store, receive, donate, earn, spend in a way that is entirely unencumbered by that state corporate apparatus. This is very, very important, especially for people who live under dictatorships and authoritarian regimes.

About 4.3 billion people live under very oppressive governments around the world, not just in China but elsewhere, including Saudi Arabia, Russia, Cuba, Venezuela, Ethiopia—I could go on. The point is that people in these places don't have the same financial privilege that we may have in London or in Tokyo or New York.

Not only is their currency usually poor at being a currency, it usually loses value pretty quickly over time versus things like the dollar or the euro or real estate. They see tremendous devaluation in their time and energy. Put into a store of value, it doesn't do a very good job at being that way to save.

But perhaps even more insidious is the way that that system is controlled. So people in authoritarian countries often get their bank accounts frozen. They don't really have property rights or free expression. And just tremendous swaths of these societies also are just generally unconnected to the outside world.

So you have a situation today where, for billions of people, money is broken. And it's only going to get worse, unfortunately, for many, especially when it comes to control, surveillance, and just social engineering. But with Bitcoin, we have a way out.

## 4.5.7 Key Takeaways, References, and Further Exploration

### Key Takeaways

Let's review the key points of this section:

1. Cryptocurrency mining and the PoW protocol require a lot of energy and can have a negative environmental impact. However, the energy needs of the PoW protocol are an essential part of the network's security.
2. Cryptocurrency projects are under pressure to be socially minded, with a focus on equity and social justice, communities serviced, accessibility, supporting a distributed workforce, and reinvesting into the community.
3. The following questions can help in analysing ESG challenges.
  - Are there more benefits to using a PoW protocol that would outweigh or offset environmental concerns?
  - Do any protocols contribute favourably to the environment?
  - Which blockchain protocols have the most positive social responsibility levels?
  - What societal pressures are building at this time that may affect blockchain technology in the future?
  - What role does good governance play in starting an organisation or implementing a new blockchain strategy?

### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 19 April, 2022.

#### 4.5.1 Overview

Bitcoin Mining Council. (2021). Bitcoin Mining Council (BMC): FAQs. *Bitcoin Mining Council*. <https://bitcoinminingcouncil.com>

#### **4.5.2 Environmental Challenges**

Carbon Offsets Guide. (2019, 12 November). How to Acquire Carbon Offset Credits. *Carbon Offsets Guide*. <https://www.offsetguide.org/understanding-carbon-offsets/how-to-acquire-carbon-offset-credits>

Herweijer, C., & Swanborough, J. (2018, 19 September). 8 ways blockchain can be an environmental game-changer. <https://www.weforum.org/agenda/2018/09/8-ways-blockchain-can-be-an-environmental-game-changer>

Wrapped. (2021). eBTC. *Wrapped*. <https://ecowrapped.com>

#### **4.5.4 Social Challenges**

Alexander, L. (2021, 10 February). New FinX Pilot in Kenya: Digital Microwork and Celo Payments - Part 1. *Medium - FinX*. <https://medium.com/finx-vc/new-finx-pilot-in-kenya-digital-microwork-and-celo-payments-part-1-51f5b200bc44>

Allison, I. (2016, 29 September). Decentralised government project Bitnation offers refugees blockchain IDs and bitcoin debit cards. *International Business Times*. <https://www.ibtimes.co.uk/decentralised-government-project-bitnation-offers-refugees-blockchain-ids-bitcoin-debit-cards-1526547>

del Castillo, M. (2017, 13 June). United Nations Sends Aid to 10,000 Syrian Refugees Using Ethereum Blockchain. *CoinDesk*. <https://www.coindesk.com/markets/2017/06/13/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain>

Kline, T. (2021). Introducing Edge & Node: Unveiling Edge & Node following successful Mainnet launch of The Graph. <https://edgeandnode.com/blog/introducing-edge-and-node>

Solana. (2021). Documentation. <https://docs.solana.com>

The World Bank. (2019, 16 August). World Bank Issues Second Tranche of Blockchain Bond Via Bond-i. <https://www.worldbank.org/en/news/press-release/2019/08/16/world-bank-issues-second-tranche-of-blockchain-bond-via-bond-i>

#### **4.5.5 Governance Challenges**

Allison, I. (2018, 26 October). IBM and Maersk Struggle to Sign Partners to Shipping Blockchain. *CoinDesk*. <https://www.coindesk.com/markets/2018/10/26/ibm-and-maersk-struggle-to-sign-partners-to-shipping-blockchain>

Statista Research Department. (2021, 23 September). Container shipping - statistics & facts. <https://www.statista.com/topics/1367/container-shipping>

Wolfson, R. (2020, 15 October). Global shipping leaders join IBM and Maersk blockchain platform. *CoinTelegraph*. <https://cointelegraph.com/news/global-shipping-leaders-join-ibm-and-maersk-blockchain-platform>

## **Further Exploration**

[World Economic Forum - Building Blockchains for a Better Planet](#)

[Blockchain Research Centre's Research Papers](#)

# 4.6 Organisational Considerations

## 4.6.1 Overview of Organisational Considerations

### Overview

This section will explore organisational considerations as you move forward in planning and implementing your blockchain strategy. We will compare the blockchain platform with traditional platforms and explore unique strategies for utilising the more novel approach of a blockchain platform. We will also review a spectrum of organisational structures and the inherent challenges blockchain projects present.

### Vocabulary Check

This section introduces the following terms.

- [flatarchy](#)
- [holacracy](#)

## 4.6.2 Organisational Structures and *The Nature of the Firm*

### Organisational Structures and *The Nature of the Firm*

As Ronald Coase hypothesised in his work, *The Nature of the Firm*, firms came to exist as an economically preferred structure from which to conduct transactions—that individual transactions of any sort are more feasible when within a hierarchical structure with a central authority. The firm removes much of the negotiating process and its resulting cost that would otherwise exist in the individual price mechanism.

With existing case law supporting its various structures, the firm as a legal entity can serve as a basis of understanding when forming a blockchain project's organisational structure.

### Spectrum of Organisations

Organisational structures exist on a spectrum with the traditional, hierarchical model on one end and the decentralised, flat model on the other. Characteristics of these two models are as follows:

- **Traditional/hierarchical**
  - Vertical, top-down management structure

- Employment contracts
- Salaries
- Individual reputation typically derived from quality and continuity of contributions to the codebase
- **Decentralised**
  - Flat structure
  - No employment contracts—only communities with different types of stakeholders
  - Incentive is contributing to a network and its aggregate value
  - Individual reputation typically derived from quality and continuity of contributions to the codebase

Other types of organisations blend some of the characteristics of the two extreme models as follows (Morgan, 2015):

- **Flatter traditional:** A traditional hierarchical structure with some layers removed and wider contributions to the decision-making process.
- **Flatarchy:** A traditional hierarchical structure, but with separate departments of innovation that need autonomy over decision-making and processes.
- **Holacracy:** An organisation in which individuals and teams have control over processes.

## Case Studies: Two Firms That Have Successfully Decentralised (Somewhat)

### Johnson & Johnson

In a traditional organisational structure, the leadership team must decide and plan a restructuring of the company to a more decentralised one. Johnson & Johnson, with more than 200 business lines and over 100,000 employees, made the decision to do that.

In a 2008 interview at the Wharton Leadership Conference, William Weldon, the former Johnson & Johnson chairman and CEO, spoke about the firm's decision to operate as a decentralised organisation. To summarise, Weldon explained that there are pros and cons to the structure—a local management team of an individual company has more understanding of how the company could and should operate there in terms of consumer behaviour, local governments, and workforce. While this gives the corporate leadership team less control over the company, the benefits come through strong local leadership and a net profitable company (Knowledge@Wharton, 2008).

Johnson & Johnson fits in the flatter traditional model structure. The company still retains a hierarchical structure, but has moved its business lines into flatter, more decentralised organisations.

### Illinois Tool Works Inc.

Illinois Tool Works (ITW, Inc.) has been in business since 1912 and is universally recognised as a successful decentralised, entrepreneurial company. The company encourages seven divisions that operate separately to think and act like smaller companies—a move that establishes a nimble approach to customers' needs. Since the mid-1980s, the company has been utilising the 80/20 business process, meaning that all of the company's business units focus on the 20% of the customers that generate 80% of the profits. This system is most effective due to its decentralised structure (Sheedy, 2015).

Like Johnson & Johnson, ITW, Inc. fits in the flatter traditional model structure.

### 4.6.3 The Blockchain Platform's Advantages Over the Traditional Platform

#### The Blockchain Platform's Advantages Over the Traditional Platform

In Module 1, we learnt about the Bitcoin and Ethereum platforms and the concept of platforms, in general. A platform's holistic business model creates value by handling consumer-to-business or business-to-business transactions in a digital environment. In addition, a platform's structure allows for a wide, cross-border and decentralised audience.

According to an article on platform strategy for MIT's Sloan School of Management, platform development for most business models is a strategy that companies should move toward as soon as possible. Organisations should not fear the competition of existing platform giants, such as Apple or Google. Instead, they should rely on their own industry domain expertise, strong customer relationships, and desire to collaborate with their partners. Platform strategies will ideally harness the power of artificial intelligence, data analytics, and other leading technologies (Stackpole, 2021).

Blockchain applications are always platforms because, by definition, they broker transactions between parties. Traditional digital platforms, such as Google and Amazon, create and maintain an ecosystem within which multiple parties interact and transactions are fostered. Blockchain platforms are based on distributed ledger technologies that invite participants including suppliers, buyers, miners, app providers, and exchanges to carry out various transactions.

Blockchain platforms bring some advantages to an organisational structure that traditional organisations do not. The following are examples of applications comparing a blockchain platform with a traditional organisation:

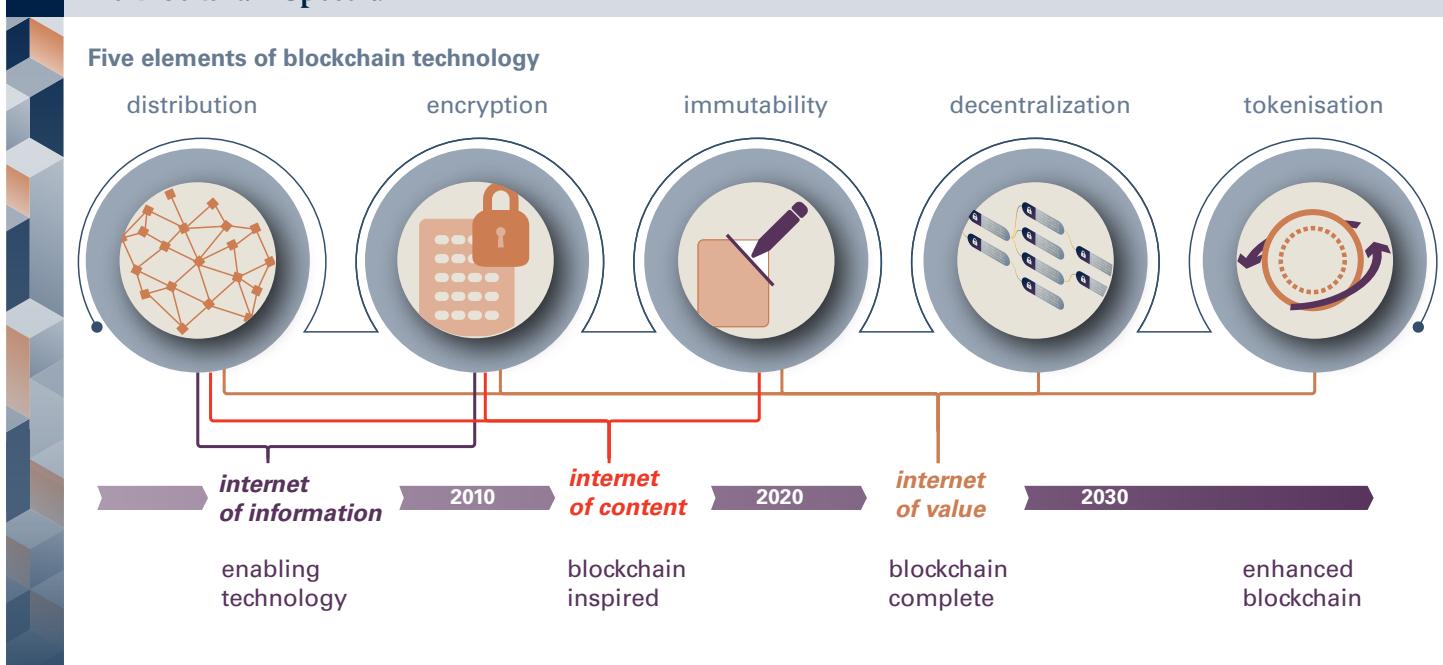
	<b>Traditional</b>	<b>Example</b>	<b>Blockchain</b>	<b>Example</b>
Transparency	Transparency is limited to public reporting requirements or published material.	Holding a public company annual shareholder meeting.	Transparency is inherent in distributed ledger technology.	DAO issues native tokens for users to participate in governance.
Trust	Multi-organisational trust is difficult due to frictions like data validation and differing goals.	A supply chain involves several organisations and is reliant on each organisation sharing timely and valid data.	Validated, transparent distributed ledger promotes trustful multi-organisation collaboration.	A supply chain across multiple organisations has the exact same access to blockchain data.
Identity	Identity validation is usually manual or reliant on a third party.	Processing a bank loan application.	Identity is validated through digital identity methods such as reputation score or decentralised identifier (DID).	The customer presents a QR code to verify ID online to rent a car.
Data/file storage	Cloud, local, or third-party options.	Storing sensitive customer files in a data vault.	Data/file storage has immutable and everlasting potential on a blockchain.	Storing sensitive customer files on the blockchain with cryptography.

Blockchain platforms do bring some potential disadvantages that potential users need to consider. Their design may be too complex for a particular application, for example. In addition, the immutable nature of blockchain transactions may be too rigid for specific applications.

## Case Study: The Global Blockchain Spectrum

Gartner, Inc., a global business consulting strategist, developed the Global Blockchain Spectrum in 2019. An understanding of the spectrum may aid in the development of a blockchain platform and its corresponding organisational structure. It offers a perspective of blockchain technology's near-term future and is based on five elements. The spectrum consists of four archetypes that are currently in development and presented in a timeline as follows:

## The Blockchain Spectrum



The archetypes within the spectrum consist of foundational building blocks upon which developers can build future blockchain solutions. The building blocks are (Panetta, 2019):

### Blockchain-Enabling

Encryption and distribution technologies work together to create the base for building future blockchain solutions. Peer-to-peer networking, messaging, distributed computing, and cryptography make up the initial building blocks of the spectrum.

### Blockchain-Inspired

This archetype adds immutability to the blockchain-enabling distribution and encryption technologies. As denoted by its name, the archetype does not have the decentralisation and tokenisation processes that are central to blockchain applications. Instead, the projects focus on reconfiguring existing processes for improved efficiencies and best practices. They are, therefore, limited in scope, although they do provide a framework for developing future blockchain-complete projects. Gartner states that this archetype will dominate enterprise implementations through the early 2020s.

### Blockchain-Complete

Blockchain-complete solutions will emerge around the year 2023, according to Gartner. Decentralisation and tokenisation will round out the five elements of the blockchain foundation, and enterprise-ready projects will deploy smart contracts to tokenise digital or physical assets. This archetype represents the total value proposition of blockchain technologies.

## **Blockchain-Enhanced**

Approximately two or three years after blockchain-complete technology solutions are launched and active in enterprise business cycles, enhancements to these projects will emerge, including the Internet of Things (IoT) and artificial intelligence (AI). IoT may offer mobile blockchain solutions with seamless hand-offs between devices, while AI will likely improve user experiences and other blockchain interactions. Notably, Gartner projects the evolution of decentralised self-sovereign identity (SSI) in this phase, which will allow people to own, control, and share their digital identities, typically through a digital wallet.

This Gartner case study presents a technological viewpoint of the blockchain ecosystem's development cycle. There will likely be variations to the model shown here.

### **4.6.4 Other Organisational Challenges**

#### **Other Organisational Challenges**

In addition to platform structure, the following are other primary areas of consideration when developing a blockchain project:

##### **Adherence to Laws and Regulations**

What laws and regulations affect the project in its current state, and what could affect the project in the future when more regulations may be in place that will affect how it operates? Consider the following legal areas that could impact your project:

- Public law
- Private law
- Criminal law
- Financial and regulatory law
- Trade and industry-specific law

##### **Data Protection**

Earlier in this module, we learnt about certain governments' data privacy efforts to protect their citizens from exposure. Consider the following questions and add your own to this high-profile area of the ecosystem:

- Does the data on the blockchain network need protecting?
- Who controls the blockchain network where the data resides?

- How does the network ensure stored data complies with national and global regulations?
- What data truly needs to be stored on the blockchain?
- Can privacy technology such as zero-knowledge proofs be utilised for data protection?

## Human Resources

How does the structure and governance model of a blockchain platform affect the following human resource components?

- Organisation structure
- Culture
- Talent acquisition
- Scaling
- Diversity and inclusion

## Guest Video: Emerging Technologies in Emerging Markets for Organisational Training

In the following video, Morgan Mercer, Founder and CEO of Vantage Point, discusses the opportunity to use emerging technologies in a training programme.



We actually deploy worldwide. And we're doing a deployment right now with a global company based out of Europe, Americas, Asia, etc. And we run into so many quote-unquote problems around, well we can't use certain headsets in certain markets because we can't use Facebook in Asia. And certain areas within Asia, we can't use certain things that we would normally do within the Americas because we're constrained by GDPR. And depending on the company, there's GDPR plus, plus.

And so one thing that I think about is even within the confines of what we're doing with virtual reality or with anything where—one of the benefits of VR is that you have such access to understanding around behaviours. And that's truly the power of the technology where in the future, we'll be able to literally write algorithms where we can predict behaviours and create training programmes that adapt real-time. And that's the future.

And so with that, it means that you also have a very high level of access to user information around their behaviours, their awareness, their knowledge, etc. And a lot of the questions that we get from companies are, well how do you protect users? And I tend to be—I'm very user friendly.

And a lot of companies aren't that way. We see a lot of companies that don't actually own up or take accountability to the level of data and information that they have around people and the ways that they use it. And so I

always say, we will never highlight or pinpoint the one person in your organisation because our goal is to actually use the training programme to bring them closer to being a more self-aware or empathetic individual.

With blockchain, the data and information that we collect, or any company collects, any VR training company collects, can actually be owned by the end user versus being owned by a company. And that is incredibly powerful in and of itself.

So I think that any time you work within an emerging market, that's why I'm so passionate about all emerging technologies, there's always this question of, is it more dangerous or is it powerful? And it really depends on the way that you use it, and who's creating with it.

## Timescale Considerations

Timescale considerations are important factors in organising a blockchain project. Module 5 will explore the project's research, design, and implementation in more detail but this section will present a high-level view of a project's timeline as part of the overall organisational considerations.

In its second Global Enterprise Blockchain Benchmarking Study, the Cambridge Center for Alternative Finance analysed 67 live enterprise blockchain networks and reported that most blockchain projects progress through four stages to achieve full production status. The study noted that two-thirds of projects' timelines were consumed by the Proof of Concept (PoC) to In Production stages. Following are the four stages cited by the study (Rauch et al., 2019):

- **Initial Exploration.** This stage involves research and the exploration of blockchain protocols that will be appropriate for the project.
- **Proof-of-Concept (PoC).** Design strategy and feasibility testing are integral in this stage.
- **Pilot/Trial.** This stage involves the project's deployment and monitoring in a production-simulated environment.
- **In Production.** This stage marks the full deployment of the project and extends into a refinement and scaling phase.

In addition to the project's timeline, the post-project analysis will add an important review process to the project's future or the other projects undertaken.

## 4.6.5 Key Takeaways, References, and Further Exploration

### Key Takeaways

Let's review the key points of this section:

1. Organisation models exist on a spectrum, with flat hierarchies on one end and vertical on the other. Each has its advantages and disadvantages depending on the overall strategy and purpose of the organisation. Blockchain organisations lend themselves to a more flat and decentralised structure, with communities of stakeholders cooperating together to maintain or build the network's value and their own reputations.
2. A platform is a business model that creates value by connecting consumers and producers, orchestrating the supply and demand of particular goods and services, and making transactions less expensive and more efficient. Blockchain works well on top of platforms, which connect a large number of decentralised suppliers and consumers.
3. The archetypes on which developers build new blockchain projects are blockchain-enabling, blockchain-inspired, blockchain-complete, and blockchain-enhanced.
4. In addition to technological innovation, blockchain projects need to consider laws and regulations, data protection, and their unique human resource needs.

### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 19 April, 2022.

#### 4.6.2 Organisational Structures and *The Nature of the Firm*

Morgan, J. (2015, July 23). The Complete Guide To The 5 Types Of Organizational Structures For The Future Of Work. *Medium*. <https://medium.com/jacob-morgan/the-complete-guide-to-the-5-types-of-organizational-structures-for-the-future-of-work-ae9b646a8aaf>

Knowledge@Wharton. (2008, June 25). Johnson & Johnson CEO William Weldon: Leadership in a Decentralized Company. *Knowledge@Wharton Podcast*. The Wharton School. <https://knowledge.wharton.upenn.edu/article/johnson-johnson-ceo-william-weldon-leadership-in-a-decentralized-company>

Sheedy, J. (2015, December 9). Illinois Tool Works: Extreme Decentralization. *Harvard Business School's Technology and Operations Management*. <https://digital.hbs.edu/platform-rctom/submission/illinois-tool-works-extreme-decentralization>

### **4.6.3 The Blockchain Platform's Advantages Over the Traditional Platform**

Panetta, K. (2019, 14 October). The 4 Phases of the Gartner Blockchain Spectrum. *Gartner*. <https://www.gartner.com/smarterwithgartner/the-4-phases-of-the-gartner-blockchain-spectrum>

Stackpole, B. (2021, 4 August). Considering a platform strategy? The time to move is now. *MIT Sloan School of Management*. <https://mitsloan.mit.edu/ideas-made-to-matter/considering-a-platform-strategy-time-to-move-now>

### **4.6.4 Other Organisational Challenges**

Rauchs, M., Blandin, A., Bear, K., & McKeon, S. (2019). 2nd Global Enterprise Blockchain Benchmarking Study. *Cambridge Centre for Alternative Finance*. <https://www.crowdfundinsider.com/wp-content/uploads/2019/09/2019-ccaf-second-global-enterprise-blockchain-report.pdf>

## **Further Exploration**

[One Trust - Creating an ESG Strategy: 4 Challenges & How to Address Them](#)

# 4.7 Challenges Framework

## 4.7.1 Overview of Challenges Framework

### Overview of the Challenges Framework

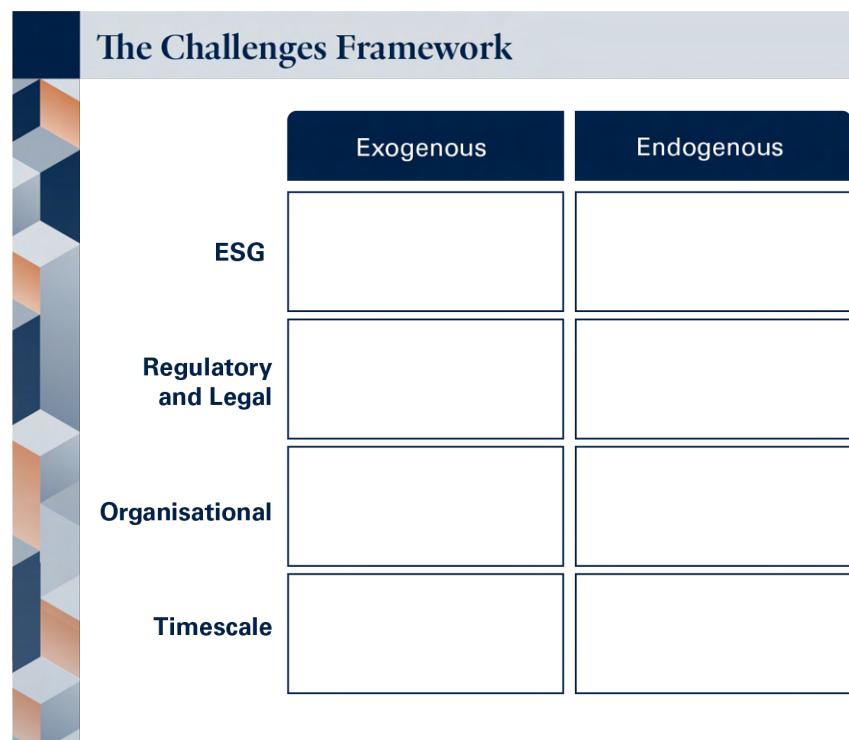
As you consider your blockchain project and its suitability as a business use case, take the time to explore the legal, regulatory, ESG, and organisational challenges, which are essential factors to consider during any stage of your project's life cycle. The following framework will guide you through identifying and managing these potential challenges.

There are a number of important considerations that make up this framework. They are:

- Endogenous and exogenous variables
- Regulatory, legal, and ESG challenges
- Organisational considerations
- Timescale considerations

Let's explore these further.

This framework can be used for blockchain projects after you complete this programme too and will help you complete your Capstone project.



## 4.7.2 Endogenous and Exogenous Variables

### Endogenous and Exogenous Variables

Understanding and working with endogenous (internal) and exogenous (external) variables will play a key role in your blockchain project's development and outcome. To summarise, exogenous factors represent external variables independent of the project, and endogenous factors represent internal variables within the organisation that directly affect the project and any interactions with it. For each challenge, determine the endogenous and exogenous factors that are influential variables or that could be influential variables after the project's launch.

- **Endogenous** can be manipulated and controlled. What variables are we able to influence?
- **Exogenous** cannot be manipulated or controlled/are not affected by other variables. What variables are out of our control?

For a successful project outcome, proactively manage the endogenous variables while lowering your dependency on the exogenous variables. You control the project.

## 4.7.3 Regulatory, Legal, and ESG Challenges

### Regulatory, Legal, and ESG Challenges

To navigate the process of structuring your project so that it becomes a sound yet nimble enough operation to withstand the pressures of an evolving industry, consider the following questions about the regulatory, legal, and ESG components of your organisation:

#### 1. Are regulations in place to guide the development and deployment of our blockchain use case?

Any new business use case deserves the underlying strength of regulatory guidelines. This could be especially challenging when implementing a blockchain strategy, as we have learnt about voids in certain areas of blockchain regulations. Practice due diligence when structuring your blockchain business to gain a firm understanding of what the regulations are—locally, regionally, and nationally.

#### 2. Does the legal framework exist for our blockchain use case? If not, how do we structure our concept to withstand legal pressures?

Give careful thought to its legal framework when structuring the project. The blockchain industry has seen very few legal challenges. As a result, there is a low level of case law that would establish a strong legal framework.

As part of legal considerations, ask: How can I position this project to adjust and remain legally compliant to any new regulations that my government enacts?

### **3. Will my blockchain business positively or negatively impact ESG factors?**

As we have seen, proof-of-work (PoW) protocols may have consequential environmental impacts. Bitcoin mining operations, for example, create a more significant demand on the earth's energy resources than other protocols. As public attention becomes more focused on these issues, it becomes increasingly important for you to research and deploy the ideal blockchain protocol for your business. In this process, consider the following:

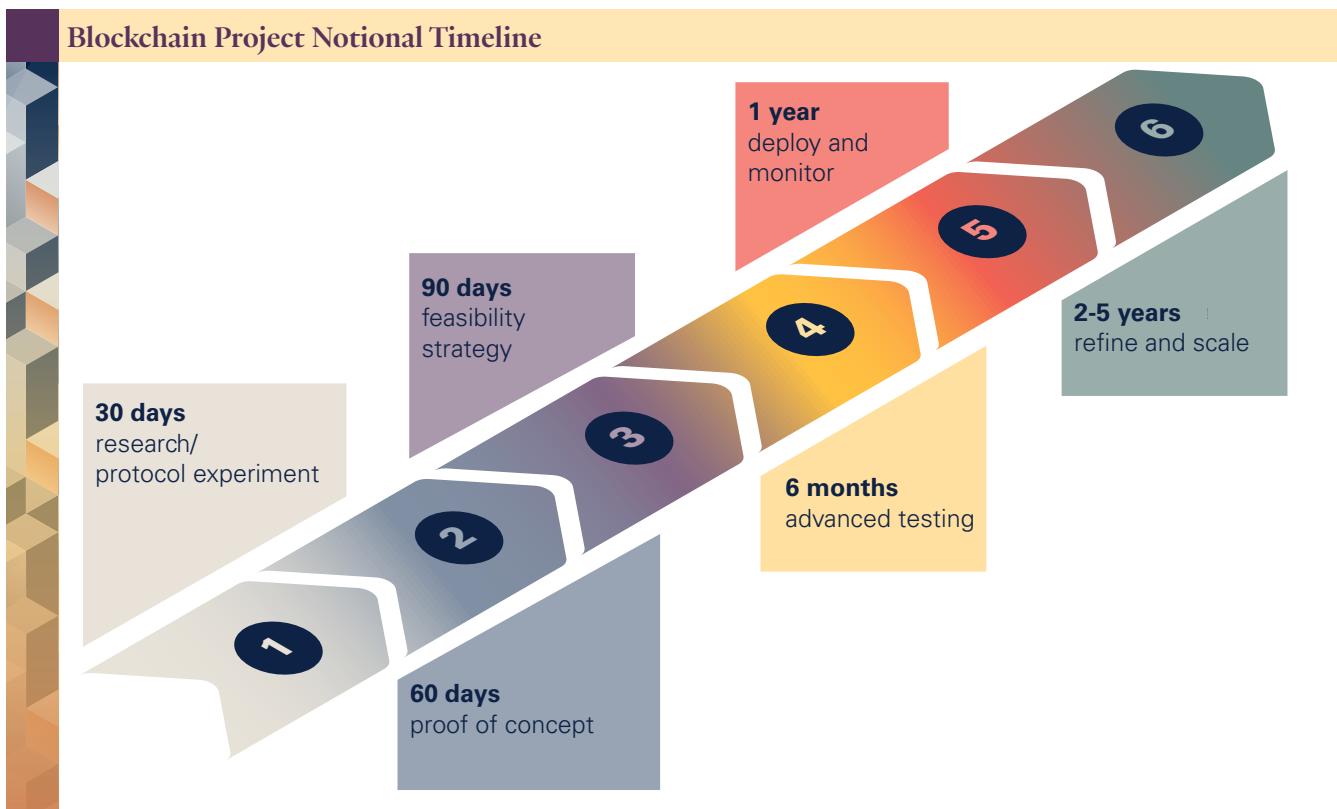
- Environmental
  - Should you purchase carbon offsets for balancing your blockchain's energy usage?
  - Should you employ alternative energy sources that are sustainable for the environment?
- Social
  - Is your project inclusive and accessible to a wide population, or does it exclude certain populations?
  - Does the project make use of a distributed workforce that provides equitable payment for contributions?
- Governance
  - What type of governance structure best suits your organisation?
  - Do regulatory controls influence your organisation's governance?

While your blockchain project does not need to address every regulatory, legal, or ESG challenge, it is good practice to have these considerations in the project's plan. As blockchain continues to evolve, becoming familiar with these concepts will serve a project well in the longer term.

#### **4.7.4 Timescale Considerations**

##### **Timescale Considerations**

Implementing your blockchain strategy should account for timescale considerations as your project develops. Use the following basic timeline to outline the steps needed for each stage of the project.



Note that this exercise is only an example of a potential timeline for your project. The timeline is designed to generate some thought processes for the different stages of a project's implementation.

#### 4.7.5 Key Takeaways

##### Key Takeaways

In this Challenges Framework, you should have developed an understanding of the following:

1. The distinction between endogenous and exogenous variables as they relate to the legal, regulatory, and ESG challenges of your blockchain project.
2. Laws and regulations that will affect your blockchain project.
  - What laws and regulations exist currently?
  - What do I need to pay attention to in legislative and regulatory agencies?
3. ESG issues that relate to your blockchain project.
  - Does my project positively address specific ESG issues?
  - Do certain ESG issues impact my project?
4. Timescale considerations for your project.

# 4.8 Case Study - BitMEX and Know Your Customer, Anti-Money Laundering

## 4.8.1 Overview of BitMEX

### Overview of BitMEX

As we have learnt in Module 4, physical borders do not constrain blockchain regulatory and legal issues. The blockchain ecosystem has an international reach, and it is incumbent on a blockchain organisation to operate lawfully in the countries where it conducts business. Although policymakers are still defining blockchain-specific regulations, organisations must follow existing regulations and laws. In the case study that follows, we will explore the legal issues faced by the founders of BitMEX, a leveraged Bitcoin trading platform.

### Vocabulary Check

This section introduces the following terms.

- [commodity](#)
- [derivative](#)
- [exchange-traded fund \(ETF\)](#)

### Case Study: BitMEX and Know Your Customer, Anti-Money Laundering

The Bitcoin Mercantile Exchange (BitMEX) began in 2014 with a concept conceived by one of its co-founders, Arthur Hayes. As a young investment banker with a degree from the Wharton School of Business and a background in exchange-traded funds (ETFs), Hayes understood market-making—facilitating the execution of buy and sell trades in the financial markets.

Hayes had become a bitcoin investor several years before Citibank let him go in 2013. In October 2013, the Tokyo-based Mt.Gox Bitcoin exchange on which Hayes conducted his trades was allegedly hacked, and investors found themselves struggling to convert their funds to fiat currency. Hayes successfully withdrew his funds and came to the realisation that exchanges in the Bitcoin environment offered a single point of failure.

After trying out some manual exchanges with the yuan in China and witnessing hacks on other exchanges, Arthur Hayes saw the need for an online exchange that facilitated derivatives contracts. A derivative is a financial contract whose value depends on an underlying asset—bitcoin in this case. The online exchange would enable investors to trade on the future price of bitcoin, whether the price would increase (long) or decrease (short).

Partnering with Ben Delo (COO), an Oxford-educated British mathematician and programmer, and Sam Reed (CTO), a young American and enterprising early bitcoin miner, Arthur Hayes (CEO) co-founded BitMEX—a peer-to-peer platform for trading leveraged bitcoin contracts. The exchange is domiciled in the Republic of Seychelles, located in the western Indian Ocean.

The founding members managed BitMEX through its infancy with painfully low trading volume. However, in late 2015, they restructured the exchange to enable users to leverage their trades at a ratio of 100:1. A user could put up US \$10,000 and execute a trade for US \$1,000,000, for example. By 2018, billions were traded on BitMEX, and it was deemed the largest trading platform by volume. However, this astounding leverage ratio alarmed regulators in the US, who had a keen memory of the 2008 global financial crisis that resulted from over-leveraged mortgage loans.

The trading terms on BitMEX are unambiguous, and the platform expects investors to approach their margin trades with a “buyer beware” mentality. The trustless environment in which bitcoin and other cryptocurrencies operate requires an increased level of personal responsibility. Yet, many sceptics and supporters considered the BitMEX model to be more gambling than investing. One such supporter, Jehan Chu, a programmer affiliated with Sotheby’s auction house, compared BitMEX to the NASDAQ—“if the NASDAQ was located in Las Vegas” (Ciralsky, 2021).

The lack of Know Your Customer (KYC) requirements attracted investors to BitMEX. They were not required to provide proof of identity and could, therefore, anonymously execute trades. Subsequently, there were few, if any, anti-money laundering (AML) controls in place.

KYC procedures work to safeguard financial organisations from criminal exposure through illicit money transactions. As part of the US Bank Secrecy Act, the Federal Reserve requires its member financial institutions to implement a KYC policy to remain in compliance with regulatory and sound banking practices. These policies have more detailed requirements to verify a customer’s identity and their intended business activities.

In the US, the government strengthened AML and counter-terrorist financing (CTF) controls after the 11 September 2001 terrorist attacks. FINRA requires its member broker-dealers to implement a written AML program that complies with the Bank Secrecy Act. Knowing the platform omitted these two controls, BitMEX excluded American customers from using the exchange by blocking US IP addresses. Eager American investors easily avoided this block, however, by disguising their locations through the use of virtual private networks (VPNs), which establish an encrypted private network over an otherwise public network.

By mid-2019, BitMEX was processing over US \$10 billion daily. The volume and meteoric rise of this young company brought attention that would highlight the perceived darker side of the exchange, including:

- Foregoing regulations and creating a “house rules” investor environment
- Perceived arrogance and disdain for authority
- Creating BitMEX as an offshore exchange in the Seychelles, which has no regulations

- Perceptions of front-running (trading on advanced knowledge, sometimes known as insider trading) their clients and deriving half of their profits from liquidations, creating an unhealthy (and illegal) incentive

On 1 October 2020, the US Commodities Futures Trading Commission (CFTC) filed charges against Arthur Hayes, Ben Delo, and Sam Reed in addition to BitMEX's various holding companies. With those charges, the CFTC issued the following statement:

The complaint charges BitMEX with operating a facility for the trading or processing of swaps without having CFTC approval as a designated contract market or swap execution facility, and operating as a futures commission merchant by soliciting orders for and accepting bitcoin to margin digital asset derivatives transactions, and by acting as a counterparty to leveraged retail commodity transactions. The complaint further charges BitMEX with violating CFTC rules by failing to implement know-your-customer procedures, a customer information program, and anti-money laundering procedures.

On 1 October 2020, the US Department of Justice (DOJ) filed criminal charges against the three men and Gregory Dwyer, the BitMEX head of business development. All participants were charged with violating the Bank Secrecy Act by evading US anti-money laundering requirements (McSweeney, 2020).

**Sam Reed** was arrested on 1 October 2020 in Massachusetts. He was released on a US \$5 million bond.

**Ben Delo** flew from the United Kingdom to New York on 15 March 2021 for arraignment. He was released on a US \$20 million bond and permitted to return to the UK.

**Arthur Hayes** continued to elude law enforcement, but he agreed to fly to Hawaii on 6 April 2021 for his arraignment. He was released on a US \$10 million bond.

All three parties have pleaded not guilty to violating the Bank Secrecy Act and conspiring to violate it by failing to put sufficient AML controls in place. Each charge carries a potential five-year sentence. They will be tried in the US District Court for the Southern District of New York in late 2021 or early 2022.

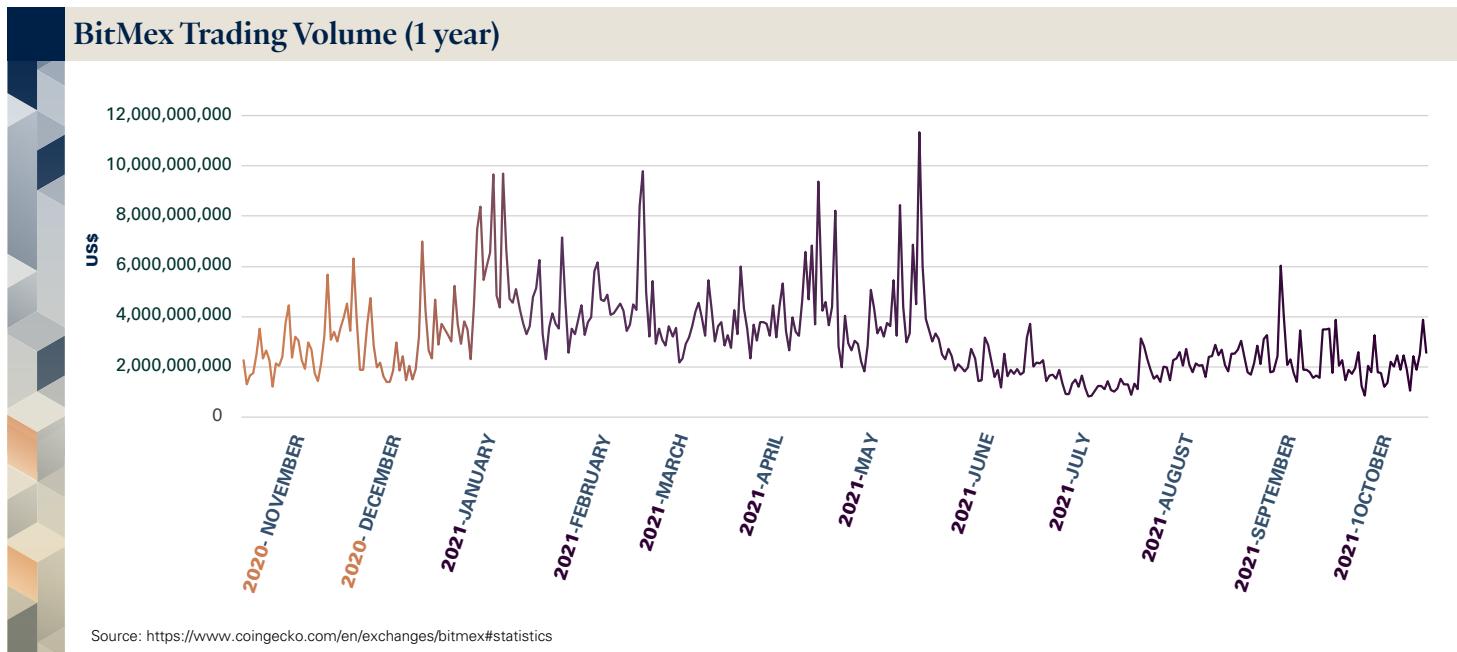
Separately, the three parties were sued on 30 October 2020 by plaintiffs alleging the men withdrew significant sums of money once they learnt about investigations and pending charges from US regulators and law enforcement. The plaintiffs claimed that over US \$440 million was looted from various accounts on the BitMEX exchange.

The fourth defendant, **Gregory Dwyer**, has a trial date set for October 2022.

## 4.8.2 What Is Next for BitMEX?

### What Is Next for BitMEX?

The co-founders stepped down from their positions within one week of the indictments in October 2020. BitMEX now has KYC protocols in place. BitMEX implemented its user verification program on 28 August 2020 to block US investor participation in the exchange and satisfy other KYC requirements.



The exchange's trading volume has rebounded and sees days with over US \$10 billion trading volume. While BitMEX has remained operational throughout the indictments and arrests, however, its future may depend on the outcomes of the various criminal and civil cases against it.

### Case Analysis

Having read this case, consider the following questions:

- Was BitMEX intentionally designed to sidestep the US laws that regulated KYC and AML activities? Do you think BitMEX is a haven for money laundering and other financial crimes?
- What were BitMEX's key mistakes along the way and what did you learn from them? How can you apply these lessons to your blockchain technology project?
- What would you implement early on in the idea or development stage of a blockchain technology solution to avoid a legal situation like BitMEX faces?

- How will AML and KYC affect your blockchain technology project? What steps should you take to be compliant with these regulations?
- Did the US indictments against the co-founders present a double standard compared to the money laundering activities at traditional large investment banks? As stated in a Vanity Fair article dated 4 February 2021, “In the world of high finance, charging corporate officers in their individual capacity is rare” (Ciralsky, 2021).
- Did the co-founders have nefarious intentions to drain investors’ accounts when it became impossible for investors to fulfil the demands of 100x margin trading—and when the legal troubles began mounting against the company and its co-founders?

### **4.8.3 Key Takeaways, References, and Further Exploration**

#### **Key Takeaways**

Let's review the key points of this section:

1. Although policymakers are still defining blockchain-specific regulations, organisations must follow existing regulations and laws.
2. Arthur Hayes saw the need for an online exchange that facilitated derivatives contracts, but paid no attention to KYC or AML laws. This negligence attracted more investors.
3. BitMEX did not comply with AML and counter-terrorist financing (CTF) controls. FINRA requires its member broker-dealers to implement a written AML program that complies with the Bank Secrecy Act, but that was missing from BitMEX.
4. BitMEX evaded this “issue” by blocking US customers from its exchange, which means the company was aware of the situation. American investors avoided this block by disguising their locations through the use of VPNs, which establish an encrypted private network over an otherwise public network.
5. BitMEX had no approval from the US Commodities Futures Trading Commission (CFTC), who filed charges against the company. The US Department of Justice (DOJ) filed criminal charges against the owners.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 19 April, 2022.

### 4.8.1 Overview of BitMEX

Ciralsky, A. (2021, 4 February). The Rise and Fall of Bitcoin Billionaire Arthur Hayes. *Vanity Fair*. <https://www.vanityfair.com/news/2021/02/the-rise-and-fall-of-bitcoin-billionaire-arthur-hayes>

McSweeney, M. (2020, 1 October). CFTC, Department of Justice file charges against owners of crypto derivatives exchange BitMEX. *The Block*. <https://www.theblockcrypto.com/linked/79483/cftc-bitmex-charges-lawsuit>

### 4.8.2 What Is Next for BitMEX?

CoinGecko. (2022). BitMEX. [https://www.coingecko.com/en/exchanges/bitmex\\_spot#statistics](https://www.coingecko.com/en/exchanges/bitmex_spot#statistics)

## Further Exploration

[Vanity Fair: The Rise and Fall of Bitcoin Billionaire Arthur Hayes](#)

[Full CFTC Complaint](#)

[Full DOJ Indictment](#)



**Module 5:**

# Strategy: How to Evaluate and Articulate a Business Case for Blockchain Technology

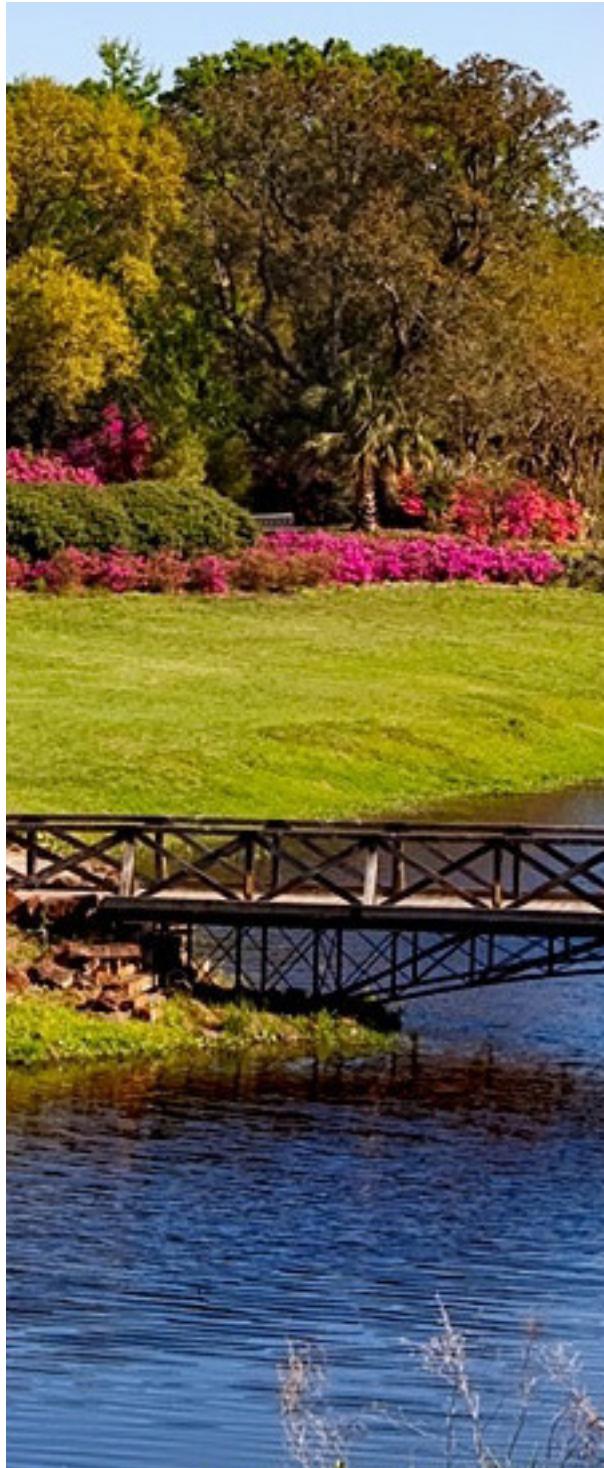
---

**Oxford Blockchain Strategy Programme**  
2022

# Oxford Blockchain Strategy Programme

## Strategy: How to Evaluate and Articulate a Business Case for Blockchain Technology

### Table Of Contents



<b>5.1 About Module 5</b>	<b>3</b>
5.1.1 Overview of Module 5	3
<b>5.2 Determining Your Use Case</b>	<b>5</b>
5.2.1 Intrapreneurs Versus Entrepreneurs	5
5.2.2 Applying Blockchain Features to Business	6
5.2.3 Defining the Problem You Want to Solve	7
5.2.4 Blockchain Suitability	10
5.2.5 Key Takeaways and References	13
<b>5.3 Market Position</b>	<b>16</b>
5.3.1 Porter's Five Forces	16
5.3.2 Blue Ocean Versus Red Ocean Strategy	19
5.3.3 The McKinsey Model	20
5.3.4 The Competition Paradox	22
5.3.5 Interoperable Systems	24
5.3.6 Key Takeaways and References	26
<b>5.4 Private Versus Public Blockchain Considerations</b>	<b>30</b>
5.4.1 Private Versus Public Blockchains	30
5.4.3 Technical Considerations	32
5.4.4 Legal, Team, and Marketing Considerations	33
5.4.5 Key Takeaways and References	34
<b>5.5 Blockchain Project Economics</b>	<b>36</b>
5.5.1 Blockchain Project Economics	36
5.5.2 Revenue Models	37
5.5.3 Technical Costs	40
5.5.4 Legal Costs	41
5.5.5 Private Blockchain Considerations	44
5.5.6 Public Blockchain Considerations	45
5.5.7 Key Takeaways, References, and Further Exploration	48
<b>5.6 Fundraising Strategies</b>	<b>52</b>
5.6.1 Overview	52
5.6.2 Venture Capital for Blockchain Projects	52
5.6.3 Enterprise Blockchain Funding	54
5.6.4 Evaluating Your Blockchain Startups Funding Needs	55
5.6.5 Crowdfunding	57
5.6.6 Angel Funding, Mergers and Acquisitions, and Corporate VC Funding	59
5.6.7 Key Takeaways, References, and Further Exploration	60
<b>5.7 Challenges to Blockchain Adoption</b>	<b>65</b>
5.7.1 Blockchain Adoption Challenges	65
5.7.2 Technology Maturity	66
5.7.3 Job Security	69
5.7.4 Coordination Across Departments	70
5.7.5 Integration of Legacy Systems	72
5.7.6 Exploring Alternative Technologies	73
5.7.7 Key Takeaways and References	77
<b>5.8 Business Case Framework</b>	<b>80</b>
5.8.1 Business Case Framework	80
5.8.2 Important Considerations	80
5.8.3 Further Exploration	84

# 5.1 About Module 5

## 5.1.1 Overview of Module 5

### Overview

Welcome to Module 5 of the Blockchain Strategy Programme!

In Module 5, you will evaluate the benefits and risks of launching a blockchain startup, or bringing blockchain technology into an organisation, and will learn how to outline a business case for blockchain applications.

You'll study the following key concepts in this module:

- How to evaluate and articulate a business use case for blockchain technology
- How to decide whether blockchain is the right solution for your business or organisation and if it makes economic sense
- The impact of blockchain projects as an intrapreneur and an entrepreneur, and the challenges related to both
- The types of financing available for blockchain projects and businesses

### Faculty Video: Module 5 Overview

In the following video, Professor Martin Schmalz, the Oxford Blockchain Academic Director, describes what to expect in this module and walks you through the subjects you will learn about this week.



Welcome to module five on strategy and how to evaluate and articulate a business case for blockchain technology. I'm Martin Schmalz. I'm the academic director of this programme and a finance professor at the Said Business School. So far in this programme, you have learned how blockchain technology works, examined how it is being used in a variety of industries, explored the many stakeholders involved in the blockchain project, and learned about the legal, regulatory, ESG, and other challenges you may encounter as you implement blockchain technology.

In this module, we will turn our attention to thinking about blockchain technology as a way of solving problems in your business and gain a competitive advantage. In other words, strategy. You will learn how to evaluate a potential business opportunity for blockchain technology and ensure that blockchain technology is the right solution and that it makes economic sense for your business to adopt it.

We will look at the impact of blockchain projects as an organisation and to prepare for those challenges. And we will end the module by exploring the various types of financing and funding available for blockchain-focused projects and businesses. I hope you enjoy module five.

## Learning Outcomes

By the end of this module, you will be able to:

- Evaluate the benefits and risks of bringing blockchain technology into a particular project.
- Develop a business case for blockchain technology in a startup or an existing organisation.
- Identify the various types of financing and funding available for blockchain-focused projects and businesses.

## Graded Assignments

You will complete individual and group assignments, which count towards your completion of the programme. This week, you will:

- Meet with your group to examine your proposed use case against the criteria in the business case framework.
- Complete a quiz on the module's content and key takeaways.
- Reflect on what you have learnt by applying it to your personal or professional experiences.

You must submit all graded assignments in Module 5 by **12 July 2022, 23:59 UTC..** (Try the [Time Zone Converter](#) to get your local time.)

## Additional Activities

In each module, we present additional activities related to the core learning. This week, you will:

- Share your thoughts with the class on a business that has implemented blockchain technology successfully and explain why you consider the project successful.

## Time Commitment

Plan to spend seven to ten hours on Module 5 this week. As there is a lot of reading material and video content, you might want to divide your work into several sessions. The module is broken up into sections by theme, giving you potential break points.

Make sure you plan time to meet with your group, and to complete the assignments.

## 5.2 Determining Your Use Case

### 5.2.1 Intrapreneurs Versus Entrepreneurs

#### Overview

When it comes to launching a blockchain project, it matters whether that project is built inside a corporation by an intrapreneur, or as an independent startup or project by an entrepreneur.

Working within an existing company, intrapreneurs are frequently driven by cost-cutting and efficiency concerns (often a request or edict to “do more with less”), and constrained by the strategic needs of their organisation: helping to increase competitive advantage within an existing market, capture new opportunities, or achieve sustainability within the business, by reducing costs and improving overall operational efficiency and revenue.

By contrast, an entrepreneur has an emphasis on revenue generation. If blockchain technology is core to your business, the technology and business models developed from it will be what primarily sustains your business. So, an entrepreneur is free to innovate and to develop a product or service that creates unique value for a new or established market.

This section provides information for both intrapreneurs and entrepreneurs.



## Discovering a Use Case

Discovering a use case for blockchain technology, whether for an internal project or as an entrepreneurial venture, requires an understanding of:

1. The way **key features and attributes of blockchain technology** apply to business and industry.
2. The **challenges** facing your business (intrapreneurs) or industry (intrapreneurs or entrepreneurs).
3. What makes a blockchain use case **suitable** (based on the blockchain suitability criteria discussed in Module 2).
4. Your **market position** and the competitive advantages of your use case.

## Vocabulary Check

This section introduces the following terms.

- [intrapreneur](#)

### 5.2.2 Applying Blockchain Features to Business

#### Applying Blockchain Features to Business

The key features of blockchain technology—a shared ledger, cryptographic-based security, and a consensus mechanism for verification—mean that it is most useful when employed in multi-stakeholder ecosystems. These attributes can often bring value across two functions in particular: record keeping and transactions. Thus, blockchain technology may be more beneficial to industries whose core processes and functions are focused in or heavily impacted by these areas.

Currently, the majority of enterprise blockchain platforms are either internal private networks or external private, permissioned networks aimed at reducing cost across a complex ecosystem of both competitive stakeholders and partners.

Much of the value of blockchain comes from cutting down on administrative tasks and transaction reconciliation, as well as doing away with some intermediaries. In particular, highly siloed industries where there is pressure to verify and transfer information or assets stand to benefit from blockchain. McKinsey & Company notes, for example, that the sectors currently capturing the most value from blockchain are financial services (including insurance), government, and healthcare (Carson et al., 2018).

But you need not work in one of these industries to benefit from blockchain technology—as long as the solution fits the problem. Consider which of the following features and attributes of blockchain technology can be used to solve challenges specific to your own industry:

- Immutable records
- Smart contracts that can reduce legal costs
- Data encryption to increase privacy
- Low-cost payment rails
- Instant settlement
- Transparency through distributed ledgers
- Asset authentication

Further, consider any challenges your organisation is facing.

- Do you need to create and verify the scarcity of digital assets—for example, to develop a token, cryptocurrency, or NFT?
- Do you need to leverage a low-cost payment rail with instant settlement? Could you reduce your transaction costs by switching from a traditional payment service like PayPal or Stripe to a stablecoin provider like Circles, USDC, or BitPay?
- Do you need a distributed ledger for transparency and authentication of assets?
- Will storing your business data on a distributed network of several nodes help keep the data more secure?

Lastly, keep in mind that the tasks, processes, and environments for which blockchain technology is most suited tend to be:

- Ongoing or automated processes with many stakeholders
- Reconciling transactions with multiple parties
- Transferring value
- Requiring permanence

### **5.2.3 Defining the Problem You Want to Solve**

#### **Defining the Problem You Want to Solve**

Companies—especially startups—must focus on identifying and solving their customers' worst “pain points”.

Nexus Mutual is a London-based VC-funded blockchain startup, built on the Ethereum platform, that provides coverage for smart contract failures and exchange hacks—a new niche market. The startup, which bills itself as an alternative to insurance, uses blockchain technology to build a risk-sharing pool owned by its users (who also vote on paying out claims). It hopes to eventually provide a range of coverage similar to that of incumbent insurance companies—including certain policies that are often prohibitively expensive, such as earthquake coverage.

By contrast, Allianz, a multinational insurance company founded in 1890, is using blockchain technology to improve business processes amongst its 23 European subsidiaries to reduce the time, errors, and effort it takes to settle cross-border claims.

Through its use of blockchain technology, Nexus Mutual wants to upend the very business model of insurance companies, whilst Allianz is creating efficiencies and cost savings to sustain and improve existing models.

Like Allianz, are you hoping to create a more efficient process for cross-border subsidiaries to settle claims with one another? Or does the problem you're hoping to solve involve external stakeholders?

## Faculty Video: In Developing a Use Case, How Can Blockchain Solve the Problem?

In this video, Professor Martin Schmalz introduces the realities of identifying a business use case that is the right fit for blockchain technology and what to understand when discovering a use case for blockchain technology, using a case study as an example.



In the midst of the hype cycle that surrounds the rise of cryptocurrencies, blockchain technology is often mistaken for being some sort of magic bullet for a myriad of business challenges facing companies today. However, the realities of identifying a business use case that is the right fit for the technology, and the challenges that come with implementing and operating this technology, are far more nuanced than many company leaders today perceive.

When discovering a use case for blockchain technology, it is important to establish a deep understanding of the challenges that are specific to your business, how they relate to the broader set of challenges facing your industry, and the specific ways in which blockchain technology can be applied to solve both of these challenges.

As you think about the challenges that are specific to your business, you should recall the blockchain suitability framework from module 2, which consists of a series of questions that can help you narrow down your list of business challenges to those that are most likely to be solved with blockchain technology. Whilst the technology is in its nascent stage of adoption, and new use cases are still being discovered, early research has shown that 43% of live enterprise blockchain networks have been launched by the finance and insurance sector, whereas 19% of all blockchain business use cases are for supply chain tracking; followed by market trading, certifications, trade finance, and payments.

In addition, 72% of enterprise blockchain networks have stated that cost reduction is a primary value proposition that they are seeking to capture with their solution. These data points can help you form an understanding of the competitive landscape, which markets are more or less contested, and what value propositions you should be seeking to capture when developing your blockchain solution.

The next step is to think about how your business challenge relates to the broader set of challenges facing your industry. This relationship between business challenge and industry challenge is critical to the successful adoption of blockchain technologies. It is essential for multiple industry stakeholders to operate within the same network in order to realise the benefits of network effects, which include cheaper cost structures and increased transactional efficiencies that can be enabled by having access to a single shared source of data. Therefore, when discovering a blockchain use case, you must seek to align the incentives of your business with those of your industry partners – and even competitors – in order for your blockchain to achieve adoption.

As an example of this, we can look at the case of AP Moller–Maersk, the largest container shipping company in the world. In 2018, IBM and DTD Solutions, a division of Maersk, announced that they were establishing a new joint venture for the purpose of launching TradeLens, a global trade digitisation platform that would aim to bring clarity and efficiency to the shipping industry. Prior to the launch, Maersk was experiencing a multitude of logistical problems in their global trade business. From inefficient paper-based processes, to poor communication between firms, and limited visibility into the status of goods as they moved through the supply chain, all of these factors contributed to high administrative costs involved with transporting shipping containers.

These challenges were also not unique to Maersk, but were part of a larger set of industry-wide problems affecting shipping companies, importers and exporters, suppliers, customs agencies, and intermodal providers around the world. The potential alignment of incentives between Maersk and other industry stakeholders enabled TradeLens to launch a solution that could, at least in theory, solve the problems being addressed with blockchain technology. The platform would use a distributed ledger to digitise and automate paperwork filings, fast-track approval of documents by the appropriate authorities, and share information about shipments and transportation plans between relevant parties more efficiently.

Finally, the last step to discovering a use case is to understand which specific features and attributes of blockchain technology should be applied in order to develop your solution. In the case of Maersk, we can highlight features such as immutability, transparency, smart contracts, and the ability to track and trace containers between different ports and terminals. These data points can help you form an understanding of the competitive landscape, which markets are more or less contested, and what value propositions you should be seeking to capture when developing your blockchain solution.

## The Case of TradeLens

To help ground the process of discovering a blockchain use case with concrete examples, we examine the case of TradeLens, one of the most high-profile examples of enterprise blockchain adoption that involved a partnership between software company IBM and shipping giant Maersk to develop a blockchain solution for the shipping container industry.

When Maersk and IBM launched TradeLens, they began with a simple pilot that involved identifying a trade lane from a port in Houston to a port in Rotterdam, then using Maersk's ships to transport shipments from Dupont, Dow Chemical, and Tetra Pak through the trade lane. As Daniel Wilson, director of business development at Maersk Line, described it (as quoted in Lal & Johnson, 2018):

We were testing the value proposition as well as the technological capabilities at the same time. As each shipment was completed, we were able to go through and identify different examples where value could be generated.

At that stage, Maersk and IBM were able to test multiple critical assumptions from one pilot, all while using their current infrastructure and without the need to involve other shipping container companies.

Maersk did not initially plan to develop an industry-wide blockchain platform. This was a consideration that was made during the pilot phase—which speaks to the importance of not anchoring the success or failure of a pilot solely to metrics like cost savings or revenue generation, but viewing it as a discovery process to test assumptions and identify where value can be created.

After the pilot, Maersk altered its strategy from what was initially going to be a blockchain platform with Maersk and IBM at the centre of a consortium of clients and suppliers to an industry-wide network that included competitors as well.

## Industry Challenges

The vast majority of today's live blockchain projects are focused not on disruptive new business models but on fostering operational efficiencies and reducing costs. According to the 2nd Global Enterprise Blockchain Benchmarking Study from the Cambridge Centre for Alternative Finance, cost reduction was the primary objective of 72% of the live networks surveyed (Rauchs et al., 2019).

Some of the more widespread uses of enterprise blockchain are the multi-stakeholder, industry consortium-led platforms. Pharmalegger, for example, is a 29-member blockchain consortium with ambitious goals to transform the healthcare supply chain, clinical trials, and how data is accessed and shared.

For all of these multi-stakeholder industry blockchains, it is important to understand the challenges shared by stakeholders across the ecosystem when discovering a use case. Think about the business challenges that your current or potential competitors, or your industry, is facing. Is there an opportunity for competing parties to mutually benefit from sharing information that can lead to cost savings across the board?

Recall the coopetition paradox, which describes how companies that are natural competitors must work together to achieve shared governance in a blockchain network while still remaining competitive. Understand, however, that multi-stakeholder blockchain consortiums will raise a multitude of other questions beyond costs for your business. In particular, what are the strategic risks to your organisation's place in a consortium, and the wider ecosystem? Would a shared ledger give competitors more insight or data that might give them an advantage? What benefits might be obtained from joining the same network, and do those benefits outweigh the potential loss of competitive edge in the market? (The answer to this question will vary depending on where each current or potential competitor is positioned in the market—are they a leader or a follower?—and how much leverage they have as a result of their current position.)

## 5.2.4 Blockchain Suitability

### Industry Organisations

Obviously, blockchain technology is not a one-size-fits-all solution to control costs or generate revenue, nor is it suitable for all scenarios. In Module 2, the content covered frameworks for understanding the suitability of a blockchain use case. This framework covered the basic criteria for leveraging blockchain technology in the areas of digital scarcity, payment rails, and distributed ledgers. As a reminder, the six questions a business should ask itself when considering implementing a blockchain solution are:

1. Is the process I am trying to apply a blockchain solution to one that is **repeatable** or can be **automated**?
2. Will this solution be applied only **once**? Or will it be part of an **ongoing** process?
3. Are multiple stakeholders involved in the process, and is it already easy to **verify that each participant is acting honestly**?
4. Is just one, or are multiple parties involved in **reconciling the different types of data** that accumulate throughout the business value chain?
5. Is **something of value being transferred** between stakeholders, such as information, money, or assets?
6. Is it **essential for all records of transactions between stakeholders to be permanent**? Would the ability to revise past transactions have a negative impact on stakeholders?

For both intrapreneurs and entrepreneurs, the goal of these questions is to help businesses narrow down the challenges they face to only those issues that stand a good chance to be solved or improved with blockchain technology. Beyond that, as mentioned earlier, concerns and specifics will vary according to group.

### Intrapreneurs

Consider organisations that currently or might partner with yours to execute or streamline certain business processes. This can include vendors, suppliers, manufacturers, resellers, retailers, and so on. What costs could they incur in the process of working with your business? How could they also realise cost savings and other benefits from operating on a shared ledger with your business and its other partners? Could they be potentially cut out? The Insurwave platform, for example—which hopes to facilitate and cut costs around the insurance-buying process—could potentially cut out brokers, whose positions could be eliminated by the efficiencies and insight gained through use of the platform.

One of the most lauded enterprise blockchain efforts has been the 2018 joint venture between global consultancy Ernst & Young (EY) and network security giant Guardtime, which launched Insurwave

along with Microsoft. Shipping giant Maersk joined the blockchain-based marine insurance platform as a pilot customer. The platform has brought a number of efficiencies and cost reductions to a notoriously paper-based sector populated by a number of players across the value chain. Typically, for Maersk to insure a single vessel involves around 50 stakeholders pushing along 100 document transactions. Such inefficiency has a price, with transaction fees making up to 40% of a premium's cost (Al Saqqaf, 2018). Other benefits, according to EY, have included claims paid in hours, rather than years; premiums that were agreed upon and settled in seconds; data visible to all players, including insurers and brokers, with insurers able to better underwrite risk; shippers better able to track assets; and insurers able to track their exposure in near real time (Crawford et al., 2018). The platform could potentially empower Maersk to eliminate brokers from the value chain.

## Entrepreneurs

As an entrepreneur hoping to discover a use case for blockchain technology, your core question is: What challenges or opportunities can I capture in the traditional business world or blockchain ecosystem through blockchain technology?

As you are building a blockchain venture from the ground up, your approach to engaging industry stakeholders will be different from a company that already has client relationships, strategic partnerships, contracts with vendors, and awareness of its main competitors (organisations with which you can potentially collaborate).

You will need to identify a target industry or sector that your use case can address. Traditional industries and sectors that are showing promise for blockchain adoption include digital rights management, supply chain tracking and logistics, healthcare, financial services, and the internet of things (IoT).

## Guest Video: Identifying Problems to Solve in the Blockchain Industry

In this guest speaker video, Robert Viglione, Co-Founder & CEO of Horizen Labs, identifies problems to solve in the blockchain industry.



For entrepreneurs who are considering entering this space, again, you really should go back to the first principle. So what problem are you trying to solve? Or do you just want to be part of the space? And maybe that's OK too, because when the internet came about, there were many businesses that launched, just realising we need to be part of the space. We want to be part of the space.

And we see a lot of entrepreneurship in the crypto industry or blockchain industry, where people just realise this is such an exciting new technology with so many things that it offers the world that we don't even understand the full set of possibilities yet. So I'll just dive right in. But if you want to take a more pragmatic entrepreneurial perspective, you start with your problem. And if your problem involves you can better do some business function if you can broadcast information and have public participation, such that you have information certainty of a public network or really the world being able to verify information, then this might be the industry for you or the technology stack that you should consider.

And as a simple example, you can contrast this with a business like Uber. Uber is a centralised company, but it has a decentralised network of agents or drivers that are actually interacting with customers on a continuous basis. Now, we can think, does Uber need to be a centralised business where all information flows to the company, and are there risks with that? Are there things that we might be able to do better if we decentralise that core, decentralise the company, and maybe have that company reside in a smart contract that's fully transparent, open, verifiable, and potentially governed by its community of users or the drivers, right? So you can see a whole different set of potential business opportunities that are derived from being part of a decentralised framework that blockchain offers.

## Opportunities

There are also sectors within the blockchain ecosystem that you can target for a new business. These include:

- **dApp infrastructure:** Building a blockchain that can support the development of decentralised applications. Examples include Ethereum, Tezos, and Solana.
- **Decentralised finance (DeFi) protocols:** Building a decentralised app that enables people to trade, lend or provide liquidity peer to peer on a blockchain. Examples are Uniswap, Sushiswap, and Aave.
- **NFTs:**
  - Building solutions to help people create and trade non-fungible tokens more easily. Examples are OpenSea and Rarible.
  - Developing gaming applications where in-game assets can be minted as NFTs and traded. Examples are Axie Infinity and Neon District.
- **Blockchain as a service (BaaS):** Building software development toolkits to enable developers to build and manage their own custom blockchains. Examples are Hyperledger, Corda, Cosmos, Polkadot, and Horizen.
- **Oracles:** Feeding real-world data into smart contracts to help them execute based on accurate information (for example, developing a price feed to help smart contracts decide to sell collateral based on specified liquidation price). Examples include Chainlink and BAND Protocol.

## 5.2.5 Key Takeaways and References

### Key Takeaways

Let's review the key points of this section:

1. Intrapreneurs serve the organisation's strategic needs by helping the organisation increase its competitive advantage within an existing market, capture new opportunities, or achieve sustainability by reducing costs and improving overall operational efficiency.
2. Entrepreneurs are free to innovate and to develop a product or service that creates unique value for a new or established market.
3. Discovering a use case requires an understanding of:
  - The way key features and attributes of blockchain technology apply to business and industry
  - The challenges facing your business or industry
  - What makes a blockchain use case suitable
  - Your market position and the competitive advantages of your use case
4. The majority of the value from blockchain technology comes from cutting down on administrative tasks and transaction reconciliation, as well as doing away with intermediaries, thus fostering operational efficiencies, increasing revenue and reducing costs.
5. For blockchain technology to be a solution to a problem, the features of blockchain technology need to match the challenges that the organisation or industry is facing.
6. Some of the more widespread uses of enterprise blockchain are the multi-stakeholder, industry consortium-led platforms such as Pharmaledger.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 14 April, 2022.

### 5.2.1 Intrapreneurs Versus Entrepreneurs

Mills, P. (2020, 7 July). What is the difference between entrepreneurship and intrapreneurship? *Academy of Entrepreneurs*. <https://aestudy.com/what-is-the-difference-between-entrepreneurship-and-intrapreneurship>

### 5.2.2 Applying Blockchain Features to Business

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018, 19 June). Blockchain beyond the hype: What is the strategic business value? *McKinsey Digital*. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>

### 5.2.3 Defining the Problem You Want to Solve

Rauchs, M., Blandin, A., Bear, K., & McKeon, S. (2019). 2nd Global Enterprise Blockchain Benchmark Study. *Cambridge Centre for Alternative Finance*. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf>

Lal, R., & Johnson, S. (2018, April, revised July 2018). Maersk: Betting on Blockchain. Harvard Business School Case 518-089. <https://www.hbs.edu/faculty/Pages/item.aspx?num=54373>

### 5.2.4 Blockchain Suitability

Al Saqqaf, W. (Host). (2018, 5 June). Insurwave – A Maersk pilot for marine blockchain insurance (No. 12) [Audio podcast episode]. In *Insureblocks*. *Insureblocks*. <https://insureblocks.com/ep-12-insurwave-a-maersk-pilot-for-marine-blockchain-insurance>

Crawford, S., Hollander, D., & Peddanagari, P. (2018, 2 September). Insurwave: blockchain-enabled marine insurance. *EY*. [https://www.ey.com/en\\_uk/insurance/blockchain-marine-insurance](https://www.ey.com/en_uk/insurance/blockchain-marine-insurance)

## 5.3 Market Position

### 5.3.1 Porter's Five Forces

#### Overview

In this section, we explore how to determine the competitive advantage blockchain technology will bring to an organisation or venture. Will implementing blockchain technology bring unique value to your organisation or industry? Are there barriers to adoption for competitors, or could they also adopt the solution?

When examining whether you or your organisation should adopt or develop blockchain technology, you need to have a clear understanding of where your current business sits, or your potential business would sit, relative to its competitors, using frameworks like Porter's Five Forces, blue ocean strategy, and McKinsey's market positioning framework. You should also evaluate whether your chosen use case can potentially shift your market positions and give your current or potential organisation a clear competitive advantage.

In the process of launching and operating a blockchain network, the lines between partners and competitors become blurred. One of your main priorities in developing your solution is to understand the competitive dynamics between external stakeholders, your position in the market, and what strategic advantages a blockchain solution can give you or your organisation even as it *mutually benefits your competitors*.

#### Vocabulary Check

This section introduces the following terms.

- [blue ocean strategy](#)
- [red ocean strategy](#)

#### Porter's Five Forces

Porter's Five Forces is a model used by businesses to assess the competitiveness of a new product or service being introduced to the market. It consists of five competitive forces that help determine a company's strengths and weaknesses in the face of market competition (Business to You, 2016).

1. **Rivalry amongst existing competitors:** How many competitors exist in your industry or sector, and how easily can they decrease your market share? What are the costs of customers switching

to a competitor, what is the growth trajectory of the industry, and is the industry one of resource abundance or scarcity?

2. **Threat of new entrants:** What barriers could prevent competitors from offering a similar solution? Barriers could include legal provisions such as trademarks or patents, development costs, talent acquisition, and the ability to achieve scale or capitalise on network effects.
3. **Threat of substitute products:** Could other products or services be used as an alternative to your own? This threat examines the number of available substitutes, the frequency with which buyers choose a substitute, the performance and perceived differentiation between substitutes, and the switching costs.
4. **Bargaining power of suppliers:** How easily can a supplier drive the cost of producing goods or services? Key factors that determine this bargaining power are the number of available suppliers, the uniqueness of each supplier, and the costs to switch suppliers.
5. **Bargaining power of buyers:** Buyers can influence the price of a good or service based on their number of customers, the significance of each customer, how price-sensitive buyers are, and the costs of switching to new providers.

As you watch the following video, consider these questions:

- What are the core competitive advantages of your use case using Porter's Five Forces framework?
- Will implementing blockchain technology make a process or product cheaper or better than that of your competitors?

## Faculty Video: Examining Porter's 5 Forces

In this video, Professor Martin Schmalz introduces the Five Forces business framework in the context of the TradeLens case study and the competitive dynamics between shipping container companies.



Central to your assessment of whether to adopt a blockchain solution is an understanding of the competitive dynamics of your industry and where you are positioned in that market. We can conduct this analysis using a traditional strategy framework, namely Porter's Five Forces. Porter's Five Forces is a model used by businesses to assess the competitiveness of a new product or service to be introduced to the market.

It consists of five competitive forces that help determine the company's strengths and weaknesses in the face of market competition. These five forces are, first, rivalry among existing competitors, second, the threat of new entrants, third, the threat of substitute products, fourth, bargaining power of suppliers, and fifth, bargaining power of buyers. But analysing Porter's Five Forces, you need to ask whether implementing blockchain technology will make a process or product cheaper or better than your competitors. And what are the potential barriers to entry? And how can a blockchain increase the value offered to buyers and suppliers?

Now, due to the collaborative nature of blockchain technology, the lines between what defines a competitor and a collaborator can sometimes become blurred. This is why, in certain cases, it may make more sense to think about your blockchain solution as an industry solution and reflect on the competitive advantages that can be attained by not just your company, but by your industry as a whole. In other words, you should examine how blockchain can help you and your competitors increase your bargaining power with external buyers or suppliers who benefit primarily from the lack of coordination and cost sharing between you and your industry competitors.

Now, let's revisit our example of Maersk and the container shipping industry. Maersk is the largest container shipping company in the world, operating in an industry in which the top five firms and their alliances represent about 80% of total market share. The threat of new entrants is relatively low, as there are already significant network effects at play between existing players in the market.

Additionally, the cost of licensing and regulatory compliance makes it challenging for new incumbents to establish a footprint. At the same time, the bargaining power of buyers is relatively high. Large firms with operations around the globe represent just 0.5% of the overall customer base for the container industry. Yet, these firms are responsible for about 50% of all container traffic.

Large firms distribute their shipments across multiple competitors and typically do not give a single shipping line more than 40% of their overall cargo. By doing so, they reduce switching costs and force shipping container companies to remain competitive with their prices. As we've discussed before, network effects can create significant competitive advantages for blockchain companies as more value accrues to the network with each additional member who joins. Now, by consolidating the top shipping container companies under one private blockchain network, each provider can potentially offer a faster and cheaper service due to automated approval processes and efficient sharing of information between the members.

This can create significant value for the large firms who benefit from the ability to track and trace their cargo and improve the flexibility and optionality of services between shipping container companies. On the other hand, as the TradeLens platform continues to grow in adoption and benefit from larger network effects, buyers could also see a decrease in bargaining power due to the increasing need to operate on the platform where most of the top shipping companies are located. Suppliers of Maersk, including fueling services, trucks, and container manufacturers, could also experience a similar phenomenon, initially benefiting from having access to a large network of shipping container companies, yet over time, experiencing a decrease in bargaining power due to the reliance on the large network established on the TradeLens platform to maintain their business.

This decrease in bargaining power by buyers and suppliers can be mitigated through the establishment of multiple shipping container blockchain networks. However, new incumbent shipping networks would face significant barriers to entry as the costs for customers and industry partners to switch from a scaled network to one that lacks scale becomes increasingly more difficult as the formal network continues to grow. Now that the TradeLens ecosystem includes already more than 300 organisations, 10 ocean carriers, and data from 600 ports and terminals, it may make more sense for other shipping companies who are not currently involved to join that network rather than to try and compete by developing a new blockchain technology for themselves.

There are some exceptions, however, such as the Global Shipping Business Network, or GSBN, which is a competing blockchain consortium based in Asia that is also made up of large shipping container companies, including firms like Hapag-Lloyd that are also operating on the TradeLens platform. Ultimately, the adoption of blockchain technology by the shipping industry is creating new and interesting competitive dynamics between firms. While container shipping companies still compete for a greater share of global cargo, we are also

beginning to see the emergence of blockchain shipping consortiums with competitive dynamics that resemble those of public blockchains, like Ethereum, Polkadot, and others. As ecosystems continue to scale in adoption, we can further examine the role that network effects play in deciding which blockchains become dominant over others, as well as the strategic benefits of creating interoperable systems that enable members to seamlessly migrate between blockchain shipping networks with minimal friction.

## Network Effects

As we discussed in the prior section, network effects dictate the amount of bargaining power that buyers and suppliers have, the strength of substitute products, and the threat of new entrants.

As a startup, you need to analyse which competitors have the largest network, and if it is possible to siphon some of this network by developing solutions that deliver value to your competitors' clients, while making the costs of switching from the competitors' service to your own very low.

An example of this strategy is the recent launch of blockchains like Solana and Avalanche. Although these players both compete directly with Ethereum, they recognised that Ethereum has the largest network—leading them to establish a bridge between the Ethereum blockchain and their blockchains so that users could seamlessly migrate to the newer blockchains to try the DeFi and NFT applications available there.

The same strategy can be applied to more traditional business environments. For example, if you were planning to launch a competing shipping container blockchain solution to TradeLens, an important consideration would be how to make it as easy as possible for TradeLens members to migrate to your blockchain to take advantage of your unique features.

### 5.3.2 Blue Ocean Versus Red Ocean Strategy

#### Blue Ocean Versus Red Ocean Strategy

While Porter's Five Forces method focuses squarely on how a company fares in a competitive market, the “blue ocean” strategy, developed by W. Chan Kim and Renée Mauborgne, is about exploring the advantages of creating entirely new markets through innovation. In their book, *Blue Ocean Strategy* (first published in 2004), they examine how successful companies navigate from a “red ocean” strategy, in which a firm must find a competitive edge in a highly saturated market, to a “blue ocean” strategy, where a firm innovates its way into a brand new market and captures total market share.

For example, the Ethereum blockchain successfully executed a blue ocean strategy. While a red ocean strategy would have involved competing directly with bitcoin as a store of value, with the blue ocean strategy, Ethereum created a new market where blockchain technology could be applied as an infrastructure layer for decentralised applications. As Ethereum was first into this market, it was able to create new demand and capture value uncontested. As the network has attracted more developers who launch new applications, the costs of servicing each new end user decrease as users spread across a wider number of operators and service providers, unleashing economies of scale.

## Considerations for Entrepreneurs

You can leverage the blue and red ocean strategy when considering which markets to target for your use case as an entrepreneur. Without the backing or resources of an established company, it may be more challenging for you to pursue a blue ocean strategy and try to discover value in uncontested markets. However, those same disadvantages may also play to your favour, as your position as an entrepreneur gives you greater flexibility to experiment and search for new opportunities without having to win approval from upper management or convince internal stakeholders to rally to your cause.

### 5.3.3 The McKinsey Model

#### The McKinsey Model

McKinsey & Company has developed a model to look at blockchain strategies and how market dominance relates to a company's regulatory influence (Carson et al., 2018). As follows, the model classifies companies as either leaders, conveners, attackers, or followers, and describes the typical impact or effects of each.

##### Leader

Leaders must act quickly to maintain their dominant position and establish a new industry standard. Dominant players can leverage their current position to pursue new ventures while being less constrained by regulation or the need to coordinate on standards. However, leaders risk remaining stagnant and failing to take advantage of their market position to innovate.

According to a report by the Cambridge Center for Alternative Finance (CCAF), over 70% of enterprise blockchain networks originated from companies in leadership roles with a dominant market position (Rauchs, 2019).

##### Convener

While conveners also hold dominant market positions, greater regulatory and standardisation barriers hamper them from directing efforts for blockchain adoption. It is therefore important for conveners to spearhead partnerships with industry stakeholders to shape and capture the value of new blockchain standards.

Conveners should focus on high-value blockchain use cases that require a common set of industry standards to be adopted, such as trade finance.

## Follower

Followers have lower market dominance and are therefore less able to influence other industry stakeholders to join or support a blockchain use case. Followers must keep an eye out for emerging blockchain consortiums so that they can quickly join them and establish a position in a growing trend that could disrupt complacent market leaders and create openings for new players to achieve market dominance. The inability to invest the upfront costs to join new private permissioned blockchain networks can lead to greater costs down the road from being left behind and trying to catch up.

## Attacker

Attackers are typically new market entrants with little to no existing market share (that is, startups).

Seeking new and disrupting technologies to adopt is essential for their survival, so they seek to adopt blockchain use cases with the highest disruptive potential. Such use cases include services that disintermediate the dominant market players.

Peer-to-peer applications in finance, insurance and property are examples of attacker-type market players.

A useful tactic for companies deploying a blockchain attacker strategy is to partner with a dominant company to leverage that company's influence.

## Considerations for Intrapreneurs

Once a company develops an understanding of the competitive dynamics of its use case, it must determine how to execute its use case based on market positioning relative to its competitors. For example, a market leader like Amazon or Facebook would have a different perspective on its analysis of Porter's Five Forces or the blue ocean strategy compared to a market follower with fewer resources and industry leverage.

The ability to successfully venture into an uncontested market is determined by an organisation's tolerance for risk. Naturally, market leaders can afford to take on greater risks, as their positions are already secure, whereas followers must move more cautiously or risk losing what little advantage they have.

In the McKinsey model, two critical market factors determine a company's market positioning: market dominance, or the ability of a player to influence the key parties of a use case, and standardisation and regulatory barriers, or the requirement for regulatory approvals or coordination on standards. Is your company already a dominant player in the market? If so, can you leverage this position to minimise regulatory barriers and establish new standards for blockchain adoption in your industry?

These market factors are essential for blockchain projects to succeed because they ultimately determine which market participants can and cannot establish a key competitive advantage for their blockchain-based solutions.

## Considerations for Entrepreneurs

How you execute your competitive strategy as a startup will also depend on your current position in the market. Based on McKinsey's market positioning framework, most startups will typically fall under the attacker or follower category. The difference between being an attacker or a follower depends on what type of leverage your venture currently has or the level of risk you are willing to take.

For example, while you may not have an established network to attract partners or clients to your blockchain, having access to proprietary technology, such as a unique method for achieving consensus on the blockchain that is more scalable, or access to a large capital base to fund new cutting-edge ideas, could give you the leverage you need to establish a position as an attacker.

Without these advantages, a more conservative approach would be to become a follower and quickly join an existing network that is beginning to show signs of growth and adoption. Here, you can establish a position in a growing trend that could disrupt complacent market leaders and create openings for new players to achieve market dominance.

### 5.3.4 The Coopetition Paradox

#### The Coopetition Paradox

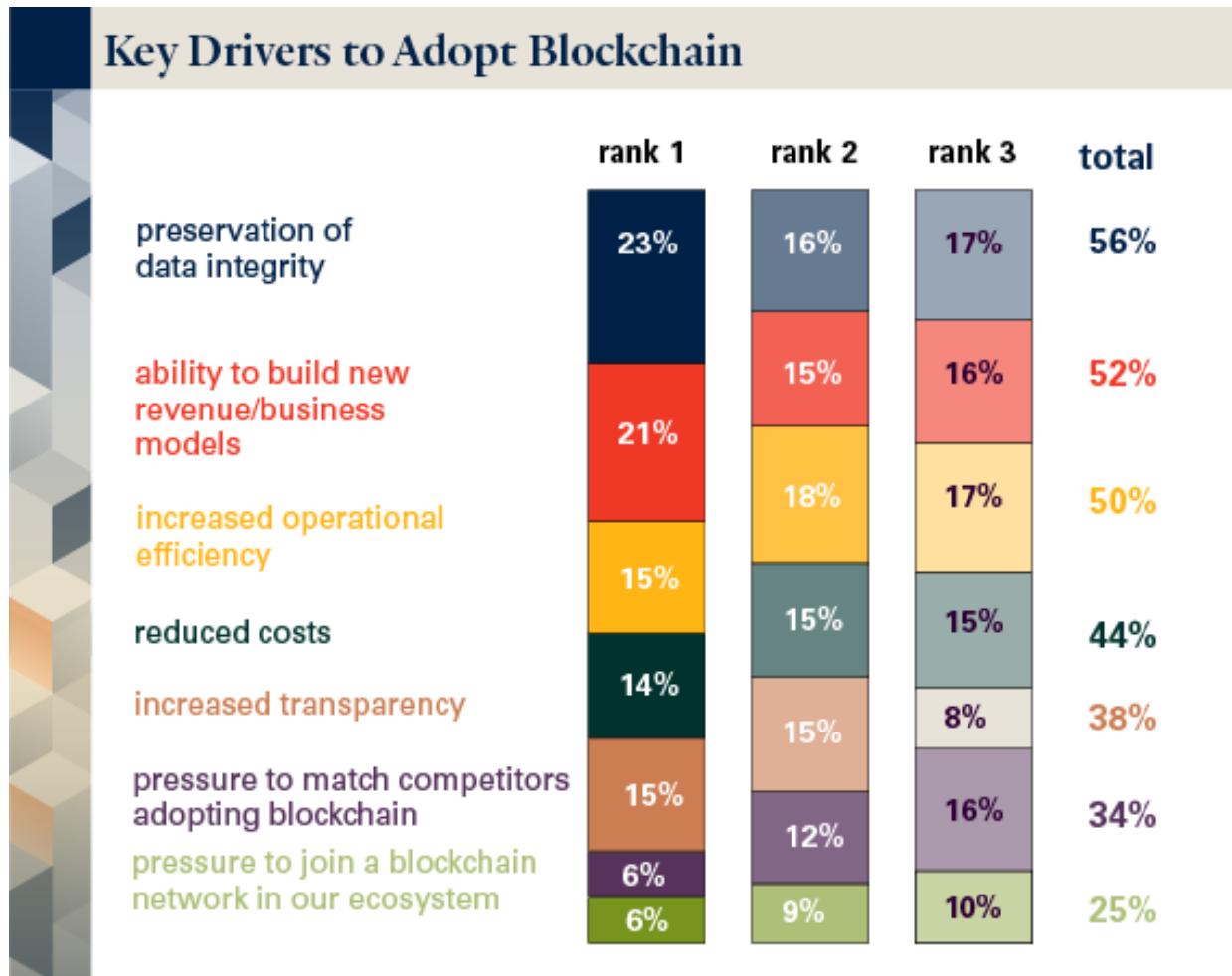
The coopetition paradox describes how companies that are natural competitors must cooperate to achieve shared governance in a blockchain network while still remaining competitive.

Some of the difficulties around recruiting members to join your network may occur because competitors are naturally inclined to choose what is best for improving their business over cooperating with peers. A 2019 research report published by EY revealed that pressure to join a blockchain network started by another company or consortium ranked at the very bottom of the list of reasons for organisations to adopt blockchain technology (Forrester, 2019). Instead, the top three reasons for adopting blockchain technology were preservation of data integrity, the ability to build new revenue or business models, and increasing operational efficiency as seen in the "Key Drivers to Adopt Blockchain" visual here.

A note on reading this visual: of the 212 blockchain decision makers from multiple regions, 23% ranked "preservation of data integrity" as the number 1 driver for considering blockchain, 16% ranked it as number 2, and 17% ranked it as number 3. In total, 56% ranked this driver among their top three drivers.

The study also revealed that companies that have enough resources are starting their own blockchain networks instead of joining existing networks launched by their competitors. The need to own and exert control over the access rights and revenue flows of a blockchain is a persistent deterrent, preventing companies from joining private blockchain networks or fully embracing public blockchains.

The emergence of multiple private blockchain networks within a single industry can lead to potential problems as industry players become further entrenched in their siloed networks of economic activity. This can lead to a lack of industry-wide standardisation, as well as adaptation challenges for consumers of blockchain services.



## Coopetition: TradeLens and GSBN

TradeLens and the Global Shipping Business Network (GSBN) are two competing blockchain networks that offer a paperless and transparent way for shipping container companies, suppliers, customer agencies, and other stakeholders to connect, exchange data, and share costs to streamline business operations across the shipping supply chain. TradeLens is a for-profit joint venture between IBM and Maersk, the largest shipping container firm in the world. Maersk has a 51% ownership of the joint venture behind TradeLens, with IBM owning the other 49% (Lal & Johnson, 2018). GSBN is a consortium of nine shipping container companies that have a strong presence in the Asian market. These companies formed their new consortium partly out of concerns over a lack of neutrality from Maersk (The Maritime Executive, 2020). GSBN works with a technology provider, CargoSmart, which provides the blockchain software and services for profit (Johnson, 2019).

The key difference between GSBN and TradeLens is in the legal status of the platforms, and the way membership is structured. GSBN's structure was intended to enable more shipping companies to have a hand in initiating the launch of the consortium, with the organisation insisting that "collaboration is the main way of introducing innovation and digital transformation to the supply chain" (Baker, 2018). GSBN is focused on creating a data marketplace that enables data providers and consumers to trade and receive fair value for their data. The organisation also plans to implement strong data management and governance frameworks that enable shipping companies and other partners to retain control over data shared through GSBN.

TradeLens	GSBN
For-profit venture	Nonprofit venture
Initiated by Maersk and IBM (51% and 49% owners respectively), with other entities joining after launch (Lal & Johnson, 2018).	Initiated by CargoSmart and launched as a collaborative effort between nine shipping container companies and CargoSmart.
Technology provider (Hyperledger supported by IBM) owns a large stake in the venture.	Technology provider collaborates with the venture. No public information exists about ownership stakes in the nonprofit.
Received limited antitrust exemption in January 2020, allowing shippers to publish and subscribe to data about cargo movements (Ledger Insights, 2020).	Applying for similar antitrust exemption (Molod & Neuburger, 2020).

GSBN's technology provider, CargoSmart, is itself a partnership between tech companies like Oracle, Microsoft Azure, AntChain, and Alibaba Cloud—all of which are competitors with IBM and Hyperledger (Quarmby, 2021). This highlights how competition amongst market leaders within a particular industry, as well as between BaaS providers, can lead to the emergence of new competing private blockchain networks.

Hapag-Lloyd is also a shareholder in the GSBN consortium (CargoSmart Ltd., 2020). However, Hapag-Lloyd, along with firms including CMA-CGM, have joined both GSBN and TradeLens. When asked why, a Hapag-Lloyd spokesperson replied, "We take a look at where it makes the most sense to get involved. ... Currently, GSBN and TradeLens are the two initiatives with the largest number of participants and where we see the best opportunities to develop blockchain in container logistics" (Kapadia, 2019). CMA-CGM and Hapag-Lloyd may have a presence on both networks to avoid any risks that might come with lack of control or ownership of the TradeLens platform, as they were not founding members of TradeLens.

### 5.3.5 Interoperable Systems

#### Interoperable Systems

Building interoperable systems could solve many of the challenges like those that the shipping industry faces. Consortium members that can communicate and transfer data between both networks

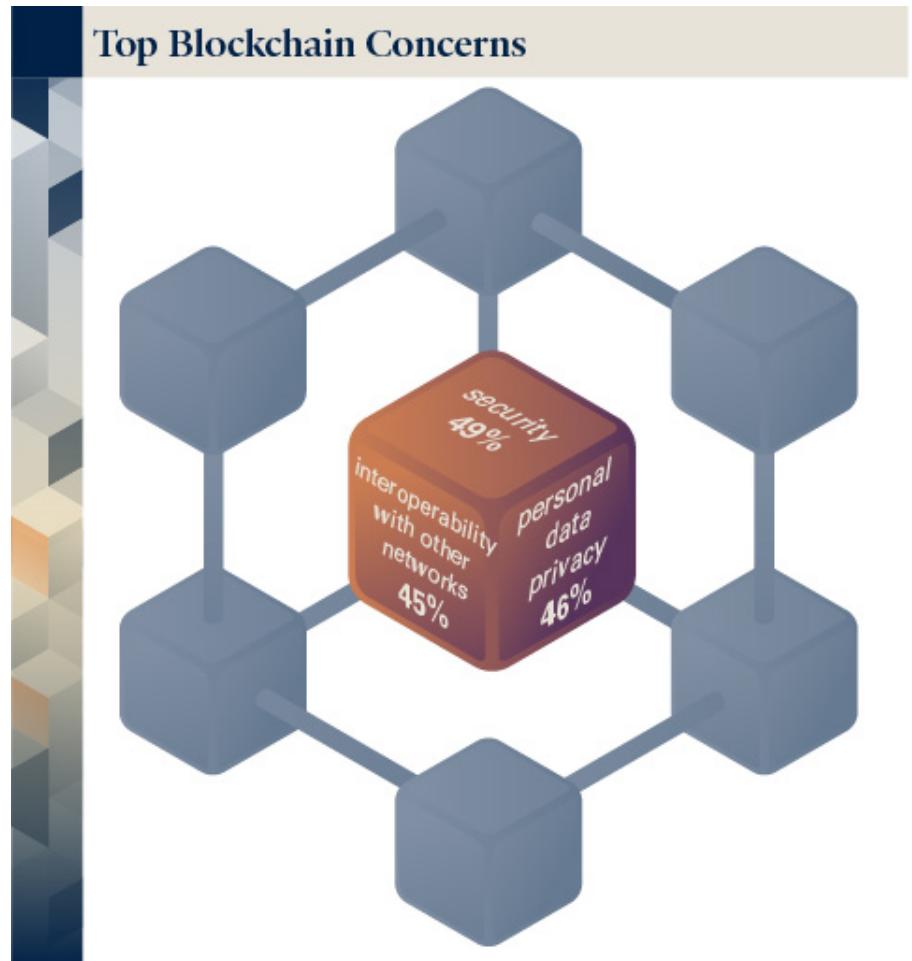
seamlessly could avoid the costs of joining two separate networks. Companies would not have to integrate their legacy systems with blockchain networks to share and receive data (TradeLens, 2020).

In addition to separate networks, many industries also face challenges from a lack of standardisation. Interoperability could facilitate the creation of industry standards for ecosystem members and other stakeholders to adhere to. Michael White, CEO of Maersk, has expressed interest in such solutions (as quoted in Lal & Johnson, 2019):

As TradeLens evolves, I sincerely doubt there will be only one platform. ... But they can't be competing. There needs to be interoperability, and the way to give that interoperability is to have standards. Where standards are in place, we'll embrace them. It's easier to connect to a host of carriers if they're agreeing on the same standards.

## Interoperability Risks

While TradeLens and other platforms may see benefits in building systems that reduce friction between shipping networks, such systems could create disadvantages for other stakeholders—for example, BaaS providers like Hyperledger and Oracle might no longer be able to require members to set up separate accounts for each network. Interoperability features can also lead to privacy concerns for blockchain members who may have joined a private blockchain over a public one to avoid the same data exposure risks that a highly interoperable private blockchain could cause. In the same EY study that revealed the companies' top reasons for adopting blockchain technology, interoperability and privacy were cited as two of these companies' top three biggest concerns (Forrester, 2019).



One way to resolve privacy concerns is through the application of zero-knowledge proof cryptography, which enables private blockchains to communicate and confirm the validity of transactions to each other without sensitive details about the transactions being revealed. However, some predictions suggest that this cutting-edge sector within the blockchain industry may still be five or more years away from enterprise adoption (Benjamin, 2021).

## Guest Video: What Are Zero-Knowledge Proofs?

In this guest speaker video, Robert Viglione explains zero-knowledge proofs.



I'll just emphasise that zero-knowledge proofs are a key bridging technology that is really just coming to the market in a meaningful way—beyond, say, coin anonymity or coin transfer privacy—and now we're looking at zero-knowledge proofs as a class of cryptography that makes broadcasting information to the public, to a public ledger, a public blockchain.

You can broadcast information in encrypted form, but actually make use of that information; actually have applications that use that information—wireless encrypted—without revealing the information; still make use of it. It's a property in cryptography called homomorphic encryption that is key, because you can publish information to a public ledger and not reveal it, but still do important things with it.

The first use case for zero-knowledge proofs in the blockchain context was trying to make coin transfers in private. This was really pioneered by a company called the Electric Coin Company, and resulted in the public blockchain project called Zcash. Now, there are many other companies, like Horizen Labs, that are abstracting this concept, this key bridging technology, such that we can do things like have a whole bunch of different types of applications to solve different problems that are more about data privacy, which is a really important concept, especially in an era of GDPR where we all realise that data privacy is something that we have taken for granted for too long.

Many technology companies have been harvesting the economic benefits of a whole bunch of data without users really understanding that. Zero-knowledge proofs allow people to take control of their data again and still make use of it in an economically meaningful way. That's why we're so excited about this technology.

### 5.3.6 Key Takeaways and References

#### Key Takeaways

Let's review the key points of this section:

1. Porter's Five Forces is a model used by businesses to assess the competitiveness of a new product or service being introduced to the market. It consists of five competitive forces that help determine a company's strengths and weaknesses in the face of market competition. They are:
  - Rivalry amongst existing competitors
  - Threat of new entrants
  - Threat of substitute products
  - Bargaining power of suppliers
  - Bargaining power of buyers

2. You can consider the blue ocean strategy and red ocean strategy when considering which markets to target for your use case as an entrepreneur.
  - The blue ocean strategy is about exploring the advantages of creating entirely new markets through innovation.
  - The red ocean strategy is where firms must find a competitive edge in a highly saturated market and beat the competition using existing demand.
3. The McKinsey model looks at blockchain strategies and how market dominance relates to a company's regulatory influence. It classifies companies as either leaders, conveners, attackers, or followers.
4. An organisation's tolerance for risk determines its ability to successfully venture into an uncontested market. Market leaders can afford to take on greater risks, as their positions are already secure, whereas followers must move more cautiously or risk losing what little advantage they have.
5. Intrapreneurs: Once a company develops an understanding of the competitive dynamics of their use case, they must determine how to execute their use case, based on market positioning relative to their competitors.
6. Entrepreneurs: How you execute your competitive strategy as a startup will also depend on your current position in the market. Based on McKinsey's market positioning framework, most startups will typically fall under the attacker or follower category.
7. The coopetition paradox describes how companies that are natural competitors must cooperate to achieve shared governance in a blockchain network while still remaining competitive.
8. Building interoperable systems could solve many of the challenges like those that the shipping industry faces, as companies would not have to integrate their legacy systems with blockchain networks to share and receive data. Interoperability could facilitate the creation of industry standards for ecosystem members and other stakeholders to adhere to.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 14 April, 2022.

### 5.3.1 Porter's Five Forces

Business to You. (2016, 3 August). Porter's Five Forces. <https://www.business-to-you.com/porters-five-forces>

### **5.3.2 Blue Ocean Versus Red Ocean Strategy**

Kim, W., & Mauborgne, R. (2005). *Blue Ocean Strategy*. Harvard Business Review Press.

### **5.3.3 The McKinsey Model**

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018, 19 June). Blockchain beyond the hype: What is the strategic business value? *McKinsey Digital*. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>

Rauchs, M., Blandin, A., Bear, K., & McKeon, S. (2019). 2nd Global Enterprise Blockchain Benchmark Study. *Cambridge Centre for Alternative Finance*. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf>

### **5.3.4 The Coopetition Paradox**

Baker, J. (2018, 11 June). Leading carriers launch new blockchain platform. *Lloyd's List*. <https://lloydslist.maritimeintelligence.informa.com/LL1124961/Leading-carriers-launch-new-blockchain-platform>

CargoSmart Ltd. (2020, 26 February). GSBN Counts Down to Inauguration as Its Shareholders Sign Shareholders' Agreement. *Globe Newswire*. <https://www.globenewswire.com/en/news-release/2020/02/27/1991505/0/en/GSBN-Counts-Down-to-Inauguration-as-Its-Shareholders-Sign-Shareholders-Agreement.html>

Forrester. (2019, November). Seize the Day: Public Blockchain Is on the Horizon. *EY*. [https://assets.ey.com/content/dam/ey-sites/ey-com/en\\_gl/topics/blockchain/ey-public-blockchain-opportunity-snapshot.pdf](https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/blockchain/ey-public-blockchain-opportunity-snapshot.pdf)

Johnson, E. (2019, 12 July). Dual blockchains for shipping tests interoperability. *Journal of Commerce*. [https://www.joc.com/technology/dual-blockchains-shipping-test-interoperability\\_20190712.html](https://www.joc.com/technology/dual-blockchains-shipping-test-interoperability_20190712.html)

Kapadia, S. (2019, 15 July). CMA CGM, Hapag-Lloyd, Cosco formally sign on to GSBN blockchain platform. *Supply Chain Dive*. <https://www.supplychaindive.com/news/cma-cgm-hapag-lloyd-cosco-gsbn-blockchain-cargosmart/558754>

Lal, R., & Johnson, S. (2018, April, revised July 2018). Maersk: Betting on Blockchain. Harvard Business School Case 518-089. <https://www.hbs.edu/faculty/Pages/item.aspx?num=54373>

Ledger Insights. (2020, 7 January). TradeLens supply chain blockchain gets U.S. antitrust exemption. <https://www.ledgerinsights.com/tradelens-supply-chain-blockchain-antitrust-shipping>

The Maritime Executive. (2020, 27 February). Nine Companies Sign Up for Global Shipping Business Network. <https://www.maritime-executive.com/article/nine-companies-sign-up-for-global-shipping-business-network>

Mollod, J., & Neuburger, J. (2020, 3 June). Another Blockchain Supply Chain Shipping Consortium Files for Federal Antitrust Exemption. *Blockchain and the Law*. <https://www.blockchainandthelaw.com/2020/06/another-blockchain-supply-chain-shipping-consortium-files-for-federal-antitrust-exemption>

Quarmby, B. (2021, 10 September). New blockchain platform aims to track one-third of all shipping containers globally. *Cointelegraph*. <https://cointelegraph.com/news/new-blockchain-platform-aims-to-track-one-third-of-all-shipping-containers-globally>

Wagner, N., & Wiśnicki, B. (2019). Application of Blockchain Technology in Maritime Logistics. *DIEM: Dubrovnik International Economic Meeting*, Vol. 4 No. 1, p. 155-164. [https://www.researchgate.net/publication/337835524\\_APPLICATION\\_OF\\_BLOCKCHAIN TECHNOLOGY\\_IN\\_MARITIME\\_LOGISTICS](https://www.researchgate.net/publication/337835524_APPLICATION_OF_BLOCKCHAIN TECHNOLOGY_IN_MARITIME_LOGISTICS)

### 5.3.5 Interoperable Systems

Benjamin, G. (2021, 2 June). Gartner Blockchain Hype Cycle: Where We Are & What's Next. *iMi Blockchain*. <https://imiblockchain.com/gartner-blockchain-hype-cycle>

Forrester. (2019, November). Seize the Day: Public Blockchain Is on the Horizon. *EY*. [https://assets.ey.com/content/dam/ey-sites/ey-com/en\\_gl/topics/blockchain/ey-public-blockchain-opportunity-snapshot.pdf](https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/blockchain/ey-public-blockchain-opportunity-snapshot.pdf)

Lal, R., & Johnson, S. (2018, April, revised July 2018). Maersk: Betting on Blockchain. *Harvard Business School Case 518-089*. <https://www.hbs.edu/faculty/Pages/item.aspx?num=54373>

TradeLens. (2020, 26 February). TradeLens working with ZIM and Wave to offer members expanded capabilities and added flexibility. <https://www.tradelens.com/press-releases/tradelens-working-with-zim-and-wave-to-offer-members-expanded-capabilities-and-added-flexibility>

# 5.4 Private Versus Public Blockchain Considerations

## 5.4.1 Private Versus Public Blockchains

### Overview

Now that you've explored business use cases and your current or potential market position, you need to consider the type of blockchain to use. Will it be a public or private blockchain? Private blockchains are usually used in enterprises and are permissioned, whereas public blockchains are permissionless and open in terms of participation and, specifically, with regard to the ability to read or write on the ledger.

Both intrapreneurs and entrepreneurs can build a project on an existing private blockchain, create a new private blockchain, or build a project on an existing public blockchain. It is uncommon and very costly to develop a new public blockchain, which generally makes this option unrealistic.

When exploring public versus private blockchains, there are many considerations to take into account—namely in the areas of tokens, technical ability, legalities, marketing, team, revenue, and costs. In this next section, we focus on understanding the main differences between public, private, and hybrid blockchains and touch on other considerations to take into account.

### Permissioned Versus Permissionless Blockchains

Today, most enterprise blockchains are private and permissioned, and restrict access to only members who are fully or partially trusted by others on the network. Private blockchains preserve the privacy of members by denying non-members access to view the data being stored and transacted on the network. In the case of TradeLens, a permissioned blockchain, only shipping container companies, suppliers, customs agencies, intermodal providers, and other verified industry stakeholders are allowed to access and transact on the blockchain.

Typically, consortium-led blockchains have chosen to remain private, permissioned blockchains that employ a consensus mechanism that does not require the energy-intensive PoW consensus mechanism that Bitcoin, a public blockchain, uses. This is partly for scalability reasons and partly for privacy reasons. A private blockchain achieves faster scalability by limiting the number of nodes required to validate transactions. The downside of relying on fewer nodes, however, is that the blockchain may become more centralised, which makes it more vulnerable to attacks, as each node is more critical to the overall functioning of the network. Pharmaledger has stated that it may look into "anchoring" its current private blockchain to a public blockchain, which would act as more proof that the private blockchain has not been altered (Morris, 2020).

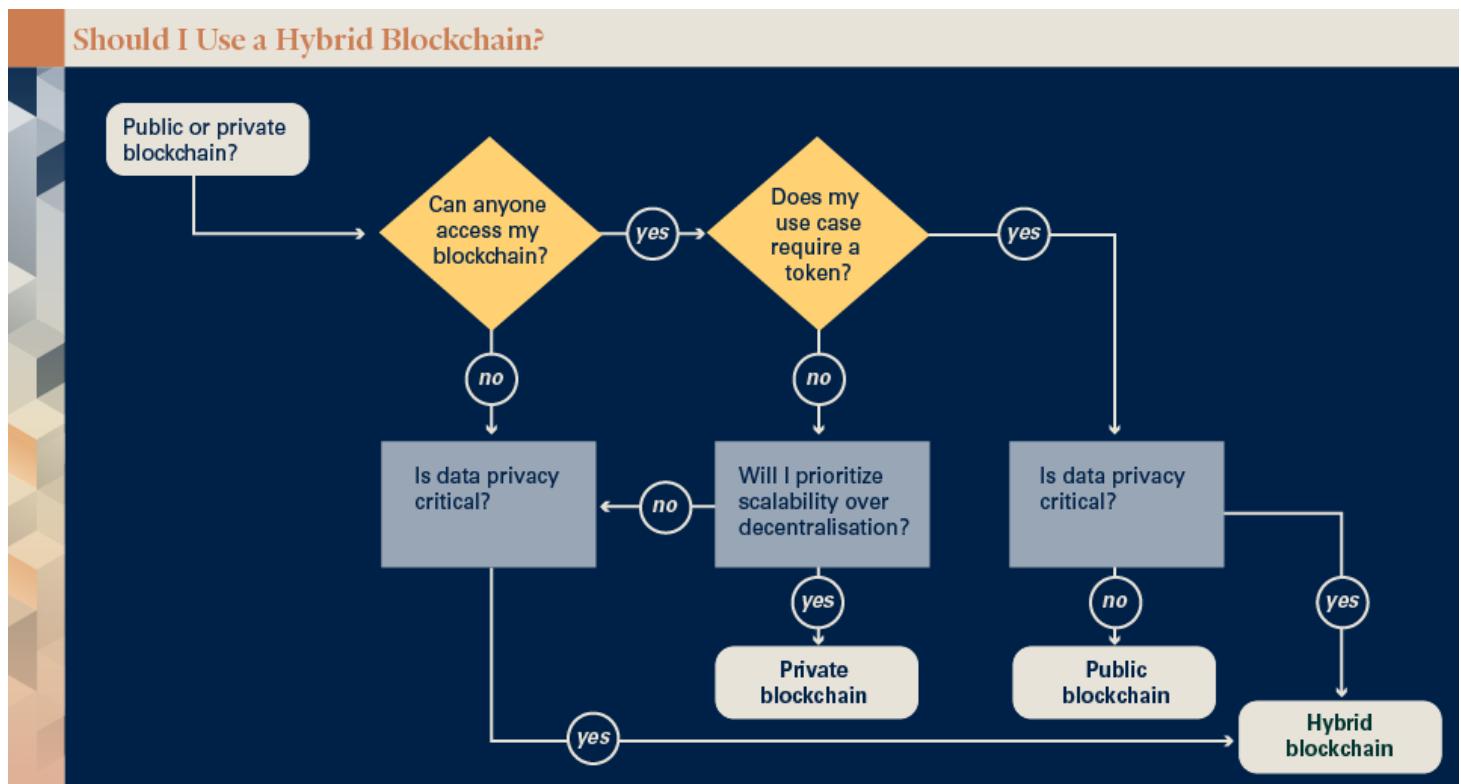
Public blockchains, by comparison, are permissionless and pseudo-anonymous, meaning that transaction data is publicly visible and can be traced through public key addresses. A public permissionless blockchain enables anyone to access the network and become a miner or validator.

This lack of censorship enables a wider variety of participants to join the network; however, this can also lead to nefarious actors using the blockchain to participate in money laundering or other crimes.

## Hybrid Blockchains

A hybrid blockchain is also a viable alternative to public and private blockchains. Using BaaS providers such as Hyperledger Sawtooth, you can make certain components of your blockchain public and permissionless, while keeping others private. You can also set up a private blockchain that is interoperable with a public ledger, such as HyperLedger Besu, which is interoperable with the Ethereum blockchain.

Questions on whether to build on a public, private, or hybrid blockchain can be answered in the form of this decision tree:



### 5.4.2 Tokens

#### Tokens

Tokens can be used on either public or private blockchains, depending on whether your use case requires a cryptocurrency or token. The difference between a cryptocurrency and a token is that cryptocurrencies have their own blockchains, such as Ether or Bitcoin, while tokens are built on

an existing blockchain, such as UNI and Aave. Both a cryptocurrency or a token can serve many purposes on a blockchain:

- It can be used as a faster and cheaper means of transferring value on the network.
- It can serve as a monetary tool to create incentives for users to adopt and take action on the network.
- It can be used as a store of value that can (with the right regulatory framework) represent an investable asset similar to owning equity in a business.

Not all blockchains require a native cryptocurrency or token. You can choose to use a stablecoin to move value across the network or simply record IOUs on the blockchain, which can be settled off-chain through a more traditional means of payment. A cryptocurrency or token is an optional feature for private blockchains, while on public blockchains, a native token or cryptocurrency is required to power the network. A public blockchain's native token rewards users for participating in node consensus and network governance. This is a necessary feature when dealing with parties on a blockchain network who do not know or trust each other and whose incentives may not all be aligned.

### 5.4.3 Technical Considerations

#### Technical Considerations

There are also technical considerations involved in selecting a blockchain type. The size of the developer community influences the decision on a public versus private blockchain. Additionally, what the blockchain solution is optimising for affects the protocol layers.

As a reminder, a blockchain platform has an application layer, a network layer, and a protocol layer.

Application layer:

- How will your application be designed to cater to different end user types?

Network layer:

- How many nodes are run, and who can run them?
- What is the cost of mining nodes?
- Which consensus mechanism should you use?

Protocol layer:

- Are you optimising for speed, programmability, or payments?
- What is the size of the developer community and customer support for the blockchain?

## 5.4.4 Legal, Team, and Marketing Considerations

### Legal Considerations

Legal considerations look at the structure of your blockchain solution. Are you setting it up as a consortium, company, foundation, or joint venture (or a decentralised autonomous organisation, or DAO, in the case of a public blockchain solution)? Other considerations to take into account:

- Know your customer (KYC) and anti-money laundering (AML)
- Protection of information and IP
- Tax filing and financial reporting
- GDPR compliance

There are several legal and logistical considerations that come with launching a cryptocurrency that is rare:

- Is it classified as a utility or a security token?
- Are there any restrictions on who can buy it?
- How will the token be distributed, and what is the breakdown of allocations to insiders versus the public?
- How do you comply with securities laws?

These factors can increase the complexity and costs of developing your blockchain-based solution and should be addressed with the help of legal counsel.

### Guest Video: Legal Considerations When Implementing a Blockchain Solution

In this guest speaker video, Edmund Schuster, Associate Professor of Corporate Law at the London School of Economics, shares his advice on legal considerations when it comes to developing a blockchain solution.



So, what tip can a lawyer give students who may be thinking about starting a blockchain project; who may already be involved in one? At what point should the law come in? It has now, I think, been accepted that it's really important to get lawyers involved early on in the process, to get some comfort on what the exposure is: not just of the project and the firm, but also on the people acting. Under what circumstances could there be liability; could there even be criminal charges in some cases?

I think my advice would be, be very careful with shopping around for legal advice. I've seen advice given by seemingly competent lawyers that is very problematic. Part of the reason is that entrepreneurs sometimes believe that the best approach to getting some legal safety net is to find somebody who will sign a document saying that what you've planned is OK.

That often involves going from one lawyer to the next, and perhaps also being fairly generous in the fee arrangement, until somebody signs it. And then people often wave these pieces of paper around and say, well, I have a legal opinion that says this is not a securities offering, this is a utility token – or something like that.

My advice would be, don't do that. If you get pushed back by the first two lawyers, there's probably a reason for it. And, yes, there are so many lawyers on this planet, you will find somebody who will sign it. But you should never rely on that.

## Team and Marketing Considerations

To implement a blockchain solution, you need the right team. Consider these questions:

- What are the essential roles for developing my dApp? How do I recruit for those roles?
- What are the essential roles for developing my blockchain? How do I recruit for those roles?

Marketing considerations are important as well, because if not enough people use your blockchain, what is the point of developing it? Insurance giant Axa, for example, shut down its Ethereum-based flight insurance product, Fizzy, because of low demand (Hill, 2019). Consider these important questions:

- Who is meant to use my blockchain, and what benefit do they get out of it?
- What is the right distribution channel for users to access the network and receive messages?
- What strategy can I employ to maximise the value of each new user in order to acquire new users? What messaging can be used to convince developers to build on my blockchain (a consideration for public blockchains)?

### 5.4.5 Key Takeaways and References

#### Key Takeaways

Let's review the key points of this section:

1. Both intrapreneurs and entrepreneurs can build their own private blockchain or use an existing public blockchain in their organisation or business.
2. Private blockchains are permissioned and generally used in enterprises, whereas public blockchains are permissionless and public.

3. When exploring public versus private blockchains, there are many considerations to take into account in the areas of tokens, technical ability, legalities, marketing, the team, revenue, and costs.
4. Private blockchains preserve the privacy of members by denying non-members access to view the data that is stored and transacted on the network.
5. Public blockchains are pseudo-anonymous, meaning that transaction data is publicly visible and can be traced through public key addresses.
6. Typically, consortium-led blockchains have chosen to remain private, permissioned blockchains that employ a consensus mechanism that does not require the energy-intensive mining-based consensus mechanisms that public blockchains do.
7. Using BaaS providers such as Hyperledger Sawtooth, you can make certain components of your blockchain public and permissionless, while keeping others private. You can also set up a private blockchain that is interoperable with a public ledger. These are called hybrid blockchains.
8. A cryptocurrency or token is an optional feature for private blockchains, while on public blockchains, a native token or cryptocurrency is required to power the network.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 14 April, 2022.

### 5.4.1 Private Versus Public Blockchains

Morris, N. (2020, 3 March). 12 global pharmaceutical firms join EU blockchain consortium PharmaLedger. *Ledger Insights*. <https://www.ledgerinsights.com/pharmaledger-pharmaceutical-blockchain-eu>

### 5.4.2 Tokens

Liquid. (2018, 30 October). What's the difference between public and private blockchains? <https://blog.liquid.com/whats-the-difference-between-public-and-private-blockchains>

### 5.4.4 Legal, Team, and Marketing Considerations

Hill, E. (2019, 10 November). AXA drops Ethereum-based flight insurance platform. *Yahoo! Finance*. <https://uk.finance.yahoo.com/news/axa-drops-ethereum-based-flight-160027248.html>

# 5.5 Blockchain Project Economics

## 5.5.1 Blockchain Project Economics

### Blockchain Project Economics

The economics of a blockchain project for both intrapreneurs and entrepreneurs primarily centres around identifying methods for profiting from the venture. Implementing a blockchain project will be based on two primary economic considerations:

1. **Technical and legal costs.** There are several areas of consideration in understanding the cost of a blockchain project, including:
  - What are the upfront costs?
  - What are the ongoing costs?
  - How and when will the costs be funded?

Costs can vary significantly depending on the industry you are targeting, the scale of your blockchain project, and whether you build on a public or private blockchain.

2. **Revenue models.** What type of direct revenue or indirect revenue through cost savings will the project generate?

In this section, we will examine the costs of using blockchain technology to solve a business problem as well as potential revenue models. A strong business use case must make good economic sense, regardless of the project's entrepreneurial or intrapreneurial status.

As you progress through this module, you will gain a better understanding of the development and maintenance costs of a blockchain project, which will enable you to form a more accurate understanding of whether the benefits of utilising a distributed ledger solution outweigh the costs of the solution itself. We will explore the development, operational (including mining), and maintenance cost considerations for a blockchain project, as well as the various business models that can be deployed to generate revenue from your blockchain solution.

### Vocabulary Check

This section introduces the following terms.

- [bug bounty](#)

## 5.5.2 Revenue Models

### Revenue Models

A blockchain project can generate revenue in several ways. Understanding the potential revenue streams for a specific use case is vital to its success.

### Profits Through Cost Savings

As you've learnt, most live blockchain projects currently centre around cost savings and operational efficiencies—partially because blockchain technology is relatively new. As the technology matures, the focus may shift to revenue generation. As an example, Allianz's live blockchain project is an internal one that allows its 23 European subsidiaries to settle cross-border claims much more swiftly. The insurance multinational, however, has stated that it is open to allowing partners onto the platform in the future. This shift toward profits will benefit entrepreneurs, who must quickly generate revenue and find product-market fit (Ledger Insights, 2021).

For entrepreneurs and, eventually, for intrapreneurs who move beyond efficiency gains and cost savings, there are different revenue models to consider, depending on whether a blockchain project is public or private. Both public and private blockchains can support revenue models based on transaction fees and subscriptions. Private blockchains also support membership fees and data access fees, whilst public blockchains can generate revenues from token sales.

### Guest Video: Blockdaemon's Business Model

In this guest speaker video, Konstantin Richter, CEO and Founder of Blockdaemon, explains the company's business model. Blockdaemon offers an easy-to-use blockchain management platform for companies and organisations.



So Blockdaemon is a purely venture-backed entity. And so from the capitalisation side, we've decided very early on to go for normality. Because one of the other big factors, when you work with the Fortune 500s, is the companies they can associate with need to have a certain pedigree on a legal level. They need to be based in the US. They want to see a clear corporate ownership structure. They want to see balance sheets that are reliable. They have other factors than just the technology to evaluate when they partner with someone.

As a business, the way we make money in revenue is we have different types of customers. A very large segment of those are foundations, which are the physical, often pro bono entities that support the software development of a blockchain, which is supposed to be free and open-source, and run by the community. But very often, these things have been created by some financial event, raised a bunch of money, then created an institute, for example, that ensures that developers will build on said blockchain.

And for a protocol, it's important that you have a vibrant community. Each of these protocols—some of them valued at \$10, \$20 billion—don't initially have a lot of usage. They might have 100 engineers playing around

with it. But ultimately, what they all want to become is the predominant software and blockchain infrastructure of their age. So they're very ambitious, very well capitalised.

And they want to make sure that companies and individuals have as easy a job to do in order to connect to these blockchains. And that's what they come to us for—to say, Blockdaemon, can you please make your platform—which is, ultimately, three-click deployments and connectors to nodes and blockchains—available to our protocol? So we can point institutions when we meet them and say, hey, you guys should offer our token. Or you should build on our platform.

And then they're like, well, we have to read all these documents, learn all this stuff. No, no, you don't. You go to Blockdaemon and just click three buttons. And you're connected. And you can connect your app to the blockchain.

And so we're an enabler for these foundations because we are fairly widely used and accepted as a quality provider. They come to us and they want to get listed on our marketplace. And on that marketplace, you can click a button. And then we sell you all these different nodes. Plus, when somebody connects via Blockdaemon, we give these insurances and guarantees around performance and stuff.

And so for most of the foundations, it's a way to ensure that they get institutional adoption. It makes their life a lot easier. And so they incentivise us by doing so, by offering us grants, or paying us, or giving us tokens—token consideration. And then we build technology, and then we sell that technology to their users. So it's a nice business model. And we like it. So we get paid to build something we then sell to people. And so that's the math we like.

## Blockchain Revenue Models

In Module 2, we outlined some of the common business models organisations employ for digital scarcity, payment rail, and distributed ledger use cases. In the following table, we take a closer look at how revenues are generated within each of the three models:

Digital Scarcity	Payment Rail	Distributed Ledger
Collect transaction fees from the trading of digitally scarce assets	Collect transaction fees from cross-border payments	Using the Blockchain as a Service (BaaS) model, charge a subscription fee for clients to operate on a distributed ledger
Lend or stake assets to earn interest	Provide stablecoin liquidity and charge fees to convert real fiat currency to stablecoins	Offer real-time analytics services to identify risks and ways to optimise ledger operations
Provide custodial services (wallets)	Provide Stablecoin lending services	Earn fees from distributed ledger transactions
Generate revenue from price appreciation of underlying digital assets	Offer a subscription service to operate a stablecoin payments network with end user accounts and crypto-to-fiat on- and off-ramps	Charge fees to tokenise assets

Based on your use case, which of these revenue-generating models makes the most sense? Consider if it is possible to combine revenue models from traditional business, such as building an ecommerce platform on top of your blockchain. Or, consider if your business lends itself to creative, new models based on tokenomics—for example, could you issue tokens that could be then used to reward users for performing certain tasks to benefit other users, such as sharing content or referrals?

## Guest Video: Coinbase Business Model

In this guest speaker video, Emilie Choi, President and Chief Operating Officer at Coinbase, introduces the Coinbase business model and what makes up the company's revenue, such as "green shoots".



The business model today and historically has largely been predicated on transaction-oriented fees that result from folks buying and selling crypto. And that makes up a large part of our revenue. What we talked about in the S-1 and what we spend a lot of time doing now is investing in more sustainable, predictable SaaS-like types of revenue.

And we have a bunch of things that we called green shoots. Those include things like staking. They include things like assets under custody fees. They include the services that you could provide as a prime brokerage, including lend and borrow.

And I think the thing that's cool and refreshing is that we have this very strong, robust transactional business model, but we're using a lot of our resources to build these newer revenue models that are more predictable. And so we have this interesting new type of business model that we think we're pioneering. And some of those green shoots may take off, some of them might be less successful. We are already seeing a lot of fruit in some of them, and so we're going to continue to double down as we move forward.

### 5.5.3 Technical Costs

#### Technical Costs

Both private and public blockchain projects have significant technical costs in terms of infrastructure, storage, implementation, and usage. Following is a visual breakdown of these four different cost categories and the descriptions for each (Holbrook, 2020):

Costs	Private Blockchain	Public Blockchain
Infrastructure	Developing a node network infrastructure	Validation (including hardware, energy, etc.)
Data storage and transfer	Storing node data: hardware server or cloud storage	Miners storing node data: hardware server or cloud storage
Development and implementation costs	Salaries for blockchain developers and IT integration expert salaries  Number of team members required  Length of time costs are incurred	Salary costs for the core team of dApp developers  Budget for bug bounties  Incentives for open-source developer community participation
Usage and maintenance costs	Team members to maintain the blockchain and provide customer support  Sharing costs across members of the consortium	Gas fees to use the dApp and deploy upgrades  Distributing costs across the network

## Infrastructure

Infrastructure relates to developing a node network, and costs include the following fixed or variable categories:

- Data centre: leasing, utilities (power, cooling, supplies), and insurance
- Maintenance contracts
- Labour
- Hardware: servers and storage
- Software licensing
- Inspections and audits
- Service providers: bandwidth

## Data Storage and Transfer

Data storage refers to the costs to store transaction data that is recorded across the network of nodes. Storing the history of transactions on a blockchain can be quite costly, especially as usage builds over time. Data transfer costs include the costs of transferring data from a company's on-premises database to a cloud service provider, such as AWS or Microsoft Azure, which can incur significant bandwidth costs.

## Development and Implementation

Development costs are primarily a function of the costs of developers, which run near US \$150,000 to \$200,000 per year (Petrashchuk, 2018). An enterprise blockchain project can take up to 25 months to fully execute, from proof of concept to production. Building a dApp can take less time but depends on the complexity of the project.

Implementation costs can include the cost of acquiring the talent to develop and deploy the blockchain solution, procurement of resources and contractors who will support the development and deployment processes, and the cost of training stakeholders who will be expected to utilise the solution.

## Usage and Maintenance

Maintenance costs include the costs to perform updates, testing, quality assurance, audits, and other functions essential to blockchain operation. You will also need to consider the costs of hiring staff as part of the maintenance costs for your enterprise blockchain solution, including developers, auditors, legal counsel, and so on (Acharya et al., 2019).

### 5.5.4 Legal Costs

#### Legal Costs

As you consider the type of blockchain platform for your project, plan for legal assistance to help you understand if and how the platform and the organisation that it operates within should be registered as a legal entity. You will also need a legal team in place to guide you through the compliance process for storing and transferring data amongst different legal jurisdictions, particularly between the US and EU. Your team will need to provide guidance around the construction of smart contract rules to make sure there is a process for enforcing actions in the traditional legal system in case the smart contracts fail or external factors create scenarios that were not accounted for when the smart contract was written. General dispute resolution between blockchain members and financial reporting requirements will also need to be handled by your legal team.

In addition, consider the following legal cost scenarios for a public blockchain:

- **Security registration.** Legal advice from experts familiar with jurisdiction-based regulatory guidelines and laws will help you prepare for the potential of a cryptocurrency or token being considered as a security.
- **Nonprofit foundation.** You should seek legal consultation if the blockchain and its assets will be managed by a newly established nonprofit foundation, either domestically or offshore.

## Intellectual Property (IP) Rights

In the course of developing a blockchain solution, it is important to consider what intellectual property (IP) is being brought into the network, as well as what IP will be produced as a result of different companies coordinating together on a blockchain.

The establishment of legal entities such as a joint venture can help to mitigate some of the challenges that may arise from IP sharing and ownership, especially as your blockchain network continues to grow and incorporate new members.

Joint ventures can have clauses in place to designate a share of ownership of the IP created on the blockchain to all members, or only certain members based on how early they joined the network, how much they contributed to the development of the network or similar factors.

Similarly, members should establish contractual agreements on what forms of IP are being brought into the relationship and by which parties. For example, a pharmaceutical company joining a blockchain consortium for supply chain management might want to separate out the IP that protects its process for manufacturing and distributing new drugs, while also ensuring that the company retains a share of the IP generated from any new process that might arise as a result of working with multiple industry stakeholders (including competing pharmaceutical companies, suppliers, distributors, and so on) under a shared ledger.

Intellectual property within a blockchain can also be managed using “Smart” IP rights (Clark & McKenzie, 2018). Smart IP rights essentially enable members to record and control access to certain IP using smart contracts. Rules can be written into a smart contract that enable access to proprietary data (such as trademarks or patents) for a specific set of members, and only in exchange for a royalty fee or for a limited period of time. These rules would automatically be enforced through the smart contract code, reducing legal costs and increasing transparency and auditability.

## Smart Contracts

Smart contracts are neither smart, nor are they contracts—so notes tech research firm Gartner (Litan, 2020). Yet organisations employing them, and especially enterprises, must be aware of the potential legal risks they can pose and understand what it takes to make them legally enforceable.

As we have learnt in previous modules, smart contracts are pieces of code stored on a blockchain that automatically execute when certain predetermined conditions are met and verified. For example, Etherisc, a Swiss decentralised insurance startup, uses smart contracts to automatically pay out claims for its crop insurance product for Kenyan farmers once the terms of the claims—certain weather conditions—have been met and verified (Etherisc, 2021).

Increasingly, however, smart contracts are being deployed to automate more complex transactions that, once executed, may then also trigger other smart contracts. For example, TradeLens uses smart contracts to automate a number of repetitive tasks across its platform.

As Gartner notes, there are three main challenges to consider when employing smart contracts:

1. Once executed, reversing a smart contract's actions—that is, an immutable transaction—can be very difficult, if not impossible. It is important, then, to ensure that all parties understand the logic of the smart contracts in place.
2. Smart contracts can run forever if nothing is put in place to stop them. That means any mistakes in the code will continue running as well.
3. Users are often unaware of the extent of a legal framework they need to put in place for a blockchain network.

What about the legality of a smart contract and whether or not it can be legally enforceable?

According to legal research firm Practical Law, for a smart contract to be legally enforceable, the terms of the contract and the process of “agreeing” to a smart contract must have all the components that make a traditional contract enforceable (Neuburger et al., 2019).

For example, a company uses a smart contract that is automatically programmed to pay its employees biweekly. Just because the smart contract is functioning does not mean the employee is legally entitled to compensation unless specific terms are coded into the contract that can be legally enforced, such as:

- An offer and acceptance.
- An exchange of consideration (in this case, the employer’s agreement to pay each employee and the employee’s agreement to perform the services for which the employee is to be paid).

Smart contracts may also not be effective as a means to transfer legal ownership of tokenised real-world assets (such as property) without the pre-approved terms of a formal transfer of property rights being embedded into the smart contract prior to its transfer of the token.

To develop legally binding smart contracts within a blockchain consortium, it is recommended that all members and participants are made aware of, agree to, and sign traditional legal contracts whose terms will then be reinforced through the smart contracts. Similar to the process of creating an account on a website, these terms can be shared as a “terms of service” agreement that must be signed as a condition for participation in the blockchain network.

## Legal Liability for Smart Contract Errors

What happens when the actions of the smart contract deviate from the legally enforceable terms agreed to by both parties? Who is liable, and what are the methods of restitution?

Practical Law recommends signing ancillary agreements with any outside developer or third-party service responsible for creating the smart contracts (Neuburger et al., 2019). These agreements can include representations, warranties, and covenants that the code operates and will operate as

expected, thereby holding the third party legally responsible for breach of contract between the initial parties that was purely a result of the smart contract's failure.

## Hybrid Contracts

Other considerations, such as jurisdiction, governing law, indemnification, and dispute resolution, can be addressed through the use of hybrid contracts, which are defined as traditional contracts that reference the execution of certain terms through a smart contract while addressing issues that cannot easily be addressed in code form.

### 5.5.5 Private Blockchain Considerations

#### Private Blockchain Considerations

Private blockchains are generally used to connect members of an industry. Intrapreneurs and entrepreneurs who want to pursue this option have options such as:

- Join an existing blockchain and build out a consortium or marketplace for their partners on that blockchain.
- Create an entirely new blockchain.

If you form a consortium, you can invite industry members to join with the goals of sharing costs, technical expertise, and industry knowledge, among other benefits. Costs should be shared amongst members of your consortium based on the particular governance framework designed for your blockchain project. Many of these costs can also be applied to full in-house private blockchain solutions.

#### Join an Existing Blockchain

Joining an external blockchain and building a consortium can work well for companies that do not have a large number of international subsidiaries or in an industry whose members are already working together. The blockchain is external to all of the companies that join it, and only members have access to the blockchain or to specific transactions on the blockchain.

Joining an existing enterprise blockchain can offer long-term cost savings over developing a whole new blockchain and infrastructure, and the existing blockchain can also include a support system to implement a project more efficiently. Membership typically requires an upfront investment of US \$500,000 to US \$1 million for the first one or two years, according to Ledger Insights (Morris, 2019). However, these figures are not always evenly split across all members. It is not unusual for one or two members to fund a majority of the upfront costs in the early stages in exchange for a majority of the equity in the joint venture or a larger share of the revenues—thus, joining a blockchain can perpetuate power imbalances on the blockchain or in the industry. For example, because IBM and Maersk made

the initial investment in TradeLens, the joint venture behind the project is majority-owned by those companies. Further, TradeLens charges cargo owners to access data for their shipments (Johnson, 2019).

## Marketplace

In addition to building a consortium on an existing private blockchain, your company can build a marketplace that funds further development and maintenance costs through membership fees. Fees vary depending on the industry, number of members, and specific value proposition each network offers.

Aerospace manufacturing company Honeywell has built a marketplace called GoDirect Trade, where members can trade used aviation parts on the blockchain with transparent insight into the history of each part recorded in a shared ledger. Companies must pay a fee of US \$15,000 to join the marketplace (GoDirect Trade, 2021).

## Developing a New Blockchain

If your company is complex enough, such as a multinational corporation with multiple subsidiaries, you can consider developing your own blockchain. Companies that do this usually use Blockchain-as-a-Service (BaaS) providers such as Hyperledger.

Amazon Web Services offers a membership management account in which users can authenticate and authorise individual identities for participation within their blockchain network.

## 5.5.6 Public Blockchain Considerations

### Public Blockchain Considerations

Many options exist for building a project on a public blockchain. Two of the most common include building a dApp for financial or other services and forming a DAO for a collective interest with a distributed form of governance. Building an entirely new public blockchain can also be a possibility, though costs are prohibitive.

### Developing a dApp

Developing a decentralised application (or dApp) on a blockchain such as Ethereum, a proof-of-stake (PoS) blockchain network, is one of the most efficient ways to build and deploy a public blockchain solution and has many benefits (Doyle, 2021):

- **Ownerless apps:** Once the app is deployed on the Ethereum network, anyone can use the dApp, and it cannot easily be taken down.
- **Lack of censorship:** No entity can prevent users from deploying dApps, submitting transactions, or reading data on the Ethereum network.
- **Anonymity:** Users do not have to reveal their identity to use or deploy a dApp.
- **Built-in payments:** Developers can use the native token ETH or their own token for making payments. No third-party payment services are required to be integrated.
- **Cryptographic security:** Cryptography is used to prevent bad actors from forging transactions and enable trust to be placed in smart contract code that self-executes.
- **Plug-and-play capability:** Open-source code enables developers to build new applications on top of existing code infrastructure with ease.
- **Lower possibility of downtime:** The Ethereum network is highly decentralised, and therefore experiencing downtime on the network is less likely compared to centralised systems with single points of failure.
- **Complete data integrity:** Transactions and data stored on the Ethereum blockchain are immutable and transparent to the public.

In addition, developers tend to favour launching new chains and dApps that use a PoS consensus mechanism because of the high hardware costs and limited ability to launch scalable dApps on PoW blockchains. PoS blockchains also reduce the entry barrier for outside participants to become validators, enable more scalable applications to be developed, and give developers greater flexibility over how they can design their blockchains from the protocol layer to the application layer.

If you are developing a dApp on a blockchain like Ethereum, your costs will primarily be concentrated on development, maintenance, and the compliance costs associated with managing a token. Because you are developing your dApp on top of open source code, you can seek to minimise development and maintenance costs by incentivising participants to contribute to your project. Contributors can earn tokens to help identify and fix bugs or could participate in competitions (known as “hackathons”) to develop new features that help make your dApp more appealing for consumers.

## Forming a Distributed Autonomous Organisation (DAO)

The DAO is becoming a frequently used organisational structure for blockchain projects that want to utilise a distributed governance model and involve a collective of members with a similar interest. The costs associated with DAOs are comparable to building a dApp on Ethereum or building a public blockchain. In addition, a DAO is mostly reliant on the smart contract that sets forth the rules on how it will operate—voting processes, for example. Therefore, legal assistance from experts in DAOs is advisable. We will cover many other features of DAOs in Module 6.

## **Building a Public Blockchain**

If you plan to develop your own public blockchain, the costs of validation under consensus mechanisms such as proof of work (PoW) and PoS will be one of your main considerations. As discussed in previous modules, PoW can be prohibitively expensive, demanding specialised hardware and significant computational power for mining, while PoS requires the blockchain's native tokens to be staked and does not demand much hardware beyond a basic laptop.

While PoW has garnered a reputation for being the most highly secure consensus mechanism, and the most decentralised, it frequently cannot achieve the kinds of low-fee, high-transaction throughput necessary for most consumer-facing applications to function at scale. As covered in Module 4, the mining process is also highly energy-intensive, which negatively impacts the environment and will hurt your organisation's ability to remain compliant with environmental, social, and governmental (ESG) regulations.

With energy-intensive processes come prohibitively high costs. Mining hardware and electricity require a facility that can host and power machines. Using bitcoin mining as an example, we can estimate these costs to come to an additional 20% of mining costs or US \$3 million (MiningCrate, 2021). This would bring the total to approximately US \$18 million in upfront and operating expenses to mine a single bitcoin per day.

While this is quite expensive, with earnings of US \$36,000 per day on average (75% profit margin when counting just the cost of electricity), your annual revenue would be US \$13.1 million. This means you can expect to earn a profit within two years when factoring in all other expenses. This, of course, depends on other factors, such as the price of bitcoin, the hashrate, and difficulty adjustment set by the network.

Perform a detailed analysis of mining costs should you consider the PoW protocol.

### **5.5.7 Key Takeaways, References, and Further Exploration**

#### **Key Takeaways**

Let's review the key points of this section:

1. The economics of implementing a blockchain project will be based on two primary economic considerations: revenue models and project costs.
2. Project considerations differ when implementing a public blockchain versus a private blockchain.
3. Both public and private blockchains can support revenue models based on transaction fees and subscriptions.

4. Private blockchains will also support membership fees and data access fees, whilst public ones can generate revenues from token sales.
  5. Revenue is generated differently amongst the three use cases of digital scarcity, payment rail, and distributed ledger.
  6. The cost areas to consider when developing a blockchain include infrastructure (hardware/software), data storage and transfer, legal, development and implementation (including team, maintenance, and support), and usage and maintenance.
  7. One of the key ways that private enterprise blockchains fund the development and maintenance costs is through membership fees. Fees vary depending on industry, number of members, and specific value proposition offered by each network.
  8. If you plan to develop your own public blockchain, one of your main considerations will be costs of validation under consensus mechanisms such as PoW and PoS.
  9. PoW can be expensive, demanding specialised hardware and significant computational power for mining, while PoS requires the blockchain's native tokens to be staked and does not demand much hardware beyond a basic laptop.
10. Developing a decentralised application (or dApp) on Ethereum, a PoS blockchain network, is one of the most efficient ways to build and deploy a public blockchain solution. Benefits include:
- Ownerless apps
  - Lack of censorship
  - Anonymity
  - Built-in payments
  - Cryptographic security
  - Plug-and-play capability
  - Lower possibility of downtime
  - Complete data integrity
11. The establishment of legal entities such as a joint venture can help to mitigate some of the challenges that may arise from IP sharing and ownership.
12. Intellectual property within a blockchain can also be managed using "Smart" IP rights. Smart IP rights essentially enable members to record and control access to certain IP using smart contracts.
13. While smart contracts can serve as a more efficient and secure replacement for a traditional legal contract, they should not be considered a substitute for a legal contract under the court of law, as the outcomes of a smart contract are not always legally enforceable.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 14 April, 2022.

### 5.5.2 Revenue Models

Ledger Insights. (2021, 23 July). Allianz launches blockchain claims solution in 23 countries. <https://www.ledgerinsights.com/allianz-launches-blockchain-claims-solution-in-23-countries>

### 5.5.3 Technical Costs

Acharya, V., Prakash, N., & Yerrapati, A.E. (2019, 6 September). *Oracle Blockchain Quick Start Guide: A practical approach to implementing blockchain in your enterprise*. Packt Publishing.

Holbrook, J. (2020, 11 February). *Architecting Enterprise Blockchain Solutions*. Sybex.

Petrashchuk, H. (2018, 16 March). How Much Does It Cost To Hire A Blockchain Developer? You Team. <https://youteam.io/blog/how-much-does-it-cost-to-hire-a-blockchain-developer>

### 5.5.4 Legal Costs

Clark, B., & McKenzie, B. (2018, February). Blockchain and IP Law: A Match made in Crypto Heaven? *World Intellectual Property Organization*. [https://www.wipo.int/wipo\\_magazine/en/2018/01/article\\_0005.html](https://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html)

Etherisc. (2021, 16 August). Etherisc Update: Etherisc and Acre Africa Announce First Payouts through blockchain based platform with over 17,000 Kenyan Farmers insured during First Season. <https://blog.etherisc.com/etherisc-update-etherisc-and-acre-africa-announce-first-payouts-through-blockchain-based-platform-a0c5194214f4>

Litan, A. (2020, 3 March). Smart Contracts are Neither Smart nor are they Contracts. *Gartner*. <https://blogs.gartner.com/avivah-litan/2020/03/03/smart-contracts-neither-smart-contracts>

Neuburger, J.D., Choy, W.L., & Milewski, K.P. (2019). Smart Contracts: Best Practices. Practical Law. <https://prfirmppwwwcdn0001.azureedge.net/prfirmstgacctpwwwcdncont0001/uploads/dc2c188a1be58c8c9bb8c8bab91bbac.pdf>

### 5.5.5 Private Blockchain Considerations

GoDirect Trade. (n.d.). Frequently Asked Questions (FAQs). <https://www.godirecttrade.com/faq>

Johnson, E. (2019, 19 August). Maersk works to monetize TradeLens. *The Journal of Commerce* [https://www.joc.com/technology/maersk-works-monetize-tradelens\\_20190819.html](https://www.joc.com/technology/maersk-works-monetize-tradelens_20190819.html)

### 5.5.6 Public Blockchain Considerations

Doyle, M. (2021, 18 February). Building A Decentralized Future With dApps. Next Big Thing Academy. <https://theworldwecreate.net/insights/building-a-decentralized-future-with-dapps>

MiningCrate. (2021). Fully Loaded Mining Farm. <https://www.miningcrate.com/pages/%F0%9F%92%B1-paid-challenges-open-now-%F0%9F%92%B1>

Morris, N. (2019, 29 January). The cost of enterprise blockchain membership. *Ledger Insights*. <https://www.ledgerinsights.com/enterprise-blockchain-cost>

### 5.5.7 Key Takeaways, References, and Further Exploration

Takyar, A. (2019, 11 December). How to determine the cost of blockchain implementation. LeewayHertz. <https://www.leewayhertz.com/cost-of-blockchain-implementation>

## Further Exploration

We can broadly outline the dApp development sequence as follows (Takyar, 2019).

- **Design:** Creating a blueprint for a prototype, user interface specifications, user experience design, wireframes, application user flow, and so on.
- **Development:** Writing software, refining, and testing.
- **Deployment:** Deploying applications on blockchain networks, Android or Apple, or cloud platforms.
- **Migration:** Migrating existing applications systems to the blockchain network (mostly applicable for intrapreneurs not building a business from the ground up).
- **Maintenance:** Performing upgrades and updates along with running tests to make sure the application performs smoothly.
- **Integration:** Integrating the application into your existing or new IT architecture, or using third-party tools to integrate cloud hosting and storage services, notification systems, and collaboration tools.

# 5.6 Fundraising Strategies

## 5.6.1 Overview

### Overview

In this section, you will learn about strategies that organisations and entrepreneurs use to fund their blockchain projects and startups. You will also learn about the strategies deployed to launch a successful crowdfunding campaign, in addition to the risks and considerations associated with issuing tokens.

### Vocabulary Check

This section introduces the following terms.

- [crowdfunding](#)
- [crypto custody](#)
- [governance token](#)
- [security token](#)
- [utility token](#)
- [venture capital](#)

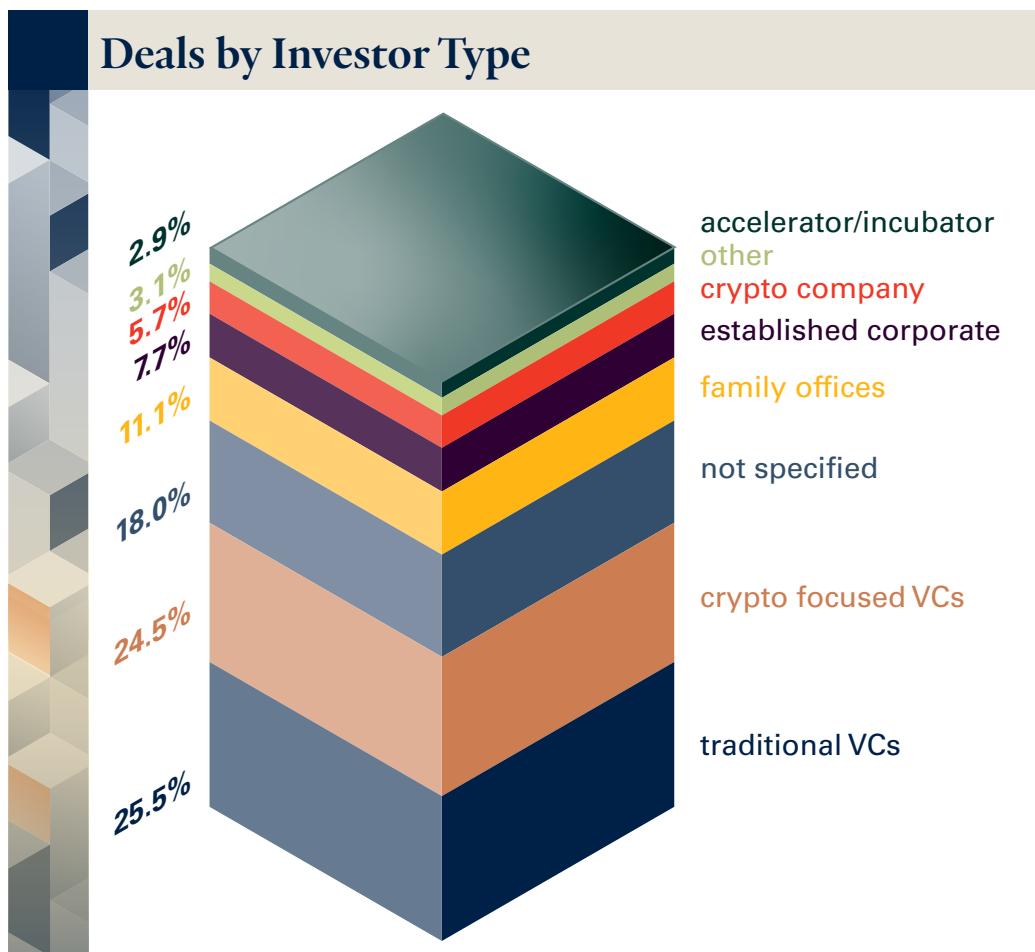
## 5.6.2 Venture Capital for Blockchain Projects

### Venture Capital for Blockchain Projects

Although initial coin offerings (ICOs) originally commanded the most funding for innovation and growth in blockchain technology, intense regulatory scrutiny of ICOs has since shifted dominance in the field to venture capital (VC). Venture capital plays a major role in both entrepreneurial and enterprise (intrapreneurial) blockchain projects, even during periods of depressed valuations:

- **VC deals.** According to Cointelegraph Consulting's Blockchain Venture Capital Report for 2020, 942 venture capitalists have invested in over 2,700 private equity deals involving startups and

enterprise projects in the blockchain space since 2012 (Cointelegraph Consulting, 2021). Over US \$7 billion has been raised by blockchain startups in the first six months of 2021 (Browne, 2021).



- **Banks.** Blockdata reported that 55 out of the world's top 100 banks, ranked by assets under management (AuM), have invested in cryptocurrency and blockchain companies in the first seven months of 2021. The following table shows the top five banks by funding size and their investment summaries (Wouters, 2021):

Company	HQ	Number of Investments	Size of Funding Round
Standard Chartered	London, UK	6	US \$380M
BNY Mellon	New York, US	5	US \$321M
Citibank	New York, US	14	US \$279M
UBS	Zurich, CH	5	US \$266M
BNP Paribas	Paris, FR	9	US \$236M
<b>Total</b>		39	US \$1,482M

- **Crypto custody.** Fintechnews Switzerland further reports that Barclays in New York, with 22 investments, was the most active investor (2021). The report also showcased the crypto custody

aspect of bank investments, as 23 of the top 100 banks, ranked by AuM, were active in this space. With crypto custody, banks provide storage and security services for digital assets, primarily for institutional investors such as hedge funds.

- **Investor type.** The following chart provides an overview of blockchain investor types in 2020 (Cointelegraph, 2021). Just over 25% were traditional VCs, with crypto-focused VCs making up an additional almost 25%.
- **Funding by country.** Lastly, in its Blockchain Report 2020, CB Insights provides a breakdown of funding by country from 2015 to 2019. The United States ranks first with 51%, followed by China and Switzerland, whose combined total is around 24%.

## SAFTs

A simple agreement for future tokens (SAFT) is an investment contract that enables developers and cryptocurrency startups in the US to raise funds from accredited investors without violating securities laws. The framework allows for companies to sell a SAFT to receive funds in exchange for issuing documentation to the investor stating that they will receive a cryptocurrency at some point in the future if one is created (Peters, 2021).

### 5.6.3 Enterprise Blockchain Funding

#### Enterprise Blockchain Funding

For enterprise or intrapreneurial blockchain projects, funding typically comes from an organisation's capital or cash flow. It is only when a project has the potential to be sold or used by other companies that it can be spun off from its corporate parent and receive venture capital funding. Industry consortiums like TradeLens or Pharmaledger are created separately as their own companies, typically as joint ventures, where founding members of the consortium fund the project. Pharmaledger has also received government funding because of its potentially significant role in healthcare. For the typical, small single case experiment inside an enterprise, however, companies usually cover the costs from their IT budgets.

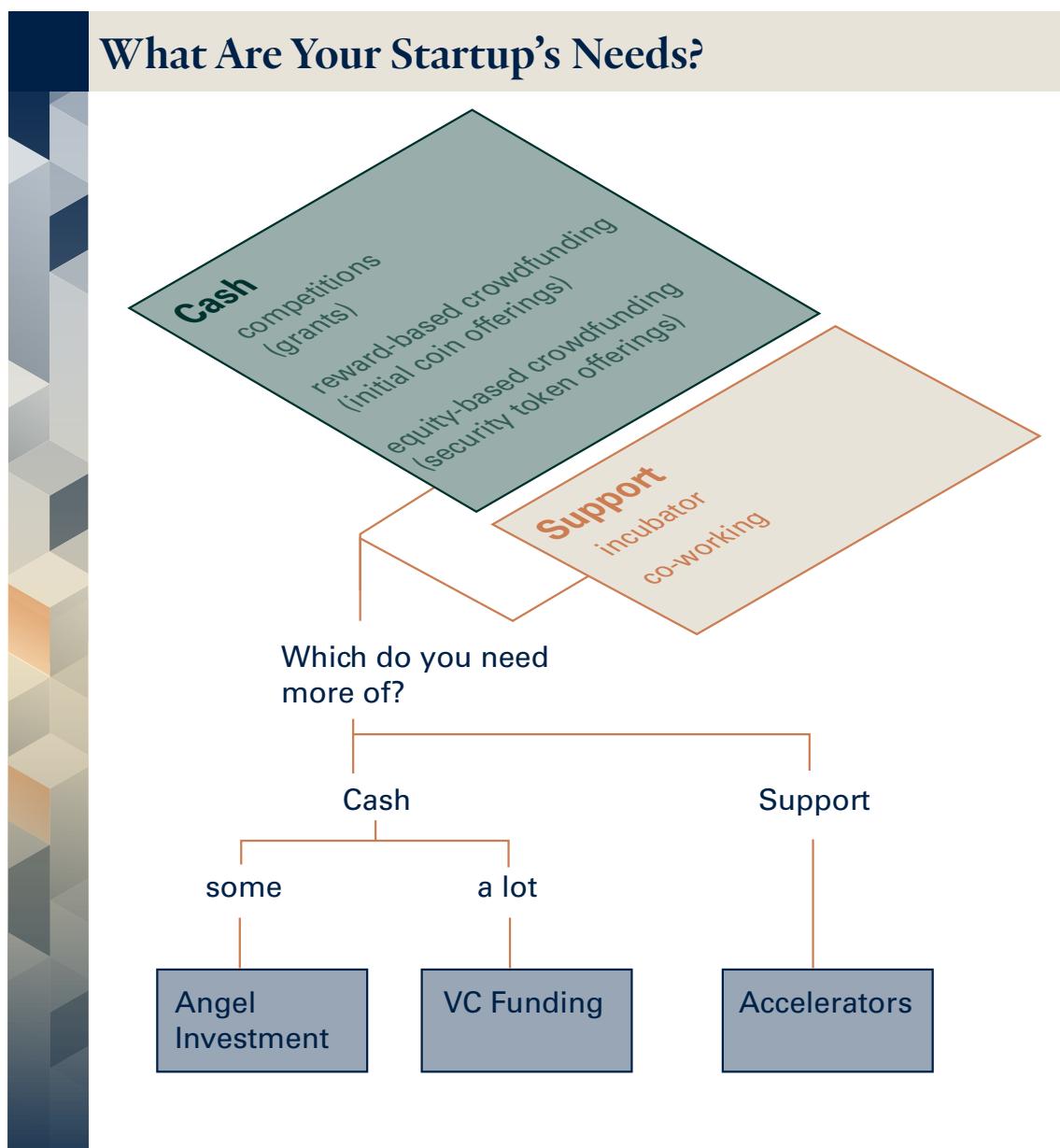
But what about enterprise blockchain startups, an area that was growing strongly in 2018? According to CB Insights, a technology research firm, the funding for enterprise blockchain startups in 2019—US \$434 million, with US \$200 million being raised by Ripple alone—paled in comparison to non-enterprise blockchain funding, which garnered US \$2,356 million (CB Insights, 2020). The consultancy noted that this disparity in funding for enterprise blockchains, which it defines as “software for enterprise processes excluding the management, custody, or trading of cryptocurrencies”, partially reflected the “coordination problem” that multi-stakeholder blockchain consortiums often face (CB Insights, 2020).

## 5.6.4 Evaluating Your Blockchain Startups Funding Needs

### Evaluating Your Blockchain Startup's Funding Needs

As with any startup, funding sources for blockchain startups vary depending on what stage the business is in and what type of support it needs to get to the next level. The decentralised and community-driven nature of the blockchain space has enabled startups to take advantage of multiple fundraising options and be more flexible in choosing when to take in VC funding, if at all.

When deciding which fundraising option to pursue, startups must determine whether to prioritise receiving cash (in small or large quantities, such as through angel or VC funding) or support via incubators or accelerators. Both options come with their own benefits and drawbacks.



## Common Alternative Funding Sources

Blockchain entrepreneurs commonly, but not always, pursue the following funding sources prior to VC funding:

### Accelerators

Although not the most common method of fundraising in the blockchain industry, accelerators can offer both funding and strategic support (such as network, resources, and mentorship) to startups. Typically, accelerators in the blockchain space are started by blockchain protocols that wish to encourage developers to build projects in their ecosystem. In exchange for providing grants, support, and technical advice, these protocols facilitate organic growth within their network. Popular accelerators include ConsenSys Labs, Binance Labs, and Tribe Accelerator.

Startups can benefit from joining an accelerator if they are in the pre- or post-seed funding stage and are looking to join a network that offers complimentary dApps they can use to access their target customers. Traditional accelerators like Techstars or Y Combinator, which are not supported by a blockchain network, prefer to take equity in the startups they are funding and supporting as opposed to requiring the startup to build in any particular blockchain.

### Incubators

Incubators provide promising projects with the ability to build, network, and collaborate with industry experts virtually or within a physical office space. While incubators and accelerators offer similar services, incubators generally do not offer funding. They do offer strategic support, networking, and even physical office space to promising projects. Many governments, universities, and corporations offer incubators, including R3's Venture Development Program and Singapore's government-backed LongHash.

### Network Supported Funds (Grants)

Existing blockchain networks set up grant programs for the purpose of bootstrapping projects within their own network to facilitate its expansion. Examples include:

- Borderless capital (previously known as Algo Capital) funds products that drive access and adoption to the Algorand blockchain network.
- The Dash Investment Foundation funds traditional businesses through the Dash DAO.
- Gitcoin funds projects in the Ethereum ecosystem.

## 5.6.5 Crowdfunding

### Crowdfunding

One of the unique aspects of building a blockchain startup is the ability to leverage the technology to gain instant access to retail investors via token-based crowdfunding models. Crowdfunding in the blockchain industry is normally associated with the offering of tokens to both accredited and non-accredited investors via multiple fundraising models.

Raising capital via crowdfunding is designed to be transparent, efficient, and accessible to a wide audience without the need for intermediaries like lawyers or underwriters. The blockchain project issues digital tokens that represent shares in the project to investors residing anywhere in the world. Rules are coded into the smart contract that execute the distribution of tokens, such as lock-up periods for startup founders or special voting rights for owners.

Crowdfunding faces drawbacks connected to a lack of regulatory certainty, the need to build and constantly manage a community, and the potential for investors to be very short-term in their support of the token. Instant access to liquidity can lead to extreme volatility and loss of value if the project does not meet expectations or there is a shift in market sentiment. Additionally, lack of strategic, technical and promotional support from retail investors may make execution of the project difficult even with a large source of funding.

### Crowdfunding Models

Crowdfunding models differ by the cost and time it takes to fundraise and by the level of required regulatory compliance.

**Initial coin offering (ICO).** An ICO is a form of token-based fundraising that was popularised by the Ethereum network in 2017 and 2018. To launch an ICO, developers code a smart contract to create a type of token known as an ERC-20 token, which is then distributed to investors who purchase the token in exchange for ETH. The stated purpose of these ERC-20 tokens varies by project. However, they are typically designed to offer some type of utility within the dApp or protocol the project is launching. For example, Filecoin is used to pay for cloud data storage space on Filecoin's peer-to-peer network.

ICOs have come under scrutiny due to the high volume of fraudulent projects in 2017 and 2018, and suffer from the same drawbacks as other crowdfunding models. ICOs are typically launched through non-profit foundations, with the funds being collected and managed by a DAO that the foundation supports.

**Initial exchange offering (IEO).** IEOs are a variation of ICOs in which blockchain startups partner with centralised exchanges to vet and launch the project's tokens to their audience. IEOs emerged as a solution to the high volume of fraudulent ICOs that were being launched by anonymous teams with copy-pasted whitepapers and fake promises about the potential of their projects. Exchanges like Binance and Bitfinex began operating as intermediaries between the projects and retail investors,

conducting due diligence on behalf of investors to ensure the teams and projects were trustworthy before listing their tokens. This fundraising method has also come under scrutiny from investors and regulators who have accused the exchanges of being complicit in the promotion of fraudulent IEOs (SEC, 2020).

**Initial DEX offering or initial DeFi offering (IDO).** Unlike IEOs, IDOs are essentially a permissionless form of fundraising because they allow founders to list their tokens on any decentralised exchange (DEX). IDOs have become increasingly popular as DeFi and DEXes have grown to attract more capital from retail investors. Through an IDO, founders launch their token on a DEX or by creating a liquidity pool on Uniswap, a popular DeFi app network, and a small percentage of the tokens are released to the market to initiate price discovery. Although this method creates a lower barrier to entry for founders looking to raise capital, it also brings back the same challenges that come from a lack of vetting new projects. As a result, launchpad platforms have emerged, such as Polkstarter, DAO Maker, and PAID Network, that help to vet the quality of IDOs and investors to make sure they are complying with KYC/AML laws.

**Security token offering (STO).** STOs are essentially ICOs that occur under a strict regulatory framework. This means that tokens are issued with the intention of being labelled as registered securities and are therefore only available to accredited investors in certain markets, who must go through a KYC/AML process to invest. While STOs are more costly and take longer to launch, their clear regulatory status makes them more attractive to institutional investors. Popular platforms for launching STOs include Polymath, Harbor, and Securitize.

## Legal Implications for Issuing Tokens

The most important legal consideration to make when issuing tokens is determining whether the tokens classify as a utility or a security. A utility token is a token or cryptocurrency that has some form of functionality within the blockchain network it inhabits. An example is UNI, a token created by the decentralised exchange Uniswap that allows holders to vote on proposals made by the community. This type of token is also referred to as a governance token. By contrast, security tokens are tokens that explicitly represent an investment contract, similar to a stock or bond.

The most common framework for classifying whether a token is a security or utility is the Howey Test, created by the SEC in 1946 to determine whether a transaction is considered a security. The Howey Test uses the following criteria (Reiff, 2021):

- There is an investment of money.
- There is an expectation of profits.
- The investment of money is in a common enterprise.
- Any profit comes from the efforts of a promoter or third party.

To avoid having a token be classified as a security, issuers must consider the following questions:

- What is the stated purpose of the token? Are statements made that could imply a promise of future profits for buyers?
- What is the distribution mechanism of the tokens? How many tokens will the founding team hold compared to the community?
- Is the blockchain network already built with user adoption prior to issuing the token?

Any project interested in launching its own token should consult legal counsel on these matters.

## Strategy for Successful Crowdfunding

To successfully launch a fundraising plan and raise funds for token distribution, token issuers should follow these steps:

1. Outline the value proposition.
2. Develop a whitepaper.
3. Design the “tokenomics”.
4. Create token distribution plan.
5. Build a community and spur engagement.
6. Optimise fundraising strategies for ease of access to tokens.

More details on this crowdfunding strategy are available in the Further Exploration section at the end of this module.

## 5.6.6 Angel Funding, Mergers and Acquisitions, and Corporate VC Funding

### Angel Funding, Mergers and Acquisitions, and Corporate VC Funding

Other funding options for blockchain entrepreneurs include angel funding, mergers and acquisitions (M&As), and corporate VC funding.

**Angel investing** (also known as angel funding or angel financing). This category of investors includes both institutions and friends and family. This group normally provides the first round of funding to help support the development of a minimum viable product or to scale an existing product that is beginning to show signs of traction. A typical angel investment is between US \$15,000 and US \$250,000 (Upcounsel, n.d.). Angel investors funding crypto-based startups can follow the SAFT method, invest in the company’s equity, or both.

As a founder, it is important to select angel investors who can provide not only capital but also strategic support in terms of marketing, product development, or follow-up rounds of funding. Blockchain startups typically look for high-profile influencers and opinion leaders to fund their projects to establish early credibility. .

**Mergers and acquisitions (M&As).** M&As have become a common alternative to traditional fundraising as crypto companies look to capture market share and expand their operations more quickly by acquiring other crypto companies with valuable technology or talent that is still difficult to obtain. Two examples include Binance's acquisition of CoinMarketCap, a large data aggregator of cryptocurrencies, and Tron's acquisition of BitTorrent, an Ethereum competitor and one of the largest providers of Torrent software. Facebook, a non-crypto company, acquired Chainspace, a smart contract research firm.

**Corporate VC funding.** This group of investors includes corporations looking to gain exposure to the blockchain space through a strategic investment in an outside company, which they may acquire at a later point as a way to integrate blockchain technology into their organisation. Overstock is one of the earliest examples of a corporation funding a blockchain project. The company created a subsidiary called Medici Ventures with the goal of funding blockchain-related companies.

## 5.6.7 Key Takeaways, References, and Further Exploration

### Key Takeaways

Let's review the key points of this section:

1. **Venture capital** funding is the predominant funding source for blockchain startups and a major funding source for enterprise projects.
2. **Enterprise** projects also utilise OpEx and CapEx as traditional funding sources.
3. **Accelerators, incubators, and network grant programs** are alternative ways to receive monetary and strategic support.
4. **Crowdfunding** by issuing tokens is another fundraising option, with different models requiring different time, cost, and levels of compliance. ICOs, IEOs, IDOs, and STOs all have benefits and drawbacks to consider.
5. **Angel funding** includes institutions as well as friends and family, raising money, and building strategic support and early credibility.
6. **Mergers and acquisitions** are another way to quickly capture market share and expand operations to acquire talent or technology. Firms may also invest in a company they may choose to acquire at a later point.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 14 April, 2022.

### 5.6.2 Venture Capital for Blockchain Projects

Browne, R. (2021, 22 July). Blockchain start-ups raised a record \$4.4 billion in the second quarter despite the slump in crypto prices. *CNBC*. <https://www.cnbc.com/2021/07/22/blockchain-start-ups-raise-record-funding-despite-crypto-slump.html>

CB Insights. (2020, March). The Blockchain Report 2020. <https://www.statista.com/statistics/1235117/worldwide-blockchain-funding-by-geography>. Original report: [https://www.tagonline.org/wp-content/uploads/2020/05/CB-Insights\\_Blockchain-Report-2020.pdf](https://www.tagonline.org/wp-content/uploads/2020/05/CB-Insights_Blockchain-Report-2020.pdf)

Cointelegraph Consulting. (2021). Blockchain Venture Capital Report. *Cointelegraph Consulting*. <https://mercuryredstone.com/wp-content/uploads/2021/04/Cointelegraph-consulting-venture-capital-report.pdf>

Fintechnews Switzerland. (2021, 25 August). 55% of World Top Banks Have Invested in Blockchain and Crypto Companies. *Fintechnews Switzerland*. [https://fintechnews.ch/blockchain\\_bitcoin/55-of-world-top-banks-have-invested-in-blockchain-and-crypto-companies/48147](https://fintechnews.ch/blockchain_bitcoin/55-of-world-top-banks-have-invested-in-blockchain-and-crypto-companies/48147)

Peters, K. (2021, 1 July). Simple Agreement for Future Tokens (SAFT). *Investopedia*. <https://www.investopedia.com/terms/s/simple-agreement-future-tokens-saft.asp>

Wouters, S. (2021, 4 August). Top Banks Investing in Crypto & Blockchain Companies. *Blockdata*. <https://www.blockdata.tech/blog/general/banks-investing-blockchain-companies>

### 5.6.3 Enterprise Blockchain Capital

CB Insights. (2020, March). The Blockchain Report 2020. [https://www.tagonline.org/wp-content/uploads/2020/05/CB-Insights\\_Blockchain-Report-2020.pdf](https://www.tagonline.org/wp-content/uploads/2020/05/CB-Insights_Blockchain-Report-2020.pdf)

Holbrook, J. (2020, 11 February). Architecting Enterprise Blockchain Solutions. <https://www.amazon.com/Architecting-Enterprise-Blockchain-Solutions-Holbrook/dp/1119557690>

### 5.6.4 Evaluating Your Blockchain Startup's Funding Needs

Perlman, D. (2016, 21 March). From Accelerators to Venture Capital: What is best for your startup? *Gust*. <https://blog.gust.com/from-accelerators-to-venture-capital-what-is-best-for-your-startup>

## **5.6.5 Crowdfunding**

Reiff, N. (2021, 5 July). Howey Test. *Investopedia*. <https://www.investopedia.com/terms/h/howey-test.asp>

SEC. (2020, 14 January). Initial Exchange Offerings (IEOs) – Investor Alert. *U.S. Securities and Exchange Commission*. <https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia-initialexchangeofferings>

## **5.6.6 Angel Funding, Mergers and Acquisitions, and Corporate VC Funding**

Upcounsel. (no date). How Much Do Angel Investors Usually Invest? *Upcounsel*. <https://www.upcounsel.com/how-much-do-angel-investors-usually-invest>

## **5.6.7 Further Exploration**

Terehin, A. (no date). 10 Best ICO White Paper Examples. *Agente*. <https://agentestudio.com/blog/10-best-ico-white-paper-examples-structure-and-design>

The Blockchain Writer. (2020, 25 September). How to Write a Blockchain White Paper. *The Blockchain Writer*. <https://theblockchainwriter.com/f/how-to-write-a-blockchain-white-paper>

Watkins, R. (2021, 17 May). Messari: Initial Token Allocations for Public Blockchains. *@RyanWatkins\_*. [https://twitter.com/RyanWatkins\\_/status/1394283802009145348](https://twitter.com/RyanWatkins_/status/1394283802009145348)

## **Further Exploration**

### **Detailed Strategy for Crowdfunding a Token Distribution**

To successfully launch a fundraising plan and raise funds for token distribution, token issuers should follow these steps. Lead with your project's value proposition, and let potential investors understand why they should read the whitepaper and consider investing in the project.

STEPS	DESCRIPTION	SUPPORTING STEPS
1 Outline your value proposition	<p>Answer these questions:</p> <ul style="list-style-type: none"> <li>• What problem are you trying to solve within the blockchain ecosystem or in the traditional business world?</li> <li>• How is your solution different from competitors?</li> <li>• Do you have any traction so far (e.g., user adoption, total value locked for DeFi projects, etc.)?</li> <li>• Do you have developers, advisors, or investors on your team who have prior experience building successful blockchain businesses?</li> </ul>	---
2 Develop a whitepaper	<p>A whitepaper is your project's formal documentation that outlines the value proposition, the technical details for executing the project, and the token's economics, or "tokenomics".</p>	<p>The standard outline for a whitepaper is as follows (The Blockchain Writer, 2020):</p> <ul style="list-style-type: none"> <li>• Executive Summary</li> <li>• Introduction</li> <li>• Current Industry Problems</li> <li>• Solution (value proposition)</li> <li>• Tokenomics</li> <li>• Allocation of Funds Raised from the ICO</li> <li>• Team and Advisors</li> <li>• Web Presence</li> <li>• References</li> <li>• Disclaimers</li> </ul> <p>In the references below, you can view 10 top examples of whitepapers from projects that launched ICOs (Terehin, n.d.)</p>

STEPS	DESCRIPTION	SUPPORTING STEPS
3 Design Tokenomics	<p>Tokenomics (or token economics) is defined as the economic incentive models (including distribution and rewards) created within a blockchain through the use of tokens or cryptocurrencies (Anatha, 2021).</p> <p>While tokenomic models may differ between blockchains, blockchains like Bitcoin, Ethereum, Cardano, and others have adopted a common set of models.</p>	<ul style="list-style-type: none"> <li>In a <b>deflationary model</b>, tokens have a maximum supply that is never increased. Examples include Bitcoin and Cardano.</li> <li>In an <b>inflationary model</b>, tokens increase in supply over time based on algorithmic rules or through factors such as supply and demand. Examples are Ethereum and EOS.</li> <li>In a <b>dual-token model</b>, two tokens exist within a single blockchain. One serves as a store of value, and the other serves as a utility. An example is Terra, which has LUNA and UST.</li> <li>In an <b>asset-backed model</b>, tokens are backed by underlying assets, such as fiat currencies, commodities, or other cryptocurrencies. Examples include Tether (USDT) and DAI.</li> </ul>
4 Create a Token Distribution Plan	<ul style="list-style-type: none"> <li>Signal to the public how decentralised you aim to make your project.</li> <li>Determine your pre-mining parameters. Pre-mining is the process of creating tokens to be allocated to insiders of your company (founders, developers, early investors) prior to releasing them to the general public. Note that pre-mines that allocate a large portion of the total supply to insiders are often criticised in the crypto space as being antithetical to the ethos of decentralisation and community-driven networks.</li> <li>Create transparency in the token distribution process.</li> <li>Be cautious if the majority of tokens are held by a few insiders, as this may be a signal to markets of an early investor token offload and might alert regulators to the potential of an unregulated security.</li> </ul>	<p>Utilise more organic and merit-based strategies for issuing tokens such as:</p> <ul style="list-style-type: none"> <li>Only allow new tokens to be issued through a PoS or PoW mining process, meaning that anyone who is willing to stake or mine the cryptocurrency will earn the newly issued tokens. (Satoshi launched bitcoin in this way.)</li> <li>Airdrop a large percentage of the total supply of tokens to users who adopted the platform early, then enable those users to stake their tokens or provide liquidity to users who wish to earn fees in the form of more tokens (a process known as “yield farming”).</li> <li>Launch contests or bounties that encourage people to identify bugs, create marketing content, or contribute to your blockchain in other ways to earn tokens as a reward.</li> </ul>

STEPS	DESCRIPTION	SUPPORTING STEPS
5 Build a Community and Spur Engagement	<p>Popular platforms for building and engaging with your community include Twitter, Telegraph, Discord, and Youtube.</p> <p>You can also drive engagement using token reward incentives such as giveaways and bounties.</p>	---
6 Optimise Fundraising Strategies	<p>Identify strategic influencers, industry partners, and investors.</p> <p>Consider partnering with centralised exchanges to make it easy for the public to purchase your tokens with their credit card or bank account.</p>	---

# 5.7 Challenges to Blockchain Adoption

## 5.7.1 Blockchain Adoption Challenges

### Overview

Every new technology faces adoption challenges. Some of these challenges stem from concerns about the maturity of the new technology, including whether and when the technology will provide promised benefits. As systems move increasingly online and interactions become digital, questions about privacy and intellectual property (IP) can arise.

For intrapreneurs, introducing blockchain technology into an existing organisation comes with additional concerns. These range from objective factors, such as lack of technical feasibility, to more subjective factors, like concerns about job security or general resistance to change.

In this section, we will explore examples of challenges to blockchain acceptance within an organisation and how to overcome these challenges.

### Faculty Video: Blockchain Adoption Challenges

In this video, Professor Martin Schmalz highlights the challenges to consider when adopting blockchain technology, including the costs, security risks and the difficulties of getting other stakeholders to join your blockchain network.



So as you assess the viability of your use case, it is always important to ask whether one really needs blockchain features and if the problem you're trying to solve could also be solved with an alternative, perhaps cheaper, and simpler technology. A blockchain should not be viewed as just another add-on feature to your business. And like other disruptive technologies, such as AI or machine learning, implementing blockchain features can fundamentally change the nature of your business from one that is centralised to one that is decentralised and distributed.

As a result, your organisational structure may need to be altered or adopted to accommodate the integration of this new technology and new forms of shared governance. So let's look into that. Additionally, changes to your database architecture will be resource intensive and may require a more specialised technical team to manage. In certain cases, the use of smart contracts could replace traditional legal processes with codified laws.

This is a feature that lacks full regulatory clarity and could lead to complications between members if not supported by underlying traditional legal contracts. Transactions on a blockchain will be permanent unless consensus can be achieved by a majority of nodes on a network to effectively roll back a transaction, as we have learned. Now this will be rather more challenging to accomplish compared to having a complete authority over your database.

So that's, of course, a feature of the technology that can also be a limitation or challenge. Furthermore, due to the limited number of nodes controlled by a handful of entities, there is a debate about whether private permissioned ledger is technically any more secure than a standard centralised database. At the same time, public permissionless ledgers have many of their own flaws, including consensus mechanisms that consume massive amounts of energy are vulnerable to centralisation and are subject to security failures from 51% attacks, for example.

There are also concerns about the pseudonymous nature in which data is stored and shared on a public network, in addition to the lack of clear distinction between public key addresses engaging in legal activity and those associated with money laundering or other financial crimes. While blockchains can potentially help companies increase the security transparency and integrity of data shared between stakeholders, they can also add significant maintenance costs, may compromise performance, and inhibit scalability.

So all of these factors may result in less of a competitive advantage for companies than one might hope when considering a blockchain solution, at least if not properly taken into consideration before jumping into action.

## Vocabulary Check

This section introduces the following terms.

- [application programming interface \(API\)](#)
- [software development kit \(SDK\)](#)

### 5.7.2 Technology Maturity

#### Technology Maturity

Obstacles that face both intrapreneurs and entrepreneurs include resistance to new technology, concerns about how quickly a blockchain solution can produce tangible benefits, and questions surrounding privacy and IP.

#### Resistance to New Technology

A critical factor in managing resistance to blockchains is in creating awareness amongst current and future stakeholders of where the technology exists in its journey to mainstream adoption. If the technology is too early in its adoption cycle for tangible benefits to be obvious, gaining traction among your organisation or potential investors may be difficult. Managers or investors who believe that a solution has been proposed too late could also resist adoption.

## Guest Video: Barriers to Enterprise Adoption of Blockchain Technology

In this guest speaker video, Robert Viglione speaks about the maturity of blockchain technology and how this can affect the adoption of blockchain solutions.



Thus far the biggest barrier I would say, the most important barrier early on, say over the last 10 years, has been immature products and just very new technology. This can be looked at in the life cycle of how other technologies, important technologies, have come to the marketplace. Initially, they're products and platforms built by geeks for geeks, that's the way we look at it. But then eventually you cross over this boundary where you start productising these things and really thinking from a market perspective about usability, about actual problems that you're solving in the market. And not just building cool technology for the sake of cool technology, but actually solving real problems.

And in the process of solving the real problems you build the user interfaces. You build the products that are actually designed for the customers, the end users, whether they're retail or enterprise clients. And thus far as an industry, we've really just started crossing over that boundary of thinking about tangible real problems for solving, and tangible real customers that come from outside of our industry such as enterprises.

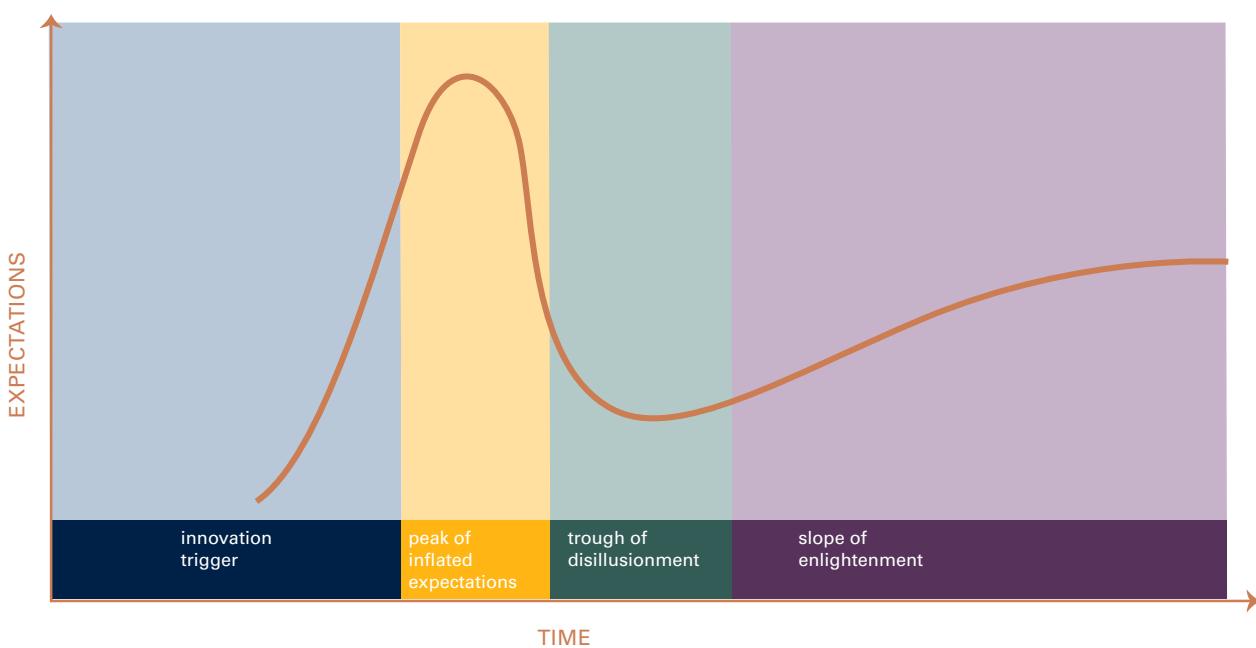
Because really the first set of abusers of our industry, and the first set of use cases, came endogenously or internal to crypto and things like decentralised finance, things like smart contracting, they were solving purely digital domain problems. But now as we're crossing over and solving real problems in the supply chain as an example for companies out there outside of our industry, we really need to think about making the technology much more accessible and usable. So I would classify this is that central problem that many companies like Verizon Labs are focusing on.

## Gartner Hype Cycle

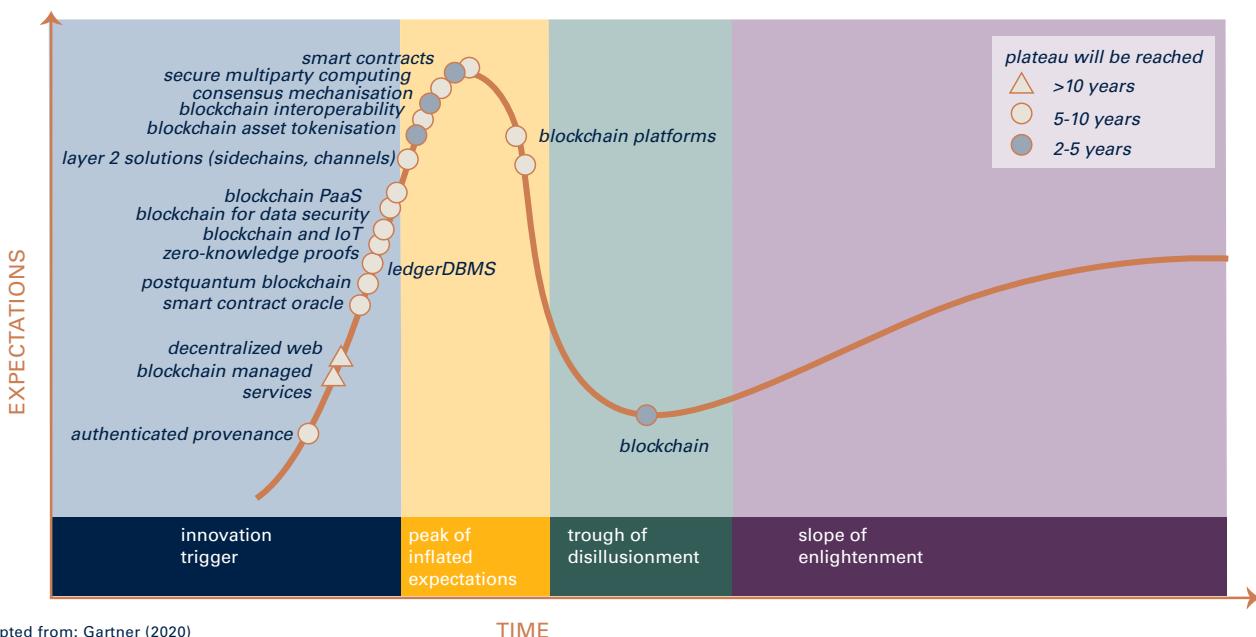
The Gartner Hype Cycle provides a graphic illustration of the ways that expectations change around emerging technologies and applications (Benjamin, 2021). The cycle passes from the initial “innovation trigger” through periods of inflated expectations, disillusionment, enlightenment, and finally, productivity.

A 2020 report shows the positions of different aspects of blockchain technology on the Hype Cycle, with blockchain as a whole currently midway through the “trough of disillusionment” and two to five years from productivity (Benjamin, 2021). Some specific aspects of blockchain technology, including smart contracts, are currently in the realm of inflated expectations, while others, including zero-knowledge proofs, dApps, and a decentralised web, are still in the innovation trigger stage. When you pitch a blockchain use case to potential investors or an internal team, you should know where the technology falls on the Hype Cycle.

## The Hype Cycle



## Blockchain Hypecycle



Adapted from: Gartner (2020)

## Timely and Tangible Benefits

Many organisations and investors assume that a blockchain solution will immediately produce commercial benefits, without taking into account factors such as testing different blockchain as a service (BaaS) providers, evaluating the pros and cons of using a public or private blockchain, developing a legal framework alongside the pilot, and the ability to convince industry stakeholders to join your blockchain and participate in the pilot. A study by the CCAF reports that 62% of discontinued enterprise blockchain projects cited the inability to realise tangible benefits as a major reason for discontinuation (Rauch et al., 2019).

A blockchain project typically takes up to 25 months to fully execute from initial exploration to production, with benefits typically arriving at the production stage.

At the onset, companies should focus on single use case solutions with clearly defined outcomes. The first use case for blockchain technology was Bitcoin, while the internet's first commercial use case was email (Iansiti & Lakhani, 2017). In designing your blockchain solution with a single use case in mind, you narrow the scope of what needs to be delivered and can more easily manage expectations.

Maersk and IBM launched TradeLens with a simple pilot that used Maersk's ships to transport shipments from three firms through a single trade lane. The pilot allowed Maersk and IBM to test multiple critical assumptions, and then to alter their strategy from a single blockchain platform to an industry-wide network.

## Privacy and IP

Both intrapreneurs and entrepreneurs may face resistance from organisations and funders who have concerns about privacy and intellectual property. Zero-knowledge proofs have begun to show promise as a way to protect data privacy on blockchains. However, because this technology is still experimental, most vendors are relying on private blockchains on which they can easily restrict transaction visibility from the outside world.

### 5.7.3 Job Security

#### Job Security

Intrapreneurs who propose blockchain technology solutions face additional hurdles. Even if an organisation's management is comfortable with the state of a new technology, individual employees may have concerns about job security. For blockchain, these concerns can centre among accounting, legal, and operations departments.

However, while blockchain technology has the potential to make many business processes more efficient, blockchain technology is too early in its adoption cycle to replace standard accounting, legal, or operational practices or the employees and executives in these roles. For example, legal and financial personnel will remain necessary: smart contracts are not always legally enforceable, and internal control over financial reporting (ICFR) standards currently do not recognise smart contracts as a viable technology for facilitating financial reporting (BDO, 2019). Additionally, while blockchain technology advances have outpaced regulations in most countries, financial reporting requirements will likely remain the same.

Companies considering blockchain technology can ensure that activities in the blockchain network fit into a traditional legal and accounting framework. Financial roles could be valuable in helping to translate blockchain-based activities into more traditional accounting standards, as they seek to mitigate financial reporting risks and communicate to individuals and groups about ways blockchain

technology offers greater transparency and traceability of financial records (Deloitte, 2020). For joint ventures, legal and financial personnel might answer questions around whether all transactions within the network constitute financial activities performed by the joint venture and whether each individual organisation is responsible for reporting transactions that occur within the network on their balance sheet in addition to the joint venture's balance sheet.

## 5.7.4 Coordination Across Departments

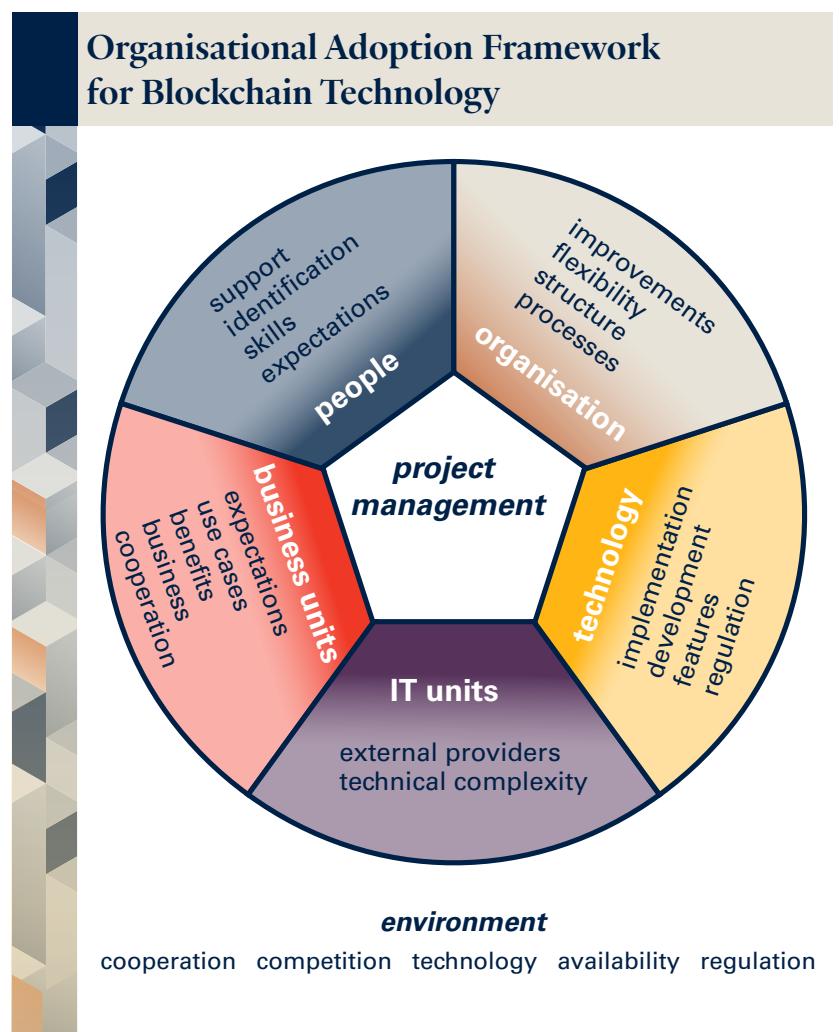
### Coordination Across Departments

Internal challenges to adoption can also stem from a lack of coordination across departments. Businesses must make sure that a blockchain solution becomes not only a part of the organisation's IT infrastructure but also a part of the overall organisational structure.

ProcessLab, a research centre at the Frankfurt School of Finance & Management, interviewed nine blockchain industry experts to understand the dimensions, success factors, and obstacles of the adoption of blockchain technology within an organisation (Holutiuk & Moermann, 2019). These interviews uncovered seven dimensions that are relevant to the organisational adoption of a blockchain solution:

- Organisation
- Business units
- IT unit
- Technology
- People
- Project management
- Environment

In this framework, a core five dimensions—organisational structure, business units, the IT unit, technology, and people—are coordinated by project management, while the environment “surrounds and influences” the adoption of the blockchain (Holutiuk & Moermann, 2019). The framework provides guidelines for success for each dimension:



- The **organisational structure** must be flexible and receptive to improvements and allow people to migrate between the business units and IT units.
- **Business units** should focus primarily on business benefits (including cost savings and revenue capture), growth expectations, new use cases, and compliance.
- The **IT unit** focuses on the complexities of implementation, integration with existing systems, and day-to-day management of the network. This unit also provides a proof of concept for the use case in coordination with the business units.
- The **people** dimension identifies talent that has the industry knowledge and experience to work as developers, consultants, managers, or legal counsel on the blockchain project—though organisations should keep in mind that such talent is currently “expensive and rare in the market” (Holutiuk & Moermann, 2019).
- Blockchain **technology** itself is an important dimension, though this dimension can also be where the organisation has the least control. Organisations can manage expectations about the blockchain project using the Gartner Hype Cycle and seek to establish consortiums that lead to further development and application of blockchain technology.
- The **project management** dimension coordinates the five core dimensions to achieve high-level strategic goals for the blockchain solution, such as establishing the level of autonomy that project teams have to develop the solution and educating the organisation at large about the value of blockchain technology.
- The **environment** dimension pertains to all other external components that influence the organisation’s adoption of a blockchain solution, including current and potential consortium members, technology providers, and regulatory bodies. The “right” environment will welcome new ideas, correctly understand associated businesses, attract fitting employees, and exhibit high project management capabilities.

The following table summarises each of these dimensions and lists further success factors and obstacles for each.

Dimensions	Success Factors	Obstacles
People	<ul style="list-style-type: none"> <li>• Internal know-how</li> <li>• Skilled people</li> <li>• Improved acceptance</li> <li>• Motivation</li> </ul>	<ul style="list-style-type: none"> <li>• Missing know-how</li> <li>• Low acceptance</li> </ul>
Organisational structure	<ul style="list-style-type: none"> <li>• Internal know-how</li> <li>• Internal cooperation</li> <li>• Management support</li> <li>• Acceptance</li> </ul>	<ul style="list-style-type: none"> <li>• Inflexible structure</li> <li>• Missing support</li> </ul>

Dimensions	Success Factors	Obstacles
Technology	<ul style="list-style-type: none"> <li>• Integration in IT architecture</li> <li>• In-house/internal development</li> <li>• Flexible infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>• Legacy systems</li> <li>• Underdeveloped specifications</li> <li>• Low market maturity</li> </ul>
Business unit	<ul style="list-style-type: none"> <li>• Resources</li> <li>• Internal cooperation</li> <li>• Valid use cases</li> </ul>	<ul style="list-style-type: none"> <li>• Missing resources</li> </ul>
IT unit	<ul style="list-style-type: none"> <li>• Resources</li> <li>• Internal cooperation</li> <li>• Understanding of business</li> <li>• In-house development</li> <li>• IT resources</li> </ul>	<ul style="list-style-type: none"> <li>• Missing resources</li> <li>• Compliance</li> </ul>
Project management	<ul style="list-style-type: none"> <li>• Internal cooperation</li> <li>• Cooperation with partners</li> <li>• Management support</li> <li>• Environment</li> <li>• Acceptance</li> <li>• Project management skills</li> <li>• Motivation</li> <li>• Planning</li> <li>• Speed</li> </ul>	<ul style="list-style-type: none"> <li>• Low acceptance</li> <li>• Compliance</li> <li>• Bad communication</li> <li>• Missing willingness</li> </ul>
Environment	<ul style="list-style-type: none"> <li>• Cooperation with partners</li> <li>• Focus on customers</li> </ul>	<ul style="list-style-type: none"> <li>• Potential regulation</li> <li>• Hype as a problem</li> <li>• Low market maturity</li> <li>• Elevated expectations</li> <li>• Missing regulation</li> <li>• Uncertainty about development</li> </ul>

## 5.7.5 Integration of Legacy Systems

### Integration of Legacy Systems

To overcome technical resistance to a blockchain solution, you must be able to clearly outline how to integrate the solution into your company's existing technical systems.

An integrated blockchain enables the following process:

1. Your business applications input data into the blockchain network.
2. External business applications make updates that reflect the current state of the network.
3. The blockchain network makes updates that reflect the current state of the outside world.

On its own, a blockchain resembles a closed, sandbox-like environment. You must connect data about the transactions in your use case—such as product shipments, business purchases, or user verifications—to the blockchain network so that nodes on the network can verify these transactions and update the ledger. You must keep the ledger in sync with your existing business applications, including enterprise resource planning (ERP), customer relationship management (CRM), and human resources (HR) systems, to avoid parallel systems operating in silos.

## Integrating with a Blockchain Network

To integrate with a blockchain network, your business applications send transactions to and receive transactions from the nodes on the network. Applications can integrate with a blockchain through application programming interfaces (APIs) and through events (Buch, 2020).

With APIs, a blockchain uses a software development kit (SDK) to communicate with each node locally or remotely through an RPC, HTTP, IPC, or any other open source API call mechanism. SDKs also provide standardised integration mechanisms for submitting transactions to the blockchain network and performing searches (or queries) for specific ledger data. Blockchain SDKs are typically available in different programming languages, including NodeJS, Java, Python, GoLang, and Rust.

For event-based integration, smart contracts trigger events that the blockchain SDK captures through components called “event handlers” that are connected to the blockchain’s APIs. These event handlers submit updates and notifications to off-chain components such as an ERP or CRM system. Event-driven integrations enable blockchains to communicate with external systems in real time.

### 5.7.6 Exploring Alternative Technologies

#### Exploring Alternative Technologies

Blockchain technology involves coordination, costs, and legal challenges and can require significant efforts to achieve buy-in and implement at an existing company. If blockchain technology does not offer an ideal solution, you may want to consider alternative technologies. These technologies exist on a spectrum from centralised to decentralised and include centralised payment networks and ledgers, decentralised and cloud storage services, and distributed databases and ledgers.

## Faculty Video

In this video, Professor Martin Schmalz covers several technologies that could provide a cheaper and more efficient alternative to solve your business problem than a blockchain.



You should consider if other database solutions might be a better fit for the problems you are trying to solve, including a centralised payment network, such as VisaNet, or a centralised ledger, such as Amazon's Quantum Ledger Database, or a distributed database, such as Oracle, Microsoft, or Orbit db open-sourced project, cloud service providers, such as Amazon Simple Storage Service, or S3, a decentralised storage service, such as the InterPlanetary File System, or IPFS, or other distributed ledger, such as directed acyclic graph, or DAGs, which include technologies, like Hashgraph or IOTA tangle.

The difference between these options comes down on whether a company prioritises cost savings in the development and maintenance of their database, network security, performance, reliability, or data integrity or perhaps scalability for the solution. It's a trade-off. You can't have it all.

You should also consider the challenges of convincing new members to join your blockchain if that is what the industry dynamics require. The value of a blockchain is often directly tied to the number of participants transacting on the network. That means that if a business cannot convince other industry players to join its blockchain network, then the network will be unable to capture and authenticate the necessary data from the external business environment that is required to reduce the cost structures and create efficiencies in how counterparties transact. Without a certain critical mass of adoption, a blockchain use case will simply not be feasible or economically viable.

For example, in the TradeLens case, suppliers transporting goods across a shipping network cannot rely on a blockchain that has data gaps due to only a limited number of shipping companies having their transport routes recorded on that blockchain. You need all of them recorded on the same blockchain. Industry players will need to be convinced of the business and technical merits of joining your blockchain solution. Business merits include cost reduction, capturing network effects, incremental revenue generation, and the forging of new market models. Technical merits include the potential for more secure and immutable forms of data storage, the use of cryptography to maintain minimal levels of privacy and the use of smart contracts to automate transactions in a more transparent and secure manner.

Factors such as IP rights and protection must also be considered when convincing industry stakeholders, particularly competitors, to join your blockchain solution. One of the early obstacles that Maersk and IBM faced in launching TradeLens was the concern from rival shipping carriers, like CMA CGM and Hapag-Lloyd, about who would ultimately own the underlying IP created on the blockchain. These companies were initially skeptical about Maersk and IBM's ability to maintain neutrality on the TradeLens platform and whether this could potentially lead to their IP or sensitive data being exploited by Maersk to gain a competitive advantage. In other words, there is a governance challenge, and trust is necessary despite the claims by some that blockchain technology, by construction, does not require a trust by its participants.

So these concerns are part of a larger set of challenges that can best be summarised as the competition paradox. The competition paradox describes how companies that are natural competitors must in fact cooperate in order to achieve shared governance in a blockchain network while still remaining competitive. The solution to this problem comes down to better forms of shared governance of the blockchain as well as in the traditional

business environment. On the blockchain, activities such as private key management, running different types of nodes, setting and removing access privileges and authorising certain transactions will all need to be assigned to members based on a variety of factors, such as the amount of funding contributed to the consortium, the level of expertise in managing a certain set of tasks, or who has a controlling share of the network's IP.

A succession plan also needs to be put in place in case members leave the network or are being replaced by new entities. In the traditional business world, companies should consider creating formal legal arrangements for new members who join their blockchain, such as incorporating them as equal or minority owners within the joint venture or granting them access to a percentage of the revenues from the joint venture. In cases where members operate in fragmented markets, delegating final authority over decisions on how the system, data, and investments of the blockchain will be led and managed to an industry body or regulator can be the best solution. These intermediaries can serve the role of keeping all network members aligned in their strategic goals as the network grows and priorities change.

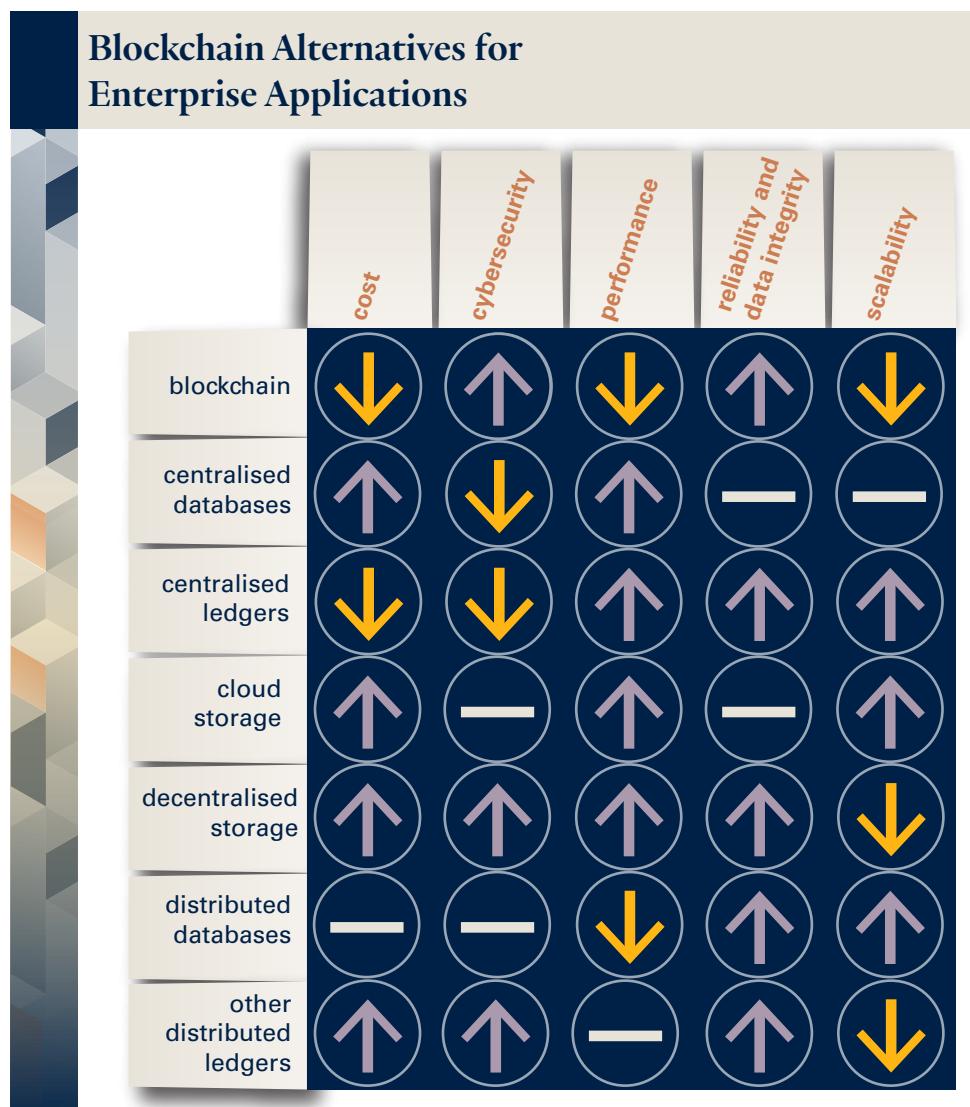
## Alternative Technologies

To decide which alternative to blockchain you want to use, consider whether your solution should prioritise cost savings in the development and maintenance of your database, network security, performance, reliability and data integrity, or scalability.

### A centralised payment network such as VisaNet

The main benefits of a centralised system are speed and reduced costs. Blockchains that are deployed in a distributed or decentralised manner require resources and therefore cost to compute and transact on-chain. If these costs are too high or are not distributed effectively between blockchain members, they can significantly hamper an organisation's ability to gain any real value from the technology.

If your goal is to offer a solution for processing payments, you may want to consider a



payments network such as VisaNet, which currently processes 2,000 transactions per second but has the capacity to process up to 65,000 transactions per second (Visa, 2017).

### **A centralised ledger such as Amazon's Quantum Ledger Database (QLDB)**

Amazon's Quantum Ledger Database enables you to set up a shared ledger with several features of a blockchain, including cryptographically verifiable audit trails and immutability. Centralised ledgers offer the ability to scale your applications in the same cost-effective way you would with a cloud service provider. The downsides of centralised ledgers are increased security risks due to single points of failure and reliance on an intermediary to provide the service.

### **A distributed database such as Oracle, Microsoft, or the OrbitDB open source project**

The main difference between a distributed database and a decentralised database is how consensus is achieved to update the ledger. Distributed databases consist of many nodes that are geographically distributed yet rely on a centralised source to make decisions on what data the other nodes receive and what changes need to be made to the network. Nodes on decentralised databases are independent, each having its own copy of the ledger and requiring consensus to determine what the current state of the network should be. In both cases, the network can function if one or more nodes stop working. However, distributed systems rely more on nodes that have authority over all other nodes for the network to remain operational.

Oracle and Microsoft have offered distributed ledger solutions for many years. OrbitDB is a more recent solution provider that offers peer-to-peer distributed networks for developing decentralised applications without the need of a blockchain. OrbitDB also offers the ability to make private transactions and allows applications to run even when the applications are not connected to the internet.

### **A cloud service provider such as Amazon S3**

Storing the history of all transactions that occur on a blockchain ledger can become quite costly over time. This can become a challenge for private blockchains that rely on a small number of nodes that must store all the transaction data that accumulates from the network. Amazon Simple Storage Service (S3) cloud storage offers a more cost-effective and scalable storage solution for enterprises looking to adopt distributed ledgers. Estimated costs to store one megabyte of data on the Ethereum network are approximately US \$13,820, compared to just a few cents on Amazon S3 (Lawton, 2021). In addition to storage, data governance and security can be outsourced to Amazon S3, which reduces the overhead costs of running a blockchain or distributed ledger system.

### **A decentralised storage service such as the IPFS**

The main drawback of using Amazon S3 is that you are relying on a centralised entity or intermediary to store all of your network's data. Nearly 5,300 out of 8,933 Ethereum nodes (over 57%) currently run on centralised cloud hosting providers, with 25% on Amazon alone (Stevens, 2019). To minimise the risks of centralisation, companies are turning to decentralised storage service providers like the

InterPlanetary File System (IPFS), Storj, and Filecoin. With IPFS, data is stored across a peer-to-peer network. Combining decentralised data storage with centralised applications can enable you to develop more scalable and flexible services while retaining a high degree of security and transparency for the data that backs up your applications. For example, you can maintain a centralised copy of your database that allows you to perform transactions and queries quickly and back up your data on IPFS so that you always maintain a secure, transparent, and immutable archive of your data in case your centralised application is ever attacked or your Amazon account becomes inaccessible.

## A distributed ledger such as a DAG

Other distributed ledgers, such as Hedera Hashgraph's directed acyclic graphs (DAGs) and Iota Tangle, can process up to 10,000 transactions per second (Hussey & Copland, 2021) and use a "gossip protocol" (Hedera Hashgraph, 2020). With a gossip protocol, instead of mining, nodes share information about transactions with each other at random and achieve consensus through a "gossip sync" in which a piece of information that has been synchronised by multiple nodes is linked to a timestamped event. Each event then links to another event.

### 5.7.7 Key Takeaways and References

#### Key Takeaways

Let's review the key points of this section:

1. The challenges that intrapreneurs face range from factors like lack of technical feasibility to poor company culture fit or resistance to change and a lack of coordination across departments.
2. Resistance to new technology is an obstacle that faces entrepreneurs and intrapreneurs. Other concerns include concerns on the speed at which blockchain can produce tangible benefits and questions around privacy and IP.
3. To overcome technical resistance, you must be able to clearly outline how to integrate the solution into your company's existing technical systems.
4. The Gartner cycle passes from the initial "innovation trigger" through periods of inflated expectations, disillusionment, enlightenment, and finally, productivity. Some aspects of blockchain technology, such as smart contracts, are currently in the realm of inflated expectations, while others, such as zero-knowledge proofs, dApps, and a decentralised web, are still in the innovation trigger stage.
5. Blockchain technology is too early in its adoption cycle to replace standard accounting, legal, or operational practices or the employees and executives in these roles.
6. There are seven dimensions that are relevant to the organisational adoption of a blockchain solution:

- Organisation
- Business units
- IT unit
- Technology
- People
- Project management
- Environment

7. To integrate with a blockchain network, your business applications send transactions to and receive transactions from the nodes on the network. Applications can integrate with a blockchain through application programming interfaces (APIs).
8. A blockchain project may not be the right solution for your business. To decide whether to use blockchain technology or an alternative, consider what your company prioritises: cost savings, network security, performance, reliability and data integrity, or scalability for your solution.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 14 April, 2022.

### 5.7.2 Technology Maturity

Benjamin, G. (2021, 2 June). Gartner Blockchain Hype Cycle: Where We Are & What's Next. *iMi Blockchain*. [https://imiblockchain.com/gartner-blockchain-hype-cycle/#What\\_is\\_the\\_Gartner\\_hype\\_cycle\\_for\\_emerging\\_technologies](https://imiblockchain.com/gartner-blockchain-hype-cycle/#What_is_the_Gartner_hype_cycle_for_emerging_technologies)

Iansiti, M., & Lakhani, K. (2017, January–February). The Truth About Blockchain. *Harvard Business Review*. <https://hbr.org/2017/01/the-truth-about-blockchain>

Rauchs, M., Blandin, A., Bear, K., & McKeon, S. (2019). 2nd Global Enterprise Blockchain Benchmark Study. *Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School*. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf>

### **5.7.3 Job Security**

BDO. (2019, June). Understanding Internal Control Over Financial Reporting. <https://www.bdo.com/insights/assurance/corporate-governance/understanding-internal-control-over-financial-repo>

Deloitte. (2020, 14 December). How Blockchain Impacts Financial Reporting Controls. *The Wall Street Journal*. <https://deloitte.wsj.com/articles/how-blockchain-impacts-financial-reporting-controls-01607976132>

### **5.7.4 Coordination Across Departments**

Holotiu, F., & Moermann, J. (2019). Dimensions, Success Factors and Obstacles of the Adoption of Blockchain Technology. *Australasian Conference on Information Systems*. [https://acis2019.io/pdfs/ACIS2019\\_PaperFIN\\_040.pdf](https://acis2019.io/pdfs/ACIS2019_PaperFIN_040.pdf)

### **5.7.5 Integration of Legacy Systems**

Buch, H. (2020, 19 June). Enterprise Integration and Interoperability of Blockchain. *Network Computing*. <https://www.networkcomputing.com/network-security/enterprise-integration-and-interoperability-blockchain>

### **5.7.6 Exploring Alternative Technologies**

Hedera Hashgraph. (2019, 18 December). What is gossip about gossip? <https://hedera.com/learning/what-is-gossip-about-gossip>

Hussey, M., & Copland, T. (2021, 1 April). What is Hedera Hashgraph? *Decrypt*. <https://decrypt.co/resources/hedera-hashgraph>

Lawton, G. (2021, 25 May). 6 alternatives to blockchain for businesses to consider. *TechTarget*. <https://www.techtarget.com/searchcio/feature/6-alternatives-to-blockchain-for-businesses-to-consider>

Stevens, R. (2019, 26 September). A quarter of Ethereum nodes run on Amazon Web Services. *Decrypt*. <https://decrypt.co/9683/a-quarter-of-ethereum-nodes-run-on-amazon-web-services>

Visa. (2017, 9 August). Visa Fact Sheet. <https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf>

# 5.8 Business Case Framework

## 5.8.1 Business Case Framework

### Overview

In this section, we will wrap up what we have learnt so far in this module by providing a framework of questions you can use to evaluate whether or not you have a strong business case for your blockchain solution. The answers to these questions will help you craft a persuasive pitch to stakeholders on whether or not to pursue a blockchain solution.

Taking all the information you have learnt from this module, you should evaluate the business case for your blockchain solution by answering the following questions.

## 5.8.2 Important Considerations

### Important Considerations

#### 1. Which business problem are we attempting to solve?

Identifying what business problem to solve with blockchain technology requires first understanding the blockchain suitability criteria, which consists of six questions to help you determine if blockchain is the right technology to apply to your business problem:

1. Can the process be automated?
2. Will the process be ongoing?
3. Are there multiple stakeholders?
4. Are there multiple reconciliation parties?
5. Is something of economic value being transferred?
6. Is there a need for recorded data to be permanent?

Filter your list of business problems through the blockchain suitability criteria. If most of the questions do not apply to your business problem, then perhaps blockchain technology is not the right solution.

## **2. Is blockchain technology the only or clearly the most efficient technology to solve this business problem?**

To determine if blockchain technology is the right technology to solve the business problem, you need to analyse the alternative solutions that are offered by the market. While your business problems may align well with the blockchain suitability criteria, you will want to consider the challenges of adopting blockchain technology (including challenges with shared governance and satisfying the needs of stakeholders who may have conflicting interests), changes to your database architecture that will be resource-intensive and may require a more specialised technical team to manage, lack of regulatory clarity around the use of smart contracts, and the implications of managing a ledger in which transactions are immutable.

Keeping all of this in mind, consider whether other database solutions might be a better fit for the problems you are trying to solve, including:

- A centralised payment network, such as VisaNet
- A centralised ledger, such as Amazon's Quantum Ledger Database (QLDB)
- A distributed database, such as Oracle, Microsoft, or OrbitDB
- A cloud service provider, such as Amazon Simple Storage Service (S3)
- A decentralised storage service, such as the InterPlanetary File System (IPFS)
- Other distributed ledgers, such as directed acyclic graphs (DAGs), which include technologies like Hashgraph or Iota Tangle

The difference between these options depends on whether a company prioritises cost savings in the development and maintenance of its database, network security, performance, reliability and data integrity, or scalability for its solution. It's a tradeoff—you can't have it all.

## **3. Are there barriers to adoption for competitors?**

What keeps your competitors from simply copying your blockchain solution? Recall the instructions from Academic Director Martin Schmalz about Porter's Five Forces and the TradeLens case study. We discussed how network effects could create significant competitive advantages for blockchain companies, as more value accrues to the network with each additional member who joins.

Although many blockchains are built on open source technology and can be replaced, launching a successful blockchain network with many users can create barriers to entry for competitors, as the costs for customers and industry partners to switch from your scaled network to a new, smaller network increase as your network continues to grow and attract more users.

#### **4. What are the other barriers to adoption?**

Other barriers to adopting a blockchain solution include development and maintenance costs, legal and security risks, privacy and confidentiality concerns, and managerial resistance. You must weigh all of these factors against the potential benefits, which include reduced costs, increased transparency and operation efficiency, and exploration of potential new business models.

#### **5. Do you need a network effect for your solution to be successful?**

Consider if a network effect is the only thing that enables your blockchain to be successful. This narrows the list of problems you can attempt to solve, as you must pursue opportunities that align with the incentives of multiple stakeholders to gain adoption and capture network effects. If you observe a competitor that has launched its own blockchain and has already achieved significant adoption and network effects, you might want to consider joining that blockchain rather than trying to establish your own.

#### **6. Will implementing this technology make a process or product cheaper or better than your competitors' processes or products?**

The answer to this question will depend on how blockchain technology is implemented within your organisation. For example, if you are not strategic about how you manage data storage costs, handle IP rights amongst consortium members, and pursue only suitable opportunities, you might make decisions that ultimately put you at a greater disadvantage to your competitors than when you started.

Remember that as you assess the viability of your use case, it is always important to ask whether you really need blockchain features, or if the problem you are trying to solve is better suited to an alternative technology. A blockchain should not be simply a “feature” for your business. Unlike other disruptive technologies, such as AI or machine learning, implementing blockchain features can fundamentally change the nature of your business from one that is centralised to one that is decentralised and/or distributed. As a result, your organisational structure might need to be altered to accommodate the integration of this new technology and new forms of shared governance.

#### **7. Given the analysis you've just completed, will implementing blockchain technology provide your business with a competitive advantage or not?**

This is the ultimate question that you must answer once all of your analysis is done. Additionally, what might seem like a clear answer, when run through a theoretical framework, must still be proven out through the development of a proof-of-concept prototype to understand if there is indeed a practical application for blockchain technology within your organisation.

## Guest Video: Prudential's Approach to Introducing Innovative Concepts

In this video, you'll hear from Federico Spagnoli, Regional President of Prudential Financial/Latin America and Lead for Product Innovation and Ecosystem for all emerging markets, as he provides advice on things to think about when implementing blockchain solutions.



We all know that in bringing some of these big ideas to large organizations is not an easy task. You need to convince a number of key stakeholders, you need to get the funding, and then the support to be able to start executing some of these initiatives. In my personal experience, I like to refer to three tips that have helped me to do so.

One, I typically say properly frame the opportunity. If you are thinking about blockchain technology, probably is something relatively new, and very different from what the rest of your peers or subordinates, or team members, are being exposed to.

So what about having a framework where you can clearly state, in the short-term, what are some of the opportunities that you are expecting to deliver? Think about your core business, your core products, and then frame by when this new emerging technologies or solutions that you are bringing to market, are expecting to impact your results.

So you clearly are managing the expectations. The challenge is when you bring a brand new initiative that may take months or even years to see a material impact in the results of an organization. The misunderstanding is that that is going to generate effects the next quarter, or the next year. So properly framing that is very important. And I typically say earn your right to invest for the future by delivering the present.

The second tip that I typically provide in this type of considerations, is first shoot bullets, then cannon balls. And this is not my phrase. It's from Jim Collins, from Good to Great. And the idea here is, think about this idea of testing and learning.

For example, in my case, I'm promoting and sponsoring the development of what we call a Wellness Ecosystem in Proventa International. And we started in one of our smallest operations, where the costs were not that high, and if you made mistakes, were not so significant for the firm. That gave a number of the stakeholders a peace of mind, when it came to the risk mitigation aspect.

And the last one and very important is, I encourage to get out of the building really fast. Again, that is not my phrase, that is from the Lean Startup Methodology. It's this idea that don't wait for the perfect solution, or to get all the approvals, all the funding.

If there were some prototypes, even if you can start with an A/B testing on a survey, in a website, getting exposed to your idea to prospect clients, get some initial feedback and based on that feedback, go back to the drawing board and keep improving your product. Don't wait until everything is perfect, go for it.

## 5.8.3 Further Exploration

### Further Exploration

Use the resources shared below to learn more about how to develop a proof of concept for your blockchain use case and practical ways to test your assumptions.

- [Architecting Enterprise Blockchain Solutions by Joseph Holbrook](#)
- [Blockchain For Enterprise](#)
- [Oracle Blockchain Services Quick Start Guide](#)



**Module 6:**

# Looking Forward: What the Future Holds

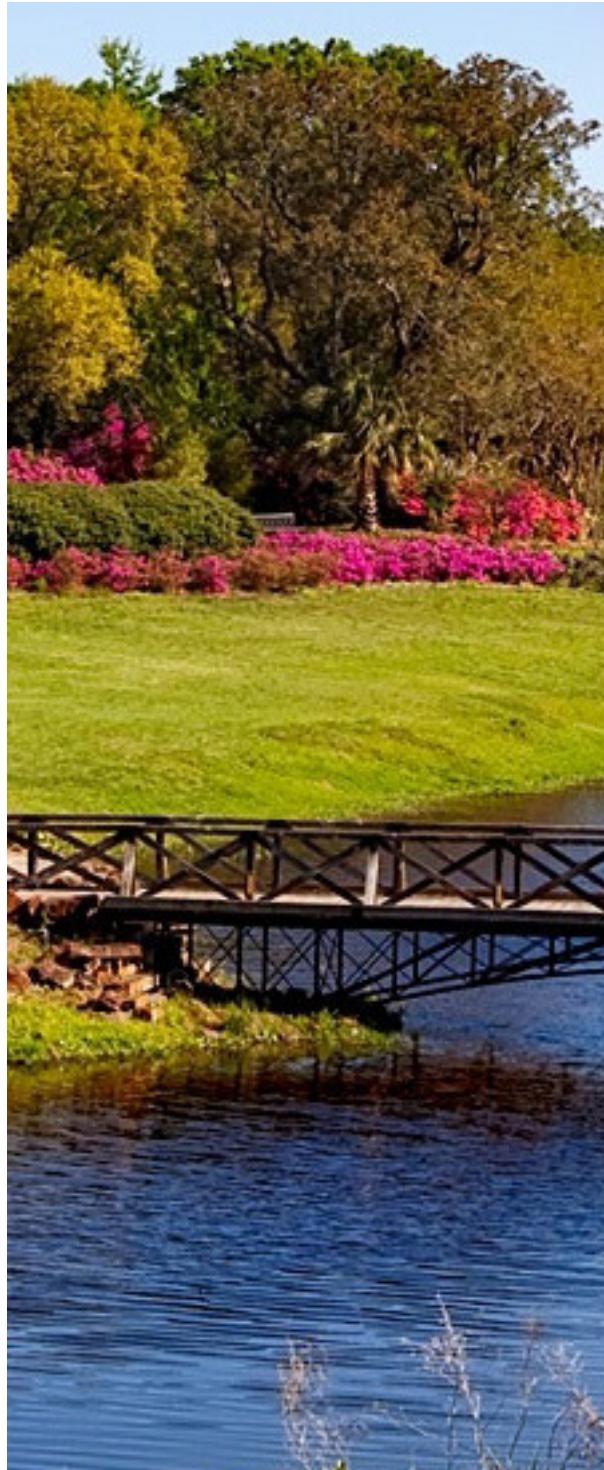
---

**Oxford Blockchain Strategy Programme  
2022**

# Oxford Blockchain Strategy Programme

## Module 6: Looking Forward: What the Future Holds

### Table Of Contents



<b>6.1 About Module 6</b>	<b>3</b>
6.1.1 Overview of Module 6	3
<b>6.2 Decentralised Finance (DeFi)</b>	<b>5</b>
6.2.1 Overview	5
6.2.2 What is DeFi?	6
6.2.3 Value Propositions of DeFi	7
6.2.4 DeFi Risks	11
6.2.5 Key Players in DeFi	14
6.2.6 The Future of DeFi	15
6.2.7 Key Takeaways, References, and Further Exploration	17
<b>6.3 The Future of Central Bank Digital Currencies (CBDCs)</b>	<b>21</b>
6.3.1 Overview	21
6.3.2 CBDCs as the Competitor	21
6.3.3 A CBDC's Impact on Negative Interest Rate Policy	22
6.3.4 The Case Against CBDCs	23
6.3.5 CBDCs Around the World	26
6.3.6 Key Takeaways, References, and Further Exploration	28
<b>6.4 The Future of Non-Fungible Tokens (NFTs)</b>	<b>32</b>
6.4.1 Overview	32
6.4.2 NFTs Revisited	32
6.4.3 The Future of NFTs	34
6.4.4 Case Study: Tokenising the Land Registry in the Republic of Georgia	37
6.4.5 Key Takeaways and References	39
<b>6.5 Compute and Connectivity</b>	<b>42</b>
6.5.1 Overview	42
6.5.2 Compute and Connectivity Revisited	42
6.5.3 The Future of Compute and Connectivity	43
6.5.5 Key Takeaways, References, and Further Exploration	46
<b>6.6 Other Blockchain Concepts</b>	<b>48</b>
6.6.1 Overview	48
6.6.2 Reputation Marketing	48
6.6.3 Prediction Markets	52
6.6.4 The Future of Distributed Autonomous Organisations (DAOs)	54
6.6.5 The Digital Civilisation Initiative	61
6.6.6 Key Takeaways and References	63
<b>6.7 Case Study: Blockchain for the Public Good</b>	<b>66</b>
6.7.1 Overview	66
6.7.2 From Radical Markets to RadicalXChange	67
6.7.3 References and Further Exploration	70
<b>6.8 Getting Involved in a Blockchain Ecosystem and Keeping Skills Fresh</b>	<b>71</b>
6.8.1 Overview	71
6.8.2 Online and Protocol Communities	71
6.8.3 Social and Offline Communities, Contributions, and Volunteering	74
6.8.4 Keeping Skills Fresh and Looking Forward	79
6.8.5 Key Takeaways and References	81
<b>6.10 Congratulations</b>	<b>83</b>
6.10 Programme Wrap-up	83

# 6.1 About Module 6

## 6.1.1 Overview of Module 6

### Overview

Welcome to Module 6 of the Blockchain Strategy Programme!

In addition to enabling you to focus on completing your Capstone project, this module includes deeper dives into some of the topics that have already been covered, as well as a few new ones—including a forward-thinking case study about blockchain for the public good. Use this material as an opportunity to explore what the future might look like for some of the leading-edge blockchain applications, including how to get involved in a blockchain ecosystem and how to keep your skills fresh. This module will also outline some of the ways you can become more involved in the global blockchain community, including the tools, resources, and references that you can continue to use after the course.

You'll study the following concepts in this module:

- Decentralised finance (DeFi)
- Non-fungible tokens (NFTs)
- The creator economy
- Central bank digital currencies (CBDCs)
- Distributed autonomous organisations (DAOs)
- Reputation marketing
- Prediction markets
- Compute and connectivity
- Blockchain for the public good
- How to get involved in a blockchain ecosystem and keep skills fresh

## Learning Outcomes

By the end of this module, you will be able to:

- Recognise how to get involved in a blockchain ecosystem.
- Identify ways to stay up to date with the fast-moving blockchain technology space.
- Speculate on the future of blockchain applications, including decentralised finance (DeFi), non-fungible tokens (NFTs) and creator economics, governments and CBDCs, and more esoteric ideas such as reputation markets, prediction markets, and distributed autonomous organisations (DAOs)

## Graded Assignments

You will complete individual and group assignments, which count towards your completion of the programme. This week, you will:

- Meet with your group to develop your final slide deck and video that you will use to present your blockchain technology use case to either VC investors or the board of directors at an organisation.

You must submit your Capstone by **19 July 2022, 23:59 UTC**. (Try the [Time Zone Converter](#) to get your local time.)

# 6.2 Decentralised Finance (DeFi)

## 6.2.1 Overview

### Overview

Decentralised finance (DeFi) is an emerging sector of the cryptocurrency and blockchain industry that has grabbed the attention of mainstream audiences and financial institutions around the world with its recent growth and disruptive potential. This section will define decentralised finance and its value propositions, components, risks, and key players. In addition, we will analyse the growth of the DeFi industry and provide some perspective on its future potential.

### Vocabulary Check

This section introduces the following terms:

- [automated market maker \(AMM\)](#)
- [crypto bank run](#)
- [decentralised exchange \(DEX\)](#)
- [liquidity pool](#)
- [market maker](#)
- [oracle](#)
- [rug pull](#)
- [Web 2.0](#)
- [Web 3.0](#)

## 6.2.2 What is DeFi?

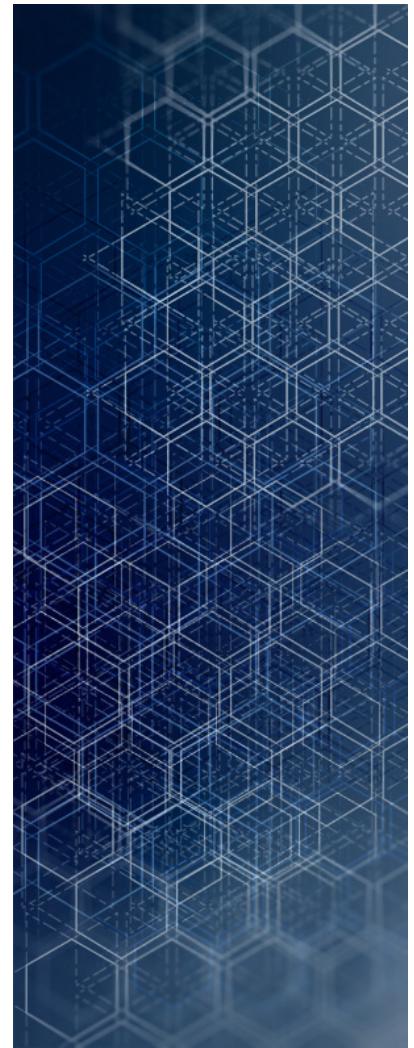
### What is DeFi?

In the traditional financial system, many activities require multiple intermediaries: Banks maintain custody of funds, manage the process of lending and borrowing, and facilitate the transfer and settlement of money between accounts using intrabank and interbank systems such as ACH and Fedwire. Brokerage services receive and fill orders to buy or sell securities with the help of other institutions that serve as market makers. Credit Suisse and Citadel Securities are some of the market makers that help create liquidity in the market by buying and selling securities within their own accounts.

While a large number of intermediaries remain necessary, industries including finance have sought to reduce costs through disintermediation, or “cutting out the middleman” (Codjia, 2017). Already by 2013, institutional investors in private equity had made direct investments that outperformed both co-investments and traditional private equity partnership investments made through intermediaries (Fang et al., 2013). Instead of taking out a loan, consumers and companies can turn to crowdfunding through platforms such as Kickstarter. Such disintermediation by means of the internet is often called the B2C, or business-to-consumer, model (Hayes, 2021).

DeFi provides similar disintermediation services, making most financial activities possible through peer-to-peer networks through blockchain technology. DeFi disintermediation provides financial alternatives to individuals who might not use the traditional banking system. Further, DeFi solutions also offer efficient access to capital and interest earnings while offering privacy, control over custody of funds, and censorship resistance: Blockchain networks do not have a central authority or gatekeeper that prevents anyone from participating in the network, as long as participants follow the network’s rules, or an authority that changes or removes transactions on the network (Binance Academy, 2020). Because of the immutable nature of blockchains, participants also cannot change or remove transactions. DeFi, in general, offers a new alternative source for financial services.

Web 3.0, the next evolution of the internet and distributed networks, plays an important role in DeFi. Whereas Web 2.0 is dominated by a handful of organisations, such as Google and Facebook, that act as intermediaries, Web 3.0 enables users to interact via peer-to-peer networks. Additionally, while major players in Web 2.0 offer their services in exchange for ownership of users’ personal data, which they can then sell, DeFi exchanges allow participants to maintain ownership of their personal data. Data ownership provides individuals control over how their personal data is used or not used by outside parties.



## 6.2.3 Value Propositions of DeFi

### Value Propositions of DeFi

Some of the traditional financial activities disrupted by DeFi include self-custody of funds, lending and borrowing, trading, automated market making, liquidity providing, and yield farming.

### Self-Custody of Funds

The first step in transitioning from traditional finance to decentralised finance involves the self-custody of users' funds using a digital wallet, also known as a non-custodial wallet, which is used to store, send, and receive cryptocurrencies and tokens on a blockchain. The wallet owner maintains control and security of their funds instead of a third-party custodian, such as a bank, which cannot assume control of the funds or prevent the wallet holder from making a transaction.

Note that while no third-party custodian can prevent wallets from making transactions, it is possible for an operator like Centre, a “governed network powered by price-stable crypto assets”, to ban a particular wallet address (Centre, n.d.). However, this practice is extremely uncommon and would typically involve a directive from law enforcement.

A digital wallet has two primary components:

1. **Private key:** The private key is denoted by a randomly generated series of numbers and letters that is only known to the owner.
2. **Public key:** The public key can be given out to anyone who wishes to send funds to the owner of that digital wallet.

Through public key addresses, users can view transactions that occur on a blockchain, also known as “on-chain,” by following the movement of funds between public key addresses, which is a critical component of blockchain’s transparency. While the name of a person who owns a particular wallet address is never associated with that address on the blockchain, the balance of that wallet is easily verifiable in addition to any of that wallet’s transactions to and from other wallets on the blockchain, rendering the whole blockchain system more transparent.

Digital wallets come in two forms (Cryptopedia, 2021b):

- **Cold wallets** are hardware wallets similar to hardware storage drives that are not connected to the internet, thereby making them more secure because hackers are less likely to get access to them offline. Popular cold wallet providers include Ledger and Trezor.
- **Hot wallets** are digital wallets that are connected to the internet. Popular hot wallet providers include MetaMask and Trust Wallet.

## Digital Wallet

A digital wallet has **2 components**



**A private key:** A randomly generated series of numbers and letters known only to the owner.



**A public key:** Given out to anyone who wishes to send funds to the owner of that digital wallet.



Cold wallets are hardware similar to storage drives and are not connected to the internet. They are more secure.



Hot wallets are digital wallets that are connected to the internet.



There are **2 forms of digital wallet**

## Lending and Borrowing

Smart contract-based lending was one of DeFi's first applications to gain popularity. Projects like ETHLend, which later became Aave, developed a protocol that would enable users to enter peer-to-peer collateral lending arrangements run entirely on smart contracts. Some use cases for borrowing in this way include:

- In DeFi, **interest rate arbitrage** is when one takes advantage of different lending and borrowing rates on different decentralized platforms, providing for an immediate, risk-less profit. For example, one can benefit by borrowing from a platform with lower rates and lending on the platform with higher return rates. Interest rate arbitrage depends on market price inefficiencies which are more common in emerging markets, such as the crypto market (WSUM Network, 2021).

- In a **carry trade strategy**, a user borrows an asset at a low rate on one platform and invests in a different asset at a higher rate of return on the same or a different platform.
- In **conversion to fiat currency**, a user borrows against one of their cryptocurrency holdings, converts the borrowed funds to fiat currency, and uses that currency to make a purchase or other investment in the traditional markets—for example, to buy a house or car, or to purchase stocks.

Smart contract loans offer a trustless and transparent transaction between parties using highly censorship-resistant computer code. Like the “trustless” activities described in Module 1, trustless platforms do not require participants to know or trust each other, and do not require a third-party intermediary to function. These collateralised loans are most popular among cryptocurrency traders who trade with leverage, meaning they borrow capital in order to take a long or short position on a cryptocurrency.

Decentralised exchanges (DEXs) and other DeFi protocols use smart contract loans as a way to provide their customers with leverage while protecting lenders by writing rules in the code that will trigger a liquidation if the price of the collateral asset falls below a certain threshold. Such failsafes, in addition to transparent blockchain ledgers that allow easy verification of collateral ownership, could enable lenders to rehypothecate collateral (reuse the collateral for the lenders’ own purposes) multiple times across different platforms and networks without creating systemic risk. However, while some may view this as a more trustworthy alternative to traditional lending platforms, smart contract loans are also vulnerable to hacks or faulty code that can lead to loss of funds with little to no legal recourse.

## Trading

Decentralised exchanges enable traders to exchange cryptocurrencies peer-to-peer instead of requiring intermediaries. DEXs also offer additional benefits of enhanced (Vermaak, 2020):

- **Security:** DEXs, where each user keeps their funds in individual wallets, are less attractive to hackers than centralised exchanges that store all of their users’ funds on-platform. Central exchanges can also engage in “exit scams”. Following the death of the co-founder and CEO of QuadrigaCX, once the largest crypto exchange in Canada, the Ontario Securities Commission (OSC) found the organisation to be a Ponzi scheme (Collie, 2020).
- **Privacy:** While central exchanges have know-your-customer (KYC) controls that require participants to provide personal data, because DEXs have no central authority, DEXs do not implement these controls.
- **Control:** With no central authority to freeze assets or block withdrawals, DEXs offer users more control over their funds. Note, however, that CoinMarketCap’s primer on DEXs points out that “not all decentralized exchanges are created equal, and in practice they range from quasi-decentralized to fully decentralized” (Vermaak, 2020).

DEXs also do not have the same fees as traditional exchanges, which pay brokers who connect customers with specialists who can execute those customers’ orders (Carey, 2021). However, trades on a DEX tend to have additional fees, which differ between each exchange. For example, the

Ethereum network charges “gas” fees for the computational power required to execute an operation (Wilcox, 2020).

## Automated Market Making

While accurate price readings would certainly improve the use of DEXs, there were still major problems around the lack of liquidity, which meant that DEX users were forced to buy digital assets not based on the most accurate price but the price in which there was enough liquidity to fill their orders, which could often be higher than the current trading price in more liquid exchanges.

To solve this issue, protocols like UniSwap developed the automated market maker (AMM). An automated market maker is a set of protocols that leverage liquidity pools to allow digital assets to be traded in a permissionless manner while maintaining efficiently priced markets. Unlike a traditional market, a DeFi AMM is always available for trading, and relies on these liquidity pools instead of interactions between buyers and sellers (Cryptopedia, 2021a).

## Liquidity Providing

A liquidity pool is formed when users input one of each token in a pair that others wish to trade. Pools will typically require each user to input different quantities of each token for them to equal the same value.

For example, a liquidity pool could be started for an ETH/DAI trading pair by a user inputting 1 ETH and 3,200 DAI (based on a sample ETH price of US \$3,200) for a total dollar value of US \$6,400, or 2 ETH and 6,400 DAI for a total value of US \$12,800. This formula could repeat for any amount of the ETH/DAI pair.

Users who input token pairs into a pool are called liquidity providers or LPs. LPs receive LP tokens, which represent their ownership stake in the liquidity pool. If a user wishes to stop being a liquidity provider, they can sell their LP tokens to get back the tokens that they initially put in. However, as discussed further below, the ratio of tokens they put in may not always be the same as what they get back.

Once an ETH/DAI pool is formed, other users can buy and sell ETH or DAI by exchanging their ETH with DAI or vice versa from the pool. Each time this occurs, LPs are compensated from the fees that outside traders pay to exchange digital assets with the pool. The fees are distributed to LPs through their LP tokens. LPs are compensated in proportion to the amount of capital they contributed to the pool. So, if a user’s ETH and DAI account for 20% of the pool, they earn 20% of the fees.

The discrepancy in the ETH price within the pool compared to the price of ETH trading on centralised exchanges creates an arbitrage opportunity for traders to exploit. Seeing this opportunity, traders add DAI to the pool and take out ETH, which ultimately restores the ratio of ETH and DAI within the pool, allowing the price to return to the same price that is reflected on other exchanges.

The combination of smart contract price feeds, arbitrage opportunities exploited by traders, and liquidity provider incentives enable AMMs to serve as a critical feature in facilitating efficient markets on decentralised and permissionless exchanges.

## **Yield Farming**

In the DeFi space, lending tokens to liquidity pools and earning fees from transactions is called yield farming (Dedezade et al., 2020).

Yields are primarily a function of the demand for leverage in the crypto markets. Demand to borrow in order to go long or short in a highly volatile market (and during a bull market) leads to more traders willing to pay higher interest rates to acquire leverage. This is what enables the yields for lending in crypto markets to be higher than in traditional financial markets.

Additionally, liquidity pool yields are purely a function of what percentage of the pool a person owns. Because so many different tokens can be traded, anyone with a relatively modest amount of capital can set up a pool to enable users to trade small-cap tokens, thereby earning the majority of the transaction fees and generating yields far above what is offered in traditional financial markets where such models are currently not available.

Cryptocurrency projects will often allocate large portions of their tokens to form liquidity pools that incentivise traders to participate in yield farms where they earn fees on their tokens. Within yield farms, these fees can result in users earning annual percentage yields (APYs) of 20% to 1,000% or more. However, there are cautions to be noted for these high yields. First, the yields almost never last for more than a few weeks because the token supply is limited, and the high yield incentivises more people to farm the token. This leads to the rewards being divvied out to an increasing number of people over a short time frame, which means fewer rewards for each person.

Second, most traders who earn a large number of a new project's tokens through yield farming tend to immediately sell them to retain the value that was earned in stablecoins or in a token they view as having more long term value. As more people pursue the same strategy, the price of the token drops considerably due to overwhelming selling pressure. Ultimately, the declining price of the token neutralises any gains that could have been made from the high APY.

### **6.2.4 DeFi Risks**

#### **DeFi Risks**

DeFi is also fertile ground for exploitation and other risks. We will explore the risks associated with the various value propositions discussed in the previous section.

## Custody Risks

If the public identifies a wallet address as belonging to a hacker who recently stole funds, the wallet's public key address, as well as any other affiliated addresses, can be banned. This means the public key address will be marked as an address involved in criminal activity, and decentralised exchanges can ban the address from depositing funds to their platform, make users aware of the address, and use methods of consensus to prevent the address from participating in the network.

The biggest risk of self-custody is the loss of funds due to hacks or mistakes made by the owner. If funds are sent to the wrong address, no central authority can authorise the reversal of the transaction. Additionally, if a hacker gains access to a user's private keys, the hacker can drain all of the funds in the user's wallet with little to no recourse for recovering the funds.

As funds have increased in the cryptocurrency space, the frequency and sophistication of hacks has also increased. One of the more recent forms of hacking involved the perpetrator stealing funds from a user's wallet simply by setting up faulty smart contracts that were designed to give them access to a person's private keys once they interact with the contract and confirm their digital signature.

Users have had funds stolen simply by connecting their wallets to a DeFi application or NFT page to view the site's contents. In 2021 alone, 32 incidents of hacks and fraud have led to a total value of US \$2.99 billion being stolen from individuals and institutions using different forms of self-custody (Mozée, 2021).

## Lending Risks

In collateral-based lending contracts, the collateral value must stay at a certain level for the lender to protect themselves. If the price of ETH were to fall from US \$3,200 to \$1,600, the size of the collateral compared to the loan issued would go from a ratio of 2:1 to 1:1, meaning the lender no longer has a margin of safety to protect their investment in case the price of ETH falls further.

If the ETH price were to fall any further, the lender would be holding onto collateral that is now worth less than the amount of money they lent to the borrower. In a low-trust environment where the counterparty is often anonymous, and there is no reputation or credit scoring system, the lender runs the risk of the borrower not paying back the loan because there isn't an incentive to do so.

For this reason, lending smart contracts often have a "liquidation price", which is the collateral's low-end price that triggers an automatic sell to protect the lender from losses.

## Automated Market Making Risks

The AMM model also has some downsides—primarily, impermanent loss, which is a loss of funds that occurs during the process of providing liquidity. The loss happens when there is a price change between the tokens staked. When the price of one of the assets increases, for example, an arbitrageur may take advantage by purchasing the tokens, which leaves the liquidity provider in a loss situation (Jakub, 2020).

In one example, a rug pull occurs when the developers of a DeFi project back out of the project and take the investors' funds. (They effectively "pull the rug out" from under the feet of investors, leaving investors with unfulfilled promises and empty wallets). A common warning sign of a rug pull is over-hyped token prices that suddenly rise dramatically (Binance Academy, 2021).

Likewise, similar to a traditional bank run, a crypto bank run can occur when a lack of customer confidence in a bank's credit results in panic and an excessive withdrawal of funds, which can force the bank to close because it has no funds left to satisfy the late depositors. In DeFi, a bank run happens when anything, valid or hype-induced, causes a panic amongst liquidity providers, and investors pull their funds. Like in a rug pull, there may be no funds left to be withdrawn by those who realise too late what is happening.

## Other DeFi Risks

In their paper titled "DeFi and the Future of Finance", Duke University Professor Campbell Harvey and his colleagues, Ashwin Ramachandran and Joey Santoro, write about the risks that should concern participants in DeFi (2021):

- **Smart contract risk.** Since DeFi is based on computer code that is available to the public once it is deployed, there is a wide surface exposure to would-be exploiters. A simple logic error in the code might be easily detected, or an attacker could withdraw funds beyond the platform's intended functionality through an economic exploit by manipulating certain variables within the market that the contract is based on.
- **Governance risk.** This risk in DeFi involves humans managing the protocol risk through a tokenised governance structure. Tokens represent votes, and a malicious actor could attempt to gain control through votes. This risk is alleviated at least partially by limiting the supply of tokens through the initial governance model.
- **Oracle risk.** Considered the largest system threat to DeFi, oracles provide the external data needed in some DeFi platforms. Prediction markets are one example of a system that relies on oracles. The oracle becomes vulnerable to attack if the attacker's potential profit from corruption becomes larger than the oracle's cost of corruption. Also, there is a known risk of outages, which could have a large downstream effect.
- **Scaling risk.** Ethereum has been the primary DeFi "layer 1" platform. As a proof-of-work (PoW) platform, the fixed block size and slow transaction speed are a hindrance to the scaling needs of DeFi. PoS aims to resolve this dilemma. Specifically, Ethereum 2.0 and its sharding process will allow horizontal scaling and speed up transaction times.
- **DEX risk.** Discussed earlier in this section, automated market maker DEX risk involves smart contract risk as the system is based on its code. Impermanent loss is the other primary risk factor which occurs when two assets have imperfectly correlated returns and high volatilities. Sharp price movements could expose this risk. Despite the label, the loss is in fact permanent, unless the prices go back to their old levels. Order-book DEX risks include the scalability issues for their

underlying platform and the risk of a single market maker for each asset pair that could result in large spreads.

- **Custodial risk.** For the retailer, self-custody poses a risk if the private key is lost. Delegated custody could also be affected by lost private keys due to a hack.
- **Regulatory risk.** As regulations become more prevalent in DeFi, the markets and exchanges risk losing liquidity from a lack of participation or abrupt withdrawals due to imposed regulations, taxation, or other enforcements considered burdensome to the system.

The risks outlined here should be applied to the broader blockchain ecosystem in addition to DeFi. Scaling, exploitations, and regulatory pressures, for example, could affect NFTs and other public blockchain use cases.

## Insurance Offers a Solution

Decentralised insurance is among the newest yet most critical innovations to occur in the DeFi space. Decentralised insurance has received so much attention primarily because decentralised insurance, if executed correctly, can resolve many of the risks that this section has covered.

Decentralised insurance leverages smart contracts to pool funds together and issue payouts to claimants based on the fulfillment of conditions defined in the insurance smart contract, in line with the voting consensus of the same network of people who are funding the insurance pool. In contrast, in the traditional insurance model, decisions about whether to pay a claimant are made by a central authority—the insurance company—whose business often depends on the company not paying out too many claims each year. This creates a potential conflict of interest that decentralised insurance protocols can mitigate.

Currently, the most popular DeFi insurance protocol is Nexus Mutual, which primarily covers users against exchange hacks or smart contract failures that lead to exploits. In the future, Nexus Mutual's plan is to offer insurance coverage for crypto wallets as well as more traditional insurance products, such as earthquake or fire coverage (Nexus Mutual, n.d.).

### 6.2.5 Key Players in DeFi

#### Key Players in DeFi

The key players in DeFi include prominent exchange and liquidity protocols as well as those who provide information on DeFi activity that occurs at any moment.

**DeFi Pulse** reports market activity in near-real time, which helps AMMs and other investors follow trends and strategise on their holdings. The site includes specific market indices and reporting mechanisms such as:

- Total value circulating (TVC)
- Total value locked (TVL)
- Custodial dominance
- Maker dominance
- Market capitalisation

It is possible to analyse historical volumes in DeFi categories such as TVC and TVL. DeFi Pulse reports the following top TVLs by category as of 11 October 2021 (DeFi Pulse, 2021):

- **Aave** is the top lending platform, with US \$14.5 billion TVL. It is a multi-chain open-source protocol that was established in 2017 to enable the creation of money markets.
- **Curve Finance** is the top DEX, with US \$13.5 billion TVL. It is a DEX liquidity pool on Ethereum that launched in January 2020 and specialises in efficient stablecoin trading.
- **Synthetix** is the top derivatives platform, with US \$1.8 billion TVL. It launched in February 2019 and tracks the values of real-world assets.
- **Uniswap** has been a strong participant and influencer as an automated liquidity provider since 2018. It is the second-largest DEX, with US \$6.6 billion in TVL, behind Curve Finance.

## 6.2.6 The Future of DeFi

### The Future of DeFi

As it encroaches on the traditional finance space, DeFi has also provided financial inclusion to many in the world who do not participate in traditional finance systems. With DeFi, the only requirement is an internet connection and a cryptocurrency balance in a wallet. This ecosystem is young and will likely develop a broader adoption rate as it becomes more widely understood.

However, although the DeFi space continues to stabilise in terms of protocols that are more sound and adept at preventing exploitation, it remains vulnerable to unethical activities. Cautious due diligence is warranted for participants at all levels.

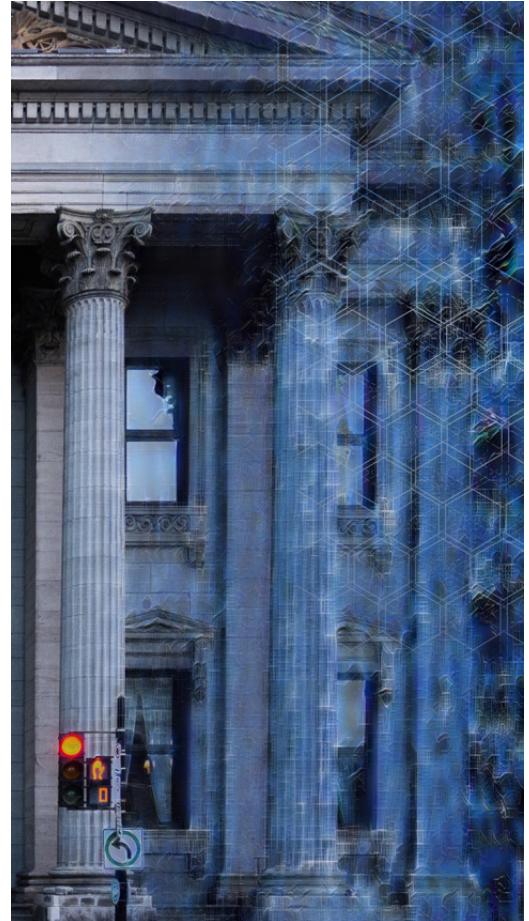
### Banking

DeFi increasingly poses challenges to the current banking system. One important area where DeFi could outperform incumbent institutions in the near future is increased financial inclusion. Traditional banks have tried for some time to engage underbanked individuals—those who have limited to no

access to traditional financial services—by offering services without KYC and physical bank account requirements, but have largely been unsuccessful due to regulatory concerns. DeFi's relatively low thresholds to entry, looser lending requirements, and simplicity offered by mobile access have enabled projects such as the Kenyan Microwork project, in which workers receive payment for completed work through a mobile phone, and then use the same mobile device to transact or store that payment. Access to financial services through blockchain technology can also fulfil an organisation's environmental, social, and governance (ESG) commitments and provide assistance to refugees in times of global crisis.

Many improvements in traditional digital banking services have begun to allow for faster and cheaper international transfers of funds. For example, Wise (formerly known as TransferWise) offers one of the cheapest methods for international funds transfers in fiat currencies. The platform is straightforward and presents the user with a snapshot of the entire transaction (Wise, 2021).

Such cross-border transactions made with bitcoin and other cryptocurrencies are even more efficient, however, as crypto transfers eliminate the need for a fiat currency exchange or intermediaries like a bank or transfer company. In addition, cryptocurrency transfers are usually faster (often near-instant) than traditional services.



## Guest Video: DeFi and Financial Inclusion

In the following video, Yves Messy discusses the benefits of DeFi for those without or limited access to traditional financial services.



DeFi, obviously known as decentralised finance, is a new category of blockchain-based financial instruments and financial services that are notorious or famous for not requiring anything more than a balance and a blockchain address. And when compared to traditional financial services around the world that usually require extensive know-your-customer requirements, extensive due diligence requirements, extensive credit histories, and identity as a requirement itself, in order to access these traditional services, DeFi is standing out as a new type of financial industry that provides services to just anyone without any discrimination whatsoever.

That changes things for financial inclusion, because financial inclusion itself has been historically a huge issue where 3 billion people in the world don't have an identity card and are therefore excluded from the global financial industry. So DeFi is a potential answer to this, in that a farmer in somewhere in Nigeria without an identity can suddenly buy a bit of Ethereum, get an address on Ethereum and access to banking services, access DeFi loans on Avi, invest in future performance of stock indexes, on binance stocks—about a type

of cryptocurrency system that mirrors the price of stocks, and allows people with an Ethereum address to essentially access the future performance of that stock without having to give any identity themselves. So this is a game-changer for financial inclusion. And over time we'll see these DeFi products being increasingly bridge to centralised entities. But for now, you can essentially just have an internet connection anywhere in the world, and build a financial life the way that was impossible 20 years ago.

## Beyond DeFi

Ethereum's creator, Vitalik Buterin, believes DeFi should think beyond the narrow confines of a financial platform. In his keynote address to the Ethereum Community Conference, he implored the stakeholders to innovate beyond dApps for finance, using decentralised social media as one example of a direction Ethereum could diversify with its DeFi-oriented technology. One feasibility challenge of decentralised social media involves transaction costs, and that must be solved. If every tweet became an NFT, for example, what would the transaction cost be for each of them?

As more and more layers are developed on the Ethereum platform, Buterin says, DeFi should not be the primary deliverable, although it has been a welcomed one. With increased layers, financial risk increases and creates the threat of collapse. Buterin strongly encourages the community to move beyond DeFi (Haig, 2021).

### 6.2.7 Key Takeaways, References, and Further Exploration

#### Key Takeaways

Let's review the key points of this section:

1. Decentralised finance, or DeFi, is an emerging sector of the crypto and blockchain industries that leverages blockchain technology to make most financial activities possible through peer-to-peer networks, thus removing intermediary layers. Instead, DeFi facilitates transactions using Web 3.0, which allows users to interact while owning and maintaining control of their own data.
2. Value propositions of DeFi include:
  - Self-custody of funds through the use of a digital wallet
  - Lending and borrowing through peer-to-peer arrangements using smart contracts
  - Trading without intermediaries on a decentralised exchange (DEX)
  - Permissionless, liquidity pool-based automated market-making
  - Providing liquidity through token pools

3. DeFi transactions involve risks that include:
  - Custody risks
  - Lending risks
  - Automated market-making risks
4. DeFi insurance offers a solution to some of these risk factors, and utilises smart contracts to pay claims.
5. Key players in the industry, including the largest and most influential exchanges and reporting entities, include DeFi Pulse, Aave, Curve Finance, Synthetic, and Uniswap. DeFi Pulse reports market activity in real time, and the other four organisations all have billions in total value locked (TVL) yearly.
6. The future of DeFi involves a broader set of risks, competitive pressures with traditional banking, and a nudge by Ethereum's founder to explore beyond DeFi.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 26 April, 2022.

### 6.2.2 What is DeFi?

Binance Academy. (2020, 2 April). Censorship-resistance. <https://academy.binance.com/en/glossary/censorship-resistance>

Codjia, M. (2017, 26 September). What Is Financial Disintermediation? *Biz Fluent*. <https://bizfluent.com/info-8310903-financial-disintermediation.html>

Fang, L., Ivashina, V., & Lerner, J. (2013, August). The Disintermediation of Financial Markets: Direct Investing in Private Equity [working paper 19299]. *National Bureau of Economic Research*. [https://www.nber.org/system/files/working\\_papers/w19299/w19299.pdf](https://www.nber.org/system/files/working_papers/w19299/w19299.pdf)

Hayes, A. (2021, 6 July). Disintermediation. *Investopedia*. <https://www.investopedia.com/terms/d/disintermediation.asp>

### 6.2.3 Value Propositions of DeFi

Bloomenthal, A. (2021, 31 August). Market Maker. *Investopedia*. <https://www.investopedia.com/terms/m/marketmaker.asp>

Carey, T. (2021, 20 October). Payment For Order Flow (PFOF). *Investopedia*. <https://www.investopedia.com/terms/p/paymentoforderflow.asp>

Centre. (no date). Website home page. <https://www.centre.io>

Collie, F. (2020, 10 July). Not your keys, not your coins: lessons from QuadrigaCX fraud. *Investment Executive*. <https://www.investmentexecutive.com/news/industry-news/not-your-keys-not-your-coins-lessons-from-quadrigacx-fraud>

Cryptopedia. (2021a, 14 March). What Are Automated Market Makers? *Cryptopedia*. <https://www.gemini.com/cryptopedia/amm-what-are-automated-market-makers>

Cryptopedia. (2021b, 4 July). Hot Wallets vs. Cold Wallets. *Cryptopedia*. <https://www.gemini.com/cryptopedia/crypto-wallets-hot-cold>

Dedezade E., Phillips, D., & DiSalvo, M. (2020, 23 November). What is Yield Farming? Beginner's Guide. *Decrypt*. <https://decrypt.co/resources/what-is-yield-farming-beginners-guide>

Hayes, A. (2020, 6 October). Loan-to-Value (LTV) Ratio. *Investopedia*. <https://www.investopedia.com/terms/l/loantovalue.asp>

Hayes, A. (2021, 29 August). Liquidity. *Investopedia*. <https://www.investopedia.com/terms/l/liquidity.asp>

Sharma, T. (n.d.). What is a Blockchain Oracle? A Detailed Overview. *Blockchain Council*. <https://www.blockchain-council.org/blockchain/what-is-a-blockchain-oracle-a-detailed-overview>

Vermaak, W. (2020, 6 December). What Are Decentralized Exchanges (DEX)? *CoinMarketCap*. <https://coinmarketcap.com/alexandria/article/what-are-decentralized-exchanges-dex>

Wilcox, L. (2021, 4 September). Understanding Ethereum fees: How gas works. *Luno*. <https://www.luno.com/blog/en/post/understanding-ethereum-fees-how-gas-works>

WSUM Network (2021, 6 April). DeFi—Arbitrage and Carry Trade Strategies. <https://wsum.network/2021/04/06/defi-arbitrage-and-carry-trade-strategies>

### 6.2.4 DeFi Risks

Binance Academy. (2021, 4 November). Rug pull. <https://academy.binance.com/en/glossary/rug-pull>

Harvey, C., Ramachandran, A., & Santoro, J. (2021, 5 April). *DeFi and the Future of Finance*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3711777](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3711777)

Jakub. (2020, 21 August). What is Impermanent Loss? DeFi Explained. *Finematics*. <https://finematics.com/impermanent-loss-explained>

Mozée, C. (2021, 31 August). Cryptocurrency hacks and fraud are on track for a record number of incidents in 2021, data shows. *Markets Insider*. <https://markets.businessinsider.com/news/currencies/cryptocurrency-hacks-fraud-cases-record-bitcoin-ethereum-wallets-breaches-defi-2021-8>

Nexus Mutual. (no date). Get covered against smart contract failure & exchange hacks. *Nexus Mutual*. <https://nexusmutual.io>

### 6.2.5 Key Players

DeFi Pulse. (no date). DeFi Pulse. <https://defipulse.com>

### 6.2.6 The Future of DeFi

Haig, S. (2021, 22 July). Ethereum must innovate beyond just DApps for DeFi degens: Vitalik Buterin. *Cointelegraph*. <https://cointelegraph.com/news/ethereum-must-innovate-beyond-just-dapps-for-defi-degens-vitalik-buterin/amp>

Wise. (2021). Home page. <https://wise.com>

## Further Exploration

### Trading

Trading is another function that has traditionally been managed by centralised institutions, including banks, clearinghouses, market makers, and brokerage services. In the traditional financial system, centralised exchanges (or CEXs) use order book matching services to match the highest price a buyer is willing to pay for a security with the lowest price a seller is willing to accept for that security. Order book matching engines require fast and highly scalable infrastructure to process millions of transactions per second. Similarly, market makers rely on fast trading infrastructures to identify inefficiencies in the price of securities which they can exploit for a profit. Together, order book matching engines and market makers help facilitate orderly and efficient markets for individuals and institutions to trade securities.

### Oracles

One of the first solutions that enabled DEXs to get accurate price readings was the development of smart contract oracles. Oracles are decentralised protocols that receive external data from different on-chain or off-chain sources, verify and authenticate the data, and feed it into smart contracts to help the contracts execute based on accurate and near real time information (Blockchain Council, n.d.).

# 6.3 The Future of Central Bank Digital Currencies (CBDCs)

## 6.3.1 Overview

### Overview

Module 2 introduced the concept of a central bank digital currency (CBDC), which is, in its simplest terms, a sovereign version of a stablecoin or cryptocurrency. Oxford's Dictionary of Economics defines a central bank as "A bank which controls a country's money supply and monetary policy. It acts as a banker to other banks, and a lender of last resort. In some countries, including the UK, the central bank is also the main regulator of other banks" (Oxford Reference, 2021).

A CBDC is similar to electronic cash in that it does not involve paper currency. While electronic cash is typically part of a traditional demand deposit account, however, a CBDC requires a separate digital wallet and exists in the cryptocurrency ecosystem, relying on blockchain technology for its infrastructure. A CBDC, then, represents another valid form of currency used in myriad ways to benefit the bank and, in theory, its constituent banks or citizens. In this section, we will analyse two considerations that could compel a central bank to create a digital currency, as well as some opposing views.

## 6.3.2 CBDCs as the Competitor

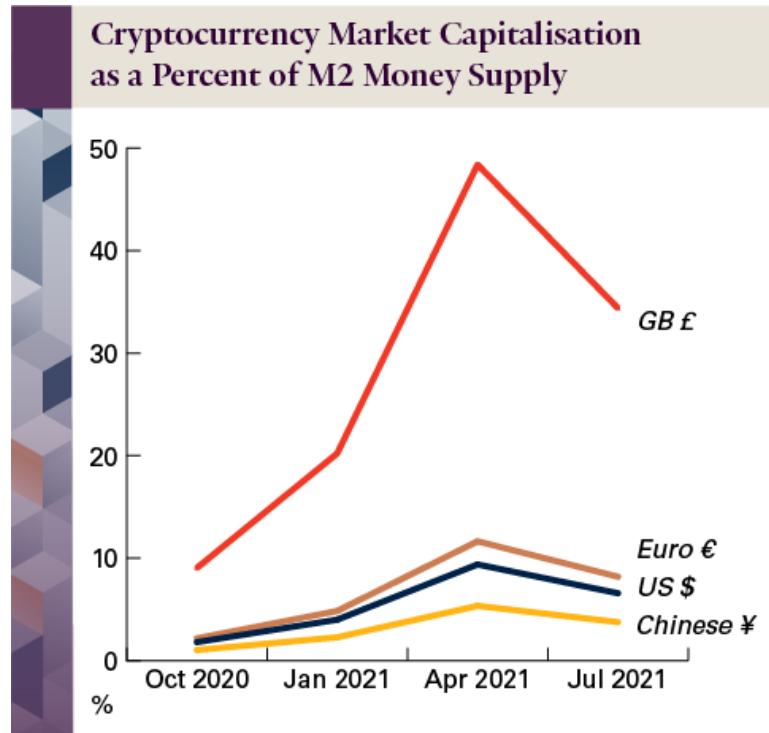
### CBDCs as the Competitor

In Module 2, we learnt that CBDCs could be exploited by an authoritarian government and used for unethical practices. However, some countries may see the need for a CBDC to provide financial inclusivity for their citizens. In capitalist countries, establishing a CBDC could provide the central bank with a competitive foothold in cryptocurrency growth. In fact, in many countries with large economies, the percentage of cryptocurrency market capitalisation to M2 money supply has increased dramatically in the last year. M1 money supply and M2 money supply are defined as follows by the US Board of Governors of the Federal Reserve System (2021):

- **M1 money supply** is composed of physical currency and coin outside the US Treasury, Federal Reserve Banks, and the vaults of depository institutions; demand deposits, travelers' checks, other checkable deposits, and negotiable order of withdrawal (NOW) accounts. M1 includes the most liquid portions of the money supply because it contains currency and assets that either are or can be quickly converted to cash.
- **M2 money supply** is everything listed in the M1 money supply plus near money, which includes savings and money market deposits less than US \$100,000 and omitting IRA and Keough balances at depository institutions.

Accompanying is a graph that shows the percentage of cryptocurrency market capitalisation to the M2 money supply for the US, Europe, and China. The main takeaway from this analysis is that the percentages substantially increased over the course of a year. This is a trend worth paying attention to as it may be an indicator of a central bank's efforts to launch its own digital currency.

The chart also reflects the volatility of cryptocurrency prices as indicated by the larger percentages in the April 2021 timeframe. Still, the overall trend is upward. One other point to note is the Covid-19 pandemic's effect on the M2 money supply. Many central banks increased their money supply to stimulate their economies. Without this, it may be that cryptocurrency market caps were at an even higher percentage. However, that cannot be stated with certainty, as cryptocurrency prices may have been impacted by the pandemic as well.



### 6.3.3 A CBDC's Impact on Negative Interest Rate Policy

#### A CBDC's Impact on Negative Interest Rate Policy

Regarding a government's control over interest rates, a CBDC would allow more discretion in assigning interest rates by certain demographics. A CBDC could make a negative interest rate policy more attainable through such demographic controls.

In addition, a central bank could more easily establish a negative interest rate policy (NIRP) through the use of a CBDC. The late Marvin Goodfriend, an American economist and professor at Carnegie Mellon University, makes a case for negative interest rates in his paper, "The Case for Unencumbering Interest Rate Policy at the Zero Bound". Specifically, he describes three approaches central banks could use to create the ideal conditions to effectively execute a negative interest rate policy (Goodfriend, 2016):

- **Abolish paper currency.** In a NIRP environment, holding paper currency provides individuals with the assurance they will only lose the purchasing power of their currency over time due to inflation while still retaining its face value, even if it means earning 0% interest. By abolishing paper currency, retail bank depositors would be left with no alternative but to keep their funds in electronic bank accounts where negative interest rates can effectively take hold. While such an action would face resistance from the public today, the increase in adoption of digital currencies

and mobile payments solutions, such as Venmo and CashApp, makes the likelihood of resistance decrease over time.

- **Introduce a market-determined flexible deposit price of paper currency.** In doing so, central banks could deter the use of paper currency by making it as costly for consumers to acquire as it would be for them to deposit the funds in their bank accounts and incur losses from negative interest rates. The price of paper currency is normally tightly controlled by central banks to either supply the market with more cash to satisfy excess demand or remove cash from the market to satisfy excess supply. To deter the use of paper currency, central banks could adopt a more market-driven approach to pricing paper currency and allow the deposit price to rise according to the level of demand for cash. This would naturally correlate to the steepness of NIRP. As interest rates become more negative than they were initially, an increase in the deposit price of paper currency would ultimately make the cost of acquiring and holding cash not worth the benefits of avoiding NIRP.
- **Provide electronic currency (to pay or charge interest) at par for deposits.** This action would enable central banks to pay or charge interest on electronic currency held by individuals in the same way that central banks currently pay and charge interest on reserve balances held by commercial banks. Instead of tightly controlling the price of paper currency, central banks would now use their ability to pay and charge interest as a tool to fix the price of electronic cash: they would pay interest to encourage demand for electronic cash through saving, and charge interest to encourage supply through spending. This would ultimately make electronic cash the preferred method for holding fiat money over paper currency.

Although Goodfriend's proposed NIRP strategies focus on fiat money, these same strategies could apply to a central bank's implementation of a CBDC, as a CBDC is very similar to electronic cash. With all currency being electronic, and electronic cash being the cheapest and most convenient form in which consumer and commercial banks can move and store money, central banks would be able to set negative interest rate policies for fiat or digital currencies.

### 6.3.4 The Case Against CBDCs

#### The Case Against CBDCs

There is much discussion and investigation into the benefits of central banks launching a digital currency. There is also some dissent worth noting, however, as this discovery process continues. Some opposing viewpoints from the United States, Europe, and the United Kingdom are presented below.

## United States

Two high-ranking officials from the US Federal Reserve System have offered a sceptical outlook on a US CBDC. Federal Reserve Chair Jerome Powell announced in May 2021 that the Fed would publish a discussion paper with the results of the central bank's research on creating a digital currency and its implications.



Christopher J. Waller, a member of the Federal Reserve Board of Governors, presented his views opposing CBDCs on 5 August, 2021 at the American Enterprise Institute in Washington, DC, framing his primary thoughts around two questions (2021):

- What problem would a CBDC solve?
- Alternatively, what market failure or inefficiency demands this specific intervention?

In his analysis, Waller focuses on a general public account-based CBDC, which would require an individual to hold an account directly with the Federal Reserve Bank (FRB) instead of with a commercial bank. He reviews the current relationship between the FRB and commercial banks and notes that Congress did not establish the FRB to provide accounts directly to the public but, instead, to provide accounts and support to the commercial banks. A CBDC may put the government, via the FRB, in direct competition with the commercial banks. Economically speaking, that should only happen when there is a need to address market failures. Waller reinforces this point several times in his speech, and notes that congressional legislation would be required to make it happen.

In addressing the question of what problem a CBDC would solve, Governor Waller puts forth several ideas in the form of questions for which he had significant rebuttals, including these:

- Would a CBDC result in a larger and more efficient payment system?
- Are existing payment services too slow or too expensive?
- Would a CBDC offer financial inclusion for those without access to payment systems?

Waller's remarks conclude with a final question about stablecoins posing a threat to the FRB's monetary policy, which Waller counters by explaining that commercial banks, stablecoins, and any country that pegs its exchange rate to the US dollar all have a vested interest in the strong valuation of that dollar (Waller, 2021).

## Europe

In a working paper published by the European Central Bank in January 2020, two major arguments were discussed as counters to the benefits of a CBDC (Bindseil, 2020):



- **Structural disintermediation of the commercial banking sector.** The wider presence of central banks in the commercial banking system could lead to depositors opting for CBDC deposits, thus creating a drain on commercial bank deposits. Moreover, low yields on deposits at commercial banks could also cause funds to shift to a less risky CBDC and, therefore, increase funding costs for banks.
- **Systemic runs on banks in times of crisis.** Further commercial bank instability could arise in crisis situations, especially if depositors do not feel their money is safe in a commercial bank. If a bank run occurs, depositors may shift their funds from private or public commercial banks to the CBDC that the central bank governs.

The European Central Bank is investigating the implementation of a CBDC, and while the paper presents several benefits of doing so, these potential negative outcomes warrant a careful consideration in the CBDC exploration process.

## United Kingdom

In August 2021, Redfield & Wilton Strategies, a member of the British Polling Council, conducted a poll for the nonpartisan political and policy news organisation, Politico. The company surveyed the views of 2,500 Britons on a potential UK CBDC, already nicknamed Bitcoin (Smith-Meyer, 2021). This poll largely revealed that Brits are more suspicious of than excited about the benefits that a CBDC would offer. Some of the notable discoveries are as follows (Redfield & Wilton Strategies, 2021):



- Only 24% of the people surveyed believe a digital pound will bring more benefits than harm; 30% said it would bring more harm than benefits; the remainder were undecided.
- 73% were wary of the threat of cyberattacks on and hacking of the central bank.
- 70% were concerned about losing payment privacy.
- 45% were aware of a CBDC's potential environmental impact.
- 62% were fearful of having their digital funds seized by public authorities.

Politico reports that one of the primary areas of consideration the Bank of England has in issuing a CBDC is that of public trust. This poll reveals the uphill battle faced by the central bank in pursuing this endeavour (Smith-Meyer, 2021).

## **6.3.5 CBDCs Around the World**

### **CBDCs Around the World**

At the T20 Summit, held on the 4–6 October, 2021, in Italy, Kristalina Georgieva, Managing Director of the International Monetary Fund (IMF), spoke on digital currencies with specific mention of CBDCs. She stated that the IMF looks at digital currencies from a macroeconomic and financial stability standpoint. She also claimed the CBDC is the most reliable form of digital currency as it is backed by the state and integrated into the state's monetary policy. Georgieva concluded her remarks with the acknowledgement that CBDCs are still a novelty, and the IMF has a crucial role in their development in terms of interoperability and their impacts on monetary policy (Okuwoga, 2021).

#### **The Bahamas**

Launched in October 2020, the Sand Dollar, the CBDC for the Bahamas, is the first-ever CBDC launched by a central bank (Okuwoga, 2021).

#### **The Eastern Caribbean Currency Union (ECCU)**

The Eastern Caribbean Central Bank launched DCash in March 2021. It is the first CBDC launched by the central bank of a monetary union and was piloted by four of the eight countries in the union (Ledger Insights, 2021).

#### **Europe**

In a speech during a panel discussion at the UK G7 Presidency Conference on 8 October 2021, Fabio Panetta, Executive Board Member of the European Central Bank (ECB), announced the ECB's intent to explore the implementation of a CBDC. Citing its potential to provide stability for the digital finance ecosystem, domestic and global, the European Central Bank has started the investigation phase of a retail CBDC (Norrestad, 2021).

#### **UK**

The Bank of England announced the CBDC Taskforce in March 2020. There has been no commitment by the government to implement a digital currency, but it recognises the benefits of doing so. The task force will direct its strategic approach and coordination between UK authorities (Bank of England, 2021).

#### **Switzerland**

In June 2021, the Swiss Bankers Association published a discussion paper that mentioned a successful feasibility study and implied that a Swiss CBDC was virtually inevitable (Swiss

Bankers Association, 2021). However, the purpose of the paper was to contribute to the general discussion surrounding digital currencies, and Switzerland has not committed to implementing a CBDC.

## **Sweden**

The eKrona (Swedish CBDC) launched in September 2021 (Contreras, 2021).

## **Nigeria**

The Central Bank of Nigeria launched the eNaira in October 2021 (Crawley, 2021).

## **Cambodia**

The National Bank of Cambodia launched the Bakong digital currency in October, 2020 (Takemiya, 2021).

## **China**

As one of the world's first countries to implement a CBDC, China has ambitious plans for its digital yuan. The CBDC research began in April 2020, with the goal of piloting the digital yuan during the 2022 Beijing Winter Olympics. By mid-January 2022, ahead of the games, the People's Bank of China (PBOC) reported that more than 261 million individual users had set up digital wallets with 87.5 billion yuan (US \$13.78 billion) worth of transactions completed (Liao, 2022). In February 2022, during the Beijing Winter Olympics, the digital yuan was being used to make payments of 2 million yuan (US \$315,000) per day (Jones, 2022).

## **Japan**

The Bank of Japan launched a liaison and coordination committee to prepare for an initial proof-of-concept phase scheduled for April 2021. In July, the government stated there would be a clearer picture in 2022 of what the country's CBDC would look like, noting the impacts it would have on financial institutions and their settlement systems (Sinclair, 2021).

## **Australia**

In September 2021, the Reserve Bank of Australia announced it planned to hire a CBDC expert to research the viability and impacts of a CBDC. The Australian Senate has not committed to pursuing a CBDC, however (CBDC Insider, 2021).

## Guest Video: Are CBDCs a Legitimate Long-Term Strategy?

In this video, Yves Messy speaks about who seems to be getting CBDCs right, and whether they are a long-term strategy.



I think CBDCs, which is what they're called, are an essential part of the digitization of finance, period. There is no way around it. And in the world where cryptocurrencies are, as I mentioned earlier, developing entire economies which are untethered from traditional finance, it's important that central banks, bank actors, learn to, essentially, be digital first by definition and build on those, leveraging additional exponential technologies like AI, IoT, edge computing, and everything else.

So right now, there's a big race around the world. And I'm very lucky that I was able to work on this CBDC blueprint with R3, the largest company developing CBDCs. And what we've seen, what I've seen personally as examples, is Sweden, which recently announced the e-krona in practice, which is distributed with a number of Swedish banks. And they're able to distribute these to their customers.

Another great example is the Swiss National Bank. And they've recently had the e-Swiss franc, which is now bankable and is now being used to help pay for tokenized assets in a Swiss ecosystem today. These countries are getting it right.

One country that may be getting it in a way that's probably interesting and worth analyzing is China. Because, of course, you have an issue, when developing CBDCs, where a government should decide how much privacy their citizens should have when everything is digitized. And they, frankly, own the infrastructure where the information is being produced. So I think there'll be constitutional battles around the privacy of CBDCs. But Sweden and Switzerland are probably the most advanced today in terms of how to put these in practice while respecting human rights and personal privacy.

### 6.3.6 Key Takeaways, References, and Further Exploration

#### Key Takeaways

Let's review the key points of this section:

The question of whether or not a government should pursue the creation of a CBDC involves many factors that are unique to that government. In this section, you learnt about two potential justifications for pursuing a CBDC:

- CBDC as a potential monetary policy solution
- CBDC as a mechanism for implementing a negative interest rate policy

In addition, you learnt reasons against pursuing a digital currency:

- It is unclear what problem CBDC solves. Or, what market failure or inefficiency demands this specific intervention?
- Concerns about privacy and cyber attacks.
- Possible disintermediation of the commercial banking sector and systemic runs on banks in times of crisis.
- The environmental impact.

Lastly, you learnt about the position on CBDCs held by the managing director of the International Monetary Fund and several worldwide efforts to launch a CBDC.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 26 April, 2022.

### 6.3.1 The Future of Central Bank Digital Currencies (CBDCs)

Oxford Reference. (2021). Overview Central Bank. *Oxford University Press*. <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095558535#:~:text=Quick%20Reference%20A%20bank%20which%20controls%20a%20country%27s,is%20also%20the%20main%20regulator%20of%20other%20banks>

### 6.3.2 CBDC as the Competitor

Board of Governors of the Federal Reserve System. (2021, 28 September). Money Stock Measures - H.6 Release. *Federal Reserve System*. <https://www.federalreserve.gov/releases/h6/current/default.htm>

Board of Governors of the Federal Reserve System (US). (2021, 25 October). M1 [M1SL]. *FRED, Federal Reserve Bank of St. Louis*. <https://fred.stlouisfed.org/series/M1SL>

CoinMarketCap. (2021, 6 October). Total Cryptocurrency Market Cap. <https://coinmarketcap.com/charts>

Take-Profit.org. (2021). China Money Supply Data. <https://take-profit.org/en/statistics/money-supply-m1/china>

### **6.3.3 A CBDC's Impact on Negative Interest Rate Policy**

Goodfriend, M. (2016, August 26). The Case for Unencumbering Interest Rate Policy at the Zero Bound. *Jackson Hole Economic Policy Symposium*. [https://www.kansascityfed.org/documents/7033/GoodfriendPaper\\_JH2016.pdf](https://www.kansascityfed.org/documents/7033/GoodfriendPaper_JH2016.pdf)

### **6.3.4 The Case Against CBDCs**

Bindseil, U. (2020, January). Working Paper Series: Tiered CBDC and the financial system. *European Central Bank*. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf>

Redfield & Wilton Strategies. (2021, 13-14 August). Bitcoin Poll Results. *Politico*. <https://www.politico.eu/wp-content/uploads/2021/08/19/Bitcoin-Cover-Sheet.pdf>

Smith-Meyer, B. (2021, 23 August). Bitcoin? No thanks, UK survey says. *Politico*. <https://www.politico.eu/article/cryptocurrency-survey-uk-central-bank-digital-currency-fintech>

Waller, C. J. (2021, 5 August). CBDC: A Solution in Search of a Problem? *Board of Governors of the Federal Reserve System*. <https://www.federalreserve.gov/newsevents/speech/waller20210805a.htm>

### **6.3.5 CBDCs Around the World**

Bank of England. (2021, 8 September). Central bank digital currencies. <https://www.bankofengland.co.uk/research/digital-currencies>

CBDC Insider. (2021, 16 September). Reserve Bank of Australia Now Hiring CBDC Expert. <https://cbdcinsider.com/2021/09/16/reserve-bank-of-australia-now-hiring-cbdc-expert>

Chainalysis. (2021, 3 August). Insights: [Report Preview] Why is China Launching the Digital Yuan? *Chainalysis Insight*. <https://blog.chainalysis.com/reports/china-report-preview-digital-yuan>

Contreras, S. (2021, 10 September). Sweden Launches World's Second Digital Currency Backed by a Central Bank. *DailyCoin*. <https://dailycoin.com/sweden-launches-worlds-second-digital-currency-backed-by-a-central-bank>.

Crawley, J. (2021, October 25). Nigeria's eNaira CBDC Goes Live. *CoinDesk*. <https://www.coindesk.com/policy/2021/10/25/nigerias-enaira-cbdc-goes-live>.

European Central Bank. (2021, 8 October). Speech: Stay safe at the intersection: the confluence of big techs and global stablecoins. *European Central Bank*. <https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211008~3c37b106cf.en.html>

Jones, M. (2022, 16 February). Over \$315,000 in digital yuan used every day at Olympics, PBOC official says. *Reuters*. <https://www.reuters.com/technology/around-300-mln-digital-yuan-used-every-day-olympics-pboc-official-says-2022-02-15/>

Ledger Insights. (2021, 1 April). Eastern Caribbean launches central bank digital currency pilot DCash. *Ledger Insights*. <https://www.ledgerinsights.com/eastern-caribbean-launches-central-bank-digital-currency-cbdc-pilot-dcash>.

Liao, R. (2022, 18 January). China's digital yuan wallet now has 260 million individual users. *Yahoo*. <https://techcrunch.com/2022/01/18/chinas-digital-yuan-wallet-now-has-260-million-individual-users/>

Norrestad, F. (2021, 2 September). Monthly development of the money supply M2 in the euro area from January 2018 to July 2021. *European Central Bank*. <https://www.statista.com/statistics/921364/value-of-m2-money-supply-in-euro-area>

Okuwoga, T. (2021, 6 October). 110 Countries are Exploring CBDC At Some Stage, Says IMF Managing Director. *Bitcoinist*. <https://bitcoinist.com/110-countries-are-exploring-cbdc-at-some-stage-says-imf-managing-director>

Sinclair, S. (2021, 5 July). Japan's CBDC to Get a Clearer Picture by 2022, Says Government Official: Report. *CoinDesk*. <https://www.coindesk.com/markets/2021/07/05/japans-cbdc-to-get-a-clearer-picture-by-2022-says-government-official-report>

Swiss Bankers Association. (2021, June). Discussion paper: New Currencies for Switzerland? [https://www.swissbanking.ch/\\_Resources/Persistent/a/1/2/9/a1290092308e4ccb8d08841bfec49e97600cf1e9/SBA\\_Discussion\\_Paper\\_CDBC\\_EN.pdf](https://www.swissbanking.ch/_Resources/Persistent/a/1/2/9/a1290092308e4ccb8d08841bfec49e97600cf1e9/SBA_Discussion_Paper_CDBC_EN.pdf)

Takemiya, M. (2021, 30 August). Cambodia's digital currency can show other central banks the way. *World Economic Forum*. <https://www.weforum.org/agenda/2021/08/cambodias-digital-currency-is-showing-other-central-banks-the-way>

## Further Exploration

### The Case for Unencumbering Interest Rate Policy at the Zero Bound

The case Professor Goodfriend makes for a NIRP involves central banks utilising electronic cash. He does not specifically mention the use of a CBDC. Consider the following questions in reviewing this case study and share your thoughts with your class:

- Does a CBDC work for each of the three approaches?
- How would a CBDC be utilised for each approach?
- Does this case study indicate any reasons that would discourage the use of a CBDC?

## 6.4 The Future of Non-Fungible Tokens (NFTs)

### 6.4.1 Overview

#### Overview

Module 2 introduced the concept of non-fungible tokens (NFTs) and the digital scarcity associated with them. The allure of that digital scarcity is commonly associated with art and other collectables. As such, these tokens have realised early success in the blockchain ecosystem. A growing use case for NFTs is the tokenisation of physical world assets such as land registries. In this section, we will learn how NFTs are positioned for the future through the perspectives of:

- An in-depth understanding of what an NFT is
- The tokenomics of NFTs
- An NFT land registry project case study

#### Vocabulary Check

This section introduces the following terms:

- [ERC-20](#)
- [ERC-721](#)
- [ERC-1155](#)
- [tokenomics](#)
- [user interface \(UI\)](#)

### 6.4.2 NFTs Revisited

#### NFTs Revisited

NFTs are digital assets—and each one represents something unique, such as a work of art, a certificate, a collectible, land, or music. They are non-fungible, meaning one NFT cannot be exchanged for another NFT of the same asset, and they cannot be replaced. No NFT is equal to any other NFT—each NFT has a unique digital signature. In contrast, money, for example, is fungible and can be exchanged and replaced. One US dollar is always equal to another US dollar (Conti et al., 2021).

The ERC-721 token has been and continues to be the primary standard for NFTs on the Ethereum network. The ERC-1155 token offers an improvement on that standard by allowing one smart contract to represent multiple fungible and non-fungible tokens. In addition, the ERC-1155 allows for batched operations which will result in reduced network costs (OpenZeppelin, n.d.).

The accompanying chart shows cumulative NFT users over time for ERC-721 and ERC-1155 (combined) projects.

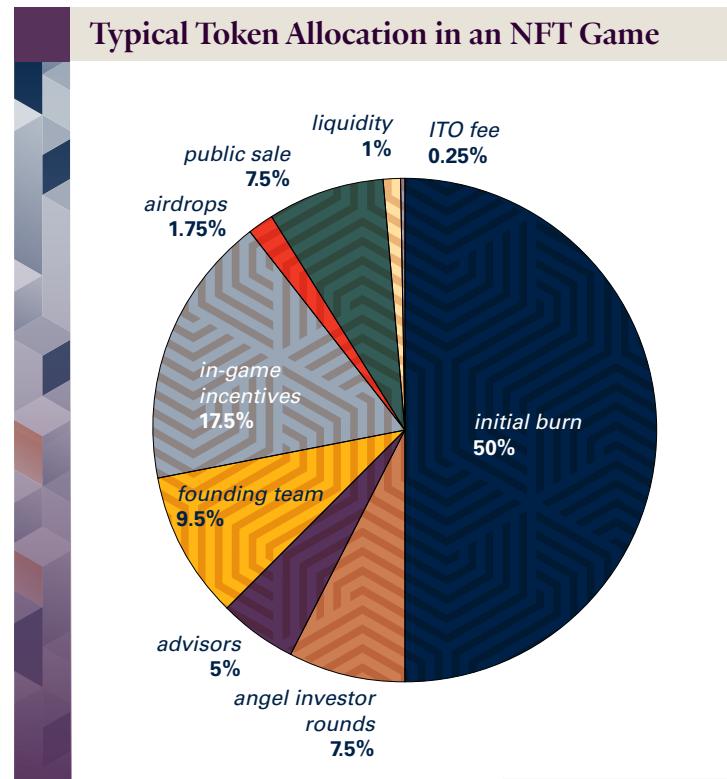
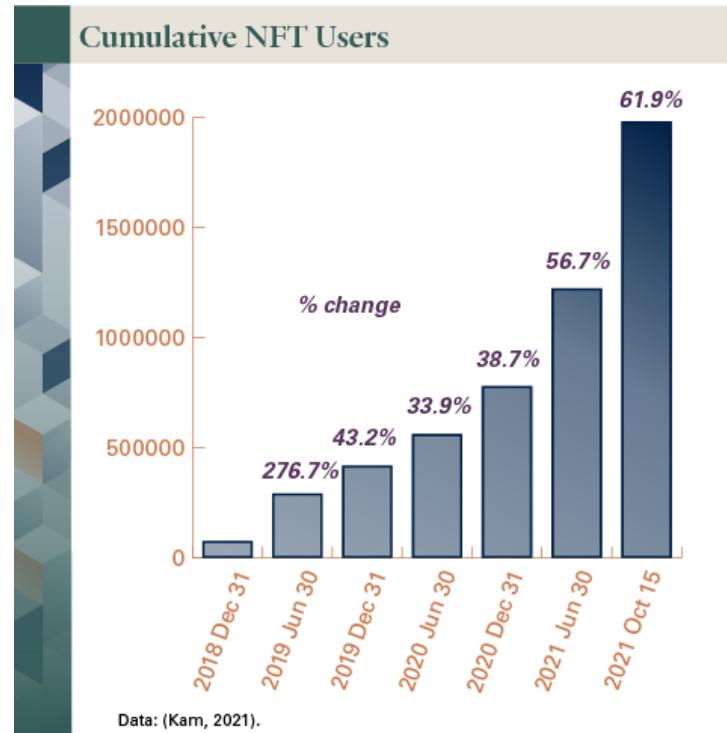
## Tokenomics

Simply stated, tokenomics is not about demand and supply of cryptocurrencies alone, but also about the economics of crypto tokens.

Economists measure fiat currency money supplies and report their figures based on how liquid the supply is. M1 represents the very liquid cash and cash-like money supply, and M2 represents all of M1 plus the near-cash money supply. These are the two primary figures reported, although there are categories for less-liquid money supplies. Nations around the world have printed new currency in times of need—pandemics and bank bailouts, for example.

With cryptocurrencies, tokens are created on a pre-set algorithmically determined issuance schedule. Economists can accurately predict how many coins will have been created at a point in time: for example, only 21 million bitcoin will be produced, and the production schedule will conclude in approximately the year 2140. Not all coins have maximum supply caps, however. Questions to consider in understanding a particular cryptocurrency's supply include (Langridge, 2021):

- How many tokens currently exist?
- How many tokens will exist in the future?



(Shafiq, 2021).

- What amount of tokens have been lost, burned (permanently removed on purpose), or deleted?

Tokenomics for an NFT include the supply and demand characteristics of the token, but there are other considerations too. There might be incentives or rewards, airdrops (free tokens distributed to wallet addresses), and investor allocations. To better understand the many tokenomics considerations of an NFT, let's look at the EpicHero 3D NFT (EPICHERO), a play-to-earn NFT game built on the ERC-721 token standard.

As described by the technical author Hassan Shafiq, EpicHero is a 3D NFT war game operating on the Binance Smart Chain. The game provides incentives, known as reflection rewards, to its token holders in BNB coins, and it has a burning mechanism that decreases the number of heroes in the game over a certain period. There is a card marketplace where players can trade battle card NFTs. Holders of EPICHERO tokens can vote for the heroes they want in the game.

A 5% buy tax and 15% sell tax are charged on token transactions, and 50% of these taxes are rewarded back to EPICHERO token holders (Shafiq, 2021).

The EpicHero game has multiple factors that affect the supply and demand of the EPICHERO token. Any time a burn occurs, the decreased supply and demand for the token may cause its price to increase, for example. The ERC-721 token allows for a myriad of ways to be creative in utilising a token, such as in this game.

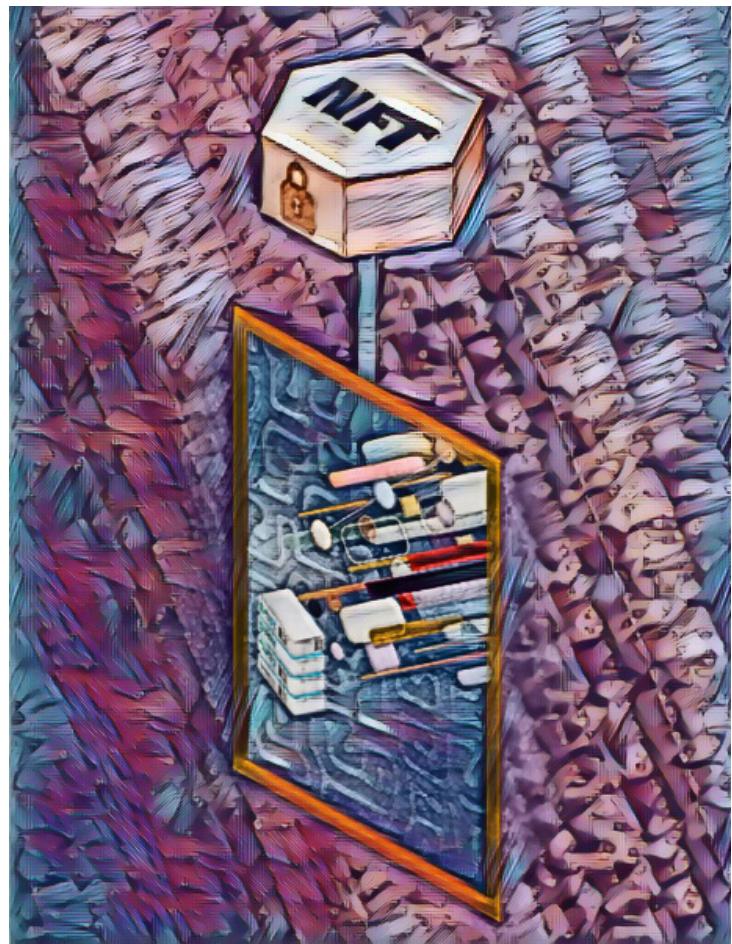
#### **6.4.3 The Future of NFTs**

##### **The Future of NFTs**

The internet public is generally familiar with the concept of NFTs, but questions remain. With regard to the NFT frenzy in general and digital art in particular, “people ask, ‘Why on Earth would someone pay millions of dollars for a JPEG that I can simply ‘right-click/save’ to my hard drive?’” (Casey, 2021).

A digital artwork NFT contains provably scarce markers of value and represents specific rights—granted by the copyright owner of that artwork—to that digital artwork, which is not the same as simply possessing a digital image of the artwork.

Michael Casey, Chief Content Officer at CoinDesk, explains that the enforcement of digital rights was widely forfeited in the pre-Bitcoin era due to the lack of a decentralised



tracking mechanism like the non-fungible token. If not tokenised, digital property is easily replicated. The digital world learned to license certain media that would be widely distributed, such as music and books. The licenses typically granted personal use of the work rather than ownership and thus curbed the piracy that had become rampant (Casey, 2021).

According to Casey, the arrival of social media set new licensing standards. Platforms like Facebook and Twitter required users to sign over their content's copyright, thereby allowing the platforms' other users to share the content with even more users. This created and perpetuated the network effect. The allure of mass coverage of user content drew in many commercial organisations that wanted their content broadcast widely in this dominant media space. However, what these entities gained in coverage, they lost in the forfeiture of direct relationships with their communities, now controlled by the large platforms.

## The Role of NFTs in the Creator Economy

Creators own the underlying content of the NFT associated with it. The NFT does not grant ownership to a buyer. Instead, the asset owner controls only the rights that accompany the NFT. A buyer of an NFT for a work of art, as an example, can have certain media rights for usage of the art, but that depends on what the copyright owner of the art grants along with the NFT. Still, the use of NFTs in the creator economy could help restore one-to-one buyer/seller relationships that were lost to big sales platforms like Amazon. In addition, NFT communities are being formed, as well as DAOs, that directly support certain collectives in the creator economy (Casey, 2021).

As NFT use has increased exponentially, NFT markers for digital property rights are budding in opportunity. NFT growth is probable in mainstream areas such as gaming, fashion, real estate, DeFi NFTs, events, and more. The potential is open-ended at this early phase of the NFT market.

Infrastructure is growing in support of the NFT market and the creator economy at large. For example, some platforms cater to the content creator by streamlining the NFT creation process. What was once only managed by blockchain engineers in a development environment is now built behind the user interface (UI), making it as intuitive as possible and attracting more users without programming skills. These platforms may offer educational services and a supportive community in addition to a turnkey-style solution to launch an NFT. Infrastructure is an area to monitor in the fast-growing NFT space.

## Unique NFT Use Cases

Fractionalised NFTs and NFTs and DeFi represent some creative and forward-thinking approaches to tokenising digital assets:

**Fractionalised NFTs.** Similar to fractionalised bitcoin ownership, fractionalised NFTs represent a small percentage of ownership. At this point, however, the NFT's fraction is no longer an NFT, as it has become fungible, meaning the fractional values are equal and exchangeable. There are two major goals with fractional NFTs (Manoylov, 2021):

- Investors without much capital can participate in the purchase of an NFT that they might not otherwise be able to afford. This process also allows the investor to diversify their NFT holdings affordably.
- The property owner can reach a larger investor audience and, therefore, increase their access to liquidity for the sale of their NFT. Because of this wider reach, speculators may bid up the price as well.

Fractional and PartyBid are two platforms that allow fractional NFTs.

**NFTs and DeFi.** Borrowing through decentralised finance involves pledging cryptocurrency to collateralise the loan. The collateral is usually an amount greater than the loan amount and can be double the loan amount in some cases. A new collateral option is to pledge an NFT as collateral on a DeFi loan. Should the borrower not repay the loan, the NFT becomes available for foreclosure and transfers to the lender at the lender's discretion. The NFT asset is held in escrow, and the terms of the loan are locked into a smart contract, ensuring the automated functionality of the loan.

- The risk for the lender lies in establishing the loan-to-value ratio and the NFT asset's price fluctuations.
- The borrower's risk is primarily based on the loan terms and ability to repay or lose the NFT asset.

## Guest Video: NFT Future Use Cases

In the following video, Yves Messy reviews some innovative use cases for NFTs in the near future.



NFTs have come to public mainstream lately because, of course, they're 10,000 to 50,000% return on investment for many people who were initially involved. And these prices have dramatically crashed recently—90% down at the time this is being recorded.

And what I'm dealing with now personally as a VC and as a developer myself is there was a lot of people now thinking, yes, there was a speculative wave around NFTs. Now, what can we actually do with NFTs really to add value now that the speculative wave has gone?

What this translates to in practice is that you can have an insurance policy represented as an NFT and traded by reinsurance companies. You can have a derivative contract created as an NFT, and you can have a basket of them indexed as a single DeFi token that manages these NFT contracts.

You can also have a lot more such things. You can tranche receivables and do a collateralised debt obligations, each being a basket of DeFi interfacing with other stablecoins or fiat currencies.

I think this thinking is what's currently happening in practice. It's not theory. It's literally what was open in my computer this morning and that of many others that I know in a DeFi and blockchain space working on making NFTs a reality.

Now, what does that mean for tokenising lands around the world? I think Western countries, generally speaking, in the G8 have extensive histories, 400 year history of making appropriate rules and liquid instruments for things like buying and selling real estate. So I don't see tokenisation changing much in that context.

But the developing world—which will be responsible for more than 50% of GDP growth annually year on year going forward—doesn't have such an infrastructure and are finding themselves starting from scratch with incredibly digitised, fast-paced, liquid, and instant means of tokenising real estate. So I see this happening a lot more in developing countries, what we used to call developing countries. But I would say emerging markets. And I think that's where then innovations from countries like China, India, South Africa, Nigeria will inspire maybe changes to the way real estate is traded in developed markets, such as the UK.

## 6.4.4 Case Study: Tokenising the Land Registry in the Republic of Georgia

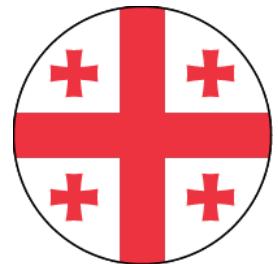
### Case Study: Tokenising the Land Registry in the Republic of Georgia

In April 2016, a global emerging technologies organisation, the Bitfury Group, announced the launch of a blockchain-based land registry in partnership with the Republic of Georgia's National Agency of Public Registry (NAPR). As the world's first blockchain-based land-titling project, this effort was to provide a strong building block in the NFT ecosystem, specifically by tokenising real estate and preserving ownership records on the blockchain (Allison, 2017).

### History of the Republic of Georgia

Georgia is a small country bordered by the Black Sea, the Greater Caucasus Mountains, Russia, Azerbaijan, Armenia, and Turkey. Its history is rich in territorial detail and involves hundreds of years of conflict and rule by outside territories and countries like Russia.

In 1989, Georgia was one of the first Soviet republics to move towards independence. In May 1991, the first presidential elections were held, with an 87% vote for Zviad Gamsakhurdia. Gamsakhurdia was expelled in January 1992, and democratic elections were suppressed until November 2003, when protestors forced the Soviet pro-government bloc to resign. Free elections were held in January 2004, the constitution was amended, and the ruling National Movement/Democrats bloc controlled the government. On 3 October 2021, the ruling party, Georgian Dream, won local elections over the United National Movement party, and the country continues to recognise its status as an ex-Soviet republic (Euronews, 2021).



### The Bitfury Group

The Bitfury Group (Bitfury) was founded in 2011 by Ukrainian friends Valery Nebesny and Valery Vavilov, its current Chief Executive Officer. The organisation has grown from a bitcoin miner and chipmaker into an enterprise-scaled technology solutions provider (Bitfury, 2021).

## Bitfury Partners with the Republic of Georgia

In July 2014, Bitfury opened its second data centre in Georgia—a 20-megawatt data centre with 3,000 servers.

The Georgian Co-Investment Fund, which was involved in Bitfury's initial funding round, dedicates a section of its website to energy consumption and untapped potential in the republic. It claims that only 25% of the country's energy potential is used, and there is potential in hydro, wind, solar, geothermal, and biomass sources; the GCF also submits that Georgia would be a good candidate to locate a large bitcoin mining data centre (GCF, 2021).

## The Land Registry Project

Since 2004, Georgia has made strides in its property registration systems, according to Weiss & Corsi. The National Agency of Public Registry (NAPR) was formed that year, and it took over the property registration functions. NAPR formalised the registration process through legislative changes. Overall efficiencies were achieved in this move to digitised property registrations and other registrations such as IDs, birth and wedding certificates, and passports. The number of employees was reduced substantially, and the NAPR actually became a net revenue producer for the national budget.

During the Global Blockchain Business Council summit in 2016, Bitfury announced its intention to provide services to governments, and its first project was the land titling pilot in Georgia. Bitfury already had two data centres and strong relationships there, and Georgia had already established a digitised system for registering property. Georgia was eager to explore the possibilities of blockchain and continue to improve on its reformed government, which was marked by strong business and banking systems. The partnership was formed (Weiss & Corsi, 2017).

Bitfury signed a one-year pilot with NAPR in April 2016 and began recording property registries to the blockchain. The pilot was designed to record the registrations on the blockchain while keeping the existing registration process intact and available as a backup. The pilot was reported a success: service delivery time had fallen from one, two, or three business days to several seconds, and operational costs decreased by 90%. Real-time audit capabilities were realised with this new technology.

The second phase of the pilot programme began in February 2017, with smart purchase and sale contracts added to the functionality (Weiss & Corsi, 2017). This meant that the buy/sell process would be handled online and would utilise the blockchain for property and data verification. In April 2017, Bitfury released its Exonum blockchain platform, and Georgia's land titling registrations moved to the new framework. Prior to Exonum, Bitfury recorded these registrations to the Bitcoin blockchain. With Exonum, this would still happen with a daily hash digest of everything transacted through Exonum recorded to the Bitcoin blockchain.

Bitfury and the NAPR hailed the project's success. According to Exonum's website, as of 2020, more than 1.5 million land titles had been registered on the blockchain. The hash code generation and storage of the transaction on the blockchain now take less than three minutes. The NAPR's existing digital property registration process was kept intact, and the blockchain layer timestamping service

was added for the issuance of digital certificates to landowners. The immutable timestamp counts as proof of ownership. The blockchain records also provide a strong audit trail that stands against the country's long history of corruption (Exonum, 2020).

## The Future of Real Estate and Land Registry Blockchain Projects

As the first blockchain-based land registry effort, the Bitfury/Georgia project was and is important to further development in real estate-based NFTs. There have been other efforts to pursue similar work around the world, although the scope of these projects can necessitate longer-term approaches.

The International Association for Trusted Blockchain Applications (INATBA) convened a land registry roundtable of its members in June 2020 to discuss the ways blockchain technology impacts the real estate and land registry industries. INATBA formed a Real Estate Working Group specifically to focus on land registries. The roundtable highlighted the leadership of Mariam Turashvili, head of project management at the NAPR in the Republic of Georgia, who offered Georgia's perspective on utilising blockchain technology (INATBA, 2017):

Blockchain is DLT, an immutable database, an asset management platform, a solution for democracy. It's a value exchange protocol when we're talking about land titles. It's transparent, incorruptible, cost effective, secure, unalterable decentralized and trusted... And who faces the biggest challenges to all of this? Of course, it's governments.

While the pace of real estate applications moves slower when compared to overall NFT growth rates, the foundation exists from which blockchain applications for individual nations, states, and local governments will grow. Once the technology is implemented, more complex applications are likely to emerge to include other government services.

### 6.4.5 Key Takeaways and References

#### Key Takeaways

Let's review the key points of this section:

1. NFTs are on a steep growth trajectory and include the newer technology standard ERC-1155, which broadens usage and creates transaction efficiencies.
2. A digital artwork NFT contains provably scarce markers of value and represents specific rights—granted by the copyright owner of that artwork—to that digital artwork, which is not the same as simply possessing a digital image of the artwork. The NFT for the artwork is non-fungible, meaning it cannot be exchanged for another NFT of that same artwork.
3. The land title registry programme in the Republic of Georgia is an example of a blockchain solution empowering a government to advance its services to its citizens.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 26 April, 2022.

### 6.4.2 NFTs Revisited

Conti, R., & Schmidt, J. (2021, 14 May). What You Need To Know About Non-Fungible Tokens (NFTs). *Forbes*. <https://www.forbes.com/advisor/investing/nft-non-fungible-token>

Kam. (2021). Cumulative NFT Users Over Time. *Dune Analytics*. <https://dune.xyz/queries/95070>.

Langridge, S. (2021, 13 October). What is Tokenomics? *CoinMarketCap*. <https://coinmarketcap.com/alexandria/article/what-is-tokenomics>

OpenZeppelin. (2019, 25 June). Tokens. *OpenZeppelin*. <https://docs.openzeppelin.com/contracts/3.x/tokens#different-kinds-of-tokens>

Shafiq, H. (2021, 21 September). What is EpicHero 3D NFT (EPICHERO)? Features, Tokenomics, and Price Prediction. *CoinMarketCap*. <https://coinmarketcap.com/alexandria/article/what-is-epichero-3d-nft-epichero-features-tokenomics-and-price-prediction>

### 6.4.3 The Future of NFTs

Casey, M. (2021, 15 October). NFTs Are an Internet Game-Changer. *CoinDesk Insights*. <https://www.coindesk.com/policy/2021/10/15/nfts-are-an-internet-game-changer>

Ethereum. (2021, 11 April). ERC-20 Token Standard. *Ethereum*. <https://ethereum.org/en/developers/docs/standards/tokens/erc-20>

Manoylov, M. (2021, 1 September). What the heck is a fractionalized NFT? *The Block Crypto*. <https://www.theblockcrypto.com/news+/116361/how-do-you-fractionalize-an-nft>

NFTFi. (no date). The marketplace for NFT collateralised loans. *NFTfi*. <https://nftfi.com>

### 6.4.4 Case Study: Tokenising the Land Registry in the Republic of Georgia

Allison, I. (2017, 9 November). Bitfury trumpets blockchain land registry with Republic of Georgia at Harvard and UN. *International Business Times*. <https://www.ibtimes.co.uk/bitfury-trumps-blockchain-land-registry-republic-georgia-harvard-un-1646616>

Bitfury. (2021). Bitfury. *Bitfury Group Limited*. <https://bitfury.com>

Euronews. (2021, 3 October). Georgia local elections: Ruling party Georgian Dream leads after early results. *Euronews*. <https://www.euronews.com/2021/10/03/georgia-local-elections-ruling-party-georgian-dream-leads-after-early-results>

Exonum. (2020). Improving the security of a government land registry. *Bitfury Exonum*. <https://exonum.com/story-georgia>

Government of Georgia. (2021). About Georgia. *Government of Georgia*. [http://gov.ge/index.php?lang\\_id=ENG&sec\\_id=193](http://gov.ge/index.php?lang_id=ENG&sec_id=193)

GCF. (2021). Overview. *Georgian Co-Investment Fund*. <https://gcfund.ge/en/527>

INATBA. (2020, 26 June). INATBA Convenes Land Registry Roundtable, Highlights Blockchain Use Cases. *INATBA*. <https://inatba.org/events/inatba-convenes-land-registry-roundtable-highlights-blockchain-use-cases>

Ledger Insights. (2021, 8 July). Coadjute launches blockchain platform for UK house sales. *Ledger Insights*. <https://www.ledgerinsights.com/coadjute-launches-blockchain-platform-for-uk-house-sales>

Weiss, M., & Corsi, E. (2017, October, revised January 2018). Bitfury: Blockchain for Government. *Harvard Business School Case 818-031*. <https://hbsp.harvard.edu/product/818031-PDF-ENG>

# 6.5 Compute and Connectivity

## 6.5.1 Overview

### Overview

Module 1 introduced the concept of “compute and connectivity”. Compute represents the computational power required to validate transactions on the blockchain. Connectivity represents the networking infrastructure necessary to transact and store the data in the distributed ledger system. Both compute and connectivity are important to blockchain technology, as speed, reliability, and overall computer system performance are critical to efficiently processing the high volume of transactions in the ecosystem. In this section, we will examine the future use of compute and connectivity.

*The Business Of Big Data: How to Create Lasting Value in the Age of AI* by Professor Martin Schmalz and Uri Bram explains compute and connectivity in economic terms. The big data generated by all that consumers do in their everyday lives has become the fuel on which the world’s AI business models run. As the price to collect and store all of this data decreases, companies can afford to process larger amounts of data, leading to more (and more profitable) insights—and increasing the value of compute and connectivity.

### Vocabulary Check

This section introduces the following terms:

- [composable computing](#)
- [quantum computing](#)
- [quantum supremacy](#)
- [supercomputing](#)

## 6.5.2 Compute and Connectivity Revisited

### Compute and Connectivity Revisited

Also, in Module 1, we learnt about the need for a blockchain protocol to run on a network that has typically been asset-heavy and expensive. The semiconductors and energy needed to power the network both require significant investments in capital and time. In fact, the rapid growth in blockchain

technology and its adoption worldwide has been a major contributor to a global shortage in blockchain-specific semiconductors, such as ASICs for Bitcoin mining and GPUs for Ethereum mining. These networks' energy demands continue to be scrutinised.

In the following section, we will analyse compute and connectivity infrastructures from a historical perspective and look at potential solutions for optimising both.

### 6.5.3 The Future of Compute and Connectivity

#### Compute

Since the digital revolution of the late 20th century, maintaining relevant computer hardware or software has been a challenge. In the beginning, to resolve bugs and other issues and to add new applications to computer software, users had to upgrade to a new version of the software. It was possible to use the prior version of the software, but eventually the older version became obsolete and would not function. Users also had to keep up with hardware. From a time-value-of-money standpoint, slow computing could be a waste, and slower, older hardware might not be able to run newer software effectively—or at all. This delicate balancing act began for mainstream businesses in the 1980s, when the use of desktop computers became more prevalent.

What seemed like constant updating in those early times only served to prepare consumers and businesses for the forces that drive computing needs today. It is common to charge a phone overnight and wake to an updated operating system, for example. Consumers are trained to heed the frequent reminders to perform software updates on their devices. On an enterprise scale, the management of hardware and software and the need to implement upgrades can be a challenging and time-consuming job.

#### Composable Computing

Gaining ground in the computing infrastructure space, composable computing offers a use-it-as-you-need-it approach to configuring solutions for hardware and software needs. Also known as software composable infrastructure (SCI), this infrastructure concept looks like a physical server that uses only the proportional resources needed for a specific application.

As explained by enterprise technology blogger Chris Evans, Principal Analyst with Architecting IT, composability provides a method to choose memory, storage, and compute from a pool of resources which can be returned when no longer needed. This process would happen dynamically through software services (2019).

Composable computing offers the following benefits:

- A more **flexible** combination of configurations to stay current with computing needs.

- A **dynamic** on-demand service through APIs that requires no manual intervention.
- An **efficient** process that reuses resources and optimises cost.

## Supercomputing

Supercomputing utilises multiple computing systems, typically large CPUs with high-speed connectivity, to achieve higher computing power that will solve complex algorithms. By increasing the number of transactions per second in a reliable way, supercomputing may offer scalability options for a blockchain network.

Supercomputing can also work to decrease energy consumption through faster transaction processing times. The EU's Marenostrum is a supercomputer housed at the Barcelona Supercomputing Center. Senior researcher Leonardo Bautista has worked with the Ethereum Foundation since 2018, and the group is running open-source simulations on the Marenostrum to find ways of increasing transaction speeds. Sharding is one way this is achieved, and it involves splitting the blockchain network into smaller partitions, or shards, that work in parallel to improve throughput. For Ethereum, this type of supercomputing is essential to its scalability studies as the blockchain has been running on a single computing core, and developers are pursuing a multi-core upgrade (Solana, 2021).

## Quantum Computing

Can physics be simulated on a computer? That was the question asked by physicist and Nobel Prize winner Richard Feynman at an MIT conference on physics and computation in 1981. As explained by the cryptographer and security engineer, Amira Bougera, in a Consensys blog post from 3 December, 2019, no one, at the time, thought it was possible. Classical computers could not model quantum mechanical principles of electrons existing in multiple states at once. Feynman's speech and his paper the following year was the first to pursue building such a computer (Bougera, 2021).

Now, tech giants are competing to build the first quantum computer. In an October 2019 article in *Nature*, the peer-reviewed research journal for science and technology, Google claimed to have built a high-fidelity processor known as the Sycamore. Repeated probability distribution experiments demonstrated the following results (Arute et al., 2019):

Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years.

Google's achievement represents quantum supremacy, meaning that its quantum computer performed a computation unachievable by classical computers. The company intends to use the Sycamore to test error rates, scalability, and the pursuit of other quantum applications.

Advances in supercomputing and quantum computing will benefit blockchain applications that rely on speed and performance efficiencies. Improved transaction settlement times are one of the primary benefits of these two compute optimisations.

**Risk.** With this new level of computing, quantum computing poses a threat to cybersecurity and, by extension, certain blockchain applications. In general, the SHA-256 hash function is quantum-safe, although Ethereum's elliptic curve signature scheme shows some vulnerabilities. Ethereum developers have started work on alternative cryptographic signature schemes for future releases, including Ethereum 2.0's Serenity upgrade, which will allow accounts to specify a quantum-safe signature scheme (Bougera, 2021).

## Connectivity

How permissionless can blockchain be if its infrastructure relies entirely on the internet to function? Meltem Demirors addresses this question in an article titled "Compute and Connectivity Meets Crypto". After a review of how the internet as we know it today evolved from the world wide web and its conception in the 1960s, she emphasises that much blockchain technology is too reliant on this centralised system. Yet, there are only a handful of companies or governments capable of producing mass-scale infrastructure to contribute to an emergence from the centralised network of the internet.

China has the will and capital to play a major infrastructure role, while European companies are not well-positioned due to regulatory constraints. Several US companies could produce infrastructure, and they represent wireless communications, data centres, routing hardware, and networking. Still, these companies do not represent as much collective market capitalisation as even one tech giant, such as Google, further indicating that the infrastructure is far too centralised (Demirors, 2020).

### 6.5.5 Key Takeaways, References, and Further Exploration

#### Key Takeaways

Let's review the key points of this section:

1. Balancing hardware and software improvements can be difficult, especially with blockchain and other cutting-edge technology where computing speed is paramount to usability and profitability.
2. Composable computing and quantum computing are at the forefront of computing possibilities.
  - Composable computing offers a use-it-as-you-need-it approach.
  - Quantum computing offers processing speeds that are incomparable to anything achieved in computing so far.
3. Supercomputing offers faster computing through the use of multiple computing systems and high-speed connectivity.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 26 April, 2022.

### 6.5.3 The Future of Compute and Connectivity

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., et al. (2019, 23 October). Quantum supremacy using a programmable superconducting processor. *Nature* 574, 505–510. <https://doi.org/10.1038/s41586-019-1666-5>

Bougera, A. (2019, 3 December). How Will Quantum Computing Affect Blockchain? *Consensys*. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain>

Demirors, M. (2020, 16 October). Compute and Connectivity Meets Crypto. *CoinShares*. <https://blog.coinshares.com/the-financialization-of-compute-connectivity-66beaffe7501>

Evans, C. (2019, 22 August). What is Software Composable Infrastructure? *architectingit*. <https://www.architecting.it/blog/what-is-sci>

Mordor Intelligence. (2021, January). Composable Infrastructure Market - Growth, Trends, Covid-19 Impact, and Forecasts (2021-2026). <https://mordorintelligence.com/industry-reports/composable-infrastructure-market>

Solana, A. (2021, 4 August). Supercomputing can help address blockchain's biggest problem. Here's how. *ZDNet*. <https://www.zdnet.com/article/supercomputing-can-help-address-blockchains-biggest-problem-heres-how>

## Further Exploration

[The Business Of Big Data: How to Create Lasting Value in the Age of AI by Martin Schmalz and Uri Bram](#)

# 6.6 Other Blockchain Concepts

## 6.6.1 Overview

### Overview

The concepts discussed in this section offer a view into other innovative applications as well as a case study that details an ethical approach to the advances of digital technology. Specifically, we will study the following concepts and discuss whether they have positive impacts on blockchain technology, or whether blockchain technology has a positive effect on each of them:

- **Reputation marketing:** A study of how the brand management concept translates to the digital space.
- **Prediction markets:** A look into the betting market concept and how some are utilising blockchain technology to enhance its value propositions.
- **The future of DAOs:** A look forward to the potential benefits of the rapidly growing number of decentralised autonomous organisations.
- **The Digital Civilisation Initiative:** A case study about an organised effort to promote digital technology development in ways that are responsible, transparent, and just.

### Vocabulary Check

This section introduces the following terms:

- [prediction markets](#)
- [reputation marketing](#)
- [decentralised autonomous organisation \(DAO\)](#)

## 6.6.2 Reputation Marketing

### Reputation Marketing

Traditionally, reputation marketing centred around improving or managing an organisation's brand and the perception of it in the marketplace, and may have involved a strategic reputation and brand

management plan. In the digital world, businesses and consumers develop reputations based on how they conduct business. For example:

- A user has 4.5 stars as a seller on eBay.
- A hotel has three stars on TripAdvisor.
- An Instagram influencer has a 2–3% engagement rate.

There are many more examples of how web identities develop reputations, wanted or unwanted. A person's or organisation's reputation becomes vital to good business results.

Arguably, trust is at the root of any established reputation. At the 2009 University of Pennsylvania commencement address in 2009, Eric Schmidt, then CEO of Google, said, “In a networked world, trust is the most important currency” (2009).

Schmidt likely did not know how the blockchain ecosystem would develop into a system of data and financial transactions. Yet, even as the blockchain concept was introduced to the world, Schmidt's statement demonstrates that digital networks, including blockchain networks, require trust and, by extension, reputation scoring models. In blockchain technology, for example, a wallet address benefits from a reputation score focussed on its holder's DeFi borrowing history or its performance in the number of NFTs created.

Applying this need to the digital platforms that exist a decade later, Stepan Gershuni, Lead Product Manager at the identity-enabled ecosystem developer Affinidi, writes about the importance of **persistent pseudonymous reputation** as “a foundational tool that we need to build truly scalable decentralised systems that can provide effective coordination beyond just finance” (2021). He outlines three obstacles that must be overcome to achieve a persistent pseudonymous reputation system:

- **Users' digital reputations are currently fragmented.** Between Web 2.0 and Web 3.0, one user will have multiple accounts that store their reputation score within separate proprietary systems. Gershuni suggests giving the reputation data back to the users, achieving a network-of-networks effect where reputation scores become richer and more trusted.
- **Current systems do not communicate reciprocally by default.** Current systems do not communicate reciprocally by default. Prior history and reputation are not necessarily considered from one organisation to the next. A person who applies for a bank loan must reproduce identifying information for each loan application, for example, regardless of their reputation and prior history.
- **Real life currently follows binary rules, but should allow for a spectrum of possibilities.** In a binary world, the only options are yes or no—but most situations call for multiple options. Using the previous example of a bank loan applicant, in the binary world, that person must provide all requested documents directly to the bank, even if some provided information is redundant, to satisfy identity requirements, or the applicant cannot receive the loan. In a world with a spectrum, that person may satisfy the bank's KYC protocols through an approved KYC provider, and does not need to produce a passport to further verify identity.

## Faculty Video: Blockchain's Use in Reputation Marketing

In the following video, Felip Thomaz, Associate Professor of Marketing at the University of Oxford Saïd Business School, explains the difference between traditional reputational marketing in digital applications and blockchain-oriented reputation systems.



Blockchain then plays an interesting role, or it can play an interesting role in managing reputation. When you think about trust and reputation systems as they exist today, you might think in terms of product reviews, for example, it says "I am relying on your point of view or an aggregate number of consumers points of view" right? If you ever bought a product and you're just looking at how many stars does it have, and how many reviews does it have, I don't trust it when there's one individual, but I trust when there's 5,000 individuals. You don't have any more information about those 5,000, but just because there's a critical mass of individuals, this feels trustworthy.

You're using this reputational inference. You're saying, you're using this wisdom of the masses to make a better decision. If you knew that individual, let's say that end of one says that actually, that's your best friend that made you that recommendation, then suddenly that kind of flips things. You might actually go with the N of one, the single best friend because you know them, you know their reputation, you kind of understand that their recommendation is somewhat valuable and tailored to you. It might actually weigh more than 5,000 people telling you to do something else.

So imbuing blockchain into the system is equivalent to giving a characteristic or a weight to each one of those recommendations and components. So you no longer have an empty set of 5,000 individuals that are uncharacterised. You actually know who is making recommendations, you know if they have the right to make a recommendation right? I can actually validate against another blockchain whether you made a purchase. And by looking at that I can say, actually, you're speaking with experience, you're speaking with expertise as opposed to maybe a falsified claim.

Maybe I bought 2000 recommendations and it snowballed. So there is place for a system where reputation again can be safely managed, verified, validated and used via blockchain to safeguard and lead credence to all sorts of marketing claims that currently exist in a more heuristic or psychologically safe aspect. Much in the way that I've described what this heuristic of, I just have to count to a certain number of individuals to trust an environment. You can actually have trust via reputation, via algorithm, which could be much more powerful.

What that brings us to then is, we move the locus of reputation from a centralised database right? Where you have here is this conglomerate or aggregation of individuals, or you have to trust one centralised source of information, that says this is trustworthy versus not, to leveraging one of the strengths of—in my view, the core strength of the protocols behind blockchain is that our system now becomes decentralised. And you no longer have to attribute trust to that one core centralised structure, you have trust masoned from algorithmic structure that says, no this centralised system is what actually leads me to believe that I have a well-functioning reputation system.

And I think throughout our conversation, we're going to see that the value in this blockchain protocol is going to keep coming back to this idea of it serving as a replicated state machine, meaning that everybody has access to the same information and the same reputation tracking. It is evenly distributed and equal to every node of this network. So this decentralisation and maintenance of this state of reputation so that I cannot lie to you because everybody can see what has happened is of exceptional value.

## Case Studies: ARCx and RabbitHole

Reputation marketing remains fragmented within the blockchain ecosystem. However, some use cases are taking an innovative and promising foothold.

### ARCx

ARCx has developed a DeFi Passport for its users. Phase two of the platform's evolution involves developing credit scores for Ethereum wallet users in its ecosystem, based on the following on-chain behaviours (ARCx, 2021):

- **Borrowing history.** History in other protocols, such as Maker, Compound, and Aave is evaluated.
- **Loan duration.** Duration and average health factors are considered.
- **Loan liquidations.** A history of no liquidations leads to a high-quality signal of appropriate debt management in the ARCx ecosystem.
- **Loan volume.** Outstanding loan amount and size help determine credit access limits.

Future phases will include:

- **Yield farming scores** that establish higher scores for long-term farmers.
- **Airdrop scores** that evaluate the length of time a user holds airdropped tokens.
- **Governance scores** that establish the amount of on-chain governance activity a user is involved in, and eventually will evaluate the nature of their governance.
- **Trader scores** that distinguish between bots and real identities, and provide a score that allows an exchange to offer lower rates to a real identity than to a bot, for example.

The credit evaluation factors are very much like those in the traditional financial sector. The major exception is the future portability of the DeFi Passport across multiple exchanges.

### RabbitHole

Through its Pathfinder programme, RabbitHole seeks to establish on-chain resumes for users who want to contribute to crypto projects, and for the projects to discover potential contributors. RabbitHole is in the process of decentralising to maximise its growth potential. The platform developed four Pathfinder roles (RabbitHole, n.d.):

- **Stewards:** Governance proposal writers rewarded for creating proposals on other protocols to bring in new RabbitHole quests.
- **Navigators:** Developers rewarded for creating subgraphs on The Graph to track completions of different tasks on specific protocols RabbitHole works alongside.

- **Craftsmen:** NFT creators rewarded for creating trophies that are distributed to users for completing specific quests.
- **Pioneers:** Content creators rewarded for creating content specific to individual tasks, guiding users down the nebulous “rabbit hole”.

A Pathfinder user can contribute in any of these roles and earn rewards. A user’s participation also contributes to RabbitHole’s on-chain graph of each user’s achievements, thereby establishing their resumes.

These use cases demonstrate how blockchain-focused reputation systems can be deployed. Ideally, reputation marketing infrastructures will develop and become more mainstream in public blockchain processes.

### 6.6.3 Prediction Markets

#### Prediction Markets

Sometimes referred to as betting markets or even thought of as crowdsourcing, a prediction market is a collective of individuals betting on the outcome of a future event—one that is binary in nature, such as an election or sales results. The investor executes a contract trade for a US \$1.00 payout. The collective of market participants and their predictions establishes the market prices. The more trades involved in any given market, the more effective that market is as more data is gathered with each trade.

Prediction markets are similar to futures markets, where traders buy and sell contracts that deliver an asset or commodity at a predetermined future date, based on their expectation of the underlying asset’s future price. The prediction market involves speculation on an actual event, such as a corporation’s sales results or election results (Peters, 2021).

#### Market Comparisons

Prediction Market	Futures Market	Crowdsourcing
Betting on the outcome of a future event	Betting on the future price of an underlying asset	Investing in an event or underlying asset
Aggregating beliefs	Aggregating beliefs	Aggregating work or data
Example: Election results	Example: Price of orange juice on a certain date in the future	Example: Recruiting team members for a new blockchain project

## Traditional Prediction Markets

Iowa Electronic Markets (IEM) are one of the most well known prediction markets on the internet (Peters, 2021). They are student-oriented futures and prediction markets through the University of Iowa's Tippie College of Business. The IEM is used as a teaching and research tool, and more than 100 universities worldwide have enrolled. There are two primary areas of focus with the markets (IEM, 2021):

1. **Forecasting tool.** Students learn about the economic and business relationships that determine an outcome.
2. **Incentive mechanism.** Student participation is increased through real monetary rewards.

Research and studies from the IEM are often cited publicly. For example, PS: Political Science & Politics published a 2020 United States election study based on the IEM's data. The article discussed the two organised markets for the election (Gruca & Rietz, 2020):

- The “vote-share” (VS) market had two contracts:
  - UDEM20\_VS—pays \$1 times the Democratic share of the two-party popular vote
  - UREP20\_VS—pays \$1 times the Republican vote share
- The “winner-takes-all” (WTA) market had two contracts:
  - DEM20\_WTA—pays \$1 if the Democratic two-party, popular-vote share exceeds 50%
  - REP20\_WTA—pays \$1 if the Republican vote share exceeds 50%

The study tracked market investments in the contracts and compared their price changes to significant events to determine which, if any, had the most impact on the expected WTA election outcome, and if certain events created an expected impact on Trump's vote shares (VS) while comparing his chances to previous incumbents.

The University of British Columbia's Sauder School of Business Prediction Markets focuses on Canadian politics and current events. These markets operate continuously and are considered a successful form of crowdsourcing that exists to meet four objectives:

- The markets operate as a public service through timely data aggregation—for example, collecting data faster than opinion polls during an election.
- Researchers learn trader behaviour in a controlled environment.
- Traders follow the political process more carefully.
- The markets have an educational focus on financial markets and trading strategies

The markets are open to anyone interested in these events (Antweiler, 2021).

## Blockchain Prediction Markets

Blockchain, or crypto, prediction markets use smart contracts that execute actions automatically when certain conditions are met. An oracle, or data service, feeds real-world data to the smart contract, which executes according to its code (Hertig, 2021). This can translate to lower risk for traders than traditional markets. However, smart contracts can still contain bugs or weak code that could lead to a loss of funds.

Market questions must be binary in nature—yes or no, for example—and feed that result to the smart contract. For example, a prediction market could ask the question, “Will more than three million people ride the subway in New York on Monday?” Using the Metropolitan Transit Authority’s oracle as the market’s source for data, the exact number of riders falls either into the “yes” answer or the “no” answer, and the smart contract executes accordingly. The winning traders in that market will earn what the losing traders bet—a zero sum proposition.

There are several varieties of prediction markets in this ecosystem. Following are examples, including their areas of focus:

- **Flux**—A decentralised, open source prediction market engine launched in 2020. It is a cross-chain oracle aggregator that provides smart contracts with access to economically secure data feeds.
- **Gnosis DAO**—The prediction market-driven collective, stewarding the Gnosis ecosystem through “futarchy”, or governance by prediction markets.
- **Augur**—A decentralised oracle and peer-to-peer protocol for prediction markets. Augur is free, public, open source software. Augur is a set of smart contracts written in Solidity that can be deployed to the Ethereum blockchain.
- **Omen**—A decentralisation maximalist prediction market platform launched, maintained, and governed by the DXdao. The DXdao built Omen on an open framework developed by Gnosis for prediction markets.
- **Polymarket**—An information market platform where investors predict the outcome of a global highly debated topic. The market transacts in US Dollar Coin (USDC), and there are several ways to transact.
- **Hedgehog Markets**—A prediction market that runs on the Solana platform, which results in fast and inexpensive network transactions.

### 6.6.4 The Future of Distributed Autonomous Organisations (DAOs)

#### The Future of Distributed Autonomous Organisations (DAOs)

Throughout this programme, there have been many references to DAOs. In this section, we will explore this increasingly popular organisational concept in more detail.

## Faculty Video: The Impact of DAOs on Blockchain Technology

In the following video, Martin Schmalz explains how the rise in DAOs has impacted blockchain technology.



Distributed or decentralised autonomous organisations, abbreviated DAO and commonly referred to as DAOs, have achieved staying power in the blockchain industry. A DAO is one of those newer terms that seem to gain overnight traction like DeFi or NFT. But what is its effect on blockchain technology?

The nature of a DAO with its automated rules-based governance and transparency is attractive to blockchain users, who already subscribe to the mechanics of the self-executing smart contract. DAOs had to overcome some issues in their early years.

Those who were involved in the crypto community in 2016, will recall the DAO incident, in which \$150 million worth of ether was hacked from a DAO that contained faulty code. This resulted in a hard fork of the Ethereum blockchain to restore the stolen funds, and the controversial event brought to light some of the challenges of maintaining a decentralised system, based purely on computer code.

Despite the setback, DAOs would continue to rise in popularity during the 2017 ICO boom. Another point in time that revealed the benefits, and flaws, of a completely open and permissionless system when an estimated \$4.9 billion was raised to fund many projects, some with questionable backgrounds and levels of commitment.

As a hype cycle faded in 2018, and most of 2019, the crypto industry would begin to face the realities of regulatory compliance and the consequences of unregistered securities offerings. From there, DAOs became poised in late 2019, to rise again as NFT and DeFi boom emerged throughout 2020.

While NFT volume has decreased significantly since then, the adoption of DAOs for other users has continued to increase. DAOs continued to play a key role in decentralised exchanges, as part of the DeFi space. You may be familiar with names like Uniswap, or Compound, and Aave.

They present the top three DAO exchanges with a combined market cap of \$14.8 billion, as of the 30th of June 2021. Just a year prior, the market cap was below \$1 billion US. DAOs and DeFi exchanges should continue their journey together for some time.

According to a consensus report for the second quarter of 2021, the top 20 DAOs now hold more than \$6 billion US worth of digital assets. Those digital companies represent DeFi exchanges, asset managers, gaming, risk sharing, insurance, and privacy protection.

Decentralised, governance has become appealing for a variety of projects, and there's a good amount of creativity behind them. Outside the top 20, there are DAOs that fund and build digital public goods projects created towers that assist artists and tokenising their projects, e-sport DAOs, and lending DAOs just to name a few.

There are more and more resources being committed to the DAO process. Token services, governance, treasury management, risk management, and development, are all examples of the additional push into the sector of blockchain technology.

Will DAO survive the increasing regulatory pressures felt by cryptocurrencies? There are efforts to recognise DAOs as legitimate business entities. The US state of Wyoming passed legislation in early 2021, to allow them to register as limited liability companies or LLCs, and the American CryptoFed DAO became the first legally recognised one in the United States.

The European country of Malta also recognises them as a valid legal entities. These are encouraging moves towards some regulatory status for DAOs moving forward. So while very early in its growth cycle, the energy moving into the DAOs space is forceful and quite focused. So, there seems to be an appetite for decentralised governance, in the blockchain ecosystem.

## DAO Background

The initial DAO concept was launched in May 2016 through an ICO by members of an Ethereum group known as Slock.it for the purpose of crowdfunding for various blockchain projects. It was known as TheDAO and frequently referenced as Genesis DAO. Created in the brand new Solidity language, TheDAO's smart contract coded in specifications for ownership and voting rights. This resulted in the world's first non-hierarchical and globally accessible organisation. Investors eager for proportional ownership of the DAO and its treasury of Ether participated in TheDAO's ICO, depositing ETH in return for \$TheDAO at a rate of 1 ETH for 100 \$TheDAO tokens.

However, despite early success, TheDAO soon fell victim to a hacker, who exploited a flaw in the contract that did not subtract from the token holder's contract balance when they withdrew ETH (Frontera, 2021). Ultimately, US \$150 million in Ether was drained from the smart contract.

## Growth in DAOs

Unfortunately for the initial DAO effort, a major lesson was learnt about smart contract vulnerabilities. Fortunately for the future of DAOs, that lesson was learnt early and provided valuable feedback. After the initial setback and time to develop better approaches and much tighter smart contracts, DAOs have increasingly become a preferred organisational structure in the blockchain ecosystem. A DAO can be established on whichever platform is suitable for its use case. The table below shows the increase in the number of DAOs on the Ethereum Mainnet since 1 April, 2020, as well as a dramatic beginning on Polygon, a layer 2 Ethereum network (@dauhaus, 2021):

Date	Ethereum Mainnet # of DAOs	% Increase	Polygon Layer 2 on Ethereum # of DAOs	% Increase
1 April, 2020	12	---	0	---
1 October, 2020	50	316.6%	0	---
1 April, 2021	89	78.0%	30	---
1 October, 2021	254	185.3%	303	910.0%

DAOs are also gaining in market capitalisation as tracked by CoinMarketCap. This list reported on the top 85 DAOs with a combined market cap of US \$40 billion (CoinMarketCap, 2021). There are nearly 800 DAOs across all platforms as of 1 October, 2021, according to a Dune Analytics query report. This compares to only 307 on 1 April, 2021 (@dauhaus, 2021). Unreported DAOs could drive the totals much higher.

The Uniswap and Aave DeFi exchanges represent the top two DAO tokens, with a combined market cap that exceeds US \$20 billion at 1 October, 2021. Just a year prior, their market cap was only US \$1 billion (CoinMarketCap, 2021). DAOs and DeFi exchanges are expected to continue their journey together for some time.

According to a ConsenSys report for Q2 2021, the top 20 DAOs represent DeFi exchanges, asset managers, gaming, risk-sharing insurance, and privacy protection. Decentralised governance has become appealing for a variety of projects, and there is a good amount of creativity behind them. Outside the top 20, some DAOs fund and build digital public goods projects, including creator DAOs that assist artists in tokenising their projects, eSports DAOs, and lending DAOs (Shehabuddin, 2021).

## Why DAOs?

DAOs are based on the vision and goals of their collective communities. The community establishes the governance rules, and trust is inherent in DAOs as the rules become code in the smart contract that will execute upon predetermined events. Some of the main benefits of DAOs include:

- **Governance:** One of the primary benefits of participating in a DAO is proportional ownership with voting rights in a decentralised organisation. The rules established within and between DAOs ultimately dictate how these applications in the blockchain ecosystem will interact with the external world.
- **Support for the creator economy:** Creator DAOs are different from traditional crowdfunding campaigns like Kickstarter in that the DAO token represents ownership and the freedom to trade with the token.
- **Work:** DAOs allow people to work and earn based on the merits of their work and not rely on a hierarchical ladder-climb to succeed and earn a living.
- **The developer community:** As discussed in Module 3, the developer community consistently works within a DAO structure, and DAOs offer a governance structure worthy of consideration for blockchain projects.

## Guest Video: The Nonprofit Role of DAOs

In this video, Priyanka Desai, Vice President of Operations at OpenLaw, introduces DAO projects the firm is working on and the non-profit roles of DAOs.



So actually one of the DAOs that we've put together is an unincorporated not-for-profit. It's actually a pretty interesting DAO. I think we're going to lean into that structure a bit more, but it's called MUSE0.

It's almost like a public good in some ways and that it's a community-driven, community-run internet museum. Any individual that is a artist or collector can donate an NFT similar to, maybe, a museum type of establishment where donors can donate a work. Here, you're doing an NFT. In return, if the community accepts that a part of the permanent collection, they get some tokens, which then gives them the ability to govern around this digital museum, but also vote in what subsequent works enter this collection.

So that's kind of this not-for-profit structure. One could imagine that this extends beyond, maybe, a museum or a public good and could really be applied to other public goods. Or I think I talked to someone recently that's interested in doing a not-for-profit for underrepresented NFT artists.

It's a DAO called Mint Fund that basically has capital that allows specific artists who might not have the funds to then mint their work. So I think that there's definitely some of this emerging. And I think we'll definitely see more that hits on different corners of the not-for-profit world.

I've seen some DAOs like the Longevity Research, Realm. I've seen some DAOs looking at carbon trading as well and doing some work in the environmental space, so there's definitely more to be done there and more to be seen, I think.

## DAO Governance

The formation of a DAO happens with the smart contract that specifies all the rules of how the DAO will operate. The collective that initiates the smart contract should treat this process like a thoroughly conceived business plan. Once the DAO is launched, changes will be made to the smart contract through community voting, typically. Thus, it is essential to deploy a smart contract that ensures the DAO's original intent is protected and allows the proper provisions for changes. A poorly formed DAO will quickly lose its focus, its value, and ultimately its trust.

The following table provides a high-level comparison of a DAO's typical governance structure with a traditional corporation and nonprofit organisation structures.

	Corporation	Nonprofit Organisation	DAO
Management	Board of Directors	Board of Directors	Smart contract
Ownership	Shareholders	The organisation itself	Token holders
Supervision	President/CEO	Executive Director	Curators, investors, and token holders
Workforce	Human Resources	Human Resources	Guild

- **Smart contract.** In a DAO, the smart contract is the authority for the organisation. It specifies the terms of how the organisation will run, and it is the only structure that needs to be trusted.
- **Token holders.** The token holders represent the organisation's ownership, its community. As mentioned previously, ownership is proportional, based on the number of tokens held, and typically includes voting rights.
- **Curators, investors, and token holders.** Curators, investors, and token holders all participate in DAOs by using their knowledge and skills to build a portfolio that aligns with the objectives of the DAO. NFT art curation is a trending type of curator, but some curators are incentivised to curate information and investors who pool their knowledge to form investment portfolios.
- **Guild.** The guild coordinates talent and contributors with the DAO, but also for external interactions the DAO may require.

Like traditional organisations, there are other roles within a DAO. Those listed here represent those most commonly found in the current ecosystem.

## DAO Considerations

**Creating a DAO.** As outlined in this section, the smart contract is the primary basis of a DAO's creation and existence. Like any blockchain project, it is possible to create a DAO by bringing together the resources—developers, investors, community members—and managing the process from the beginning.

There are resources to assist with the process, however. DAO creation platforms, such as DAOstack, provide a step-by-step process to assist with building and running a DAO (DAOstack, 2021). Colony is another protocol that supports creating internet organisations.

**Regulatory issues.** DAOs share the regulatory concerns of blockchain projects in general. Jurisdictional issues could occur, with major disputes among members who are spread out globally. The DAO concept is an even newer one than cryptocurrencies. Regulatory efforts have been primarily focused on those and not the specifics of how a DAO should be structured.

There are some efforts at regulation, however. The state of Wyoming in the US created a DAO law in April 2021 that formally recognises these entities. The first in the world to do so, the state can now regulate DAOs, and the DAO itself can operate unencumbered by compliance concerns. This sets a good example from which other states or countries can model their laws.

## Guest Video: DAOs—Looking Back and Looking Forward

In this guest speaker video, Priyanka Desai, VP of Operations at OpenLaw, explains the first DAO and DAO progression since then and in the future.



We're still very early. The theory and community in the Ethereum white paper was always contemplated that this idea of people pulling together capital and making decisions with each other that was written in the—early on, I think people contemplated that in 2016.

There was an attempt at doing the DAO. So this was a huge feat. I think it raised \$150 plus million at the time. I think most Ethereum holders actually participated in the original DAO. And it was in many ways a success and that there was clear demand to join and be a part of a hive mind.

There was obviously some technical failings with the original DAO, but the concept always really held strong. I mean there was a little bit of a DAO hangover for a bit, but that revived itself in 2019, 2020. And so I think now we're seeing many of these DeFi protocols, Delphi and these are massive DAOs, hundreds of people. Some people are more active than others. Some people take leadership roles.

I think that seeing the organisation move in this direction where you have just people helping to work on behalf of that DAO token and contributing for, maybe, a short amount of time or a long-winded project. It's just a very fluid structure that we're seeing with our DAO specifically because they are for profit. There's just a slightly more legal regulatory work that needs to be done. And beyond legal regulatory, there's also accounting that needs to be taken care of, with the US law are limited to 99 members.

So when you're talking about hundreds of people versus potentially with our DAOs like 60, 70, and max 99, you have a different structure. You have different levels of activity at least from what I've observed over the last two years, being very close to a lot of the DAOs that we've built and also popping in to other DAOs.

I mean, first off, I think it works extremely well. I think some of the decisions and some of the trend forecasting that I've seen from these members who've just corralled over a specific topic or a subcategory is none like I've seen really before. And this is just because a lot of these people are very online and very plugged in, but they also love the idea of working together. And on the government side really, I mean things have moved fairly swiftly like, most people are pretty happy with things.

If they're not, there's an open dialogue either online or on weekly calls to really chat through it. It's a very adaptive structure. So if people want to extend beyond it, add some governance, I think most people feel fairly comfortable in doing so. What starting to develop is the DAOs themselves and the communities within the DAOs are actually developing more DAOs and more subcommunities, focused on a particular subject matter.

So with the LAO, Flamingo was a genesis of that original project because of some of the membership there that were heavy into this idea of NFTs. With Flamingo currently today, there's about four separate DAOs that are actually coming out of that existing community just because several members have started rallying around certain subject matter and they're really excited about it. I think when you start thinking about this from the LAO to Flamingo to then four other DAOs and these are DAOs that are focused on a specific game like Zed Run. This is a DAO that's focused on the metaverse specifically like buying digital real estate and developing it.

Another DAO around a specific CryptoPunk or an NFT, where people can do joint ownership and decide as a community the fate of that NFT. And another DAO that's going to be specifically used more as a passive vehicle to really start buying more high-value NFTs. You can just start seeing a world where there's just a continuous web of different DAOs that emerge from one DAO to another.

And they're all interlinked in one way. And there's almost a tree that you can follow as where these subcultures and certain focuses actually break off. And more people, more new interesting thought comes from each of these communities what we're staying in. And I think that just speaks to the flexibility and the mobility of internet organisations as opposed to maybe some of the MeetSpace organisations that you see.

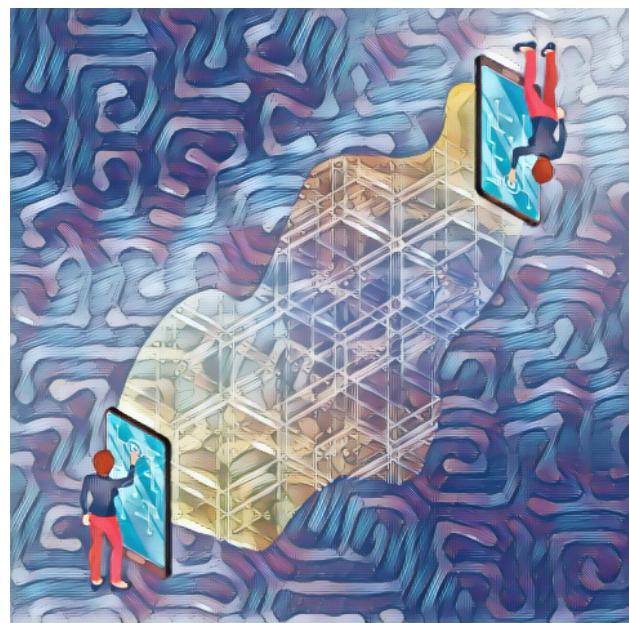
## 6.6.5 The Digital Civilisation Initiative

### The Digital Civilisation Initiative

Digital technologies have contributed to improvements in many aspects of life. The internet, mobile phones, WiFi, and computing all represent extraordinary advancements in how people function in their personal and business lives. However, there are certain notable areas of concern that are without reins in the midst of these achievements:

- **Personal privacy.** Data collection and redistribution are among the most offensive repercussions of current technology usage.
- **Centralised authority.** In what is supposed to be a primarily decentralised environment, large traditional hierarchical organisations have developed monopolies and have become subjects of government scrutiny in the last few years.
- **Manipulated consumption.** Advertisements dominate the mainstream platforms that consumers use daily. The personal privacy invasion by big tech companies and their centralised authorities has dictated what users see in search engines, social media platforms, and even news applications.

The Digital Civilisation Initiative was created with the mindset that society should play a more prominent rule-making role in how these and other technologies are deployed, with a focus on ethics, respect, and cohesion. Led by Bill Roscoe, Professor of Computing Science at the University of Oxford and Senior Research Fellow at University College, the initiative was developed in collaboration with his colleagues in Hainan, China and elsewhere. It seeks to create a society with minimal boundaries and universal standards (University of Oxford, 2021).



In a Manifesto he started in 2019 and finished in 2020, Professor Roscoe outlines the focus of the initiative and the Digital Civilization Conference (DCC). The DCC is a global community that is focused on the advancement of a fairer and more trustworthy digital civilisation. It is composed of experts and young talent in policymaking, technology innovation, business, academia, and entrepreneurship. The DCC “exists to facilitate solutions to the most pressing challenges brought about by technology towards a more balanced future” (DCC, 2020).

Digital civilisation is grounded in the definition of civilisation—the building of an ordered and functioning society by its people. One person’s rights are balanced with the rights of others and with the society’s needs as a whole, and governments exist by the consent of the society they govern. The Manifesto defines digital civilisation as follows (Roscoe, 2020):

- Digital civilisation provides structures through which we interact with governments, companies and each other, guaranteeing transparency, uniformity and adherence to common principles and rules.
- Civilisation is too important for us to allow Big Tech companies to design it for their own benefit.
- Civilisation is thus a combination of stable government, the tools and components that enable society and the people in it to function, plus the people and organisations that exist in it.

The Digital Civilisation Initiative exists, then, as a watchdog over the evolving dynamics of the tech industry, and it has a clear message: Bad behaviour in the digital world should be made impossible and unprofitable.

## Faculty Video: The Digital Civilisation Initiative

In the following video, Professor Bill Roscoe explains the Digital Civilisation Initiative in more detail.



I'm very happy to talk about the digital civilisation initiative. One of the reasons why I was persuaded to work in China was because my Chinese hosts were really keen to develop a notion of digital civilisation—which was, shall we say, internationally attractive—that would set them apart on the international stage so that they could reach out and claim to be the instigators of some great international movement.

And the digital civilisation initiative is supposed to take the completely ramshackle world of digital interaction we all have with the internet at the moment, which is, as we know, mainly mediated by the combination of American Big Tech companies and governments, all of whom basically have their own self-interests at hand, and who will make your life a total misery in terms of collecting data, and make a complete nonsense of ideas such as GDPR.

I think that GDPR is a wonderful concept in theory, and in some ways it works well, but in terms of our everyday interaction with the internet I think it's a complete failure, because I'm sure that everybody watching this will spend most of each day agreeing to terms and conditions that they probably haven't actually read in order to get trivial benefits such as connection to the internet, or to read a web page, or something like this. So GDPR creates wonderful rules, which it immediately finds a way of self-defeating, shall we say.

I see digital civilisation as a way of trying to bring the world together, in particular trying to bring China back closer to the west in terms of data standards and so on, but at the same time trying to get more fairness in society and really establish people's, shall we say, practical ownership of their own data rather than merely theoretical ownership of their own data, which is what I see GDPR as giving. For example, I think that everybody ideally should have their own settings, their own profile, in a digital civilisation app running on their iPad or whatever, which most of the time can simply answer these questions for you.

In other words, instead of presenting you with 50 pages of small print that you don't read, it should present you with machine-readable conditions, which clearly your machine can read for you much more quickly, and much more efficiently, and much more thoroughly than you're likely to do yourself.

This is an idea, I will say, at the instigation of the Chinese island of Hainan, which has ambitions—with the full blessing of the Chinese government, may I say—to become more like Hong Kong. I'm trying to develop this, these concepts of data ownership and data sharing, for them. If anybody wants to read my writings on digital civilisation, again, they can find them on my website.

## What Role Could Blockchain Play?

There are several areas of positive impact that blockchain technology can provide for this public good initiative:

- **Integrity**—By its design, blockchain technology provides transparency and the immutability of its records.
- **Trust**—Through blockchain technology's distributed ledger system and its data replication, corruption is nearly impossible.
- **Rules**—Blockchain platforms are designed specifically with rules and could provide an ideal structure for civilisations.

As it continues to evolve, the Digital Civilisation Initiative will have positive impacts on areas such as decision-making through a voting mechanism, creation of markets, property registers, licensing systems, and health records. The group will study the formation of a global blockchain, either public or permissioned, to aid in the advancement of the initiative.

### 6.6.6 Key Takeaways and References

#### Key Takeaways

Let's review the key points of this section:

This section included three specific blockchain concepts and a multi-national effort to bring civilisation to the digital world.

1. **Reputation marketing** is evolving in the blockchain space. Some use cases include portable reputation scores, colonised reputations, and a reward-based on-chain resume system.
2. **Prediction markets** operate similarly to futures markets and offer bets on the outcome of a future event. Smart contracts automatically execute based on the outcome.
3. **DAOs** are rapidly increasing in number, as the organisational governance structure appeals to blockchain project participants.
4. **The Digital Civilisation Initiative** brings focus to the need for ethics and trust in a digital society.

## References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 26 April, 2022.

### 6.6.2 Reputation Marketing

ARCx. (2021, June). Welcome to ARCx. <https://wiki.arcx.money/introducing-arcx/master>

Gershuni, S. (2021, 5 August). Bullish Case for Decentralized Reputation. *Medium*. <https://sgershuni.medium.com/bullish-case-for-decentralized-reputation-2ea254d0ee63>

RabbitHole. (no date). Introducing the Pathfinder Program. <https://www.notion.so/Introducing-the-Pathfinder-Program-ca5a1fdd96cd49868c98a2163c75edc0>

Schmidt, E. (2009, 18 May). Eric Schmidt's University of Pennsylvania commencement address. *YouTube*. <https://www.youtube.com/watch?v=6wKFQx30f6M&t=660s>

### 6.6.3 Prediction Markets

Antweiler, W. (2021). Sauder School of Business Prediction Markets. *University of British Columbia*. <https://predictionmarkets.ca/about.php>

Gruca, T., & Rietz, T. (2020, 15 October). The 2020 (Re)Election According to the Iowa Electronic Markets: Politics, Pandemic, Recession, and/or Protests? *PS: Political Science & Politics*. <https://www.cambridge.org/core/journals/ps-political-science-and-politics/article/2020-reelection-according-to-the-iowa-electronic-markets-politics-pandemic-recession-and-or-protests/39C85A907DCC60ADF52F9DFF6024E1E5>

Hertig, A. (2021, 18 February). How Crypto Transforms Prediction Markets. *CoinDesk*. <https://www.coindesk.com/tech/2021/02/18/how-crypto-transforms-prediction-markets>

IEM. (2021). What is the IEM? *Iowa Electronic Markets*. <https://iemweb.biz.uiowa.edu/media/summary.html>

Peters, K. (2021, 6 July). Prediction Market. Investopedia. <https://www.investopedia.com/terms/p/prediction-market.asp>

#### **6.6.4 The Future of Decentralised Autonomous Organisations (DAOs)**

@dauhaus. (2021, 20 October). DAOs over Time (Mainnet). *Dune Analytics*. <https://dune.xyz/queries/185740>

CoinMarketCap. (2021, 21 October). Top DAO Tokens by Market Capitalization. <https://coinmarketcap.com/view/dao>

DAOstack. (2021, 22 October). What is DAOstack? <https://daostack-1.gitbook.io/v1/introduction/what-is-daostack>

Frontera, E. (2021, 7 June). A History of ‘TheDAO’ Hack. *CoinMarketCap*. <https://coinmarketcap.com/alexandria/article/a-history-of-the-dao-hack>

Shehabuddin, S. (2021, 24 September). DAOs: Where Are You Going, Where Have You Been? *ConsenSys*. <https://consensys.net/blog/blockchain-explained/daos-where-are-you-going-where-have-you-been>

#### **6.6.5 The Digital Civilisation Initiative**

DCC. (2020). Technology in the Service of Humanity. *Digital Civilization Conference*. <https://mobile.dcc.global/#pc-dcc-index>

Roscoe, B. (2020, March-August). Digital civilisation: manifesto for a trustworthy, well regulated world. <https://blockchain.univ.ox.ac.uk/wp-content/uploads/2021/05/Bill-Roscoe-Digital-Civilisation.pdf>

University of Oxford. (2021). Bill Roscoe. *Department of Computer Science, University of Oxford*. <https://www.cs.ox.ac.uk/people/bill.roscoe>

# 6.7 Case Study: Blockchain for the Public Good

## 6.7.1 Overview

### Overview

Throughout this blockchain strategy course, you have studied many concepts that could adversely impact users and other stakeholders. The ESG section of Module 4, for example, discussed environmental, social, and governance considerations for responsible project implementation. In this section, we will study the concept of blockchain for the public good. Specifically, we will explore the RadicalxChange Foundation (RxC), a nonprofit organisation in the United States that exists to promote positive public good-specific blockchain use cases.

The RxC case study is an example of forward and outside-the-box thinking about the possibilities of blockchain technology. While some concepts may seem extreme for today's time frame, all concepts are worth exploring to understand how they were conceived, what problems they solve, and where they are in their implementation cycles. From this study, you will gain an understanding of how to develop concepts with applied blockchain technology.

The RadicalxChange Foundation was founded in 2018 by Glen Weyl, after Weyl co-authored *Radical Markets: Uprooting Capitalism and Democracy for a Just Society* with Eric Posner. The duo's vision of utilising the markets in profound ways to improve inequalities and monopolies became the subject of public discussion, bolstering their ambition. Blockchain technology is the basis for the foundation's concepts for public goods—quadratic voting, quadratic funding, private property auctions, and partial ownership, for example. We will explore these radical concepts through some key players involved with the foundation.

### Vocabulary Check

This section introduces the following terms:

- [mechanism design](#)
- [public good](#)
- [quadratic funding](#)
- [quadratic voting](#)

## 6.7.2 From Radical Markets to RadicalxChange

### From Radical Markets to RadicalxChange

As mentioned, the book *Radical Markets* and its provocative concepts stimulated public interest in the topic so much that Glen Weyl pursued the creation of the RadicalxChange Foundation as a basis to organise the movement—build community, carry the movement forward, and educate on democratic innovation.

In addition to founding the RadicalxChange Foundation, where he also serves as Chairperson, Weyl is a principal researcher at Microsoft Research and a lecturer at Princeton University. He was recently named on the Bloomberg Top 50 list of “people in business, entertainment, finance, politics, and technology and science whose ... accomplishments were particularly noteworthy” (Bloomberg, 2018) and one of Wired Magazine’s 25 leaders shaping the next 25 years of technology (RadicalxChange, 2021). Weyl states that he was inspired to develop RxC through his work in social technology for widely shared prosperity and diverse cooperation. The foundation is a social movement that exists to create a richer and more equal society (Weyl, 2020).

*Radical Markets* was grounded on the premise that the markets can be used as a way of arranging a society. The authors were inspired and motivated by economists throughout history with common ideals: They were not afraid to express theories counter to both conservative and liberal mindsets, nor were they afraid to pose innovative reforms to existing economic approaches.

The book is dedicated to the mid-20th century economist, William S. Vickrey, who wrote a paper, “Counterspeculation, Auctions, and Competitive Sealed Tenders”, based on his work with the Venezuelan government to design a fiscal system in the early 1960s. The paper studied the power of auctions to solve major social problems and helped to found a field of economics called mechanism design (Vickrey, 1961).

Mechanism design theory focuses on the problems associated with incentives and private information. Matt Prewitt explains that mechanism design tends to mirror game design theory in that it approaches the design rules and incentives to result in fewer strategic rewards for undesirable actions. For RxC, this influences the approach to building shared understandings and how to better cooperate and collaborate in self-governance with people whose worldviews are fundamentally different (Prewitt, 2021).

### RadicalxChange Values

Three main values permeate each of RxC’s ideas (RadicalxChange, 2021):

- **Fairness.** The goal of economic life should not be to accumulate assets that permit you to profit from other people’s labour. Instead, it should be to contribute to community life.
- **Democracy.** Markets are immensely powerful and useful, but they don’t govern themselves.
- **Egalitarianism.** People are not the same, but they matter the same amount.

The foundation is focused on source-code-level institutional reform and new mechanism design ideas for common economic areas such as voting and finance (RadicalxChange, 2021). Following are some RxC concepts that exemplify blockchain technology for the public good vision of this organisation.

## Quadratic Voting

Quadratic voting (QV) is a voting method that is based on the intensity of voters' preferences in collective decisions. Each voter receives a fixed number of voting credits to allocate on a ballot with multiple topics. How they disperse their credits indicates how passionate they are about certain topics. As explained in Radical Markets, the voting credits, which can be used or stockpiled for future voting referenda, buy votes according to a formula (Posner & Weyl, 2018):

- One voting credit buy one vote.
- Four voting credits buy two votes.
- Nine voting credits buy three votes.

The credits for votes continue to increase according to the quadratic formula.

Each voter votes based on the intensity of their preferences by placing more votes on a certain topic. All votes could go to just one topic or be spread across multiple topics. The outcome is a democratic process that measures community sentiment and resists uneven influence by a central authority (RadicalxChange, 2021).

## Quadratic Funding

Glen Weyl co-authored a paper with Ethereum founder and RxC board member Vitalik Buterin and a PhD candidate in economics at Harvard, Zoë Hitzig, titled "A Flexible Design for Funding Public Goods" (Buterin et al., 2019). The paper proposed extending the principles of quadratic voting to the quadratic funding (QF) concept, which provides for a decentralised and self-organised (democratic) public goods funding ecosystem. It is a matching funding process for projects accessible to the public and valuable to large groups of people. QF uses a mathematical calculation to determine how contributed funds are matched by the sponsor, such as a government or philanthropic institution.

In traditional matching funds contributions to nonprofit organisations, the match is made on a one-to-one basis or some other ratio based on the donor's contribution. Through the QF process, the matching funds are prioritised based on the number of donors who contributed and rewards broad-scale project participation. The size of the donation does not matter as much as the number of donors.

**Gitcoin Grants** is a grant programme that funds open-source projects for public benefit. Donors sponsor the QF matching fund in the Ethereum ecosystem, known as the Funders League. As of 23 September 2021, there have been 11 rounds of quarterly fundraising since Gitcoin's launch in November 2017. The programme continues to grow and has resulted in over US\$ 64 million in total funding through Q3 2021. This includes matching funds from 43,270 funders and 228,042 earners (Gitcoin, 2021).

QV has the potential to impact controversial funding programmes such as campaign finance. The more success it has in Web 3.0, the more it can positively influence everyday activities.

## Additional Initiatives

In addition to the QV and QF concepts, Rx C promotes other community-oriented and democratic initiatives:

- **Data dignity** provides the foundation for concepts around personal data to protect and even market it. Ocean Protocol provides infrastructure for data marketplaces, crypto-secure data custody, data management, data unions, trusts, and cooperatives. Mask Network is a browser extension that allows users to encrypt posts on popular social media apps with controls over who can see the posts.
- **Partial common ownership** is a radical concept around asset ownership. Its underlying theme is that assets belong to no one and everyone. An asset's current possessor self-assesses its value and pays a fee based on its value. Similar to a tax assessment, the fee can fund public goods or be dispersed as a social dividend. Then, if someone bids on that asset at a price that is more than the self-assessed value, the current possessor sells it at the assessed value, and the difference goes into the community, thus creating the public good benefit.

## Summary

Through its focus on fairness and equality, RadicalxChange has found success in some of its early concepts like quadratic voting and quadratic funding. The organisation's impact on the public good space, whether through nonprofits, governments, or other public interests, has already created effective change in the approaches to traditional processes.

## Case Analysis

Having read the case, consider using the following key questions as discussion points for a class discussion in the Riff platform:

- Does quadratic voting make sense for public elections? Why or why not?
- In what other areas of blockchain technology does mechanism design theory come into play? (Could one of these be tokenomics?)
- What other areas of public interest could benefit from these radical concepts?

## 6.7.3 References and Further Exploration

### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 26 April, 2022.

#### 6.7.2 From Radical Markets to RadicalxChange

Buterin, V., Hitzig, Z., & Weyl, G. (2019, 2 July). A Flexible Design for Funding Public Goods. *Management Science*. <https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2019.3337>

Gitcoin. (2021). \$64.9m in Results. <https://gitcoin.co/results>

Posner, E., & Weyl, G. (2018). *Radical Markets*. Princeton University Press.

Prewitt, M. (2019, 24 September). A Basic Introduction to RadicalxChange. *RadicalxChange*. <https://www.radicalxchange.org/media/blog/2019-09-24-se9s34>

RadicalxChange. (2021). *RadicalxChange*. <https://www.radicalxchange.org>

Vickrey, W. (1961). Counterspeculation, Auctions, and Competitive Sealed Tenders. *The Journal of Finance*, vol. 16, no. 1 [American Finance Association, Wiley]. <https://www.jstor.org/stable/2977633?read-now>

Weyl, G. (2020). Biography. *Glen Weyl*. <https://glenweyl.com/section/personal>

### Further Exploration

[Mechanism Design Theory](#).

# 6.8 Getting Involved in a Blockchain Ecosystem and Keeping Skills Fresh

## 6.8.1 Overview

### Overview

In a decentralised environment with little to no top-down directives, finding direction can sometimes be a challenge, and it can even be disruptive. The blockchain ecosystem quickly learnt the value of community when the creativity and exchange of ideas the Bitcoin community brought to that project became essential to its success and benchmarking status for the entire ecosystem. We will explore communities and other ways to become involved with blockchain outside the focus of your project. In many ways, the opportunities presented here will add value to a blockchain project.

### Vocabulary Check

This section introduces the following terms:

- collective

## 6.8.2 Online and Protocol Communities

### Faculty Video: How to Get Involved in an Ecosystem

In this faculty video, Professor Martin Schmalz describes how to get involved in a blockchain technology ecosystem.



As you outline the next steps for your project or a business concept, consider an affiliation with a blockchain ecosystem. That's a protocol that drives development, human involvement, and the network of nodes.

Doing so will provide you with an excellent set of resources and a support system that will help smooth out the complexities of this industry. In this programme, you have heard from several blockchain protocol leaders. All of them invite community participation in their ecosystem and offer various ways of doing that.

The number one engagement tool is through online communities that encourage participation by the users, developers, technologists, investors, and in certain cases, the miners. Find out whether communities exist. The larger ecosystems will have multiple opportunities they directly support. Ethereum, for example, has different communities for developers, researchers, and non-technical participants. And there are Ethereum meetup groups worldwide that invite participants at all levels.

In addition, there are social media venues you can consider joining.

Discord is a developer's communication platform that has channels for different communities, or "servers", as they are known. You are allowed to create your own server or simply participate in any of the other servers that are relevant to your interests. Discord is known for fostering new relationships and providing technical support for its users.

Most blockchain ecosystems will have a community on Twitter as well. That is a high traffic platform where you can share posts about your project or business, or you can follow as many ecosystems, developers, and influencers as you want and receive up-to-date news and other pertinent information.

So seek out the type of group that works best for you. And consider its casual or more formal nature. For example, will you be expected to contribute on a regular basis? Are there scheduled meet times, or is the community available any time for support and interaction? There really is a community for everyone in this space.

A second method to get involved with an ecosystem is to consider applying for grant funding. This is an opportunity to bring attention to your project and possibly receive funds to support its development.

Most protocols encourage grant applications, and many will provide assistance during the application process. Going through this process will help you see further into that protocol, and it will demand a level of formalisation of your project's vision and methodologies. This can be very helpful to clarify your own thoughts as well.

So how do you get involved in the blockchain ecosystem as a whole? How will you stay relevant in this space? Beyond the focus on your project, there are many avenues for you to become further involved in blockchain-oriented activities, in addition to the specific communities we just covered.

Consider some of the following options. Does your regional or local government have laws or regulations in place or under consideration for blockchain? Learn about existing lobbying groups or elected officials who have an interest in promoting blockchain innovation, and become a resource in that effort.

Offer to teach or be a mentor. You now possess some knowledge about a topic in which most people have very little understanding. So stretch yourself and encourage others to learn something about this industry as well.

Are you developing your project as an open source? Are you willing to share your experience with others? Talking about your work fosters your own developing mindset and creativity as well.

Consider investing or mock investing in cryptocurrencies as a way to become familiar with blockchain's native applications. You will learn a great deal by opening a digital wallet, if you haven't, and making your first crypto purchase. From my own experience, I will assert that following your own investment—even a small one—will promote deeper learning and exploration as well.

And finally, there are many resources available to deepen your knowledge of blockchain. Publications like Theblockcrypto, Chainalysis, CipherTrace, and Messari all offer relevant news stories and research data. Consult the references cited in this course for other opportunities to learn more. Now, go find your community and strive to be an active participant.

## Online Communities

Module 3 described the role that developer communities have played since those early days of Bitcoin, and they are only one example of online communities that can be a helpful resource. We will explore several more in this section.

## Protocol Communities

There are a number of protocol communities, such as those for Bitcoin and Ethereum. These groups and forums exist for all levels of participants, including developers, investors, internal stakeholders, and external stakeholders.

**Bitcoin communities.** One resource for various communities surrounding the original cryptocurrency and its platform can be found through the nonprofit organisation Bitcoin.org, which provides numerous opportunities to connect, learn, and participate. Starting with a basic how-to guide on transacting with bitcoin, the site provides information and links for individuals, developers, and businesses and is relevant for all skill and knowledge levels (Bitcoin.org, 2021).

Bitcoin Talk is one of the largest communities for everything related to Bitcoin. Active since 2009, it has more than three million members and is styled as a forum with subjects grouped by topic. A search bar offers the best method to quickly find any topic of interest (Bitcoin Talk, 2021).

Many more online Bitcoin communities are accessible through simple online searches or through one of the resources mentioned above.

**Ethereum communities.** The primary Ethereum community is located through the Ethereum.org website. The site exists specifically to accommodate all users of the platform and anyone interested in learning or participating in other ways. There is a Community tab that takes the user to the main Ethereum Community page and a “how to get involved” link that forwards to resources, such as those for:

- Developers
- Researchers and academics
- Non-technical users
- Financial professionals
- Product managers
- Marketing

The site is rich with information about grants, jobs, and upcoming events.

## Additional Online Communities

Protocols other than Bitcoin and Ethereum and other blockchain stakeholders have their own online communities. Some of those include:

- **DAO communities.** A protocol like Cardano that is structured as a DAO has a focus on distributed governance. Cardano's token (ADA) is native and sits on the actual ledger. The protocol treats its tokens, and therefore its voting stakeholders, as first-class citizens by removing the complex layer of smart contracts. Its developer community is well-supported through its portal with strong documentation, test and experimentation environments, and up-to-date technical updates. Cardano is a large PoS protocol (Cardano, n.d.).
- **Financially inclusive communities.** A protocol like Celo focuses on purpose and connectedness. The spirit of the protocol itself provides the basis for its community, whose purpose is to design for all in an effort to create an inclusive financial system. A monthly community call strengthens the mission with news and project announcements, and there is a regularly updated community events calendar. Celo encourages applications to its ecosystem venture fund, and the Alliance for Prosperity promotes collaboration within the community and provides education and support for projects (Celo, 2021).
- **Collectives.** Similar to a protocol community, a collective can exist within a protocol or as a broad concept organisation. The Solana Collective is a protocol community that supports community leaders and educators. It offers rewards for productive output within the collective to run meetups, moderate community channels, create educational content, and other items (Solana, n.d.).

There are multiple options for finding and joining a community that fits your needs and your project's needs. Sometimes good community research can help find the right fit with a protocol that will serve your project well.

### 6.8.3 Social and Offline Communities, Contributions, and Volunteering

#### Social and Offline Communities, Contributions, and Volunteering

Social media is a different concept than the online communities described above, although there are similarities. A social media site for a certain protocol may have a similar forum style as its online community with some of the same topics and members. Social media, in general, is non-specific to any protocol or blockchain entity. However, Discord and Twitter will likely have protocol-specific and notable stakeholder channels or feeds.

- **Discord:** Started in 2015 as an online gaming communication tool for players worldwide, Discord has much broader participation now, including family and children spaces. It is a major communication tool for developers in the blockchain space (Discord, n.d.).

- **Twitter:** The social networking and microblogging application conceived by Jack Dorsey launched in 2006. Today, there are over 200 million monetisable daily Twitter users worldwide (Statista Research Department, 2021). One of the most frequented Twitter handles for cryptocurrency and blockchain enthusiasts is #cryptotwitter.

## Offline Communities

- **Meetup group:** An in-person gathering for discussion, presentations, event planning, or networking.
- **Hackathon:** A coding competition event that includes networking opportunities and is frequently open to all skill levels.
- **Conferences:** Major and regional gatherings for formal educational meetings, exhibits, networking, and release of new or updated information.

## Contribute and Volunteer

Stakeholders and participants in blockchain often give their time and talent as a meaningful way to become or stay involved in their communities. Through many of the communities discussed in this section, as well as opportunities within an organisation, there are multiple ways to contribute:

- **Code contribution and debugging.** Developers and programmers often contribute code and work in communities to debug code. The open-source environment encourages this type of participation, which reinforces the success of the decentralisation concept.
- **Mentoring.** Serving as a mentor to young or newer stakeholders in the blockchain space is a valuable service to that individual and strengthens the mentor's knowledge and leadership skills.
- **Storytelling.** Sharing a vision or success story promotes the innovative strengths of the blockchain ecosystem and encourages other stakeholders in their endeavours.
- **Hosting a hackathon or conference.** While either of these requires a large amount of energy, a well-organised and thoughtfully conceived event adds value to blockchain communities. The hosting organisation typically receives added credibility and more exposure for its brand through the event, as well as natural networking opportunities that extend through the event.

## Guest Video: Advice from Industry Experts

In this montage video, you'll hear from multiple experts in the fields of blockchain and cryptocurrency as they give advice to blockchain strategists.



**Yves Messy:** My main advice for this class of blockchain strategists is to pay attention to two horses. Finance is changing fundamentally. Everyone has recognised that digital transformation needs to happen.

Unfortunately, the startups are now in a position to gain significant market share in the blink of an eye. So, blockchain strategists today need to be aware that digital transformation is happening in mainstream traditional finance, and that's a trend where you need to be asking yourself, how can you help blockchain help these digital transformation programmes in established companies? On the other hand, these DeFi and blockchain startups that are coming up now are gaining significant market share, and all of them—almost all of them—have the issue of, how can it work with the existing financial system as it's digitally transforming?

So, you can either help the legacy systems digitise in a way that's relevant, given the rise of blockchain, or you can make next-generation blockchain systems more relevant to centralised and regulated entities as soon as possible. That's my main advice.



**Priyanka Desai:** Whether your interest be in finance, art, music, etc., there's probably a DAO—and/or at least a Discord community of people—where you can just dig your heels in and really get to know the subject matter. In addition, because this space moves so quickly, keeping up with developments is super important, both legal and regulatory. But beyond that, just what people are building, what innovation is happening; and Twitter is such a good resource for that. I think most people who are in the crypto space, they get their news from Twitter, and I think it's probably the fastest way to get updates on what's happening.



**Mason Borda:** I think one of the really interesting things about the blockchain space is that everything is open and public. When you're trying to enter a new industry, traditionally it's very hard to get in. You either have to be connected or you have to send a lot of emails until you can get in the right door.

In the blockchain space, that's sort of turned on its head. All of the chat groups and all of the communities are public. They're on Telegram. They're on Discord. The opportunity for people to just hop in, evaluate the landscape, see what problems exist, to see how they can help, is always there. And that exists in every community.

That's even how I got more involved in the space, is I found some projects that I liked. I dove into the community. I saw how I could help this project get a little bit bigger, and just by virtue of doing that, you build great connections. People see how you work.

If you do a good job, they respect you. They want to pull you into new opportunities. I think that's the fun part about the space, it's, anyone can get involved. Anyone can find good opportunities and land in a place that they like. I think that's one of the exciting things about the blockchain space



**Bill Roscoe:** Blockchain is an enormously exciting area for anybody, if you're coming into either a technological or a business framework, because it offers such potential to revolutionise how we transact in society. I mean, potentially it moves us from a centralised society where we have centralised providers—providing services like banking, and insurance, and registries of this and that—to a situation where, in some sense, we could do it all ourselves by collaborating on a blockchain.

I would strongly encourage anybody thinking about blockchain to think of novel uses of this. I've already mentioned a few other ones are things like IP registry and exploitation. In general of course, one has this concept of tokenisation, which is an enormously exciting way of trading. On the other hand, it seems to me that some of the latest headlines about NFTs are taking things a little bit too far, but maybe that's just because I'm old; maybe I'm not modern enough to appreciate that these things are truly respectable.

I think that, from my own point of view, as a real believer and a proponent of blockchain, I strongly encourage people to think of things which benefit society rather than are thought of primarily as quick ways of making money.



**Yaya Fanusie:** My advice for those who are blockchain strategists, or learning to become blockchain strategists, hoping to become that: my advice is to help figure out how to balance the privacy and security tension within the blockchain space. This is a tension. The fact that anyone can create a blockchain, can have a wallet, and they can be pseudonymous—and the fact that there are serious concerns and issues with scams, fraud, illicit activity, trafficking, human trafficking, child exploitation—all these things, terrorist financing, sanctions evasion.

Blockchain strategists can't ignore one or the other. You can't just say, I'm just going to build something that's totally private. You can do that, and it will have a niche use. It will be used, but it won't be able to scale for the mainstream, so blockchain strategists are going to have to figure out how to balance this tension and how to build systems.

If you really want to strategise, strategise about how you make blockchain platforms—or at least blockchain applications—more compliant. You're just going to have to do that. How can you make this ecosystem fit? I'm not saying that you're going to just reproduce the banking system. A lot of folks don't want to think like that. They say, the banking system is inefficient, but at the same time you've got to take the best from it. You have to take it. You've got to figure out how to have a compliant ecosystem if you really want people to use all this potential innovation.



**Konstantin Richter:** I always feel that any institution, any individual, who says listen, I'm building my livelihood on top of crypto, I always urge them to run at least a Bitcoin node, because the Bitcoin network is ultimately the driver of everything here.



**Federico Spagnoli:** My main advice for this class of blockchain strategists is, as you go through this course and start applying some of the learnings, it's a good time to reflect, to zoom out, as I did when I went through this programme in the past. I was very interested and curious about the actual use cases, the technology, some of the tactics, if you will. But I also believe it's very important to have a clear blockchain strategy in mind.

How are you, for example, proposing to generate value creation through the use of this technology rather than just focusing on the platform or the product itself? Paraphrasing Todd Zenger in his article, 'What Is the Theory of Your Firm?', if you really want to zoom out and have a more holistic view of the strategy that you are trying to pursue rather than just the tactics, I advise you to focus on three elements of the strategy.

One is the foresight. By foresight I mean thinking about the trends, the different factors that are affecting the market, the industry where you are thinking about applying a blockchain-based technology and strategy. The second element is to think about the insight: in essence, the specifics of the company, the venture, the product that you are trying to release.

And last but not least, connecting the two. A well-crafted strategy identifies a complementarity of the foresight and the insight in a way that you can apply the technology and generate the value creation that is going to eventually make a real impact. I notice sometimes in my job, when we talk about potential uses of blockchain technology in situations where, yes, from a technology standpoint it makes sense, but when you try to think about how much incremental or material value you are creating, for example, to the customer, there is no real value. We all know blockchain is a complex technology. It's not cheap, it's not easy to run, so please take care of all those types of details as you think about the solutions that you are envisioning as part of this programme.



**Mimi Zou:** My advice for this class of blockchain strategists is just to become familiar with the legal regulatory policy aspects of this very fast-moving technology, because in my view, the law can do without blockchain, but blockchain cannot do without the law. I'm not saying this just as a lawyer, but I do strongly believe that the future of the development of blockchain will very much depend on the legal and regulatory frameworks that must evolve with these new technologies.

Of course, the law is not static. It's a living instrument, and so I think we really need to think about how we design the law in a way that promotes innovation; that promotes competition. My advice is to really watch this space. Keep up to date, not just with the price of Bitcoins, but also keep track of the different policies, regulations, and laws that are being really quickly issued by many different jurisdictions.

## 6.8.4 Keeping Skills Fresh and Looking Forward

### Keeping Skills Fresh and Looking Forward

While it is natural to become laser-focused on a blockchain project and the detailed tasks involved to make it successful, staying current with developments in this space is vital. Designate at least one or two trusted news sources to follow daily or weekly, and schedule some routine time to pursue opportunities within the communities that best suit your needs. Encourage others to do the same.

Consider opportunities through continued education to expand your knowledge. There are good options for blockchain peripheral courses, as well as those in other emerging technologies such as fintech and artificial intelligence. An organised plan for continued learning will serve you and your project well.

## Guest Video: Keeping Up-to-Date with Blockchain

In the following video, several of our guest speakers offer advice on keeping up with blockchain technology.



**Mimi Zou:** In terms of keeping up with this very fast-paced environment of blockchain innovation, I think obviously there are many websites that provide up-to-date news, particularly in the cryptocurrency space. I check Coinbase, Cointelegraph, CoinGecko. These are very credible sources that provide a wide range of news related not just to cryptocurrency, but more broadly to blockchain technologies.

There is general news that's pertaining to different industries. When I look at the newspapers these days, there are also suddenly sections devoted to new technologies, and for general readers that's a really good starting point. But, of course, people taking this course are already much more advanced than your general reader, so I would probably recommend subscribing to news websites.

Social media, I'm a little bit sceptical of in the age of "fake news". I think it's really important to be very selective about the sources, the news sources, that you follow. There are news aggregation sites, which are always useful because I think—if you just rely on one particular medium of news—I mean, in terms of objectivity, that can be compromised. It's good just to get a full range of different news sources and news feeds.

There are obviously industry sources like TechCrunch that I also resort to. And just really research widely. It's not just news, but there are research reports. It's like there's a research report coming out every day on something related to blockchain.

And then, finally, one that I'm trying to get into because I'm not a super tech person. I know more technology than most lawyers, and I am able to do some basic coding. I joined GitHub a few years ago. I find GitHub really useful, and sites like GitHub really useful, in terms of being able to look at what's happening in the open-source community.

When you first sign up to GitHub, it's a bit, whoa, you know this is for techies, but actually it's a fairly easy site to navigate. I would recommend checking out some of the projects that are trending, or starred projects that really give you a good glimpse into what is really cutting edge in terms of blockchain innovation, and other forms of innovation if you're also interested in AI as well. The open-source community is really where you want to try and get your head into the latest innovation and not just wait for a few months to read about it in the news.



**Yaya Fanusie:** Given that the blockchain space is fast-moving, fast-paced, probably the best way to keep up with it is really through a hodgepodge of media content that's out there. I in particular recommend that people tune in to different podcasts. Podcasting for me, I think, was a huge way that I learnt a lot about the crypto ecosystem. Whether it's a relatively mainstream, popular podcast, or some of the smaller podcasts, you have different types of crypto podcasts, almost like the above ground and the underground ones. I would say podcasts are really important.

A lot of people would mention social media. Crypto Twitter is well known, so if you can stand being on Twitter and the attention grab that it can be, attention suck that it can be, there's so much dialogue that usually happens on Twitter about crypto, from people that are building to just people that are enthusiasts. So, Crypto Twitter is a good place.

I would say it's really the social media and podcasting. Of course, there are lots of publications out there too. But I really think if you want to learn, podcasts and those interviews, that helps you get a sense of the deeper issues rather than just the headlines of what's happening in the crypto space.



**Yves Messy:** Blockchain is one of these fields where, really, unless you're a technologist, you're probably a year-and-a-half to two years away, even if you do your best in reading up about it. But one thing I've seen in person is that if you're not technically savvy, you should just attend as many blockchain conferences as possible, because these usually present the latest in what's trying to happen in the blockchain space. There are YouTube channels also that are supposed to help educate you on a daily basis, in five minute soundbites, on what's the latest this week; this month.

Otherwise, what I would say is just to go on companies' websites or look at the Financial Times' blockchain section to see which trend, however crazy, is somehow getting the interest of the established finance and insurance power brokers.



**Bill Roscoe:** Clearly, Google and web browsers are wonderful ways of doing this, but of course they can bring you a huge amount of information. So, my advice, obviously, would be to keep abreast of the news. I always keep abreast as best I can of the news, and look out for references to good things and bad things about blockchain and the like.

At the same time, I try to maintain a really good network of people who are also interested in it, then we pass things amongst each other. I have developed a pretty good network over the past few years in working on this, and we always pass each other on stories and things to look at, and this sort of thing. I mean, I don't have a magic solution to this, but it's just like following any hot topic.



**Aya Miyaguchi:** The tips on keeping up to date with what's happening with blockchain, well, especially I would focus on Ethereum. There is [ethereum.org](https://ethereum.org), like I said, and there is also the Ethereum Foundation Blog, [blog.ethereum.org](https://blog.ethereum.org). If you are more interested in technical updates, there's also Week in Ethereum News that describes bigger news and technical updates.

For those who are more technical, or who are interested in making newer updates in Ethereum 2, Eth2, there is Ben Edgington's [eth2.news](https://eth2.news), which is focused on Eth2. I would rather avoid the price talk on YouTube and elsewhere, as that lacks the deeper conversations, as I mentioned earlier.



**Priyanka Desai:** Whether your interest be in finance, art, music, etc., there's probably a DAO—and/or at least a Discord community of people—where you can just dig your heels in and really get to know the subject matter. In addition, because this space moves so quickly, keeping up with developments is super important, both legal and regulatory. But beyond that, just what people are building, what innovation is happening; and Twitter is such a good resource for that. I think most people who are in the crypto space, they get their news from Twitter, and I think it's probably the fastest way to get updates on what's happening.



**Christoph Spaenjers:** Pretty low-tech, low-tech bursts, and so my main source of information is Twitter. I mean, Twitter has its drawbacks, I think, but the nice thing about Twitter is that people link to other sources of information. People link to articles. If you use it in a smart way, if you use it intelligently, you choose who to follow, and you choose which hashtags to look up or to follow, or you choose your topics right. For me, I'm interested in YARD markets and I'm interested in NFTs, but I'm also interested in academia and lots of other things. I think there's very little news that really does not pop up on Twitter somehow.

## 6.8.5 Key Takeaways and References

### Key Takeaways

Let's review the key points of this section:

1. Developer communities play a significant role in blockchain and cryptocurrency. Communities can be protocol communities, social communities, or online communities.
2. Individuals can contribute by contributing code and debugging, mentoring, storytelling, and hosting a hackathon or conference.
3. Aside from the importance of contributing your time, talent, and experience to your community, being part of a community allows you to keep your blockchain knowledge fresh and relevant.

### References

To deliver the highest quality content, we collate information from many leading sources. References are included to attribute works to their original authors. Some of the sources used are freely available, and some are not. Subsequently, the links found in module reference lists may require you to purchase access.

The following sources were last accessed on 26 April, 2022.

### 6.8.2 Online and Protocol Communities

Bitcoin.org. (2021). Bitcoin. *Bitcoin Project 2009-2021*. <https://bitcoin.org/en>

Bitcoin Talk. (2021). Bitcoin Forum. *Bitcoin Talk*. <https://bitcointalk.org>

Cardano. (no date). Making The World Work Better For All. *Cardano*. <https://cardano.org>

Celo. (2021). Developers. Designers. Dreamers. Doers. *The Celo Foundation*. <https://celo.org/community>

Solana. (no date). Solana Collective. *Solana Foundation*. <https://solana.com/collective>

### **6.8.3 Social and Offline Communities, Contributions, and Volunteering**

Discord. (2021). *Discord*. <https://discord.com>

Statista Research Department. (2021, 12 August). Twitter - Statistics & Facts. *Statista*. <https://www.statista.com/topics/737/twitter/#dossierKeyfigures>

# 6.10 Congratulations

## 6.10 Programme Wrap-up

### Programme Director Video: Programme Wrap-Up

In the following video, Programme Director Meltem Demirors offers her congratulations on completing this programme.



You did it. Congratulations on completing the Oxford Blockchain Strategy Programme. I'm so delighted that we've gotten to spend the last few weeks together. I hope that following the completion of this course, you feel empowered with the knowledge, tools, and frameworks that you need to continue on your blockchain strategy journey.

Now, if you're looking for more resources, and I know you are, know that throughout the programme all of the references that have been made are easy for you to find and to continue to utilise. I also highly recommend staying in touch with your peers that you've connected with throughout this programme. After all, who knows who you'll go on to collaborate with in this new exciting digital future. Thanks, again, for joining me on this journey.

### Faculty Video: The Future of Blockchain Technology

In the following video, Martin Schmalz also offers his congratulations and shares thoughts on where blockchain technology is headed.



Congratulations from me as well. Bravo on completing the programme.

We've ended this programme looking forward to the great potential of blockchain technology. And I'd like to add some of my thoughts based on my research on where this technology is heading.

As you could see, there was a lot of enthusiasm in the early days of blockchain technology about how the technology would revolutionize all kinds of aspects, in all businesses, in all industries. I'm not saying it won't, but it's clear that the revolution hasn't happened quite as fast as some had anticipated.

And the reasons we've explored in this programme for this relatively slow adoption are complex and manifold. As we've seen in many cases, an entire industry has to adopt the technology for it to take hold. That's very different from earlier technologies where a single firm could adopt the technology to gain a competitive advantage.

In other cases there are cheaper solutions to satisfy the same business aim, and the main value added is really in digitization of a process rather than in blockchain technology.

In yet other cases regulatory hurdles make adoption more cumbersome than it otherwise would be.

And it's simply a complicated and costly technology to implement as well. And at the same time, innovations happen in spaces nobody has thought of just a few years back.

So my advice amid all this for you going forward is to try and follow the process we suggested in this programme that allows you to check whether this technology serves your business aim, rather than enthusiastically embrace it or reject it outright. A sober look at the facts is what's needed in this space. And you now have a basic toolkit to do so.

Other than that, hook yourself up to the online communities that work on the particular problem you're interested in. That's the best way of staying abreast of the developments.

And of course stay in touch with us. Nothing makes me happier than have students check in even years later with their learnings and insights from the real world.

So many thanks again for your efforts, and congratulations.



# Wrapping Up: Important Logistics

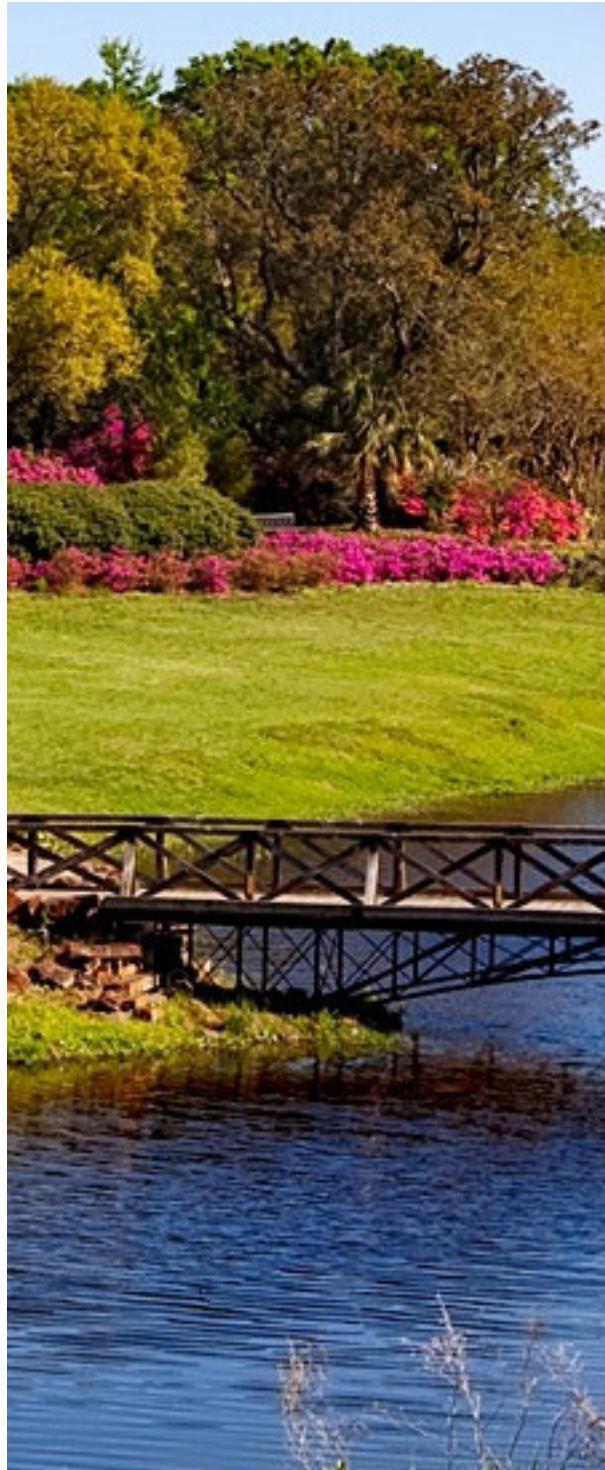
---

Oxford Blockchain Strategy Programme  
2022

# Oxford Blockchain Strategy Programme

## Wrapping Up: Important Logistics

### Table Of Contents



<b>W.2 Certificates and Badges</b>	<b>3</b>
W.2.1 Certificates and Badges Overview	3
W.2.2 Digital Badge via Credly	3
W.2.4 Digital Certificate	5
<b>W.3 Continuing Education Credit</b>	<b>6</b>
W.3.1 IACET CEUs	6
W.3.2 CPD Credit Hours	6
<b>W.4 Access to Materials and New Offerings</b>	<b>7</b>
W.4.1 Access to Online Materials Until 30 August, 2022	7
W.4.2 Upcoming Oxford Programmes Start 14 September, 2022	7
<b>W.5 Staying in Touch: Meet-up &amp; Community</b>	<b>8</b>
W.5.1 Join the Oxford Saïd Community	8
<b>W.6 Important End-of-Programme Dates</b>	<b>9</b>
W.6.1 Important End-of-Programme Dates	9
<b>Blockchain Strategy Glossary</b>	<b>10</b>

# W.2 Certificates and Badges

## W.2.1 Certificates and Badges Overview

### Credentials

When this programme ends, if you have earned a score of 50% or higher for your work and have successfully completed ID verification, you will be eligible for three types of credentials:

- A ***digital badge*** on the Credly platform. This credential is published to the blockchain, and is shareable, printable, and embeddable. You will receive an email from Credly on **3 August, 2022** with information about how to claim and share your badge. This is ideal for sharing on social media.
- A ***printed certificate*** will be physically mailed to you 7–10 weeks after the programme end date (if you decide to opt-in). We will use the mailing address you entered during the Orientation ID verification survey UNLESS we hear from you in the next section that you need the certificate mailed to a different address.
- A ***digital certificate*** available from your programme dashboard. This credential will be ready for you on **3 August, 2022**.

More information about each of these credentials follows.

## W.2.2 Digital Badge via Credly

### About Your Badge

Learning, employment, and advancement opportunities are intertwined, but a career path rarely follows a straight line. Saïd Business School, University of Oxford, wants to recognise your learning achievements and skills in a way that connects you with opportunities that can serve as milestones along your career path. That's why we issue digital credentials through the Credly platform. In addition, Credly offers **blockchain-backed credentials**. By issuing digital credentials on the blockchain, Credly is using the latest technology, supporting high-volume verification requests of future-proof and tamper-proof credentials. Upon acceptance of your badge, it will be published to the blockchain.

### What Is a Digital Credential?

Digital credentials go beyond paper certificates. They are portable, verifiable, and uniquely linked to you. They also ensure that your hard-earned achievements are owned by you, not us—you can access and utilise your digital credential whenever and however you see fit. Digital credentials make you—and your achievements—more visible to employers and your professional network.

## Share Your Achievements with Your Network

Your skills, competencies, and certifications are worth more than a static bullet point on a resume or a paper certificate hanging on the wall in your office. When your achievements are represented as a digital credential, you can share your achievements with your network in one click from Credly's Acclaim platform. Peers and employers can verify and learn more about what it is you can do, thanks to earning a digital credential from Saïd Business School, University of Oxford. And research shows that professionals who share their digital credentials to professional networking sites are discovered by employers, on average, six times more often than those who do not.

You will be able to connect your LinkedIn, Twitter, Facebook, and XING accounts to your Acclaim profile, which will enable you to:

- Post the unique badge URL on social media
- Embed the badge on a personal website
- Send the badge via email to a contact or employer
- Download the badge visual for a resumé or email signature
- Download a printable version of your badge
- Send the badge through Facebook Messenger and WhatsApp on a mobile device

## Find Your Next Career Opportunity

You've invested time and money into advancing your skills, and your Saïd Business School, University of Oxford digital credential can unlock career opportunities for you. Credly's labour market insights help you:

- Discover new skills that complement what you already know
- Connect with the next certification along your career path
- Search and apply for your next job opportunity

## Claiming Your Badge

On **3 August, 2022**, you will receive an email notification from Credly with information on how to create a profile on the Credly platform.

Once you sign in, you will be able to claim your pending Oxford Blockchain Strategy Programme badge. There will be clear instructions for claiming and sharing your badge in the email.

Have questions? You can email [oxfordsuccess@esmelearning.com](mailto:oxfordsuccess@esmelearning.com).

## **W.2.4 Digital Certificate**

This programme issues digital certificates. **Certificates will be awarded on 3 August, 2022.** When certificates become available, a link to your certificate will be visible on your [dashboard](#). You can view and print your certificate. Though there are options for sharing this certificate via social media, we recommend sharing your Credly badge instead.

### **View Your Certificate**

To view your certificate, click the link on your [dashboard](#).

### **Print Your Certificate**

To print your certificate, open the certificate in your browser, and then you may either take a screenshot to save as an image and share, or select **Print Certificate** in the certificate header. We recommend using the A4 paper setting for an optimal printing experience.

### **Share Your Certificate**

We recommend that you share your Credly badge instead of your digital certificate on your LinkedIn and other social media sites. We've outlined some of the benefits of sharing your Credly badge in the Digital Badge via Credly section of this module, and you'll get more information on how to claim and share your Credly badge in an email on **3 August, 2022**.

If you'd still like to share your digital certificate, see [How can I add my certificate to my LinkedIn profile?](#) or [Share a Web Certificate](#).

# **W.3 Continuing Education Credit**

## **W.3.1 IACET CEUs**

### **International Accreditors for Continuing Education and Training (IACET)**

We're happy to inform you that Esme Learning Solutions is accredited by the International Accreditors for Continuing Education and Training (IACET) and offers IACET CEUs (Continuing Education Credits) for its learning events that comply with the ANSI/IACET Continuing Education and Training Standard.

IACET is recognized internationally as a standard development organization and accrediting body that promotes quality of continuing education and training. Many companies, regulatory boards and organisations have been reported to accept the IACET CEU credit, and you can check the [list of organisations accepting IACET CEU credit here](#).

Successful completion of this programme with a score of 50% or higher earns you 4.2 CEUs.

## **W.3.2 CPD Credit Hours**

### **Continuing Professional Development (CPD) Hours**

We're pleased to inform you that the content of this programme has been independently certified by the CPD Certification Service as conforming to continuing professional development principles. You may declare up to **44** CPD hours for the Oxford Blockchain Strategy Programme. You can learn more about CPDs and how to use them on the [CPD website](#).

Contact [registrar@esmelearning.com](mailto:registrar@esmelearning.com) to obtain a copy of the certificate verifying that this programme is CPD-certified if needed.

# W.4 Access to Materials and New Offerings

## W.4.1 Access to Online Materials Until 30 August, 2022

### Access to Programme Materials and Riff

Access to your programme materials and to Riff will be available for six weeks after the programme ends, until **30 August, 2022**. During the six weeks, you can access programme materials from your [dashboard](#), and download the materials that you want to save.

You can [access Riff](#) by using your browser, or by using the links in the programme.

Once programme access has ended, we encourage you to stay in touch with your classmates. Check out the Staying in Touch lesson to learn more about how to join Oxford International Online Community and stay connected.

### Complete Your Downloads Before 30 August, 2022

You can find individual module, transcript, and Key Takeaways downloads in the [Downloadable Notes](#) section of the programme material.

## W.4.2 Upcoming Oxford Programmes Start 14 September, 2022

Don't forget to tell your friends about this programme! Our next presentation starts on **14 September, 2022**. For more information, see the [Oxford Blockchain Strategy Programme](#) or contact Esme Learning at [oxfordprogrammes@esmelearning.com](mailto:oxfordprogrammes@esmelearning.com).

We would be thrilled to have some familiar faces in our next six-week online programmes from Saïd Business School, University of Oxford.

And now that you've completed the Oxford Blockchain Strategy Programme, you've joined the ranks of the Oxford e-lumni network, and you're eligible to receive **10% Off** any online Oxford Programme listed on [esmelearning.com](#) by entering code **ELOXFONLINEPP10** at checkout.

For more information, follow the links below:

- [Oxford Fintech Programme](#) - next presentation starts **19 October, 2022**
- [Oxford Cyber Security for Business Leaders Programme](#) - next presentation starts **14 September, 2022**

# **W.5 Staying in Touch: Meet-up & Community**

## **W.5.1 Join the Oxford Saïd Community**

### **You Are Invited to Join the Oxford Saïd Community**

The online offerings from Saïd Business School, University of Oxford, are designed to enhance your personal development and fast-track your career. These programmes furnish you with skills to unravel complex problems and engender success across businesses.

The completion of your programme puts you in league with a global network of “e-lumni”, and offers you extensive benefits exclusive to members of this Oxford Saïd Community. You’ll be granted access to:

- A special Elumni reduced rate of 10% off of the fee on your next Oxford Saïd online programme to support your lifelong learning goals
- A dedicated group on LinkedIn—the [Oxford Executive Education Alumni group](#), an official Saïd Business school, University of Oxford alumni group for all Executive Education programmes, with over 7,000 members
- The Oxford Saïd Elumni newsletter, which will keep you updated on news, events and other opportunities at the Schools (be sure to opt-in below)
- Further opportunities to learn from Oxford faculty and thought leaders through a range of events

In addition, you’ll have access to regular networking and informational events hosted throughout the year by some of the world’s best University societies, such as the Oxford Guild—the most prominent university society in the world and among Europe’s oldest.<sup>1</sup>

Throughout its over hundred-year history, the Guild has been a source of inspiration, encouragement, and guidance to some of the best and brightest minds. The Guild’s inimitable global reach provides its members singular opportunities to meet and network with experts from various industries and backgrounds.

<sup>1</sup> [The Oxford Guild](#) (Nd). Accessed 26 April, 2022

### **Opt In to the International Online Oxford Saïd Community**

If you haven’t already, be sure to [opt-in \(in the Orientation module\)](#) to be subscribed to future Executive Education Elumni mailings about webinars and networking events from Saïd Business School, University of Oxford.

# **W.6 Important End-of-Programme Dates**

## **W.6.1 Important End-of-Programme Dates**

### **A Recap of Important End-of-Programme Dates**

*3 August, 2022*

- An email will arrive with your final programme score and a prompt to view your digital credential on your programme dashboard.
- An email will arrive from credly.com with the subject “Saïd Business School, University of Oxford Issued You a New Badge” that will have instructions for claiming and sharing your Credly badge.

*30 August, 2022:* The last day you’ll have access to this learning platform and the Riff discussion and video meeting platform.

*30 August, 2022+:* You will receive your printed Saïd Business School, University of Oxford Certificate of Achievement in the post (if you opted in to receive a printed certificate).

*Anytime until 1 June, 2029:* You may email [registrar@esmelearning.com](mailto:registrar@esmelearning.com) to verify your attendance and completion of the Oxford Blockchain Strategy Programme.

# Blockchain Strategy Glossary

**51% attack** - A cyber attack on a blockchain in which the attackers attempt to gain more than half of the computing power of a network, thereby enabling them to change or reverse previous records for personal gain.

**accelerator** - A privately or publicly funded programme that provides (financial) resources, business support, and mentoring for a fixed period of time to a cohort of growth-driven startups that have a minimum viable product (MVP) to help scale their growth.

**adversary** - A person or group of people maliciously opposing, attacking, or stealing from the person or group.

**agile** - A method of project management that utilises short phases of work, group consensus and effort, and flexibility.

**altcoin** - Any cryptocurrency or non-fungible token that is not bitcoin.

**algorithmic stablecoin** - Cryptocurrencies like Ampleforth (AMPL), Fei (FEI), or Empty Set Dollar (ESD) that are not pegged to any particular commodity or fiat currency but instead aim to achieve price stability by algorithmically balancing themselves. When the price increases, the underlying algorithm adjusts to issue more coins, and when the price decreases, it automatically buys them back from the market.

**anti-money laundering (AML)** - A set of regulations meant to prevent the crime of making illegally-obtained funds appear to be legitimate.

**API** - See *application programming interfaces (APIs)*.

**application layer** - The layer in blockchain development that represents the interface between two applications via an application programming interface (API) or a user interface.

**application programming interfaces (APIs)** - Software that enables two separate applications to communicate. For example, the Google Maps API enables businesses, such as restaurants to embed maps on their websites so that customers can find the business easily without having to access Google Maps as a separate application or website.

**asset class** - A group of investments with similar characteristics.

**atomic swaps** - Automated contract technology that enables the exchange of one cryptocurrency for another across different types of blockchains without using a third party..

**automated market maker (AMM)** - An automated system of trading protocols that underlies decentralised exchanges, using smart contracts to facilitate trades without a centralised exchange.

**backdoor** - The access to encrypted information that bypasses normal authentication methods; may be authorised or unauthorised.

**Beacon Chain** - The first platform to launch on the Eth2.0 network as a point of stake (PoS) model. See *Point of stake (PoS)*.

**big data** - The overwhelming and constantly increasing amount of data collected every day through financial transactions, retail transactions, interactions with IoT devices, and the like.

**bitcoin** - A particular type of decentralised digital currency. The bitcoin currency may be traded on the Bitcoin platform.

**Bitcoin** - The first peer-to-peer transaction protocol housed on a blockchain; developed and introduced by Satoshi Nakamoto in 2009.

**Bitcoin Core** - An open-source project that was created to maintain and release its eponymously-named client software.

**Bitcoin Exchange Traded Fund (ETF)** - An investment fund on a regulated exchange that tracks the price movement of Bitcoin.

**Blockchain as a Service (BaaS)** - A cloud-based infrastructure and management offering for companies that are creating and managing blockchain applications.

**blockchain ecosystem** - A governance structure composed of internal and external stakeholders who contribute, in different ways, to create a specific environment.

**blockchain governance** - The means by which stakeholders achieve control, direction, and coordination within a blockchain network.

**blockchain technology** - A system of records that are connected using cryptography to protect data. For more information, see *The Truth About Blockchain or Blockchain, Explained*.

**block explorer** - Website that provides access to all transactions on a particular blockchain platform using a public key.

**block reward** - A cryptocurrency miner's compensation, in the form of cryptocurrency, for finding and validating transaction blocks.

**blue ocean strategy** - A term used to describe the strategy of finding a new market that has little or no competition, where one can innovate and create new demand. The term is based on the idea that there is a vast "empty ocean" of opportunities when a new or little-known industry is discovered.

**bug bounty** - A program that provides rewards to individuals who identify errors (bugs) and other vulnerabilities in a software program or infrastructure system.

**burning** - In cryptocurrency, the process of taking tokens out of circulation.

**bytecode** - Programming code designed to run on a virtual machine, as opposed to a central processing unit, which transforms program code for a software interpreter.

**carbon credit** - Unproduced carbon emissions that are less than a polluting organisation's allotted amount. These can be sold to a purchaser needing to offset their own carbon emissions.

**card rail** - A network on which companies like Visa, American Express, and Discovery operate to transmit information about the cardholder's payment request to the merchant bank and submit a request to the cardholder's bank for payment. If approved, the bank issues the payment to the merchant's bank account.

**censorship resistance** - A blockchain platform is inclusive and non-discriminatory in terms of anyone participating in the platform or network. All rules apply to all participants.

**CBDC** - See *central bank digital currency (CBDC)*.

**central bank digital currency (CBDC)** - A digital form of money established by government regulation.

**centralised exchange (CEX)** - A trusted third-party online platform that enables the buying and selling of cryptocurrencies, both for fiat currencies (i.e., US dollar) or between digital currencies (Bitcoin, Ether).

**code repository** - A web-hosted or other file archive that stores a project's source code and is accessible by the developers, programmers, and others.

**collective** - A group of individuals who share a common interest and work together to achieve common goals within that interest.

**combating the financing of terrorism (CFT)** - Efforts by governments and their justice departments to combat the funding of terrorist activities.

**committing peer** - The entity that saves or "commits" a transaction in the ledger, after the transaction has been submitted to the blockchain.

**commodity** - A physical good that can be bought or sold for another good of similar value. For example, sugar is the same product no matter where it is bought or sold.

**composable computing** - The use of a single platform to which scalable hardware and software can be added as needed to maintain the desired level of computer processing.

**compute and connectivity** - The combination of resources required for hardware and software devices to process computations and communicate those computations with other hardware and software devices.

**Compute as a Service (CaaS)** - An offering that supplies computing resources on demand via virtual and physical resources.

**consensus** - An occurrence when all blockchain nodes agree on the validity of a new block added to the blockchain.

**consensus protocol** - Also known as consensus algorithm or consensus mechanism, it is a computational problem that miners solve to verify and validate the information being added to the distributed system, ensuring only authentic transactions are recorded on a blockchain network.

**ConsenSys** - A blockchain technology company that creates developer tools and builds custom blockchain solutions for enterprises using Ethereum's blockchain infrastructure.

**ConsenSys Quorum** - A recent merger of ConsenSys and JP Morgan's blockchain solution; Quorum. ConsenSys Quorum creates solutions for enterprises to leverage Ethereum to build blockchain applications for financial services, supply chain management and other industries.

**consortium** - An association established by two or more enterprises to pursue a common business objective. On the Hyperledger Blockchain, a consortium is a collection of organisations that operate peer nodes and join channels within a blockchain network.

**coopetition paradox** - The pursuit of both cooperation and competition between organisations at the same time.

**Corda** - An open-source platform for developing permissioned blockchain networks focused on Banking, Capital Markets, Trade Finance, Insurance, and other financial services.

**creator economy** - Businesses and communities built by highly motivated individuals around a skill, passion, or concept, using a digital platform to help them share their product(s) and grow.

**cross-chain functionality** - The ability of one blockchain to communicate with another blockchain, also known as blockchain interoperability.

**crowdfunding** - Fundraising in which investors typically gain some form of stake in a product or project, as their early investment is typically used to pay for production or startup costs. For example, Kickstarter is a crowdfunding site.

**crypto asset** - An umbrella for four categories of digital assets:

- Cryptocurrencies
- Platform tokens and crypto commodities
- Utility tokens
- Transactional tokens

**crypto bank run** - Any form of hype or panic that causes investors to pull their funds out, which could lead to remaining investors losing value in the cryptocurrency.

**cryptocurrency gain** - The increased value of a cryptocurrency from its purchase price.

**crypto custody** - Refers to the ability to move, store, and protect crypto assets. Investors can maintain direct custody of digital assets, or indirect, in which a trusted third party maintains asset custody on their behalf.

**crypto dust** - Trace amounts of crypto that are often the result of leftover crypto from a trade; the negligible remainder. Sometimes used in an attack on multiple digital wallets to attempt to identify wallet owners.

**crypto or digital wallet** - A digital storage place for holding cryptocurrencies.

**crypto fund** - A fund created to invest in a specific blockchain startup's equity and/or crypto assets, which may include crypto assets purchased on a secondary market, pre-sale, or ICO sale, and startup equity.

**crypto native users** - Those already interacting with blockchain-native platforms and services like Uniswap or Metamask.

**cryptography** - The science of protecting information from an adversary.

**cypherpunks** - A community of cryptography enthusiasts motivated by social and political change.

**C++** - A popular extension of the C programming language used for a variety of software and web functions.

**DAO** - See *decentralised autonomous organisation*.

**dApp** - See *decentralised app (dApp)*.

**dark web** - The dark web utilises specific software configurations and certain browsers to access and communicate internet content anonymously.

**data dignity** - The notion of respecting one's personal data; being completely transparent about the use of data, the value derived from it and how one can control their own personal data.

**decentralised** - A system that has no single authority or administrator.

**decentralised app (dApp)** - Applications run on protocols that consumers use, such as wallet apps.

**decentralised autonomous organisation (DAO)** - An internet-built entity that is collectively owned and managed by its community. Its members make decisions around a set of rules encoded on a blockchain network.

**decentralised exchange (DEX)** - A peer-to-peer marketplace that allows individuals to buy and sell cryptocurrencies to one another, without an intermediary, with the use of smart contracts and atomic swaps.

**decentralised finance (DeFi)** - A category of financial services, such as borrowing and lending, that operate via applications on decentralised public blockchain networks and that do not involve intermediaries, such as banks.

**decentralised platform** - A system that has no single authority or administrator and no single, centralised storage of data or element of coordination or control.

**decryption** - The process of using a password or private key to reveal encrypted digital information.

**DeFi** - See *decentralised finance (DeFi)*.

**derivative** - A financial contract between two or more parties, the value of which is linked to the value of one or more agreed-upon underlying financial assets, such as commodities, currencies, or indexes. Common examples of this financial instrument are Futures contracts, Forward contracts, Options, and Swaps.

**digital asset** - A digital file that is owned by and provides values to an individual or business.

**digitally native asset** - Digitally native assets are alternative forms of expression that most popularly come in non-fungible tokens (or NFTs).

**directed acyclic graphs (DAG)** - A graph that has both vertices and edges that are directed so that they go in only one direction, and there is never a closed loop when following any of the directions. They are used for different types of flows, including data processing flows, and to display assumptions about the relationship between variables.

**disintermediate** - To reduce or eliminate.

**distributed ledger system** - A type of database that is shared and synchronised by multiple people across different geographies and institutions.

**distributed ledger technology (DLT)** - Technology that uses multiple independent computers to store information and transactions, rather than a single centralised database.

**distributed system** - A system built of component parts located on networked computers. For example, the internet is a distributed system.

**domicile choice** - A form of regulatory arbitrage that involves operating or basing one's business in another location that has more favourable laws and regulations, thereby circumventing the laws in their current location.

**double entry accounting** - When transactions are recorded as both a debit and a credit since each transaction impacts the financial statements in two corresponding ways. For example, when a company buys something in cash, its assets increase, but its availability of cash decreases by the same amount. This is also known as "double entry bookkeeping".

**double-spending** - Part of a fraud attempt where a coin holder tries to spend the same coin twice. Blockchain technology prevents double-spending from happening.

**eclipse attack** - Attacker fools an active node into validating false transactions, blocking it from knowing about the legitimate transactions.

**encryption** - A means of protecting digital information by which text is scrambled into secret code that hides the information's true meaning so that if it is stolen, it cannot be read. An algorithm and a password or private key to decrypt the information.

**endogenous** - An organisation's internal variables that directly affect the project and any interactions with it.

**endorsing peer** - The peer that approves or endorses a transaction when it is proposed before it is submitted to the blockchain.

**enterprise blockchain** - Where companies or enterprises use blockchain technology as a service to enable specific partners they wish to transact with in a more distributed, transparent, and secure manner. These services can also form bridges to public blockchains.

**Enterprise Ethereum Alliance (EEA)** - A member-led organisation dedicated to driving the adoption of Ethereum at the enterprise level. The technology-based federated blockchain platform enables member organisations to adopt and use Ethereum technology in their daily business operations.

**ETC** - The trading symbol for Ethereum Classic.

**ETH** - The trading symbol for Ether on the Ethereum network.

**Ether** - The name of the cryptocurrency tokens used for payment on the Ethereum network.

**Ethereum** - Ethereum is a blockchain network that is similar to Bitcoin. It has its own cryptocurrency, called Ether or ETH, and can be used to build, publish and monetise decentralised digital applications on the network.

**Ethereum Improvement Protocol (EIP)** - Standard utilised by the Ethereum community to keep the protocol interoperable across implementations.

**Ethereum virtual machine (EVM)** - Ethereum's machine state—its continuous and immutable operation—that changes from block to block, according to a predefined set of rules and which can execute arbitrary machine code.

**Enterprise Resource Planning (ERP)** - A process that helps companies to integrate and manage all of their processes needed to operate. For example, ERP software can integrate a company's sales, marketing, finance, HR, and purchasing processes.

**ERC-20 token standard** - A standard that creators use to produce indistinguishable tokens to trade for other tokens.

**ERC-721 token standard** - A standard that enables creators to issue tokens that each have a unique identifier code.

**ERC-1155 token standard** - A newer token standard that allows one smart contract to represent multiple fungible and non-fungible tokens in addition to batched operations which will result in reduced network costs.

**exchange-traded fund (ETF)** - A structured asset or grouping of assets (securities, funds, commodities, and so on) traded, like a stock on an exchange.

**exchange value** - The price or value of something that is traded.

**exogenous** - Variables that are independent of an organisation and the project but that affect the project.

**extranet** - A private network that allows access only to a certain group of authorised parties.

**fiat currency** - A government-issued currency that is not backed by a commodity, like oil or gold, but rather by the issuing government itself, such as the US dollar or the euro.

**financial engineering** - The process of applying mathematical expertise to solve financial problems.

**flatarchy** - A traditional hierarchical organisational structure with a separate innovation group that requires decision-making autonomy.

**fork** - An upgrade to a protocol, either through a hard fork, which preserves the past transactions as they are or through a soft fork, which is compatible with both historical and future transactions.

**full node** - A full copy of the Bitcoin blockchain, a record of all transactions since the beginning of Bitcoin time.

**fund of funds** - A crypto fund that invests in other crypto funds, allowing for diversification of risk, similar to a mutual fund. The fund may issue a token for investor rights to the portfolio of companies.

**fungible** - An item that can be exchanged, such as a cryptocurrency or a dollar.

**futarchy** - An untried form of government, proposed by economist Robin Hanson, that has democratically elected officials who define and manage measures of national welfare, whilst market speculators are used to determine which policies will have the most positive impact on national welfare and, therefore, become law.

**foundation** - A type of entity that is classified as a nonprofit corporation or a charity. Foundations are typically formed with a core mission, which is pursued through the issuance of grants to organisations, institutions, or individuals to carry out their mission.

**game theory** - The study of interactions between rational decision-makers in a strategic setting and the formation of mathematical models to create optimal outcomes for participants.

**gas** - The name of the unit that measures the computational efforts needed to carry out specific transactions on the Ethereum network.

**GDPR** - See *General Data Protection Regulation (GDPR)*.

**General Data Protection Regulation (GDPR)** - A legal framework that sets guidelines for the collection and processing of the personal information of individuals within the European Union (EU). The GDPR sets out the principles for data management and the rights of the individual while also imposing fines that can be revenue-based. The GDPR covers all companies that deal with the data of EU citizens, so it is a critical regulation for corporate compliance officers at banks, insurers, and other financial companies. The GDPR came into effect across the EU on May 25, 2018.

**GitHub** - A website for developers to collaboratively work on code while maintaining version control.

**gossip protocol** - A procedure of peer-to-peer computer communication inspired by the form of gossip seen on social networking sites. It is used by distributed systems as a more efficient way to solve problems and to ensure that data is disseminated to all members of a group.

**governance token** - A token created by a decentralised exchange that enables holders to vote on proposals made by the community. Also called a utility token.

**Gramm-Leach-Bliley Act of 1999** - Also known as the Financial Modernisation Act of 1999, the GLBA protects consumers' personal information stored in financial institutions.

**hack** - To gain illicit access to a computer or network, usually with malicious intent. Attackers look for vulnerabilities in a blockchain network and exploit them for illegal and personal gain.

**halving** - In relation to cryptocurrency, this is the reduction of the block subsidy provided to miners by half. It is a process that ensures the issuance rate of new coins is steady until its maximum supply is reached. For example, there is an event known as "Bitcoin halving" every four years.

**hard fork** - A permanent split in the blockchain platform in order to change the code.

**hashing** - The algorithmic process of converting a varied input of data into a fixed-length output.

**hashcash** - A system based on proof of work, designed to prevent denial of service attacks and email spam. Hashcash was invented by early Bitcoin adopter and advocate, Adam Back.

**hashrate** - The total combined computational power that is being used to mine and process transactions on a PoW platform.

**Hedera Hashgraph** - A distributed ledger technology solution that leverages directed acyclic graphs as a Byzantine fault-tolerant consensus mechanism to achieve a more scalable alternative to traditional blockchains.

**hierarchical** - A vertically aligned management structure that exists in traditional corporations or firms.

**HIPAA** - The abbreviation for Health Insurance Portability and Accountability Act, which ensures a US medical patient's right to privacy and that their health information is protected from unauthorised access.

**holacracy** - An organisational structure where individuals and teams have control over the processes.

**hyperinflation** - Monetary inflation that occurs at a very high rate.

**Hyperledger** - An open-source enterprise-focused platform for developing private permissioned blockchains.

**ICO** - See *initial coin offering (ICO)*.

**IDO** - See *initial DEX offering (IDO)*.

**IEO** - See *initial exchange offering (IEO)*.

**impermanent loss** - A loss of funds caused when the ratio of tokens in a liquidity pool becomes uneven.

**incubator** - An open-ended collaborative programme designed to help startups and entrepreneurs to refine their business ideas and build their business plan. It provides a complete business infrastructure, including access to investors and a workspace with the necessary equipment.

**indexers** - Those who operate nodes on The Graph Network and stake Graph Tokens (GRT) to provide indexing and query processing services.

**Information Revolution** - The proliferation of digital information that began in the 1990s and continues to be transformed by evolving communication technologies.

**informational value** - The information associated with an item that contributes to that item's worth.

**infrastructure as a service (IaaS)** - A cloud computing offering that provides virtual resources and servers over the internet for businesses to use on-demand.

**initial coin offering (ICO)** - Similar to an IPO (initial public offering), an ICO serves to raise funds for a new coin, product, or project in the world of cryptocurrency. ICOs can be held either publicly or privately.

**initial DEX offering (IDO)** - A decentralised crowdfunding platform in the crypto space that uses liquidity pools to enable traders to buy and sell tokens, including crypto coins and stablecoins. In comparison to an ICO and IEO, IDOs offer immediate and better liquidity at every price level, making them an optimal choice for startups that need to access immediate funds and launch a token.

**initial exchange offering (IEO)** - Similar to an ICO (initial coin offering), this is a fundraising event that is run by a cryptocurrency exchange and managed through their platform so that users can buy tokens directly from their own exchange wallet

**interledger protocol (ILP)** - An open-source protocol developed to send payments across different ledgers.

**interoperability** - The ability of different systems (both hardware and software) to connect and share resources via a common format, without restrictions.

**InterPlanetary File System (IPFS)** - A peer-to-peer network used for sharing and storing data in a distributed file system.

**intrapreneur** - While an entrepreneur innovates to launch a startup business of their own, an intrapreneur innovates to build transformative initiatives from within an existing organisation.

**Java** - A general-purpose programming language designed to allow application developers to achieve WORA (write once, run anywhere) capabilities.

**joint venture** - A legal structure established by two or more enterprises to pursue a common business objective while maintaining each other's unique identities.

**key escrow** - A storage system that manages the release of private keys when certain conditions are met.

**know your customer/client (KYC)** - A protocol meant to protect consumers and financial institutions alike by ensuring that businesses have, at the very least, verified the identity of their clients and, if relevant, that they also understand their clients' risk tolerance, investment knowledge, and financial positions.

**layer 2 solution** - A solution to Bitcoin's scalability challenges, also called the lightning network. Its purpose is to expand the Bitcoin blockchain's capacity to process more transactions.

**ledger** - An accounting system that records transactions in an ordered manner.

**lightning network** - A solution to Bitcoin's scalability challenges, also called the layer 2 solution. Its purpose is to expand the Bitcoin blockchain's capacity to process more transactions.

**limited liability autonomous organisation (LAO)** - Unlike a decentralised autonomous organisation (DAO), which is not bound by any legal entity, a LAO is a registered investment entity that complies with US regulations but operates in a decentralised way.

**liquidity mining** - Also known as "yield farming," is the act of providing liquidity to enable trading of cryptocurrencies on decentralised platforms.

**liquidity pool** - A pool of tokens locked in a smart contract to facilitate trading by providing liquidity in decentralised exchanges.

**meatspace** - The physical or real world, as opposed to the virtual world (i.e. cyberspace).

**market capitalisation** - The number of currencies and their coins in circulation multiplied by their current prices; often abbreviated as "market cap".

**market maker** - A firm or individual who buys and sells securities for its own account, thereby creating liquidity in the market and profiting on the bid/ask spread.

**mechanism design** - An engineering theory that focuses on the design of economic incentives with the goal of achieving desired outcomes in strategic settings.

**medium of exchange** - Something that has value and is widely accepted in exchange for goods and services; currency, for example.

**membership services provider (MSP)** - A component of Hyperledger Fabric that is used to manage identities of all nodes on the blockchain network.

**metaverse** - A virtual and expansive universe built on augmented reality, virtual reality, and internet infrastructure.

**micropayment** - An online financial transaction involving a small amount of money.

**minting** - In cryptocurrency, creating new tokens and adding them into circulation.

**mimetic** - Money's value depends primarily on the importance that people place on it—as a medium of exchange, a unit of measurement, and a store of wealth.

**miner** - A small device known as a node that uses microprocessing and is designed specifically for the purpose of mining PoW cryptocurrencies..

**mining** - Creating new cryptocurrency through the process of solving computational problems that validate transaction blocks and work to maintain the blockchain ledger.

**mining pool** - When a group of miners combine their computing power and agree to split the bitcoin reward between participants.

**mining protocols** - A method for achieving consensus on the validity of transactions and allocating rewards to miners on a proof-of-work or proof-of-stake blockchain.

**money transmitter license (MTL)** - A legal requirement of cryptocurrency businesses in the US, as they are considered to be money transmitters like traditional financial institutions. MTLs vary across each state in terms of cost, duration, and complexity, as each state has its own money transmitter laws and regulations.

**native blockchain application** - The blockchain's original protocol that was designed and built to record and track the transactions associated with its native (original) asset.

**negative interest rate** - This occurs when, in the US—instead of paying banks to hold reserves—the Federal Reserve charges banks for maintaining their reserve balances.

**negative interest rate policy (NIRP)** - A monetary policy tool used by central banks to encourage spending, borrowing, and investing so that banks don't lose from the negative interest rate.

**net settlement** - When clearing houses batch multiple transactions together.

**network effect** - A phenomenon whereby the value of a product or service improves with increased numbers of users or participants. An example of this would be the internet itself.

**node** - The circle that holds each actor's name in a sociogram.

**non-crypto-native users** - Those who interact with decentralised applications for the first time with limited or no knowledge of the specific blockchain protocols that underpin them.

**non-fungible** - An item that is not exchangeable with other items due to their unique properties, such as a car or a work of art.

**non-fungible token (NFT)** - A digital token that represents ownership of a unique item, such as digital-only artwork, music, or games. This means that the token cannot be interchanged with something else.

**nonce** - “Number only used once”, or the number added to an encrypted block (hash) on the chain that meets specified difficulty level restrictions if and when rehashed.

**open-source** - Computer software where anyone can use, change, or distribute the software and its code.

**oracle** - A service that enables one-way transmission of external data to a blockchain. That data can then be used to trigger a smart contract within the blockchain.

**payment rail** - The system behind the transaction of sending money from one individual or company to another.

**pegging** - When a digital medium of exchange is tied to another currency to control or stabilise it. For example, stablecoins are typically pegged to a commodity or fiat currency.

**peer-to-peer** - When individuals interact directly with one another on a decentralised platform.

**petro** - Venezuela's national cryptocurrency, launched in February 2018.

**permissioned blockchain platform** - A blockchain platform that has an additional security layer, which allows only specific participants to perform certain actions.

**permissionless blockchain platform** - A blockchain platform that does not require any permission for participants to join and interact with the network. The first type of permissionless blockchain was Bitcoin.

**Ponzi scheme** - A fraudulent business enterprise is established to lure unsuspecting investors into participating in the business with the promise of some form of financial return.

**post-scarcity** - Technical advancement that enables goods and services to be produced with minimal human labour.

**PoW** - See *proof of work (PoW)*.

**practical Byzantine Fault Tolerance (pBFT)** - An algorithm that helps distributed networks come to the consensus set for the blockchain, as pBFT allows for the approval of transactions, even if some (malicious) nodes are not approving the transaction. Its goal is to protect major system failures by diluting the influence of these malicious nodes.

**prediction markets** - Markets where people trade on the outcome of future events. The current market prices are then used to make predictions of the expected value or probability of the event.

**pre-sale** - The process of making a cryptocurrency available for sale to early adopters prior to making it available to the public.

**Presidio Principles** - The World Economic Forum's set of foundational values for those building with blockchain technology and decentralised infrastructures. They established four pillars as guidelines for preserving the rights of participants in an organisation's platform.

**principles-based regulation** - A regulation established through rules that are flexible or open to interpretation by the establishing body.

**private key** - The secret access to encrypted digital information that is paired with a public key and shared by the encoder with an authorised party to enable access to the information.

**programmable consensus** - The ability for nodes on a blockchain to come to an agreement on the state of the distributed ledger via a set of rules written into code and executed autonomously. Proof of work and proof of stake are mechanisms that are also examples of programmable consensus.

**programmable money** - Money or tokens in digital form, such as CBDCs.

**proof of authority (PoA)** - A common protocol for private blockchains where validators stake their reputations by disclosing their identities instead of staking their cryptocurrency.

**proof of elapsed time (PoET)** - A consensus mechanism protocol where randomly generated elapsed time is assigned to validators in order to determine mining rights and block winners.

**proof of space** - A consensus protocol where validators prove an allocation of hard drive storage space to solve a computational problem. Also known as proof of capacity (PoC).

**proof of stake (PoS)** - A non-mining platform where participants commit a stake of their private or collective capital to the platform in the form of the platform's native tokens, which are locked for a determined amount of time.

**proof of work (PoW)** - The earliest blockchain protocol that involves miners solving complex mathematical problems/algorithms in order to place a block of transactions on the chain. A miner is rewarded if they are the first to solve the problem.

**provenance** - A record of where something has originated from.

**pseudonymous** - When the real identity of someone or something is concealed by a false or fictitious name or pseudonym.

**pseudonymity** - The state of using a false or fictitious name or pseudonym.

**public good** - A product or service that benefits the broader public in ways that are non-rivalrous and non-excludable.

**public key** - A cryptographic method to encrypt digital information and share with another party to access the encrypted information.

**Python** - A general-purpose programming language that emphasises code readability and is known for its use of significant indentation.

**quadratic funding** - A way of allocating funds for projects in a way that empowers communities to demonstrate their preference, rather than allowing a small number of individuals with deep pockets to benefit the most.

**quadratic voting** - A collective decision-making method where individuals express their preferences, as opposed to simply voting for or against something. This helps to identify issues of majority rule or voting paradox.

**quantum computing** - High-fidelity processing using quantum bits to perform computations unachievable by classical computers that use binary bits.

**quantum supremacy** - A state achieved by an organisation when its quantum computer performs a computation unachievable by traditional computers.

**ransomware attack** - An event in which attackers hack into a computer or network of computers to block usage and access to data until a ransom payment is made.

**real-world blockchain application** - A blockchain protocol's use case.

**red ocean strategy** - A strategy in which firms must find a competitive edge in a highly-saturated market and beat the competition using existing demand.

**regulatory arbitrage** - The practice of optimising loopholes in regulatory systems to avoid less favourable regulations. This might include geographic relocations, financial engineering, or restructuring activities.

**reputation marketing** - A marketing strategy that focuses on the positive content about a brand, including social media comments, reviews, and news articles. This content is then used to inform the company and to improve the brand's reputation and overall image.

**reverse ICO** - This funding method involves an established non-crypto company issuing a token as an alternative to fundraising through an initial public offering (IPO), giving it access to funds without the regulatory oversight of an IPO. Reverse ICOs have come under scrutiny in the US by the Securities and Exchange Commission, which argues that the token issues are securities.

**rug pull** - A term to describe theft in the cryptocurrency space, whereby project developers suddenly abandon a project after taking the investors' money.

**rules-based regulation** - Policy established through well-defined rules that outline a clear path to compliance.

**scalability trilemma** - The argument that a consensus mechanism can optimise for at most two of the following vectors: security, scalability (in the form of transaction throughput), or decentralisation (in the form of fault tolerance).

**scarcity** - Digital assets with a fixed or variable supply that enables consumers of those assets to more easily ascribe value to them.

**security token** - Tokenised assets issued under a regulatory framework that designates the tokens as registered securities, similar to stocks or bonds, which are registered securities under the regulation of the SEC. Security tokens can be either fungible (i.e., represent one of the issued shares in a company) or non-fungible (i.e., represent a unique asset).

**self-amending blockchain** - A platform that adapts and adopts new features natively and automatically via its unique on-chain governance mechanism.

**self-regulatory organisation** - A member-based organisational structure wherein principles and rules are established by the members, who agree to follow them or face certain penalties.

**shards** - Used in the Eth2 upgrade to spread the network's load across 64 new chains.

**shared governance** - A structural model that encourages maximum participation from different stakeholders in a decision-making process. For example, shared governance within a university setting might put the responsibility and accountability of a decision in the hands of the governing board, as well as the professional and administrative staff and students.

**sidechain** - An auxiliary blockchain connected to the parent blockchain and which may have its own protocol.

**simple agreement for future tokens (SAFT)** - An agreement for an investor to collect utility tokens at a reduced price at a future date when the system being developed is up and running. It is a way for developers and founders to raise capital without breaking securities law. The investor converts their investment into assets at that later date and can then trade the tokens without restrictions on the crypto exchanges.

**smart contract** - A programmatically executed transaction coded into a blockchain network based on predefined terms. Smart contracts are meant to be faster, more efficient, and more secure, with no need for intermediaries.

**soft fork** - A change to the software protocol wherein previous blocks are made invalid.

**software development kit (SDK)** - A package of software development tools, including documentation, frameworks, and guides, to help developers build platform-specific applications.

**solidity** - A programming language designed for developing smart contracts on the Ethereum blockchain.

**sovereign** - With regard to currency, legal tender issued by national governments.

**stablecoin** - A cryptocurrency that is meant to stay relatively constant in value and that is pegged to an asset such as gold or a fiat currency.

**staked tokens** - The native token of a PoS platform that a validator puts up to guarantee the legitimacy of a transaction they have just added to the blockchain.

**stakeholder engagement and communication plan** - An allocation of time and resources towards those who have the most impact on your project's needs; a formulaic process for developing and executing a go-to-market strategy.

**stakeholder mapping exercise** - A process in which internal and external stakeholders are prioritised based on their level of influence, interest, and participation in a project.

**staking** - The process of committing and holding funds in a certain cryptocurrency for the purpose of earning rewards and contributing to the security and consensus mechanism of that particular network.

**store of value** - An asset or commodity that retains its value relative to other assets or currencies over time. Also referred to as store of wealth.

**supercomputing** - The utilisation of multiple computing systems, typically large CPUs with high-speed connectivity, to achieve higher computing power that will solve complex algorithms.

**The Bitcoin Development Fund** - A fund launched by the Human Rights Foundation in 2020 to make the Bitcoin network more decentralised, private, and resilient so that it can be used as an effective tool for human rights activists, civil society organisations, and journalists.

**The Howey Test** - A test based on the US Supreme Court case SEC v. W.J. Howey Co., which determines whether a transaction, scheme, or contract qualifies as an “investment contract.” If so, it is considered a security and subject to registration requirements under the Securities Act 1933 and the Securities Exchange Act 1934. This test is helpful for situating cryptocurrency and blockchain projects with investors.

**third-party doctrine** - A US legal doctrine that provides that individuals who give their information to a third party can have no reasonable expectation of privacy.

**token** - A fungible virtual currency that functions as a tradable asset, or a utility that resides on a specific cryptocurrency's blockchain, or a non-fungible (non-tradable) unit of data used to validate an object as unique.

**token incentive model** - The economic model of an individual platform that incentivises users to hold on to its native token which should, in turn, increase the value of that token's price.

**tokenisation** - The process of protecting sensitive data by replacing that data with algorithmically-generated, unique identification symbols (tokens) that have no exploitable value.

**tokenised venture fund** - Also known as a tokenised fund, this type of fund models fund ownership after an ICO structure. So, a VC fund can launch its own tokenised securities and fundraise on the basis of these tokens, which can be traded on a crypto exchange once they are listed. Such a fund can then provide liquidity for investors without long-term capital commitments, which depend on how the fund is ultimately structured.

**tokenomics** - The study of the economics of crypto tokens, including how they work, their distribution, and what makes them attractive to investors.

**total value locked** - A metric used to measure the growth of the decentralised finance (DeFi) market.

**transaction volume** - The number of transactions.

**transmission control protocol (TCP/IP)** - A communication standard for computers and application programmes to share messages over a network. TCP/IP is the main communication standard behind the internet.

**trustless** - The blockchain platform does not require participants to know or trust each other, and it does not require a third-party intermediary in order to function..

**TVL** - See *total value locked (TVL)*.

**unit of account** - A definite quantity that is accepted and used as a standard for the measurement of the same quantity. Also referred to as a unit of measurement.

**use value** - An item's use purpose that contributes to that item's worth.

**user interface (UI)** - The configuration of software, hardware, and input devices that allow a user to interact with a computer.

**utility token** - A token created by a decentralised exchange that enables holders to vote on proposals made by the community. Also called a governance token.

**validator nodes** - The nodes that verify transactions on blockchain networks.

**validators** - Individuals who stake coins to help verify transactions on a blockchain network.

**venture capital (VC)** - Generally a fund or group of investors who finance startups—and occasionally lend expertise and nurture them—in the hopes of rapid commercial growth and substantial return on their initial equity stake investment.

**wallet** - A digital cryptocurrency storage device that is either virtual or physical.

**wallet address** - A digital address made up of alphanumeric characters that is used to identify a digital wallet.

**Web 2.0** - The state of the internet that reflects more user-generated content and end-user functionality than the original version: Web 1.0.

**Web 3.0** - The next evolution of the internet that provides a more decentralised method of user-content generation and allows users to interact via peer-to-peer networks.

**whitepaper** - In the crypto industry, a piece of documentation produced by developers to explain the technical specifications of a blockchain network and token structure.

**zero knowledge proofs** - A technology that uses cryptographic algorithms to enable the verification of information without revealing or sharing any sensitive data. For example, when a payment application needs to confirm you have enough funds in your account without knowing anything else about your bank balance.

**Zooko's Triangle** - A theory put forth by Zooko Wilcox-O'Hearn that naming participants in a network requires the satisfaction of three properties: human meaningful, decentralised, and secure.