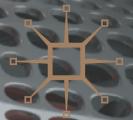


THE BOOK OF CRYPTO

The Complete Guide to Understanding Bitcoin,
Cryptocurrencies and Digital Assets



HENRI ARSLANIAN



The Book of Crypto

Henri Arslanian

The Book of Crypto

The Complete Guide to Understanding
Bitcoin, Cryptocurrencies and Digital
Assets

palgrave
macmillan

Henri Arslanian
Hong Kong, Hong Kong

ISBN 978-3-030-97950-8 ISBN 978-3-030-97951-5 (eBook)
<https://doi.org/10.1007/978-3-030-97951-5>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2022, corrected publication 2023

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Cover credit: © Willyam Bradberry/shutterstock

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To my wife and kids

Preface

In the summer of 2019, I published my book, *The Future of Finance: The Impact of FinTech, AI and Crypto on Financial Services*.¹ The book was translated into many languages, became a global top 10 best-seller in financial services on Amazon, and was named by Book Authority as one of the “Best FinTech Books of All Time”. I got tremendously positive feedback on this book from people in the broader financial services ecosystem, from regulators and central bankers to entrepreneurs and academics.

I was touched by the reception of that book, but when I always asked any reader what the one topic was they wanted to learn more about or for me to go into more depth, their answer would almost always be crypto-assets. In addition, since the launch of my last book, many ground-breaking developments have happened in the broader crypto space, from the rise of DeFi and NFTs to the entry of institutional investors and various CBDC initiatives. It became clear that something new was needed to empower readers with the fundamentals of these developments.

Writing a book is never easy and requires sacrificing hours of your “spare time” and that spare time is particularly precious when you have two young kids at home you barely see due to various work and travel commitments. But taking the time to write such a book is important as I know that so many of you around the world would benefit from this content. I started assembling the proposal for this book shortly after my previous book was published in 2019, signing the contract with my publisher on Christmas Eve 2019 as I departed for some well-deserved holidays in the Caribbean. Having a signed

contract with strict deadlines puts the much-needed pressure and discipline needed to write any book. The timing of this book was also strange, in that just a few days after the contract signing, the COVID-19 pandemic began.

Over the next two years, I would spend many weeks either at home in lockdown or in mandatory hotel quarantines. I made a point to myself that instead of wasting time watching Netflix or YouTube, I would take advantage of adverse circumstances and focus on writing this book. Large sections of this book were written in Armenia (where I spent the early part of the pandemic in 2020); Dubai (where I spent the early part of 2021); and in Hong Kong (where I had to undergo numerous mandatory 14-day hotel quarantines throughout 2020 and 2021).

I'm fully aware that you are all very busy and don't necessarily have the time to read such a book, but many of you still want to learn about crypto. I've been teaching FinTech and crypto in university for many years and the 36-hour Introduction to FinTech course I've taught at the University of Hong Kong since 2015 is the first FinTech university course in the world. But not everyone has the chance to have such courses offered in the city where they live. Even if such courses were offered, you could potentially not have the time to spend so many hours learning about a new topic (except my students who are forced to!). The same goes for a book; only someone very keen to learn about a topic (or my students again!) would spend the hours required to read it.

I've adapted my content, including crypto educational content, over the years to target two distinct audiences: the interested mass market audience and the committed niche audience. The first category includes individuals who are curious about crypto but not much more. They're keen to learn more about it but will not spend more time going in-depth. The second category includes individuals who may have started in the first category but are more curious about the topic and want to spend time going in-depth or down the proverbial crypto "rabbit hole". The content that I create for these two audiences differs a lot. For example, over the years, I've had success with my short-form educational videos and content on LinkedIn and Twitter, shared with over a half-million followers each week and translated into various languages, including French, Spanish, Arabic, and Mandarin Chinese and distributed on my various YouTube channels. Such educational videos will regularly get thousands of views per video in the first couple of days, especially my weekly Crypto Capsule videos that summarise the developments you need to know on crypto in less than 60 seconds.

Another medium that's seen success with that first audience group is my weekly LinkedIn newsletter called The Future of Money, growing tremendously since its launch in 2020 and now reaching more than 50,000 subscribers after only one year. Another is my podcast (also called The Future of Money) that I know many enjoy when driving to work or jogging and that is downloaded now each week in over 150 countries. Whilst this content is longer than my 60-second Crypto Capsule, it's again in the range of acceptable for that first audience group. Whilst shorter form content is perfect for the interested mass market audience, I know that many want to go deeper.

To empower that second audience group, the committed niche audience, I started creating more focused and tailored content. For example, I launched my own online course in December 2021 called "Introduction to Bitcoin and Crypto-Assets" on the Udemy platform which also had tremendous success and reviews.

Whilst these digital mediums have lots of advantages (which is why I continue to actively produce content), I still believe that writing a book reaches a targeted audience truly committed to learning more about a topic, whether financial professionals or students, and this may include you! Fortunately, or unfortunately, I had to rewrite numerous sections of this book several times, as the crypto industry moves so quickly. For example, I wrote the initial section on DeFi in January 2020 when the entire DeFi ecosystem combined was less than US\$1 billion and it's over US\$250 billion at the time of writing and will be bigger by the time you read this. I wrote the section on CBDCs in February 2020; the space has moved so quickly since then that I had to rewrite the entire chapter in mid-2021.

The reality is that this sector will continue to grow very fast which is why I explain most topics in this book by first discussing the fundamentals and key tenors. Whilst the data and information provided in this book are accurate up to 1 January 2022, I have ensured to cover and explain the fundamentals for each topic. This should enable you to easily understand any new development that will undoubtedly take place on each of these topics over the coming months and years.

When writing this book, I had always you, the reader in mind, and I hope this book will be useful to you, whether you're a "traditional" finance professional moving into the crypto industry and needing a reliable book to give you the fundamentals or a student learning more about this topic as a potential career path.

Writing this book required many sacrifices, but it was a pleasure doing so, as I believe it will be a valuable contribution not only to the academic literature on this topic, but also to those of you entering this exciting space

over the coming years who will need a guide to get you up to speed. Welcome to the future of finance and money and hope you will find The Book of Crypto insightful and useful.

Hong Kong, Hong Kong
January 2022

Henri Arslanian

Acknowledgements

Writing a book is an intense journey. It devours all your “spare” time, energy, and focus. I knew this going in (this is my third published book so I can’t plead ignorance), but I still underestimated it (as every author does!). But I always do it with great passion and pleasure knowing that many may benefit, and that’s very rewarding. Thanking everyone who inspired me to write this book would be impossible, but I’d like to acknowledge a few individuals who really made a difference and helped bring this book to fruition.

To the entire team at Funday, probably the best crypto-specialised digital marketing agency in the market today, and the entire team, including partners Mark Homza and Alex Baghdjian, for all the support not only on this book but across all my content, from social media videos and newsletter to podcast and online courses. Many people from the Funday team have helped tremendously, including the amazing Brent Currie for his diligent help reviewing the book, researching specific topics, and providing feedback, Ani Tarjumanyan for designing the awesome graphics and, of course, Amalya Mnatsakanyan for all her help coordinating various aspects of this book and my brand more broadly (and keeping up with my workaholic nature and perfectionist mindset!).

To the entire team at my publisher Palgrave Macmillan, in particular Tula Weis, for her incredible support during this journey, from the various extensions to the valuable feedback. This book would have never been possible without her continuous support and backing. To Michael Wykoff for his patience and meticulous proofreading and editing work; to Lisa Rivero for

help on indexing; and to Michael Mouradian for his help in the early days with research for the history of money section.

This book would have never seen the light of day without the support of my amazing family; to my dad from whom I learned the values of hard work and integrity; to my mom who taught me the importance of intellectual curiosity and giving back; and to my parents-in-law, for their incredible understanding and support.

But most importantly, to my wife Lara (and my two young kids), for their patience and understanding for entire weekends and holidays where I was physically with them, but mentally and practically in front of the computer working on this book. Now that it's done, I can finally start playing with them as I promised them so many times.

And to you, dear reader, for your passion and interest in the field of crypto, I hope you like reading this book as much as I enjoyed writing it.

Contents

1	The History of Money	1
1	The Importance of Money and Bartering	1
2	Primitive Forms of Money	4
3	The Impact of Money on the Development of Civilisations	10
4	The Invention of Coinage	12
4.1	China	12
4.2	Lydia	13
5	The Transformative Impact of Money	15
5.1	Greece	15
5.2	Rome	17
6	Faith and Money	19
6.1	Buddhism	19
6.2	Islam	19
6.3	Christianity	20
7	The Italian Bankers and the Renaissance	23
8	China and the Rise of Paper Money	25
9	Portugal, Spain and the Age of Discoveries	27
10	The Dutch Innovations	28
11	The British and the Bank of England	29
12	The American Colonies and Paper Banknotes	31
13	The Return of the Gold Standard	34
14	Leaving the Gold Standard and the Financial Crisis	37
15	The Bitcoin Whitepaper	38

2	Bitcoin	45
1	The Basics of Cryptography and Encryption	45
1.1	Early Encryption Techniques	45
1.2	Asymmetric or Public Key Cryptography	46
1.3	Early Experiments with Cryptocurrencies	47
2	The Bitcoin Whitepaper	49
2.1	The Role of Cryptography in Bitcoin	49
2.2	The Role of Decentralisation in Bitcoin	51
2.3	The Role of Immutability in Bitcoin	53
2.4	The Role of Proof-of-Work in Bitcoin	54
3	The Growth of Bitcoin	58
4	Retail Adoption of Bitcoin	70
5	Bitcoin as Legal Tender?	75
6	Bitcoin as Company Treasury	79
7	Challenges Facing Bitcoin	81
8	The Bitcoin Lightning Network	83
9	Proof-of-Stake	88
3	Ethereum	91
1	History of Ethereum	91
2	How Is Ethereum Different?	92
2.1	What Is the Concept of “Gas” on the Ethereum Blockchain?	94
3	What Is Ethereum 2.0?	97
4	The Emergence of New Blockchains and Crypto-Assets	99
1	Examples of Cryptocurrencies and Tokens	101
1.1	Algorand (ALGO)	101
1.2	Avalanche (AVAX)	102
1.3	Binance Coin (BNB)	102
1.4	Bitcoin Cash (BCH)	103
1.5	Bitcoin SV (BSV)	104
1.6	Cardano (ADA)	104
1.7	Chainlink (LINK)	105
1.8	DASH (DASH)	105
1.9	Dogecoin (DOGE)	106
1.10	Eos	107
1.11	Hedera Hashgraph (HBAR)	108
1.12	IOTA (IOTA)	109
1.13	Litecoin (LTC)	109
1.14	Monero (XMR)	110

1.15	Polkadot (DOT)	110
1.16	Polygon (MATIC)	111
1.17	Ripple (XRP)	111
1.18	Shiba Inu (SHIB)	113
1.19	Solana (SOL)	114
1.20	Stellar (XLM)	116
1.21	Tezos (XTZ)	116
1.22	Tron (TRX)	117
1.23	Vechain (VET)	118
1.24	ZCash (ZEC)	118
5	The Technology Behind Bitcoin: Blockchain	121
1	Defining the Characteristics of a Blockchain	121
2	Differences Between Private and Public Blockchains	123
3	Challenges of Blockchain	125
4	Use Cases of Blockchain	128
6	Cryptocurrencies	133
1	Fungible and Non-fungible Tokens	135
2	Payment Tokens	137
3	Cryptocurrencies	139
3.1	Decentralised Cryptocurrencies	140
3.2	Centralised Cryptocurrencies	141
3.3	Privacy Coins	142
7	Stablecoins	149
1	Fiat-Collateralised Stablecoins	152
1.1	Regulated Fiat Stablecoins	153
1.2	Non-regulated Fiat Stablecoins	155
2	Crypto-Collateralised Stablecoins	157
3	Non-collateralised Stablecoins	160
4	Facebook's Libra (Meta's Diem)	163
4.1	Libra 1.0	164
4.2	Libra 2.0	166
4.3	Diem	170
8	Central Bank Digital Currencies	171
1	Benefits for Central Banks	174
2	History and Catalysts for CBDCs	177
9	Wholesale Central Bank Digital Currencies	185
1	National Model	185
2	Cross-Border (Corridor Model)	188

3	Cross-Border (Multi-CBDC) Model	195
3.1	Compatible CBDC Systems	195
3.2	Interlinked CBDC Systems	197
3.3	Single mCBDC Multi-Currency System	198
10	Retail Central Bank Digital Currencies	203
1	Token-Based Issuance	206
2	Account-Based	210
3	Forms of Retail CBDC	211
3.1	Decentralised Approach	213
3.2	Direct Approach	216
3.3	Synthetic Approach	216
3.4	Two-Tier/intermediated Approach	218
3.5	Platform Approach	223
11	Utility Tokens and Social Tokens	233
1	Utility Tokens	233
2	When Is a Token a Security?	234
3	Social Tokens	239
12	Security Tokens	241
1	What Is Tokenisation?	241
2	Tokenisation of New Investment Instruments	243
3	Tokenisation of Pre-existing Investment Instruments	245
13	Non-Fungible Tokens	249
1	Non-Fungible Tradable Tokens	249
2	Non-Tradable and Non-Fungible NFTs	257
14	Bitcoin and Crypto Mining	259
1	The Evolution of Bitcoin and Crypto Mining	259
2	What Are Mining Pools?	262
3	The Environmental Impact Debate	263
4	Where Does Mining Take Place?	273
15	Crypto-Asset Creation and Distribution	277
1	Initial Coin Offerings	277
2	Initial Exchange Offerings	283
3	Security Token Offerings	284
4	Hard and Soft Forks	285
5	Airdrops	287
6	Liquidity Mining/Yield Farming	288

16 Decentralised Finance (DeFi)	291
1 What Is DeFi?	291
2 Can DeFi Be Regulated?	293
3 DeFi Stablecoins	296
4 DeFi Borrowing and Lending	298
5 What Are Flash Loans?	300
6 DeFi Exchanges	301
7 What Are Automated Market Makers (AMM)?	303
7.1 What is Total Value Locked (TVL)?	306
7.2 What Is Impermanent Loss When Referring to Decentralised Exchanges?	306
8 DeFi Synthetic Assets	308
9 DeFi Insurance	309
10 Aggregators	310
11 Benefits and Challenges of DeFi	311
17 Crypto Regulations and Compliance	315
1 Different Approaches to Crypto Regulations	316
1.1 A Positive Disposition to Crypto-Assets	316
1.2 A Neutral Approach to Crypto-Assets	317
1.3 A Negative Approach to Crypto-Assets	317
1.4 The Future of Crypto-Asset Regulation	318
2 Different Approaches to Crypto Tax	319
3 Crypto and Illicit Activities	321
4 Crypto Compliance	325
18 Crypto Exchanges	335
1 Centralised Crypto-Asset Exchanges	335
1.1 Fiat-to-Crypto Exchanges	337
1.2 Crypto-to-Crypto Exchanges	340
1.3 Crypto Derivative Exchanges	341
2 Decentralised Crypto-Asset Exchanges	344
3 Cybersecurity and Hacking Considerations	346
3.1 Inherent Risks with Crypto-Assets	346
3.2 Centralised Crypto Exchange Hacks	347
3.3 Decentralised Crypto Exchange Hacks	348
19 Crypto Funds	351
1 Active Crypto Funds	353
2 Passive Crypto Funds	358
3 Crypto ETFs	360
4 Venture Capital Crypto Funds	361
5 Tokenised Funds	362

20	Crypto Ecosystem Enablers	363
1	Traditional Financial Institutions	363
2	Crypto-Focused Banks	365
3	Crypto Borrowing and Lending Platforms	366
4	Institutional Investors	369
5	Crypto-Asset Custodians and Wallets	374
5.1	Third-Party Crypto Custodians	376
5.2	Self-Custody	377
6	Large Tech Firms	377
7	Service Providers	378
8	Crypto Media Ecosystem	379
21	Future Trends to Watch	381
1	Web 3.0	381
2	The Metaverse	383
3	Quantum Computing	384
4	Zero-Knowledge Roll-Ups	389
5	Decentralised Autonomous Organisations (DAO)	391
Correction to: The Book of Crypto		C1
Conclusion		395
Notes		397
Index		449

About the Author

Henri Arslanian is the former PwC Global Crypto Leader and Partner, the first Chairman of the FinTech Association of Hong Kong and an Adjunct Professor at the University of Hong Kong where he teaches the first FinTech university course globally. Henri has advised many of the world's leading crypto exchanges, funds, investors, financial institutions, and tech firms on their crypto initiatives as well numerous governments, regulators, and central banks on crypto regulatory and policy matters.

With over 500,000 LinkedIn followers, Henri is a TEDx and global keynote speaker, a best-selling published author, and is regularly featured in global media including Bloomberg, CNBC, CNN, BBC, The Wall Street Journal, The Economist, and the Financial Times. Henri was named by LinkedIn as one of the global Top Voices in Finance and is the host of the CryptoCapsules™ social media video series as well as The Future of Money podcast and newsletter. Henri was named by Onalytica as the #1 most influential individual on Finance globally on LinkedIn out of 50k+ individuals working at the top professional services and management consulting firms in the world.

Chambers Global named Henri the “highest profile FinTech consultant in Hong Kong”, Blockchain Asset Review named him the “Most Influential Crypto and Blockchain Thought Leader in Asia”, and Asian Private Banker awarded him the “FinTech Changemaker of the Year” award. Henri’s previous book *The Future of Finance: The Impact of FinTech, AI and Crypto on Financial Services* published by Palgrave Macmillan, was ranked as one of Amazon’s

global top 10 best-sellers in financial services and was recognised as one of the “Best FinTech Books of All Time” by Bookauthority. Before joining PwC, Henri spent many years with UBS Investment Bank in Hong Kong. Henri started his career as financial markets and funds lawyer in Canada and Hong Kong.

Henri speaks five languages including English, French, Armenian, Spanish, and Mandarin Chinese. He holds a Master’s in Chinese Law from Tsinghua University; a joint Global Executive M.B.A. from Columbia Business School, London Business School, and Hong Kong University; a Bachelor of Law from the University of Montreal (Dean’s List of Excellence), and a Master’s in Transnational Law from the University of Sherbrooke, where he was awarded the Governor General of Canada Gold Medal for Academic Excellence for having graduated with the highest grades of the university.

List of Figures

Chapter 1

Fig. 1	Depiction of a cowrie shell	6
Fig. 2	Depiction of a yap stone (<i>Source</i> Bartosz Cieślak, 2007)	8
Fig. 3	Traditional Native American wampum belts, on display at the link in Sutton, Ontario, during a presentation by Brian Charles, an off-reserve band member of the Chippewas of Georgina Island (<i>Source</i> Public domain)	9
Fig. 4	Lydian coins circa sixth century B.C.E. (<i>Source</i> Public domain)	13
Fig. 5	Yuan dynasty era banknote circa 1287 with its printing wood plate. The smaller Chinese characters in the bottom half of the note say “(this note) can be circulated in various provinces without expiration dates. Counterfeitors would be put to death”. Photographed at the Tokyo Currency Museum in 2007 (<i>Source</i> Public domain)	26
Fig. 6	Depiction of an eighteenth century pillar dollar (<i>Source</i> Public domain)	30
Fig. 7	The Continental currency. The phrase “not worth a Continental” is coined after the Continental Congress issues paper currency to finance the Revolutionary War. The currency would quickly lose its value because of a lack of solid backing and the rise of counterfeiting (<i>Source</i> University of Notre Dame, Public domain)	32
Fig. 8	One theory explaining the origins of the \$ sign	33

- Fig. 9 The double-spend problem. (a) Valid transaction.
 (b) Double-spending (invalid) transaction. The problem illustrated in this example is: Suppose Alice has 10 coins and then sends all 10 coins to Bob. How can Bob (and other people using the coin) know that Alice has not sent the same 10 coins to Charlie before, without having a bank to verify transactions? (*Source* Tsung-Ting Kuo, Heyon-eui Kim, and L. Ohno-Machado, “Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications,” *Journal of the American Medical Informatics Association*, September 8, 2017)

41

Chapter 2

- Fig. 1 Asymmetric encryption: public vs private keys (*Source* Public Domain) 47
- Fig. 2 Outputs of an illustrative Hash function. A hash function takes inputs of any size and creates a random output of uniform size and no relationship to the input; even very similar inputs have very different hash outputs (*Source* “File:Hash Function Long.Svg - Wikimedia Commons,” Wikimedia Commons, accessed January 1, 2022, https://commons.wikimedia.org/wiki/File:Hash_function_long.svg) 50
- Fig. 3 Bitcoin inflation vs time (*Source* bitcoinblockhalf.com) 56
- Fig. 4 Level of Bitcoin mining difficulty (*Source* BTC.com) 57
- Fig. 5 Average block confirmation times. Data as of January 1, 2022. Block times of greater than 25 minutes are not featured in this image (*Source* Coin Metrics) 58
- Fig. 6 Historical price of Bitcoin (October 2013–January 2022). The value of bitcoin has appreciated significantly but has also exhibited extreme volatility (*Source* “BTC-USD Historical Prices | Bitcoin USD Stock - Yahoo Finance,” Yahoo! Finance, accessed January 1, 2022, <https://finance.yahoo.com/quote/BTC-USD/history/>) 63
- Fig. 7 Levels of crypto ownership by generation (*Source* Richard Laycock and Catherine Choi, “A Rising Number of Americans Own Crypto,” Finder, June 14, 2021) 66
- Fig. 8 Grayscale investor profile by type. Institutional investors continued to be the primary source of investment capital in 3Q20 (81%), in line with the investor flow over the T12M (80%). Notably, family offices were a much larger portion of inflows during 3Q20, representing over 8% of the total (*Source* “Q3 Digital Asset Investment Report,” Grayscale, 2020) 68

Fig. 9	Total number of crypto-asset users and accounts (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	71
Fig. 10	Global crypto market size over time (<i>Source</i> “Measuring Global Crypto Users: A Study to Measure Market Size Using On-Chain Metrics,” Crypto.com, July 2021)	71
Fig. 11	Percentage of crypto-asset ownership by asset type (<i>Source</i> “Measuring Global Crypto Users: A Study to Measure Market Size Using On-Chain Metrics,” Crypto.com, July 2021)	72
Fig. 12	Most commonly held crypto-assets in the U.S. (<i>Source</i> “The State of U.S. Crypto Report,” Gemini, 2021)	73
Fig. 13	Key factors behind crypto ownership in the U.S. (<i>Source</i> “The State of U.S. Crypto Report,” Gemini, 2021)	74
Fig. 14	Illustration of payment channels on the bitcoin lightning network (<i>Source</i> “The State of Lightning,” Arcane Research, October 2021)	84
Fig. 15	Illustration of payment channels on the bitcoin lightning network (<i>Source</i> “The State of Lightning,” Arcane Research, October 2021)	86

Chapter 5

Fig. 1	Who initiates blockchain projects at the enterprise level? (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	128
Fig. 2	Frequently cited blockchain use cases by industry (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	129
Fig. 3	Frequently cited blockchain use cases by sector (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020 [33])	130
Fig. 4	Current challenges with traditional trade finance (<i>Source</i> Soumik Chatterjee, Vikas Singla, and Matthew Lam, “How Blockchain Can Reshape Trade Finance,” Deloitte, December 9, 2019)	131

Chapter 6

Fig. 1	Our proposed taxonomy of crypto-assets used in this text classifies tokens based on fungibility and intended usage	134
--------	--	-----

Fig. 2	Evolution of crypto terminology used by regulators (<i>Source</i> OECD [2020] “Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues,” OECD, Paris, www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emergingtax-policy-issues.htm)	135
Fig. 3	The blockchain trilemma	142
Fig. 4	Comparison between HTTP and HTTPS (<i>Source</i> “HTTP vs HTTPS: The Difference and Everything You Need to Know,” SEOPressor, November 21, 2019)	145
Fig. 5	Benefits of HTTPS and SSL (<i>Source</i> “HTTP vs HTTPS: The Difference and Everything You Need to Know,” SEOPressor, November 21, 2019)	146

Chapter 7

Fig. 1	Share of trade volume by market pair denomination (Jan 2022) (<i>Source</i> The Block Crypto, 2022)	150
Fig. 2	Average cost of sending remittances (<i>Source</i> FXC Intelligence; World Bank; The Economist, April 13, 2019)	151
Fig. 3	Global remittances to developing countries (<i>Source</i> FXC Intelligence; World Bank; The Economist, April 13, 2019)	151
Fig. 4	Why classification of stablecoins is so difficult (<i>Source</i> “Regulation, Supervision, and Oversight of Global Stablecoin Arrangements: Final Report and High-Level Recommendations,” Financial Stability Board, October 13, 2020 [48])	155
Fig. 5	Breakdown of Tether’s reserves (<i>Source</i> “Tether Reserves Breakdown as of March 31, 2021,” Tether Holdings Limited, May 13, 2021)	158

Chapter 8

Fig. 1	Most commonly used colors on banknotes (<i>Source</i> Salman Haqqi. “A Visual Guide to Banknotes Around the World,” Money, May 4, 2020)	172
Fig. 2	Most commonly used figures on banknotes by profession (<i>Source</i> Salman Haqqi. “A Visual Guide to Banknotes Around the World,” Money, May 4, 2020)	173
Fig. 3	Most commonly used animals and structures on banknotes (<i>Source</i> Salman Haqqi. “A Visual Guide to Banknotes Around the World,” Money, May 4, 2020)	173
Fig. 4	Benefits of CBDCs	174

Fig. 5	Google search volumes for bitcoin, Central Bank Digital Currency, and Facebook/Libra (<i>Source</i> Raphael Auer, Giulio Cornelli, and Jon Frost. “Rise of the Central Bank Digital Currencies: Drivers, Approaches, and Technologies.” Bank for International Settlements, BIS Working Paper No. 880, August 2020)	180
Fig. 6	How Canadians would react to the disappearance of cash (<i>Source</i> : Kim P. Huynh, Gradon Nicholls, and Mitchell W. Nicholson, “2019 Cash Alternative Survey Results,” Bank of Canada Staff Discussion Paper 20–8, August 31, 2020)	181
Fig. 7	American views on a potential digital-only dollar (<i>Source</i> “Perceptions and Understanding of Money in 2020,” Genesis Mining, 2020)	181
Fig. 8	Key differences between wholesale and retail CBDC	184

Chapter 9

Fig. 1	Different approaches to wholesale CBDC	186
Fig. 2	Bottlenecks in cross-border payments (<i>Source</i> Raphael Auer, Henry Holden, and Philipp Haene, “Multi-CBDC Arrangements and the Future of Cross-Border Payments, Bank for International Settlements,” BIS Paper No. 115, March 19, 2021)	189
Fig. 3	Credit risk arising from cross-border payments (<i>Source</i> European Central Bank and Bank of Japan, “Synchronized Cross-Border Payments,” ECB/BOJ Joint Research Project on Distributed Ledger Technologies, June 4, 2019)	190
Fig. 4	Key features of project Inthanon and project LionRock (<i>Source</i> Bank of Thailand and Hong Kong Monetary Authority, Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020 [21]), https://www.hkma.gov.hk/media/eng/doc/key-functions/financialinfrastructure/Report_on_Project_Inthanon-LionRock.pdf	192
Fig. 5	Cost breakdown per cross-border transaction (<i>Source</i> Bank of Thailand and Hong Kong Monetary Authority, Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020 [21]), https://www.hkma.gov.hk/media/eng/doc/key-functions/financialinfrastructure/Report_on_Project_Inthanon-LionRock.pdf	194

Fig. 6	Compatible CBDC approach (<i>Source</i> Raphael Auer, Henry Holden, and Philipp Haene, “Multi-CBDC Arrangements and the Future of Cross-Border Payments, Bank for International Settlements, BIS Paper No. 115, March 19, 2021)	196
Fig. 7	Linking CBDC approach (<i>Source</i> Raphael Auer, Henry Holden, and Philipp Haene, “Multi-CBDC Arrangements and the Future of Cross-Border Payments, Bank for International Settlements, BIS Paper No. 115, March 19, 2021)	197
Fig. 8	Single mCBDC arrangement (<i>Source</i> Raphael Auer, Henry Holden, and Philipp Haene, “Multi-CBDC Arrangements and the Future of Cross-Border Payments, Bank for International Settlements, BIS Paper No. 115, March 19, 2021)	198
Fig. 9	What does a CBDC stack look like? (<i>Source</i> “Multi-CBDCs: Designing a Digital Currency Stack for Governability,” Monetary Authority of Singapore, April 21, 2021)	199
Fig. 10	What does a CBDC platform look like? (<i>Source</i> “Multi-CBDCs: Designing a Digital Currency Stack for Governability,” Monetary Authority of Singapore, April 21, 2021)	200

Chapter 10

Fig. 1	Different approaches to retail CBDC	213
Fig. 2	Conceptual framework for the E-Krona pilot (<i>Source</i> “The Riksbank’s E-Krona Project Report 2,” Riksbank, October 2018 [4])	221
Fig. 3	Platform model design of the E-Krona system (<i>Source</i> “The Riksbank’s E-Krona Project Report 2,” Riksbank, October 2018 [18])	224
Fig. 4	Platform CBDC model (<i>Source</i> “Central Bank Digital Money: Opportunities, Challenges, and Design,” Bank of England, March 2020 [26])	226

Chapter 14

Fig. 1	Number of crypto assets mined (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	261
Fig. 2	Mining pool concentration (<i>Source</i> BTC.com)	263

Fig. 3	Mining pools by crypto asset (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	264
Fig. 4	National energy use compared with the bitcoin network’s energy consumption (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	265
Fig. 5	Total annualized footprints (Carbon/Electricity/Waste) as of January 2022 (<i>Source</i> Digiconomist)	265
Fig. 6	Total hashrate (TH/s) (as of January 2022) (<i>Source</i> blockchain.com)	267
Fig. 7	Mining algorithms and hardware requirements (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	268
Fig. 8	Bitcoin mining difficulty vs time (<i>Source</i> Michael Bedford Taylor, “The Evolution of Bitcoin Hardware,” University of Washington, September 2017; CoinDesk Research)	269
Fig. 9	Share of renewables in Bitcoin mining energy mix (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	271
Fig. 10	Total world renewables production (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	272
Fig. 11	Comparison between average costs of electricity in major economies (January 2022) (<i>Source</i> Pricing of Electricity by Country, ElectricRate, 2022)	275
Fig. 12	Evolution of share of bitcoin mining by country (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	276

Chapter 15

Fig. 1	Key ICOs by funding value and number of token offerings (<i>Source</i> “6th ICO//STO Report,” PwC, 2020)	279
Fig. 2	Advantages of a token sale. Whilst frequently compared, the characteristics of an ICO differ significantly from those of an IPO (<i>Source</i> : PricewaterhouseCoopers, “Introduction to Token Sales (ICO) Best Practices” [PwC], accessed January 13, 2019)	280
Fig. 3	Distribution of initial coin offerings by stage of product development at the time of the offering. Many ICOs have raised significant funding with little more than an idea (<i>Source</i> Mikhail Mironov and Steven Campbell, “ICO Market Research Q1 2018,” ICORATING, 2018 [23])	282

Chapter 16

Fig. 1	Total value lost from DeFi Hacks (2020) (<i>Source</i> “2020 Geographic Risk Report: VASP KYC by Jurisdiction,” CipherTrace, 2020)	294
Fig. 2	Trading volumes at key decentralised exchanges (DEXs) (Jan. 2022)	302
Fig. 3	Decentralised (DEX) spot trading volumes compared to centralised exchange (CEX) spot trading volumes (Jan. 2022)	302
Fig. 4	X-Y-K market makers (<i>Source</i> Vitalik Buterin, “Improving Front Running Resistance of $x^*y = k$ Market Makers,” Ethereum Research, March 2018)	304
Fig. 5	Impermanent loss (<i>Source</i> “Uniswap: A Good Deal for Liquidity Providers,” Pintail, August 30, 2020)	307
Fig. 6	The DeFi insurance process (<i>Source</i> “Nexus Mutual Gitbook,” Nexus Mutual, 2021)	310

Chapter 17

Fig. 1	Crypto tax guidance clarity by jurisdiction. The PwC Crypto Tax Index was developed to help illustrate and compare the level of comprehensiveness of tax guidance between jurisdictions. Covering 19 different areas relevant to the taxation of crypto-assets, the Crypto Tax Index measures whether a particular issue is addressed by the existing guidance of each jurisdiction (<i>Source</i> “Annual Global Crypto Tax Report,” PwC, 2021)	320
Fig. 2	Total cryptocurrency value received by illicit entities (<i>Source</i> “Chainalysis 2021 Crypto Crime Report,” Chainalysis, 2021)	322
Fig. 3	Iran’s share of Global Bitcoin Mining (2021) (<i>Source</i> “Sanctions Compliance in Cryptocurrencies: Using Blockchain Analysis to Navigate the Minefield,” Elliptic, 2021)	324
Fig. 4	Percentage of VASPs with weak or porous KYC (<i>Source</i> “2020 Geographic Risk Report: VASP KYC by Jurisdiction,” CipherTrace, 2020)	326
Fig. 5	Percentage of VASPs with weak or porous KYC by region (<i>Source</i> “2020 Geographic Risk Report: VASP KYC by Jurisdiction,” CipherTrace, 2020)	327

Chapter 18

Fig. 1	Total number of crypto users and accounts around the world (2020) (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	336
--------	--	-----

Fig. 2	Crypto customer base breakdown by region (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	336
Fig. 3	Share of crypto-crypto exchanges that conduct KYC checks (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	341
Fig. 4	Share of crypto derivatives trading by country (<i>Source</i> Christina Tkach, Sofia Sedlova, Evgeny Dmitriev and Adam Zarazinski, “Geotagging Crypto Derivatives Traders With NLP,” Inca Digital, 2021)	344
Fig. 5	Notable decentralised exchange hacks (<i>Source</i> “Chainalysis 2021 Crypto Crime Report,” Chainalysis, 2021)	347
Fig. 6	Share of storage offering throughout the crypto exchange ecosystem (<i>Source</i> “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)	348

Chapter 19

Fig. 1	Most common investors in crypto hedge funds (<i>Source</i> “3rd Annual Global Crypto Hedge Fund Report,” PwC, 2021)	355
Fig. 2	Most commonly adopted strategies of crypto hedge funds (<i>Source</i> “3rd Annual Global Crypto Hedge Fund Report,” PwC, 2021)	355
Fig. 3	Cryptocurrencies most commonly traded by crypto hedge funds by market cap (<i>Source</i> “3rd Annual Global Crypto Hedge Fund Report,” PwC, 2021)	356
Fig. 4	Percentage of crypto hedge funds involved in staking, lending, and borrowing (<i>Source</i> “3rd Annual Global Crypto Hedge Fund Report,” PwC, 2021)	356
Fig. 5	Grayscale’s cumulative quarterly inflows (2020) (<i>Source</i> “Grayscale Q3 2020 Digital Asset Investment Report,” Grayscale Investments, 2020)	359
Fig. 6	Venture capital crypto funds (<i>Source</i> “3rd Annual Global Crypto Hedge Fund Report,” PwC, 2021)	359

Chapter 20

Fig. 1	Borrowing and lending in centralised finance (<i>Source</i> “Deconstructing CeFi,” Kraken Intelligence, July 2021)	367
--------	---	-----

Chapter 21

Fig. 1	The progression of Web 1.0 to Web 3.0	382
--------	---------------------------------------	-----

List of Tables

Chapter 2

Table 1	Key features of bitcoin compared with traditional finance	52
Table 2	Stock ownership among key U.S. demographics	65
Table 3	Levels of crypto adoption by country	72

Chapter 4

Table 1	Top 20 crypto-assets by market capitalization (January 2022)	100
---------	--	-----

Chapter 5

Table 1	Key distinctions between public (permissionless) blockchains and private (permissioned) blockchains	124
---------	---	-----

Chapter 8

Table 1	Responses of Canadian residents to the disappearance of cash by demographic	182
---------	---	-----

Chapter 9

Table 1	Different approaches to multi-CBDC include compatible, interlinked, and single mCBDC multi-currency systems	196
---------	---	-----

Chapter 10

Table 1	E-Krona properties compared to cash and commercial bank money	212
---------	---	-----

Chapter 13

Table 1	Top NFT collections by market capitalization (January 2022)	255
---------	---	-----

Chapter 14

Table 1	The five most important criteria mentioned by mines include market cap, daily reward amount, price of crypto-asset, reputation, and energy requirements	262
Table 2	The share of global bitcoin mining by country shifted dramatically following China's ban on mining in 2021	275

Chapter 15

Table 1	Key differences between an ICO and an IPO broken down by regulation, token holder/shareholder rights, fundraising strategies, levels of economic exposure, and levels of transparency	281
---------	---	-----

Chapter 18

Table 1	Key differences between centralised and decentralised exchanges broken down by levels of regulatory compliance, user accessibility, liquidity, and fee structures	338
---------	---	-----

Chapter 19

Table 1	Average and median AuM of crypto hedge funds	354
Table 2	Top crypto hedge fund domiciles and top crypto hedge manager locations	357

Chapter 20

Table 1	Different approaches available to financial institutions looking at entering the crypto ecosystem	365
Table 2	Comparison between centralised and decentralised finance broken down by custody, security, main service, customer support, and accessibility	367
Table 3	Stock-to-flow metrics for key precious metals	372
Table 4	Key differences between hot and cold crypto wallets along with advantages and disadvantages of each model	375

Chapter 21

Table 1 Differences between DAOs and traditional organisations
broken down by structure, governance, and levels
of transparency

391



1

The History of Money

This book is about the future of money, with a strong focus on its latest iteration, crypto-assets, but as with many other things in life, in order to understand the future of something, it's worth looking at its history, and this could not be truer than the history of money. Many of the systemic changes that we're seeing today have occurred numerous times over the last millennia.¹ For anyone interested in the topic of the history of money, there are various interesting and insightful books that are worth looking at and you will find some of my recommendations in the footnotes. Whilst I cannot go in-depth as many of these authors can due to the focus of this book, I truly believe that it is important that we at least cover some of the key historical milestones to put the latest developments in the field of crypto-assets in perspective.

1 The Importance of Money and Bartering

If you ask any economist what money is, they will mention three necessary characteristics:

The original version of this chapter was revised: Text correction have been updated. The correction to this chapter is available at https://doi.org/10.1007/978-3-030-97951-5_22

1. **Store of value:** Meaning people can save it and use it later, smoothing out their purchases over time.
2. **Unit of account:** Provides a common base for prices.
3. **Medium of exchange:** For individuals to use to buy and sell from one another.²

The type of asset that people and civilisations have determined to meet these three characteristics and be considered “money” has evolved over time. It’s important to understand that if we did not have money, we would be reduced to a barter economy, where every item someone wanted to purchase would have to be exchanged for something that person could provide. For example, a person who specialised in fixing cars and needed to trade for food would have to find a farmer with a broken car. But what if the farmer did not want to fix his car? Or what if the farmer could only give the mechanic some unwanted eggs since he loves eggs?³ This is known as the “double coincidence of wants” problem: for barter to occur between two parties, both parties need to have what the other wants. Whilst this can work in certain situations—a student will do a friend’s homework if he repairs her bicycle in exchange—the reality is that whilst a barter system can serve as a unit of exchange, it is limited and cannot scale.

Another drawback of bartering is an inconsistent unit of account. For example, in a barter economy, the number of prices equals the number of pairs of goods, so there would be a price for car repair and eggs, another price for chicken and dresses, and so on. For example, an economy with 1,000 goods (in practice, a poor economy) would require 499,500 different prices! (The formula for those who may be interested is $Cn = n! / [(n - r)!r!]$ where n is the number of commodities and r the bilateral groups of 2.)⁴ Bartering also does not always provide a store of value. If everyone agrees that 10 oranges are worth five litres of milk, you have a unit of account and medium of exchange, but not a store of value as both items will go bad in a matter of days or weeks. This is why the concept of money is handy, as you don’t need a particular person who has a product that he will barter with you; you just need a market in which to sell your goods or services. In that market, you don’t barter for individual goods, and instead exchange your goods or services for a common medium of exchange, e.g., money. You then use that money to buy what you need from others who also accept the same medium of exchange. As people become more specialised, it’s easier to produce more, which leads to more demand for transactions and hence, a greater demand for money.⁵

Though primitive, bartering has been present throughout history and has survived in certain cases that we’ll see shortly. Bartering historically took

place between tribes where direct and possibly dangerous contact was deliberately avoided by the participants. An amount of a particular commodity would be left in a convenient spot frequented by the other party, who would take the goods proffered and leave what they considered a fair equivalent in exchange. However, if these were not considered sufficient, the goods would remain untaken until the amount originally offered had been increased. In this way, the barter system, despite being silent, was nevertheless an effective and competitive form of hard bargaining.⁶

One of the most interesting forms of early barter was the tradition of gift exchange, with a good example of the “potlach” tradition that was common amongst North American Indians. This was far more than merely commercial exchange but was a complex mixture of both private and public gatherings. Some private gatherings involved initiation into tribal secret societies and the public ones were cultural activities in which public speaking, drama, and elaborate dances were core features.⁷ One main purpose of these exchange ceremonies was to validate the social ranking of the leading participants as a person’s prestige depended largely on his power to influence others through the impressive size of the gifts offered.

Interestingly, the Canadian government, via the Indian Act of 1876, eventually banned this potlach custom, but it proved so ineffective that the Canadian government would amend the law to make it more stringent. The Revised Statutes of Canada 1927, clause 140, stipulated that “every Indian or other person who engages in any Indian festival, dance or other ceremony of which the giving away or paying or giving back of money, goods or articles of any sort forms a part... is guilty of an offence and is liable on summary conviction to imprisonment for a term not exceeding six months and not less than two months”.⁸ But the challenges of bartering arose in other contexts. For example, William Stanley Jevons begins his 1875 book on “Money and the Mechanism of Exchange” with two illustrations of the drawbacks of barter. He first relates how Mlle Zélie, a French opera singer, over the course of a world tour gave a concert in the Society Islands (an archipelago in French Polynesia) and for her fee received one-third of the proceeds. Her share consisted of three pigs; 23 turkeys; 44 chickens; 5,000 coconuts; and considerable quantities of bananas, lemons, and oranges. Thus it was a significant fee that would end up being wasted.

Jevons’s second account concerns the famous naturalist A. R. Wallace who during his expeditions between 1854 and 1862 in the Malay Archipelago (over 25,000 islands between the Indian and Pacific oceans that currently includes Brunei, East Malaysia, East Timor, Indonesia, Papua New Guinea, and the Philippines), found that in some of the islands where there was no currency, mealtimes were preceded by long periods of hard bargaining, and if

the commodities bartered by Wallace were not wanted then he and his party simply had to go without their dinner.⁹

In what may come as a surprise to many, bartering has still played a role in recent years, especially with countries experiencing hyperinflation. For example, during the German inflation of 1923, the “butter” standard emerged as a more reliable common measure of value than the German mark. After World War II, retail trade in continental Europe was often based on cigarettes¹⁰ and was commonly used during the reign of President Nicolae Ceaușescu in Romania from 1974 to 1989. Anything could be bought with cigarettes—food, electronic goods, sex, or alcohol. Cartons of cigarettes had the advantage of being easily broken up into ten packs per carton, each of which could in turn be broken up into twenty cigarettes.¹¹

There are also numerous examples of barter during the Soviet era. It's estimated that some 25% of East–West trade involved some degree of barter, with the proportion being around 40% over the course of the 1980s. Amongst the many reasons for this rebirth of barter was the fact that external trade from communist countries was normally “planned” bilaterally, and therefore lent itself more naturally to various forms of barter than does freer.¹² For example, Occidental Petroleum, a U.S. oil company founded in 1920 and based in Houston, had a \$20 billion barter agreement with the Soviet Union. In a similar spirit, PepsiCo.¹³

There are other recent examples, especially with countries that are under sanctions, from countries like Iran bartering oil for goods to China and Cuba bartering doctors in exchange for oil from Venezuela. As hyperinflation events continue to take place, it's not only governments but also everyday people forced to revert to barter. Countries like Zimbabwe, Venezuela, or Argentina which all experienced continuous episodes of inflation and hyperinflation, mainly due to bad government policies, are good examples where barter became part of daily life.¹⁴

2 Primitive Forms of Money

Due to some shortcomings of barter, it's not surprising that primitive versions of money saw the light of day and it's worth spending time to look at some of the most common, as many have had an impact that persists until today.

Throughout the world, commodities from salt to tobacco have been used as money at various points in history. Natives in parts of India used almonds; Guatemalans used corn; the ancient Babylonians and Assyrians used barley; natives of the Nicobar Islands (an archipelagic island chain in the eastern

Indian Ocean) used coconuts; and the Mongolians prized bricks of tea. Norwegians used butter as money, and in the medieval era, they used dried cod¹⁵ whilst the people of the Philippines, Japan, Burma, and other parts of Southeast Asia have used standardised measures of rice as commodity money. Norwegians used butter as money, and in the medieval era, they used dried cod.¹⁶ Salt has been used as money throughout history as well, especially in China, North Africa, and the Mediterranean, and because of its purity, salt can be cut into standardised sizes, with merchants wrapping smaller denominations of salt in a protective reed covering to reduce the danger of salt chipping and to prevent people from scraping off parts of it between trades. The modern English word “salary” and the Italian, Spanish, and Portuguese word “*salario*” are derived from the Latin word “*sal*”, short for “*salarius*”, meaning salt.¹⁷

Cattle played an important role as money throughout history and even survived in modern times amongst certain tribes in eastern and southern Africa. A good example of its impact is its use today in modern European languages. The word pecuniary, which means “related to money”, is derived from the Latin *pecuniarias*, meaning “wealth in cattle”. The English word pecunious, an obsolete term meaning “wealthy” and the more commonly used impecunious meaning “poor”, are other examples. The word cattle, meanwhile, is derived from the same Latin roots that gave us capital, another broader term for money and chattel—any item of movable personal property—is derived from the same source. Thus, modern names for two of the most important economic systems in European history, capitalism, and feudalism, can both be traced back to systems based on cattle.¹⁸ However, cattle remained in use in many parts of the world for many years. Until the twentieth century, horses were the main monetary unit of the Kirghiz of the Central Asian steppes, and formed their main store of value, though sheep were used as subsidiaries, with lambskins being used as small change.¹⁹

Even human beings have served as a measure of money. In ancient Ireland, slave girls became the common value against which items such as cows, boats, land, and houses were measured. Viking raiders and merchants sold the young women to slave traders in the Mediterranean, where they were highly valued because of their red or blond hair. Interestingly, Irish males had far less value as slaves. In parts of equatorial Africa, by contrast, male slaves had a higher value than women and children, who would be measured as mere fractions of the value of a man. Of all the forms of money, slaves proved one of the least reliable because of their high mortality rate and their tendency to escape.²⁰

Animal skins and furs proved useful in Russia, Siberia, and North America, but they had little practical use in the warmer markets of the Caribbean, Africa, South America, and southern Asia. The Canadians used the thick, luxurious beaver pelts that their large country produced and that were popular with European hatters and clothiers. Further south in the British colonies, the settlers used the skin of the North American deer, which achieved great importance in trade. Each skin was known as a buck, a word that has survived as a slang term for the dollar.²¹

From 1300 to 1521, the Aztecs flourished in what is today central Mexico and used cacao beans as money. With these cacao beans, people could buy anything from fruits and vegetables to clothes and weapons. Cacao beans became so popular as a means of exchange that it produced its own counterfeiting industry. Criminals would take the small husk of the cacao bean, empty it, and replace it with mud. They would then seal the husk and mix it with real cacao beans,²² which is probably one of the first examples of what we refer to today as the layering process in “money laundering”.

However, of the hundreds of objects that were used as money, the cowrie is the one that had the most impact (Fig. 1).

The cowrie is the ovoid shell of a mollusc spread widely over the regions of the Indian and Pacific Oceans. The most prolific single source was the Maldives whence for hundreds of years whole shiploads were distributed around the shores of Oceania, Africa, the Middle and the Far East, their values rising as they became scarcer moving further from their point of origin. Coming in various types, colours, and sizes, in addition to their religious and



Fig. 1 Depiction of a cowrie shell

ornamental qualities, cowrie shells had the advantage of being durable, easily cleaned and counted, and difficult to counterfeit.²³ These cowrie shells, especially the Monetaria moneta type of cowrie shell, were used for centuries as currency by native Africans.

Although cowrie shells would also fall victim to inflation due to the increasing supply of cowries being introduced into the economy (an early form of “quantitative easing”) by some Western nations bringing a huge number of Maldivian cowries to Africa, especially through the slave trade.²⁴ For example, when cowries were first introduced in Uganda towards the end of the eighteenth century, two cowries in the most remote regions were known to have been sufficient to purchase a woman; by 1860, it required 1,000 cowries for such a purchase.²⁵ As trade grew and cowries became more plentiful, they naturally depreciated further, but were still officially accepted for payment of taxes until the beginning of the twentieth century. By the 1920s, thousands of tons of cowries had been brought into Africa, not only from the Maldives but from other areas as they became progressively more devalued elsewhere, and in so doing, accelerated the depreciation of the cowrie in Africa. However, in East Africa, as was the case on the other side of the continent, it took until the middle of the twentieth century before cowries virtually disappeared from circulation for the smallest purchases, especially in the remotest districts.

An example of the impact of cowrie shells in Africa is the currency of Ghana, the cedi, which derives its name from those once-ubiquitous shells. The word “cedi” means cowry shell in the local Akan language, but these cowrie shells were also used extensively across India and China. The traditional Chinese character for money, 貝, (pronounced bēi) originated as a stylised drawing of a Maldivian cowrie shell. The character was later simplified to 贝 and is still used today to refer to words and characters concerning money, property, or wealth.²⁶ Whale teeth, which have great value in Fiji and a few surrounding islands, were also used to a certain extent as money, and in fact, they still play an important role in the ceremonial life and the prestige of the people. Whale teeth, however, did not prove effective in trade with other nations, who simply had no interest in them. Similarly, dog teeth were valued as a medium of exchange in the Admiralty Islands (an archipelago in the South Pacific Ocean), but outsiders frequently found them disgusting and did not want to trade for them.²⁷

Stones have been used as money throughout history. The most famous example is probably the stone currency of Yap, a cluster of 10 small islands in the Pacific Ocean (north of Papua New Guinea). These yap stones were still being used as money as recently as the mid-1960s. The stones known as



Fig. 2 Depiction of a yap stone (Source Bartosz Cieślak, 2007)

“fei” were quarried from Palau, 260 miles away, or from the even more distant Guam, and were shaped into discs varying from saucer-sized to veritable millstones, the larger specimens having holes in the centre through which poles could be pushed to help transport them (Fig. 2).

Despite centuries of at first sporadic and later more permanent trade contacts with the Portuguese, Spanish, German, British, Japanese, and Americans, the stone currency retained and even increased its value, particularly as a store of wealth.²⁸ Though of limited use as currency, they were by far the most acceptable form of money to the Yap islanders. Interestingly these yap stones have more recently caused challenges for the government of the state of Yap as many museum curators have been seeking to acquire such yap currency specimens to showcase as a specimen of one of the world’s earliest forms of primitive money.²⁹ For example, one of the largest such stones stood for decades in the courtyard of the Bank of Canada in Ottawa before being moved to the central bank’s museum.³⁰

The Wampum are a traditional shell bead of Native Americans that included white shell beads hand-fashioned from the North Atlantic channelled whelk shell (a large predatory sea snail), and white and purple beads made from hard-shelled clams (Fig. 3).

Their full name was “wampumpeag” but was typically abbreviated to “wampum”. “Peag” is the indigenous word for a string of beads and “wampum” means white, the most common colour of those beads. The clams were harvested in the summer, their meat consumed, and the shells were



Fig. 3 Traditional Native American wampum belts, on display at the link in Sutton, Ontario, during a presentation by Brian Charles, an off-reserve band member of the Chippewas of Georgina Island (Source Public domain)

then worked into beads. Wampum beads were difficult to make back then, as drilling (with stones) could shatter the clam and the dust from the drilling contained silica that was harmful to the lungs if inhaled. The shells were ground and polished into small tubes with a stone drill and then placed on strings made of plant fibre or animal tendon and woven into belts, necklaces, headpieces, bracelets, and earrings, a variety of adornments depending on the status of the wearer.³¹

The earliest account of this widespread currency was given by the explorer Jacques Cartier in 1535, who noted an unusual additional function: its usefulness in preventing nosebleeds, a curative property which his exploratory party tested and confirmed.³² The shells are mostly white but with a smaller deep purple rim. The scarcer black or blue-black wampum was usually traded at double the price of the white.

It took Europeans some time to realise how important wampum was to indigenous cultures. However, what is most remarkable is that the wampum was the currency of choice for only about 30 years starting around 1630.³³ As an indication of the essential role wampum played in early colonial days, even

amongst the white settlers, it was made legal tender in several of the original 13 American colonies. In 1637, Massachusetts declared white wampum legal tender at six beads a penny and black at three a penny, but only for sums up to one shilling. Although the wampum ceased to be legal tender in the New England states in 1661, it was still used in parts of North America for nearly 200 years afterward. For example, around 1760, demand in New England remained strong enough to justify the launch of a wampum factory in New Jersey, where an expert worker could produce up to 20 feet of wampum a day.

This factory remained in production for a hundred years and initially, the Campbell family who opened the factory farmed in the summer and produced wampum in the winter. They purchased shells from the fish market in New York City and used West Indian conches brought in on ships as ballast. The Campbell mill sponsored quahog-shucking contests in Rockaway on Long Island in which the contestants got to keep the meat and the Campbells kept the shells. One grandson invented a drill in 1812 that quickly and precisely drilled a hole in the wampum, then used a grindstone to fashion the shape. This made production quicker than traditional hand-drilling and the mill was operating full-time and became the largest employer in the area.³⁴ Between 1835 and 1866, the Campbell mill produced a million purple beads a year. But production dropped during the Civil War and by 1890, most indigenous nations had been placed on reservations, and the wampum boom was over. In an ironic evolution of contemporary globalised economics, wampum beads are now being mass-produced in China and used mainly for decorative purposes.³⁵

3 The Impact of Money on the Development of Civilisations

Whilst these examples of primitive forms of money are interesting, it's important to remember that they were not essential for the development of a particular civilisation. For example, ancient Egyptian civilisation extended from about 3100 BC to 30 BC, and during those 3,000 years, Egyptians did not use cash or cash equivalents despite their access to gold and other precious metals,³⁶ reserving gold for ritual burials instead. The Egyptians believed that gold was sacred to Ra, the sun god, and they buried great quantities of it with the corpses of their divine pharaohs.

The Incas are another example. They possessed large amounts of precious metals and saw gold as "the sweat of the sun" and silver as the "tears of the

moon”, but these were mostly used for religious art and rituals. For instance, when Atahualpa, King of the Inca Empire in Peru, became a prisoner of the Spanish conquistador Pizarro, he agreed to a ransom of enough gold to fill the room in which he was being held and twice that in silver. Atahualpa never understood that for the Spanish, gold was not just a means to please the gods.³⁷ Another example of the sacred association of gold for the Incas was that, even after conquest, when the Spaniards took the gold and silver, they decorated their new Christian temples with foil paper to imitate the sacred substances and tossed gold- and silver-coloured confetti into the air in lieu of gold dust.³⁸

Indeed, for a long time, people around the world associated gold and silver with magic and divinity, not money. Before the arrival of the Europeans in Columbia, the Chibcha Indians performed an annual ritual in which they covered their chief with gold dust. He would then dive into a sacred lake; the water washed off the gold and, thus, became a gift to the gods. The chief was known to the Spaniards as El Dorado, the Golden One, and his wealth of gold became the object of the greatest search in world history.³⁹

Then things started to slowly change. As early as the end of the third millennium BCE, the people of Mesopotamia began using ingots of precious metals in exchange for goods. There were various names for these uniform weights of gold and silver including minas, shekels, or talents, and this standardisation really started the revolution of the future of money, allowing an entire warehouse of olive oil or wheat or some cattle to be reduced in value to an easily transportable ingot of gold. Whilst this system worked with merchants, gold was too scarce and valuable for the average person looking to sell some eggs at a market or buy some wheat. It became a matter of time before we began to see fractionalisation (or tokenisation, as we will describe later when talking about crypto-assets) with smaller coins that could be more widely used. This revolution took place in Anatolia in present-day Turkey, and from there it spread around the world to become the global monetary system and the ancestor of the model we live and work under today.⁴⁰ However, it’s important to remember that the revolution started much earlier in China, which would play an important role in the history of money.

4 The Invention of Coinage

4.1 China

Although experts differ as to the exact date, it's estimated that metal cowries of bronze and copper were in general use in China at the end of the second millennium BCE.⁴¹ But Chinese coins had distinct characteristics, the first of which was that all metallic monies in China were almost invariably composed of base metals like bronze or copper. In contrast with the development of coins around the Mediterranean where precious metals like gold or silver were used, China concentrated almost exclusively on base metals for coinage, and this played an important role in the difference in the evolution of money between the two regions.⁴²

Another involuntary consequence of the usage of base metals in China was that they were easily imitated and counterfeited. The raw material costs were low, the method of manufacture was simple, and the superficial inscriptions easy to apply. Consequently, imitation was endemic, particularly the further you ventured from the centre of power, and since Chinese coins were made using base metals, precious metals still had to be weighed rather than counted, as was the case with coins. Consequently, although China was easily the first civilisation to introduce "coins", the possibility they offered were not as fully exploited as in the Western world, where once invented, their development sped ahead more quickly.⁴³

The second characteristic is that most popular Chinese monies had holes in them, primarily square holes, but circular ones as well, both kinds of which had a clear purpose. First, a rod could be inserted in them which would make the manufacturing process easier, and second, they could be strung together in groups of 50 or more coins, thus making them easier to carry and trade.⁴⁴

A third characteristic was that in China, the state played a dominant role in coinage, and although there were hundreds of mints, the state retained central control and uniformity of standards. Another difficulty that arose with Chinese coins was that emperors would not allow their names or heads to appear on their coins, thus making the dating process significantly more complicated.⁴⁵ For example, in 221 BCE, emperor Qin Shihuangdi abolished all forms of coinage except for one: a round copper coin with a square hole in the middle. Called the "*ban liang*", this coin predated the Qin dynasty, but was elevated to China's standard monetary unit until nearly the 1920s.⁴⁶

Whilst China may have had a long lead when it came to coinage, this lead was gradually overtaken when a different type of coinage was invented composed primarily of precious metals, which ultimately proved superior

for most monetary functions. Although China had a 3,000-year unbroken, continuous stretch of coinage, some of the rigid conservatism around these coins constrained them to act only as small change, not dissimilar to the role occupied by coins today in many countries. Interestingly, China would experiment with leather money, pieces of deerskin of roughly one square foot around 118 BCE. Many believe that a severe shortage of copper for coinage caused the emperor to invent this new form of money as a temporary substitute for the more traditional kind.⁴⁷ China would not issue any substantial precious metal coinage until 1890 when it would begin minting silver, and as we'll see later, the lack of progress around coinage would encourage the development of banknotes, where China had a 500-year head start over the rest of Europe.⁴⁸

4.2 Lydia

Lydia was a kingdom located in Western Asia Minor between the Hellenic world and the old Persian dominion, and its capital Sardis is in the western part of present-day Turkey. The Lydians thrived as middlemen, and whilst the exact date is a highly debated topic, it's now commonly accepted (based on texts by the Greek writer Herodotus who lived from 484 to 425 BCE) that the Lydians minted the first coins around 630 BCE. These first coins were made of electrum, a naturally occurring alloy of gold and silver, and were stamped with the lion insignia of the king.⁴⁹ What made the Lydian experiment different from the Chinese approach was that from the start, Lydian coins were linked to the king, though the idea may have originated from merchants who saw its benefits. Each of these coins was stamped with royal symbols and flattened into roundish discs, giving them the shape they have today. These marks told people that the king was guaranteeing that the electrum coin contained a 75% gold and 25% silver mix⁵⁰ (Fig. 4).



Fig. 4 Lydian coins circa sixth century B.C.E. (Source Public domain)

In addition, the Lydians introduced fractionalisation by minting these coins in various weights (an early form of security tokens). For example, the basic unit of a Lydian stater was 14.1 g, but the most popular denomination was one-third of a stater, which expanded the range of products that one could buy using these coins. Some light coins, including a ninety-sixth share (or 0.15 g), were minted, another major difference from the Chinese, who also had plenty of weightings in their early castings, but which were removed by the Qin emperor in his drive towards standardisation.⁵¹ These Lydian coins were highly successful and started to be widely circulated well beyond the Lydian kingdom, which had a major impact on Lydian society. For example, by inventing coins as we know them, the Lydians also invented seigniorage by having this embedded tax with each coin that represented the difference between the currency's face value and the cost of minting it, making the Lydian king very rich.

What Is Seigniorage?

It's important to remember that historically speaking, whoever is issuing a currency garners benefits, and as we'll see later in this book, this also holds true for stablecoin issuers. Throughout the course of history, the act of issuing money was referred to as seigniorage (which comes from the French word "*seigneur*" meaning "lord"), which represents the difference between the face value of the money and the cost to issue it. For example, if it costs 5 cents to produce a \$1 dollar note, then the issuing entity is making 95 cents of seigniorage on each \$1 banknote. It is the same principle for central banks when it comes to the treasury bills they issue.

But the Lydians innovated as well. Metallurgists working for the last Lydian king Croesus (560 to 546 BCE) figured out how to separate the electrum's components. This allowed Croesus to create standardised coins in pure silver and gold that people could use and trust. By making these nuggets the same weight and size, the Lydian king eliminated one of the most time-consuming steps in commerce at the time: the need to weigh the gold each time a transaction was made. This made Croesus even richer (thus the expression we have today "to be as rich as Croesus").⁵²

The invention of coinage also had snowball effects. For example, the Lydians became the first to set up permanent retail shops. Coins eliminated uncertainty and made transactions fast and convenient, a far cry from the haggling and bargaining needed before standardisation, and in a way, the introduction of these small value coins promoted what we know today as

“financial inclusion”.⁵³ The invention of coinage also gave rise to two of the biggest vices. First, Sardis, the Lydian capital, became home to the world’s first commercial brothels, which sold sexual services to men involved in commerce. The Greek historian Herodotus reveals stories of Lydians generating revenues from selling their own daughters, but he also notes that coins allowed women to fill their own dowries and choose whom they wanted to marry. In order to accumulate their dowries, many unmarried women of Sardis supposedly worked in the brothels long enough to secure the money necessary to have the kind of marriage (and husband) they desired.⁵⁴

In addition to brothels, another invention that came with the introduction of coins was gambling. Whilst dice had existed for some time, the Lydians added the money component.⁵⁵ Archaeological excavations clearly show that gambling and games of chance such as knucklebones thrived in the areas around the market,⁵⁶ and perhaps boosted by his wealth, Croesus decided to think big and invaded the mighty Persian Empire. But he failed, and the Persians conquered Lydia in 546 BCE and burned Croesus and his wife on a pyre.⁵⁷

5 The Transformative Impact of Money

5.1 Greece

Despite Persia conquering Lydia in 546 BCE, coinage never had a big impact in Persia, which was a vast tribute state ruled by a centralised military. The Persians didn’t build new mints and instead relied on Lydian mints, but one civilisation that took advantage of the development of coinage were the Greeks. Unlike some of Greece’s neighbours like the Persians or the Phoenicians, who already had sophisticated social systems without money, the Greeks were a largely unformed civilisation, and the adoption of money propelled them forward and past the other groups throughout the region.⁵⁸

Soon after some of the Hellenic towns in Asia Minor began to adopt Lydian coinage, it quickly spread throughout the Aegean and to leading cities in the Greek Peninsula, particularly Athens.⁵⁹ However, unlike the Lydians who preferred a mix of gold and silver, the Greeks preferred silver for their coins. There were a couple of reasons for that preference. First, Athens was only 50 km from the silver mines of Laurion, making it convenient, and second, the Greeks figured out how to isolate silver ore, discovering how to separate silver from their lead ores and, thus, able to utilise it. Finally, the

abundance of slaves allowed the Greeks to exploit those mines, where it's estimated that up to 30,000 slaves worked in the Laurion mine alone.⁶⁰

The Greeks leveraged the features of money to build markets and develop their society, and citizens had to trust the money, not the other person. Coins somewhat democratised finance as they enabled a broader segment of the population to participate in the buying or selling of goods, leading to the agora becoming a staple feature of Greek communities and this new wealth opened the doors to the city's Assembly to people of wealth, not just the sons of existing oligarchs. This influx of wealth also helped to develop democracy, which famously arose in Athens. For example, the Greek word for coinage, "*nomisma*", comes from the Greek word for law, "*nomos*" (of which the English word "numismatic", referring to the study of money, would later derive).⁶¹

What Is the Link Between Philosophers and Money?

In addition to creating new opportunities in finance, coinage also gave rise to much philosophical discourse. For example, Plato wanted to outlaw metallic coins as he equated wealth with corruption, arguing for a government-issued token for the single purpose of recordkeeping, a mix of communism with the central bank digital currencies of today that we will explore later in this book.

Inversely, Aristotle argued for private property and what we would call today "wealth management" but believed that prices should be determined by the social status of the participants, not the value of the merchandise. Others took a more pragmatic approach. Xenophon wrote a book describing how to manage the finances of an estate, a skill he called "*oikonomikos*", which became economics. This was probably the start of a long series of speeches, articles, and books on the history, role and future of money (including this one).

The Greeks used coins for many purposes, from developing a financial services ecosystem to financing their navy, coming in handy as the Persians, fresh from having conquered Lydia, launched a multi-pronged invasion of Greece in 480 BCE. But the Greeks' investment in their navy paid off; with over 300 Greek cities joining forces (known as the Delian League after the island of Delos), the Greeks had the upper hand.⁶² This reinforced the role of the Greek island of Delos (next to the island of Mykonos) not only as a commercial competitor to Athens but also as an early example of an "off-shore financial centre". Delos was seen as a neutral ground for both religion and trade and the natural choice to store the assets of the Delian league that created the financing that would allow Greece to defeat Persia. Delos attracted

merchants not only across Greece and from around the world, but also from a rising power called Rome.⁶³

In 356 BCE, a new coin entered the Greek world that depicted the head of the Greek god Zeus. However, many people confused it with the man who ordered their minting: Phillip II of Macedonia. Phillip had struck this coin to celebrate his victory in race horsing at the Olympics, but also because that was the year his son, Alexander (soon to be Alexander the Great), was born.⁶⁴ Phillip had formed one kingdom out of several previously warring tribes and transformed that unity into a growing economic and military power, soon leveraging the power of minting coins to finance his military and to take over Greece.⁶⁵ Following his death, his son Alexander assumed the throne in 336 BCE at the age of 20, and he pushed coinage to another level, by adorning coins with his image and by understanding that whoever writes the rules for money has power. He set up new mints in each land he conquered; he created standards with simple standard weights, designs, and conversion (10 pieces of silver for one gold coin); and until his death in 323 BCE, his coins were a great example of using money as a tool for propaganda.⁶⁶

5.2 Rome

Despite close contacts with Greece, Rome was slow to adopt money. The city of Rome was founded in 753 BCE, but for a long time relied on heads of cattle as units of account. Whilst this can do a basic job, it does not help with financing foreign wars or developing marketplaces like the Lydians and Greeks. The Romans would strike their first silver coin in 269 BCE, driven by the need to fund the Punic wars against Carthage. The basic unit was a silver coin called a “*denarius*”, originally worth ten asses and as this was too high for everyday actions like paying soldiers, the most common coin became the lower value “*sestertius*” (as any fan of the comic books Asterix will remember). Due to overspending, Rome had to borrow from senators and wealthy lenders leading to currency reform and the issuance of the gold “*aureus*” which kept its value over the next 200 years as Rome went from a Republic to an Empire.⁶⁷

The main mint in Rome was the Temple of Juno Moneta overlooking the Forum. Juno Moneta was the object of a cult throughout the Roman world and her name, Moneta, was derived from the Latin word “*monere*” meaning to warn. Whilst originally patroness of the city, whose job was to alert rulers of instability, she morphed into the guardian of Rome’s funds and it’s from her name Moneta that the words money and mint were derived. The Moneta mint operated around the clock, which is how the word “currency” is derived

from the Latin “*currere*” meaning to flow or circulate.⁶⁸ Interestingly, many historians have argued that money from that point had a connection with the divine and to the feminine. For example, in most European languages, money-related words are feminine in gender like *la monnaie* in French, *la moneda* in Spanish, and *die mark* in German.⁶⁹

By the second century, Rome had become a wealthy place, amongst other reasons, due to its minting of money. The Roman monetary system, built on the Greek model, soon penetrated the entire known world outside China, but unlike Greece which had used the money to build a productive market-based economy, Rome’s growth was based on tribute, making it unsustainable. The city of Rome did not produce much and the elite spent their time on entertainment and luxuries, but the coinage flow of Moneta never stopped and, unsurprisingly, gave rise to inflation.⁷⁰ Perhaps unsurprisingly, Roman emperors started getting involved in traditional forms of quantitative easing. For example, Nero in 64 CE, thinking nobody would notice, cut the silver content of the denarius, a habit that the subsequent Emperors sustained, resulting in the *denarius* decreasing from its original 100% silver content to as little as 4% by the third century BCE.⁷¹ This led to catastrophic consequences for Rome as the emperors maintained the value of the gold *aureus*, but continuously debased bronze and silver coins, which were used by the general public. For example, in 307 CE, one pound of gold was worth 100,000 dinarii and by 324 CE, it was worth 300,000. In certain parts of the empire, inflation was worse, as it is estimated that a pound of gold was worth 2,120,000,000 denarii in Egypt.⁷²

These emperors insisted that taxes remained valued against gold coins, so many in the general population, stuck with their debased denarius coins, lost their farms, and had to sell themselves into slavery. Parts of the economy even started to regress to barter.⁷³ Ironically, influential sectors of the economy, from civil servants and the army to landowning senators and the emperor himself, were happy with appreciating land and gold currency assets, but it was a struggle for the rest of the empire.⁷⁴ What Nero had done was invent fiat money (which in Latin means “let it be done”) by linking the value of money to that of the emperor’s power and not the underlying commodity or metal.

This worked for 200 years until the third century CE when Rome experienced a serious monetary crisis. By 476 CE, the date usually given for the collapse of the Roman Empire, the classical money economy that had survived in some form or shape for a thousand years collapsed. It was in such a serious state that a thousand years would pass before the money economy would return in full force. During the long period known as the Dark ages

and then the Middle Ages, money played only a minor role compared to the glory days of money in Greece and Rome at their peak.⁷⁵

6 Faith and Money

During the Dark Ages (476–800 CE) and the Middle Ages (500–1500 CE), Europe abandoned its cities (and its coins) for agricultural feudalism. As a result, the evolution of money throughout Europe stagnated during this time. However, it was a different story in other parts of the world, particularly in Asia, and somewhat surprisingly, this was often linked to the rise of religion.

6.1 Buddhism

The historical Buddha lived in the fifth century BCE. Buddhism taught people that there could be an end destination, known as the enlightenment, and that one had to prepare for the future, naturally introducing ideas like investing, saving, and credit. Buddhism was also tolerant and so merchants became big supporters of the religion, in turn helping support the spread of monasteries which became centres of savings and lending.⁷⁶ Whereas Christian monasteries in Europe relied on feudal landholdings to generate income, Buddhist monasteries in contrast often acted as quasi banks by raising funds via charity or alms and then lending it out. Buddhist pilgrimage routes developed with the emergence of the Silk Road and connected China with the rest of the world. These routes were not linked to any country; merchants didn't operate in the name of a king or a church and were often associated by kinship, like families or clans of Gujaratis, Jews, or Armenians. From 500 to 1500, these routes spread not only trade and commerce, but science and art as well,⁷⁷ and the role Buddhism played in East Asia was echoed by the expansion of Islam in West Asia.

6.2 Islam

Islam took off in the seventh century. Muhammad, a merchant, received the message of God in Mecca and in 622, he fled with his followers to Medina (in today's Saudi Arabia) and created the Muslim community. Before becoming the Prophet of God, Muhammad was a businessman, and whilst the Quran had plenty of warnings against greed, it didn't condemn commerce or wealth. The Quran encouraged wealth, so long as it was acquired in a moral way and

put to good use. For example, the Quran encouraged the *zakat*, the duty of a Muslim to give alms, thereby ensuring that the rich help the poor. But the real impact would be the Quran's prohibition against charging interest (*riba*).⁷⁸ The first Islamic coins were minted in Damascus (today's Syria) in 696 CE, including a gold dinar (based on the Byzantine solidus) and a silver dirham (the name "*dirham*", still in use today, is derived from the Roman "*denarius*"). The first Islamic mint was set up in Wasit (today's Iraq), and to address the issue of counterfeiting, the caliph at the time had an idea: any minter or moneychanger caught counterfeiting would have his hands cut off.

The Muslims brought many innovations to the world of finance and money. First, Muslim bankers invented a bill of exchange or a letter of credit (called a *sufijah*) as well as a cheque (called a *sakk*). The prohibition against charging interest never became an issue, as many techniques were developed early on to hide it in transactions (in what could be one of the earliest examples of "financial engineering" and structured products)⁷⁹ Second, the Arabs adopted the use of numerals from India. This use of Arabic numerals allowed transactions to be expressed in a decimal system using the zero, so banking instruments began to flourish, and the use of double-entry bookkeeping using Arabic numerals not only helped the development of bills of exchange, but also allowed the rise of merchant houses that could more easily keep tabs on their increasingly global operations. For example, mercantile groups such as the Arab Karimi, the Jews, and Armenians (who were not landowners or tax collectors) established large commercial institutions and markets that were a mix of warehouses, stock exchanges, and futures markets.⁸⁰

6.3 Christianity

Christianity was probably an outlier when it came to its views on wealth. For example, the Old Testament frequently focuses on the need for people to look after themselves; figures like Abraham, Jacob, and Solomon were viewed as meritizing their wealth. In contrast, the New Testament would repeatedly present Jesus' view that poverty is holy and wealth an impediment to salvation. For example, the gospels tell stories of how Jesus chased the money-changers out of the Temple of Jerusalem. He acknowledged money as a fact of life but one to be separated from the faith by his famous words: "Render unto Caesar the things that are Caesar's, and unto God the things that are God's". (Matthew 22:21).⁸¹ These ideas might make one smile when we look at the role the Vatican plays in financial services today, but this initial negative view on wealth didn't stop the adoption of Christianity and in many cases, helped it gain traction with the poor, whom Jesus said would inherit the earth.

Christianity flourished following Emperor Constantine's conversion, gradually spreading throughout the Byzantine and Italian worlds, catalysed by trade routes and markets first laid down by the ancient Greeks. Another impact religion had on the history of money came through the Crusades, a series of religious wars initiated, supported, and occasionally directed by the Catholic Church beginning in 1095 and continuing through the mid-fifteenth century. Any military operation of a scale like the Crusades required payment of vast amounts of cash for everything from supplies and equipment to allies and ransoms, giving rise to numerous intermediaries, like the Hospitallers and the Knights of the Temple. The Hospitallers, or the Order of the Knights of the Hospital of St John of Jerusalem, were first formed in Jerusalem shortly after the city's conquest by Christians in 1099, carrying out the task of tending to the casualties of the Crusades. Although the establishment of hospitals and the provision of medical care was always important to them (and continues to this day with the St. John Ambulance Brigades a good example), their commercial, military, and financial activities grew to overshadow these original charitable purposes.⁸² The Templars, or Order of the Knights of the Temple at Jerusalem, were also formed in Jerusalem in 1120, and also grew to become a formidable financial and political force.⁸³ These two orders had their own ships, armies, warehouses, and castles at several strategically placed ports and towns, from Spain and Syria to England and Egypt, and were granted powers to mint their own coins, conducting full merchant banking activities, particularly during the thirteenth and fourteenth centuries.⁸⁴ The Hospitallers and the Templars also embraced the bills of exchange that the Muslims had invented, proving pivotal when transferring large amounts of capital during the Crusades. The first known foreign exchange contract was issued in Genoa in 1156, enabling two brothers who had borrowed 115 Genoese pounds to reimburse their bank agents in Constantinople the sum of 460 bezants one month after arrival.⁸⁵

We could write entire books on the Hospitallers and the Templars (as many have done already), but the important thing to remember is that these groups grew very big and very powerful, particularly the Templars, who had a crucial impact on the history of money and banking. The Templars were often recruited from the younger sons of nobility, who inherited no titles or riches and had to pledge to a life of devotion to the church. Their initial role was to protect the pilgrims coming to the Holy Land and wasn't an easy life; they fought strenuously and ate only two silent meals a day whilst listening to religious readings. They ate meat only three times a week and as a sign of their chastity, dressed in white mantles emblazoned with a large red cross. Married men could join the order but had to live chaste lives apart from

their families and could never don the traditional white mantle reserved for the brothers who lived as perpetual virgins and never married. All knights had to stay away from women and could not kiss any woman, even a family member, and they had to sleep in shirts and pants with a cord around their waist to remind them of their vow of chastity. They kept a candle burning in their room throughout the night to discourage any immoral acts, whether alone or with someone else,⁸⁶ and maintained a strict code of warfare that virtually precluded surrender or defeat on the battlefield. Because of their willingness to die, they were some of the most feared warriors in the world, coming in handy when transporting valuables over long distances from their various castles.⁸⁷

As incredible as it may sound, the Templars became go-to bankers and grew incredibly rich (despite their vows of poverty) as their services proved very useful. For example, a knight could deposit money or take out a mortgage through the Templars in Paris and receive the money in the form of gold coins in Jerusalem. The Templars of course charged a fee for these services and also charged a fee for converting between different currencies, like a modern foreign exchange business. At their height, they employed 7,000 people and owned 870 castles and houses across Europe and the Mediterranean, stretching from England in the West to Jerusalem in the East.⁸⁸ Using bills of exchange and other financial tools, they became financiers to the French kings and various popes. However, they became too powerful for the liking of some of these same kings and popes. Following pressure from Phillip IV of France (who had been targeting the Templars for many years by confiscating their goods, torturing them, and charging them in courts), Pope Clement V finally abolished the Order around 1312 and confiscated their riches.⁸⁹ The Pope transferred some of the Templar's property to other religious groups, including the Hospitallers. Phillip IV went on to execute many of the remaining Templars, even going so far as to burn many of them alive. He asked for compensation from the Hospitallers for the money the French spent on investigations and trials of the Templars, and the Hospitallers, seeing what had happened to the Templars, quickly accepted. King Phillip of France (and Pope Clement V) had de facto crushed the greatest and most powerful financial institution of the time.⁹⁰ However, these Templars had already introduced Europe to the basics of banking and like many things in life, when these Templars disappeared, a void was created, leaving another group to take their place, this time filled by Italian bankers.

7 The Italian Bankers and the Renaissance

The void of the Templars would quickly be filled by families from the northern Italian states of Pisa, Florence, Venice, Verona, and Genoa. But these families differed from the Templars in a very important way; they did not operate from well-fortified castles, nor did they travel in heavily armoured convoys. Instead, they operated in the marketplaces catering as much to the needs of small vendors and merchants as government officials and the Church. This was a big shift compared to the Templars, who typically served only the nobility.⁹¹ These Italians set up tables and large benches from where they would conduct their activities. The word “bank” actually derives from the old Italian word “*banca*”, which means bench. The Italian bankers had the same problem the Templars had in that the Church forbade usury, the charging of interest on loans. To get around this restriction, the Italian bankers didn’t officially make any loans, but rather traded bills of exchange. The Latin for bill of exchange is “*cambium per letras*”, which means exchange through written documents. The transaction officially consisted of the sale of one form of money for another that would be paid in a different currency at a specified future date.⁹²

Italian bankers boosted commerce by making it much faster. In 1338, a shipment of coins required three weeks to go from Rouen in northern France to Avignon in southern France; the shipment faced many perils from robbers to being stolen from those transporting it directly. By contrast, a bill of exchange would only take eight days, and if it was stolen, it could not be redeemed by the thief. For these reasons, merchants were happy to pay the 8 to 12% fee involved.⁹³ Italian bankers thrived but, similar to the Templars before them, they were undone due to their dealings with the government. Some of the major Italian banking families backed Edward III at the start of the Hundred Years’ War between England and France. When Edward II defaulted on his loans in 1343, many Italian banks went bankrupt and these great losses were catastrophic for the Italian bankers, taking a century for them to regain their vigour with the rise of the Medici family.⁹⁴ Whilst the Medicis didn’t do anything particularly novel when it came to banking, they used their wealth to acquire political power and aristocratic titles and most importantly, the Medicis helped finance a great revival in art and architecture that still stands to this day in Florence. What became known as the Renaissance didn’t begin as a movement in art, but rather as a practical revival of mathematics to help bankers and merchants perform the increasingly difficult tasks of converting money, calculating interest (though technically not allowed), and determining profits and loss.⁹⁵

In 1202, Leonardo Fibonacci (also known as Leonardo Pisano after his hometown of Pisa), published *Liber Abaci*, in which he introduced Arabic numerals to Europe (even though the Arabs had themselves borrowed the numerals from India). Arabic numerals offered a great advantage over clumsy Roman numerals, which were difficult to add and subtract and which made multiplication and division very difficult. The introduction of Arabic numerals eliminated the need for an abacus, since merchants could calculate the new numbers more easily in their heads or on a piece of paper.⁹⁶ However, there was much resistance from the old guard, universities, government, and the Church, who were suspicious of these new numbers that came from “infidels”. In stubborn defiance, many European universities continued to use the abacus and to teach mathematics using Roman numerals until as late as the seventeenth century. Many governments also refused to accept the use of Arabic numerals for official purposes, claiming they could be easily forged, even by a person with little education. Soon after, merchants who became quick adopters of these Arab numerals started putting plus or minus signs to note overweight or underweight items. These signs soon became the symbols for addition and subtraction and, eventually, for positive and negative numbers.⁹⁷

The reality is that Arabic numerals democratised mathematics and made the field more accessible. In 1478, *Treviso Arithmetic*, an anonymous textbook, appeared in which the author taught the reader not only addition and subtraction, but also multiplication and division.⁹⁸ In 1484, Nicolas Chuquet introduced a system to make zeroes more easily understood by grouping them into sets of three with a marker between each set. He gave each set of three zeroes its own name and, thus million, billion, and trillion were born.⁹⁹ In 1487, Luca Pacioli, a Franciscan friar, published the 600-page masterpiece, *Summa de aritmetica geometria proportioni et proportionalita*, introducing the concept of double entry accounting, still used to this day.¹⁰⁰

Arab mathematicians devised algebra (which comes from the Arabic *al-jabr*), based on the work of ninth century Arab mathematician Muhammad ibn-Musa al-Khwarizmi. Al-Khwarizmi worked in Baghdad and borrowed many of his ideas from the Hindu work of Brahmagupta; Al-Khwarizmi's work, in turn, was translated into Latin and spread throughout Europe by Gerard of Cremona, an Italian translator of scientific texts.¹⁰¹ Al-Khwarizmi helped alleviate some of the problems of working with fractions by devising a system of decimals in place of fractions. This use of decimals, called algorism (a corruption of the name Al-Khwarizmi) eventually became the modern word algorithm.¹⁰² Mathematics was also used to revisit concepts

of philosophy and natural sciences. For example, René Descartes published his Discourse on Method in 1637 (where he coined the famous expression, “I think, therefore I am”) and Sir Isaac Newton published Principia Mathematica in 1686, one of the most important works in the history of science.¹⁰³ The development of money during the Renaissance had an indirect impact on many other aspects of society, with these ideas flourishing and spreading across Europe. But it was not only in Europe where change was taking place, as similar developments were spreading throughout Asia, particularly in China.

8 China and the Rise of Paper Money

From the eleventh to the fourteenth century, the city of Quanzhou (in today’s Fujian province, across from Taiwan) served as China’s principal port for foreign traders. It was a giant and cosmopolitan city home to Buddhist, Muslim, Christian, and Hindu communities.¹⁰⁴ At that time, China was under Mongolian control following a series of invasions that began with Genghis Khan and completed by his grandson, Kublai Khan. In 1271, Kublai Khan declared that he had a mandate from heaven to launch a Chinese dynasty, the Yuan. He then proceeded to set in motion several initiatives, including the issuance of paper money. The celebrated Marco Polo, who journeyed around Asia from 1271 to 1295, said that with regard to the money of Khanbalik (as Beijing was called back then), “the great Khan may be called the perfect alchemist, for he makes it himself”.¹⁰⁵

Marco Polo described how the Chinese manufactured paper notes (or “cards” as he called them) from the bark of the mulberry tree. As he wrote in his Travels, “All these cards are stamped with the khan’s seal, and so many are fabricated that they would buy all the treasures in the world. He makes all his payments in them and circulates them throughout his kingdoms and provinces over which he holds dominion; and none dares to refuse them under pain of death”.¹⁰⁶ In 1287, Kublai Khan issued a paper note called the *zhiyuan chao*, which was the first note that was not nominally linked to silver or any other metal. Rather, its value was based on the mightiness of the emperor (Fig. 5).

One advantage that the Chinese emperor had was de facto complete control. The Khan confiscated all gold and silver coins to ensure his paper currency was accepted and when entering China, foreign merchants were required to hand over their bullion for paper notes at rates determined by Chinese moneychangers. Their bullion was held on deposit until they left



Fig. 5 Yuan dynasty era banknote circa 1287 with its printing wood plate. The smaller Chinese characters in the bottom half of the note say “(this note) can be circulated in various provinces without expiration dates. Counterfeitors would be put to death”. Photographed at the Tokyo Currency Museum in 2007 (Source Public domain)

the country. The Khan was able to issue his paper currency and have people accept it, as he had a powerful state, an effective bureaucracy, and a cowed justice system.¹⁰⁷

As we'll see later in this book, these historical developments parallel some of the conditions that have allowed twenty-first century China to issue its own central bank digital currency (CBDC) and have everyone accept it. By 1350, China's experiment with paper money had collapsed; the emperors (in a pattern that we've seen throughout the history of money) had printed way too much, triggering rampant inflation, leading the ethnic Han Chinese to kick out their Mongolian overlords and establish the Ming dynasty.¹⁰⁸ Whilst the Ming dynasty was initially ambitious when it came to its global outlook (the epic voyages of Admiral Zheng He from 1405 to 1425 are a great example), the Ming quickly retrenched and closed themselves off from the outside world. Chinese society gradually lost its curiosity and its culture of innovation. After moving to a more isolationist stance, the Chinese emperors were initially careful with paper issuance before (once again) turning on the printing presses. By the sixteenth century, the Ming had lost control of their

currency, and China was suffering from hyperinflation, forcing the emperor in 1567 to re-allow foreign trade at China's borders. This became particularly interesting for the emperor when he found these foreigners had lots of silver, something he lacked and desperately needed to finance his armies.¹⁰⁹

9 Portugal, Spain and the Age of Discoveries

Whilst the Ming dynasty had retrenched inward, emerging power centres on the other side of the globe, particularly Portugal and Spain, were sailing the world in search of new routes and riches, not to mention a new route to Asia. Their goal was to find a course that bypassed the Muslim powers and the Italian city-states that enjoyed a lucrative trade monopoly with them. Portuguese explorer Vasco da Gama led the first European voyage to reach India by sea, reaching the Malabar coast in 1498. In 1492, Christopher Columbus thought that he had discovered a route to Asia for Spain but inadvertently stumbled upon and "discovered" the Americas.

After Columbus' arrival, it took the Spanish about 50 years to locate the major treasures, looting the great Aztec capital Tenochtitlan in 1521 and continuing their incursion into Central America before turning their attention to the Incas in the 1530s. The Spanish melted most of the gold and silver they got their hands on so as to make into ingots to send back to Spain.¹¹⁰ In 1565, the Spanish, led by Captain Miguel Lopez de Legazpi, sailed from Mexico to cross the Pacific Ocean with the goal of establishing a colony in the Philippines (known to the Spanish from a previous journey by Ferdinand Magellan, who died there). They returned the same year to Mexico, following a journey of over four months at sea. This opened entirely new trade routes and made Asian goods more affordable (by cutting out the Muslim and Italian middlemen) for sale in Europe. Chinese silk and porcelain, Indian cotton, and Asian tea and spices were shipped to Mexico and then onward to Europe, first as raw materials and then as finished products.¹¹¹

The Spanish love of gold fuelled the conquest of the Americas, but it was silver that drove trade. The Chinese had the goods the Europeans loved but had no reciprocal interest in European goods. However, China needed silver and loved the silver that the Spanish gave them in exchange for their wares and the Spanish had lots of silver. Following his conquest of the Incas in 1541 (and taking much of their gold and sending it back to Spain), the explorer Pizarro discovered the Cerro Rico (in today's Bolivia), a mountain made of silver, home to the world's biggest deposit of silver ore. But instead of sending the silver back to Spain, the Spanish quickly realised that China would pay

double or even triple the rate of silver, eventually contributing to the decline of the Chinese.¹¹²

At that time, Spain owned most of the Americas except for the easternmost territory of South America, which became Portuguese Brazil. From 1500 to 1800, the mines of the Americas provided 70% of the world's output for gold and 85% of its silver, so it's no surprise that wars between the European powers during that period focused on controlling wealth from the Americas and trade with Asia. Spain would first struggle against Portugal, but then they would both struggle against England, France, and the Netherlands.¹¹³ However, the Spanish and Portuguese had done something quite remarkable: they knit together several major economies around the globe. Unfortunately, these economies were often linked for the wrong reasons, where in Africa, for example, this new wealth from the Americas created even more demand for slaves, with Africa becoming part of the triangular trade with America and Europe. African slaves were sent to the Caribbean and American silver and Caribbean sugar were sent to Europe before being used to buy more slaves to ship to America. Following the opening of the routes to Asia, this exchange would be expanded to include the spice trade with South Asia, the silk and porcelain trade with China, the opium trade with India, and the fur trade with Siberia and Canada.¹¹⁴

Trade had become truly global, a force that nobody could stop, with money as the source of it all. Unfortunately, both the Spanish and the Portuguese squandered wealth from the Americas; Spanish kings wasted it on foreign adventures and wars and Portuguese kings blew their riches on palaces and pageantry. Not surprisingly, this caused tremendous inflation with the quantity of goods produced unable to keep up with the volume of silver shipped from America. For example, between 1500 and 1600, it's estimated that prices in Spain rose by 400%.¹¹⁵

10 The Dutch Innovations

The proliferation of coins and bonds and the rise of international trade gave way to new opportunities for moneylenders and bankers. The Dutch made three important innovations that would transform Amsterdam into the most important financial centre on the globe. First, the Amsterdam Exchange Bank, the Wisselbank, was established in 1609 as a clearinghouse for merchants dealing in numerous currencies, but what set it apart is that the Wisselbank, overseen by the Amsterdam municipal government, began

crediting merchants in what came to be known as “bank money”. The Wisselbank guaranteed to return deposits whole and not in a debased manner (e.g., with less gold or silver), establishing trust towards the bank and encouraging people to deposit for longer durations. The Dutch had invented the concept of a central bank,¹¹⁶ and then devised the idea of a joint-stock or limited liability company.

The United East India Company was founded in 1602 with a charter giving it a monopoly on Dutch trade in Asia. What was remarkable was it allowed all Amsterdam residents to subscribe and become shareholders, not dissimilar to today’s VC funds, with the initial plan for shareholders to redeem after 10 years. But when 1612 arrived, the company decided not to liquidate its assets, so shareholders had only one option: to sell those shares to someone else and thus, a third Dutch innovation took place.¹¹⁷ The stock market allowed for the trading of shares of the United East India Company, in addition to other companies. The interest was such that the city erected a “*beurs*” (thus the name bourse) where trading could take place. It would be home, of course, to the tulip bulb mania in 1636–1637, and by the end of the seventeenth century, the Dutch had amassed the most assets and savings in the world. Amsterdam had truly become a global financial centre, but the Dutch Golden Age would end in 1672 when it found itself at war with England, France, and several German duchies at the same time.¹¹⁸

11 The British and the Bank of England

In 1694, two entrepreneurs, Michael Godfrey and William Paterson, proposed the establishment of a national bank that could lend money to the government.¹¹⁹ King William liked the idea so much that he chartered the Bank of England, he and Queen Mary were two of the original shareholders. The Bank of England, based in the City of London, began as a private bank that acted as a banker to the government and primarily to fund the war effort against France as the Nine Years’ War (1688–1697) was happening at the same time as one of the many Anglo-French wars throughout history. The original Royal Charter of 1694 laid out that the Bank was founded to “promote the public Good and Benefit of our People”. The Bank’s first governor was Sir John Houblon (who was featured on the British 50-pound note for many years).¹²⁰

What made the creation of the Bank of England so unique was that it represented a truce between the government and the merchant class. Commercial banks could now get involved in borrowing and lending, but in

exchange would continue to support the government's borrowing needs and accept a certain degree of oversight in what was called the "great monetary settlement".¹²¹ Under Sir John Houlton, the Bank of England's early years were dominated by the government's pressing financing demands, encouraging the Bank of England to launch a conventional banking business, accepting deposits from the public.¹²² However, the currency plummeted in 1695, leaving the government broke and in shambles.

King William named the famed mathematician and physicist Sir Isaac Newton as warden of the British Mint. In 1717, Newton decided that the government should base its finances on gold and would coin the first-pound sterling, which contained a pound's worth of gold. The pound had previously been based on silver (the word sterling comes from the Old French *esterlin*, transformed as *stiere* in Old English, which means strong, firm, or immovable).¹²³ Following unsuccessful attempts by the Dutch and the French to introduce paper banknotes, the Bank of England introduced its first paper banknotes in 1725, denominated in the new gold-backed pound sterling with the Libra (£) symbol (the Roman unit of weight) that we still use today. In 1844, the British Parliament passed the Bank Charter Act, giving the Bank of England a virtual monopoly on the right to issue banknotes throughout the United Kingdom. The Bank of England, in turn, had to guarantee their convertibility into gold on demand and unlike paper money issued by the United States or France during their revolutions, the paper banknotes of the United Kingdom were not issued directly by the government, but rather from a private bank under a government charter.¹²⁴ The government continued to issue coins, but the Bank of England controlled issuance of banknotes. This characteristic of a central bank not under the direct control of the government is something that not only survives to this day but has also been implemented by many other countries around the world.



Fig. 6 Depiction of an eighteenth century pillar dollar (Source Public domain)

How Did the Americans Adopt the Dollar?

One might assume that the American colonies being composed of settlers from England would use the British currency of pounds, crowns, shillings, and pence, but the reality was much different, as the American colonies suffered from a constant shortage of coins. The policy in London at the time was to increase the amount of gold and silver in Britain and to prohibit its export anywhere in the world including its colonies. As a result, the American colonies were forced to use “foreign” silver coins, primarily from the neighbouring Spanish colony of Mexico¹²⁵ (Fig. 6).

The Spanish coin bore a face value of eight *reales* in the Spanish system (*real* meaning royal in Spanish). Whilst the Americans rejected both the terms *real* and *peso* as names for their new currency, the concept of eight stuck and the dollar was often referred to as eight bits or pieces of eight. To this day, the expression “two bits” still refers to a quarter.¹²⁶ The American colonists became so used to using the Spanish pillar dollar that after independence, they adopted it as the official currency. On July 16th, 1785, Congress declared that “the money of the United States of America be one dollar”.¹²⁷

12 The American Colonies and Paper Banknotes

Whilst the Italians and the British heavily influenced the history of commercial banking, the Americans undoubtedly had the biggest impact, as it was the early American colonists who really popularised paper banknotes. As early as 1690, the Massachusetts Bay Colony printed the first paper money in North America,¹²⁸ and the grandfather of paper money was undoubtedly Benjamin Franklin, who developed an early interest in paper money and wrote his first “pamphlet” on the topic at the age of 23. In 1729, he published “A Modest Enquiry into the Nature and Necessity of a Paper Currency” and operated a printing press in Philadelphia, printing cash on behalf of the Pennsylvania colony (a service that often caused his newspaper, the Pennsylvania Gazette, to be late for delivery). To this day, his visage is enshrined on the highest denomination of the U.S. dollar, the \$100 banknote.

However, colonial authorities in London were none too pleased with such activity and outlawed the use of paper money in New England in 1751, extending the ban to the rest of the colonies in 1764. In 1775, the U.S. Congress issued the Continental to finance the American Revolutionary War against Great Britain. However, due to a mix of overprinting, no solid

backing, and counterfeiting, it soon lost its value (thus the American expression “not worth a Continental”) and Congress stopped issuing it around 1780¹²⁹ (Fig. 7).

This entire experience with paper money was seen as a failure in the United States, so much so that the United States printed no paper money for nearly a century afterwards. However, whilst many Americans were turned off by money as they had lost so much of it during the war with the British, it was seen as a success by the rest of the world, who saw the Americans as having won their revolution by printing money.¹³⁰ The Americans adopted the decimal system in 1792 (pioneered by Russia around 1535) with the passage of the Mint Act,¹³¹ but the wide usage of paper banknotes needed a user-friendly system, with Thomas Jefferson later devising the idea of calling one-hundredth a dollar a “cent” (from the Latin “centum”, meaning hundred), and a tenth of a dollar a “dime” (based on the Latin “decima” meaning one-tenth). Alexander Hamilton elaborated further on the country’s monetary system in “The Report on the Establishment of a Mint”, leading to the Coinage Act of 1792, making the U.S. coinage system the first wholly decimal monetary system on earth.

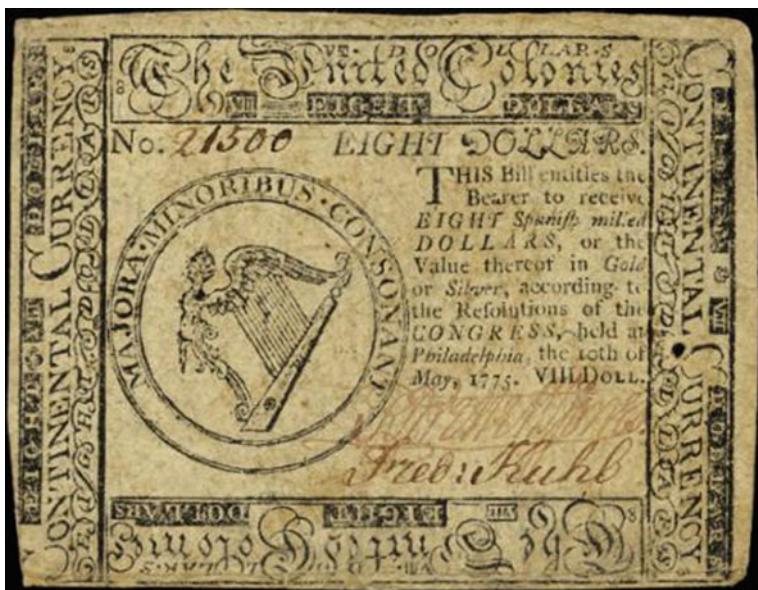


Fig. 7 The Continental currency. The phrase “not worth a Continental” is coined after the Continental Congress issues paper currency to finance the Revolutionary War. The currency would quickly lose its value because of a lack of solid backing and the rise of counterfeiting (Source University of Notre Dame, Public domain)

Paper banknotes also played a big role in the industrial revolutions from 1760 to 1840 in both the United Kingdom and the United States. For example, paper banknotes outnumbered coins in Britain in 1776¹³² with the war again acting as a revival and catalyst for paper banknotes in the United States. In 1861, in order to finance the Civil War, Congress authorised the Department of the Treasury to issue non-interest-bearing Demand Notes. These notes earned the nickname “greenbacks” because of the green ink on the back, a basic anti-counterfeiting measure used to prevent photographic copies and fakes since cameras of the time could only take pictures in black and white.

All U.S. currency issued since 1861 remains valid and redeemable at full face value. After the Treasury issued Demand Notes, Congress authorised a new class of currency in 1862 known as “United States notes” or “Legal Tender notes”, replacing Demand Notes (and continuing to circulate until 1971).¹³³ Over \$450 million worth of “greenbacks” were issued to finance the American Civil War from 1861 to 1865. The Confederacy of the South also issued its own “yellowbacks”, over \$1 billion worth, that later lost almost all their value.¹³⁴

Where Does the Dollar Sign (\$) Come From?

The dollar sign (\$) is probably one of the most recognised symbols around the world today. But as crazy as it may sound, the origins of why we use that symbol are far from clear. Many theories have emerged over the years to explain the \$ sign, with one of the most popular from libertarian philosopher and author Ayn Rand, who in a 1957 novel, claimed that the dollar sign was a symbol not only of American currency but of the nation’s economic freedom. According to Rand, the dollar sign (written with two downward



Fig. 8 One theory explaining the origins of the \$ sign

slashes instead of one) came from the initials of the United States: a capital U superimposed over a capital S, minus the lower part of the U.¹³⁵ However, as inspirational as this explanation might seem, evidence shows that the dollar sign was already in use by the time the United States was formed.

Other explanations are even more poetic. The most common Spanish coin at the time was the pillar dollar, so named because the coin showed the Eastern and Western hemispheres with a large column on either side that represented the Pillars of Hercules. Thus, there are those who argue that the modern dollar sign is derived from this pillar dollar, with the two parallel lines representing the columns and the S representing the banner hanging from them.¹³⁶ Others have argued that it is linked to Florence where due to the historic importance of the florin, the golden coins originally minted in the Italian city state of Florence, the letter F, printed as f, was originally used as the Dutch currency symbol. Some have argued that if you stretched the upper and lower parts of the sign and replace the horizontal lines with a vertical one you would have a sign very similar to the modern dollar sign.¹³⁷

Some have even linked it to slavery stating that the \$ symbol is derived from the words for “slave” (*esclavo*) and “nail” (*clavo*) in Spanish. Therefore the “S” with a nail would result in \$. The shackles worn by slaves could be locked by a nail which was passed through the rings or loops at the ends of the shackle and bent whilst it was still hot and malleable and as the enslaved constituted a store of wealth, the theory says the symbol came to represent money.¹³⁸ However, the most widely accepted explanation goes back to the Spanish peso, accepted as the basic unit of value in colonial America during the late 1700s. Handwritten manuscripts dating to that time show that the peso, formally “*peso de ocho reales*” or “piece of eight” in America, was abbreviated PS. It’s believed that as time went on, the abbreviation was often written so that the S was on top of the P, producing the \$ symbol. The data shows that the \$ first appeared in print after 1800 and was widely used by the time the first U.S. paper dollar was issued in 1875¹³⁹ (Fig. 8).

13 The Return of the Gold Standard

The gold standard played a crucial role in the development of modern finance, as the requirement to convert money into gold on demand prevents a government from making populist payments or resorting to quantitative easing. As long as citizens hold the right to turn their paper money into gold,

they hold a vote on how the monetary system is run, and if trust evaporates, they can convert those paper banknotes to gold and never touch the banknotes again.¹⁴⁰

Many in the United States had been lobbying to put the U.S. dollar on the gold standard. In 1900, Congressional passage of the Gold Standard Act made it official, followed by the Federal Reserve Act of 1913, which established the Federal Reserve as the nation's central bank and provided for a national banking system more responsive to the fluctuating financial needs of this rapidly developing country.¹⁴¹ But the Wall Street Crash of 1929 reverberated negatively around the world, and many countries soon left the gold standard behind; the Bank of England left in 1931, and France, Germany, and America quickly followed. In 1933, President Franklin Delano Roosevelt (FDR) went one step further and outright banned the ownership of gold and in 1934, a year after the nationalisation of gold, FDR nationalised silver as well.

Why Was Investing in Gold Banned in the United States from 1933 to 1974?

As families and businesses across America struggled to climb out of the depths of crisis in the wake of the 1929 stock market crash, President Franklin Delano Roosevelt attempted to dramatically increase federal spending to stimulate the economy. However, FDR's hands were tied by the Federal Reserve Act of 1913, which mandated that each bank note had to be backed by 40% gold held in federal reserves. So, for every dollar printed, the government needed to hold 40 cents of gold, but foreign and domestic holders of U.S. currency were rapidly losing faith in paper money and were redeeming dollars for gold at an alarming rate. In order to slow the process, FDR declared a "national emergency" and ordered all banks to close over a four-day span in March 1933 to prevent "the export, hoarding, or earmarking of gold or silver coin or bullion or currency". The terms of the presidential proclamation specified that "no such banking institution or branch shall pay out, export, earmark, or permit the withdrawal or transfer in any manner or by any device whatsoever, of any gold or silver coin or bullion or currency or take any other action which might facilitate the hoarding thereof; nor shall any such banking institution or branch pay out deposits, make loans or discounts, deal in foreign exchange, transfer credits from the United States to any place abroad, or transact any other banking business whatsoever".

For that entire week, Americans had no access to banks or banking services; they could not withdraw or transfer money, nor could they make deposits. One month later, an executive order made private gold possession illegal, and all Americans were required to turn in their gold to the Federal Reserve on

or before May 1, 1933 in return for \$20.67 of paper money per troy ounce. Violations of this order were punishable by up to 10 years in federal prison and a fine of twice the amount of gold not handed over to the feds. The order was quickly challenged and made its way to the Supreme Court, where it was upheld, with one notable exception: dentists, who could own up to 100 ounces of gold.

Many Great Depression era photos capturing Americans waiting in long lines at banks are often characterised as those waiting to get their money out, but in many cases, the opposite is true, with people standing in lines for hours to hand in gold. Ultimately, outlawing gold ownership was a central pillar that many argue made FDR's New Deal programs possible, which consisted of a series of public works projects and financial reforms. Without the ban, the government itself would have been in violation of its own laws against printing money. Even after President Richard Nixon took the dollar off the gold standard, allowing the dollar to freely float against other currencies, the prohibition against gold continued until 1974, when after being swayed by a pro-gold advocate he saw on TV, President Gerald Ford reversed FDR's executive order and legalised gold ownership.

In the depths of World War II, the gold standard enjoyed a mini-revival when America and 44 other countries held a meeting at Bretton Woods in the U.S. state of New Hampshire. These countries saw the opportunity for a new post-war international system that would draw on the lessons of previous gold standards and from the Great Depression and provide for much-needed reconstruction. It was an unprecedented cooperative effort for nations that had been setting up barriers between their economies for more than a decade. They sought to create a system that would not only avoid the rigidity of previous international monetary systems but also addressed the lack of cooperation amongst those countries.

After all, the classic gold standard had been abandoned after World War I, and in the interwar period, governments not only undertook competitive devaluations but also set up restrictive trade policies that worsened the Great Depression. Preparation began more than two years before the conference, with leading financial experts holding countless bilateral and multilateral meetings to arrive at a common approach. At the meeting, they put in place the orders for a new global monetary system in which the U.S. dollar carved out a central role.¹⁴² As part of the agreement, the United States promised to tie the U.S. dollar to gold at \$35 per ounce. Other countries would soon peg their own currency to the U.S. dollar. The 730 delegates

at Bretton Woods also agreed to establish two new institutions: the International Monetary Fund (IMF) was to monitor exchange rates and lend reserve currencies to nations with balance-of-payments deficits and the International Bank for Reconstruction and Development, now known as the World Bank Group, was tasked with providing financial assistance for post-World War II reconstruction efforts and economic development of less developed countries.¹⁴³ The United States also launched the Marshall Plan, with the goal of rebuilding war-torn Europe.¹⁴⁴ This system worked very well for almost 30 years, with America, Europe, and Japan witnessing high rates of growth.

14 Leaving the Gold Standard and the Financial Crisis

Initially, the Bretton Woods system operated as planned. Japan and Europe were still rebuilding their post-war economies, and demand for U.S. goods and services—and dollars—was high. Since the United States held about three-quarters of the world's official gold reserves, the system seemed secure. But in the 1960s, European and Japanese exports became more competitive with U.S. exports, the U.S. share of world output decreased, and so did the need for dollars, making converting those dollars to gold more desirable.¹⁴⁵ Fast forward to the 1970s, when the United States saw another internal crisis. The country was spending heavily on domestic social programs and funding its war in Vietnam and this increase in the money supply led to inflation and costs to the Treasury increased when other central banks made requests to convert dollars back into gold.¹⁴⁶

At the time, foreign governments could trade the dollars they received through international trade back to America for gold at \$35 dollars per ounce, but eventually, there were more foreign-held dollars than the United States had gold. The country was vulnerable to a run on gold and there was a loss of confidence in the U.S. government's ability to meet its obligations, thereby threatening both the dollar's position as reserve currency and the overall Bretton Woods system.¹⁴⁷ With a trade imbalance growing (Japan and Europe were selling more to the United States) and a ballooning federal deficit (with policymakers keen to spend more on the military and social programs) causing a drain of gold reserves, President Nixon took the dollar off the gold standard, allowing the dollar to float freely against other currencies. But gold would no longer be used as a backup to fiat currency and the phrase "Payable to the Bearer on Demand" was replaced by "In God We

Trust". Nixon ushered in the era of fiat currencies, backed only by confidence in the issuing governments and central banks, something that persists today.

Following the move away from the gold standard from the United States, other countries followed, leading to incredible growth in international trade, particularly in bank credit. It also saw many innovations in the field of finance, with the first electronic stock market, now known as the NASDAQ, created in 1971; the concept of financial futures contracts introduced at the Chicago Mercantile Exchange in 1972, and in 1977, mortgage-backed securities and securitisation saw the light of day. Politicians embraced many of these ideas as well, with the 1980s seeing a massive wave of deregulation and free market views. Regulatory restrictions were lifted, allowing banks involved in low-risk retail deposit activity to get involved in higher risk (and higher reward) investment banking. The collapse of the Soviet Union gave a further boost and brought the Eastern bloc into the capitalist mix, including China, which was gradually opening up following reforms instigated by Deng Xiaoping.¹⁴⁸

Major economic crisis events of course took place over the coming years, with the Asian financial crisis of 1997 being a prime example. But the game changer, also linked to the creation of Bitcoin, was the global financial crisis of 2008. Prior to the COVID-19 recession in 2020, the 2008 global financial crisis was considered by many economists to have been the most serious financial crisis since the Great Depression. It was caused by many factors, including predatory lending to low-income homebuyers and excessive risk-taking by financial institutions. The prestigious 164-year-old investment bank Lehman Brothers filed for bankruptcy and American International Group (AIG), the biggest insurer in America, had to be bailed out with a US\$85 billion loan by the New York Federal Reserve Bank. As turmoil spread from the financial system into the broader economy, some lost their jobs and others life savings, triggering protests and a vilification of those working in the financial sector, viewed as having had a hand in creating the crisis. A growing number of people began to wonder if the financial system's architecture needed to be completely rethought. The bright side, if any, of the global financial crisis of 2008 was that it would lead to the creation of Bitcoin.

15 The Bitcoin Whitepaper

On October 31, 2008, less than two months after Lehman Brothers filed for bankruptcy, Satoshi Nakamoto revealed a white paper entitled "Bitcoin: A

Peer-to-Peer Electronic Cash System". He shared the whitepaper on a cryptography mailing list at 2:20 pm Eastern Time on October 31 with his email titled "Bitcoin P2P e-cash paper" saying that "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party"¹⁴⁹ Interestingly, the domain "bitcoin.org" was registered just a few weeks prior at anonymousspeech.com, a site that allows users to anonymously register domain names.¹⁵⁰

Satoshi introduced an entirely new system "based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party".¹⁵¹ This was revolutionary and the whitepaper set out in nine simple pages a vision of a purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution, which is why Nakamoto's paper has become a sacrosanct document in the crypto community.

The abstract of the whitepaper reads:

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened whilst they were gone.¹⁵²

Who Is Satoshi Nakamoto?

Satoshi Nakamoto is the author of the Bitcoin white paper, but we still have no idea who he, she, or they are. Satoshi was active in various blogs and forums, including Bitcointalk, which he¹⁵³ founded, posting the first message under the pseudonym *satoshi*,¹⁵⁴ and he remained active in the

Bitcoin ecosystem until he suddenly stopped, saying that he had “to move onto other things”.

There have been numerous attempts to unearth the real Satoshi. Many have tried to analyse the time of his posts to guess where they were living (almost no posts between 5 and 11 am GMT) or their style of language (use of British spelling of words like optimise or colour), but these can be easily misleading. Some individuals who interacted with him online shared their experiences saying that Satoshi was “weird, paranoid and bossy”. Many of the individuals often mentioned as possible Satoshis, like Hal Finney or Nick Szabo, were early crypto pioneers and some tentative identifications by the media, including Newsweek, which claimed to have located the real Satoshi, have proved incorrect.¹⁵⁵ Other individuals who have claimed to be Satoshi, like Australian computer scientist Dr Craig Wright, have faced much scepticism from the crypto community. Dr Craig Wright even tried to copyright the Bitcoin whitepaper and the Bitcoin code, and soon after, others filed similar copyright requests. The reality is that we don't know, and we may never know who Satoshi is. It's also important to remember that Satoshi holds a large number of Bitcoin, estimated to be around 1 million BTC. At some of Bitcoin's higher valuations, the market capitalisation of these coins would make Satoshi one of the richest individuals on the planet. Indeed, a desire to ensure personal security may be one of the reasons Satoshi has chosen to remain anonymous, if he or she is still alive.

Many believe that it would be better if Satoshi is never discovered. Any comments that Satoshi might make would have a serious impact on Bitcoin and the broader crypto community, which could go against the decentralised idea on which Bitcoin was built. The outsized impact of comments from Vitalik Buterin on Ethereum is a good example. Also, seeing the intense questioning that Facebook's Mark Zuckerberg and David Marcus faced following the announcement of Libra (which will be also discussed in detail later in this book), was another argument for those who believe it is best that we never discover who the real Satoshi is.

Before discussing the innovations that Bitcoin brought forward, it's important to understand the problem that it was trying to solve: the reliance on financial institutions. Satoshi reaffirms this in the first line of the Bitcoin whitepaper when he mentions that “commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments”.¹⁵⁶ This problem is inherent to digital assets. In the physical world, if Alice meets Bob in person and hands him a \$5 bill, then Bob, upon inspecting it to ensure it is not counterfeit, becomes the holder of that \$5 bill that was previously Alice's. It is truly peer-to-peer and

Alice cannot possibly have spent that bill somewhere else or she would not have had it to give to Bob. This is significantly more difficult in the digital world as any type of digital asset can be easily copied at zero or minimal cost. To use the example above, Bob would not be so willing to trust that \$5 bill if Alice (and anyone else!) could easily print an unlimited amount. This is called the double-spend problem (Fig. 9).

Satoshi acknowledged that the double-spend problem had been the main hurdle facing past efforts to create a digital peer-to-peer payment system. In the whitepaper, he says:

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership. The problem of course is the payee can't verify that one of the owners did not double-spend the coin.¹⁵⁷

The double-spend problem was one that the crypto community had been trying to solve for many years. To use an analogy, when I send someone an email, an identical version of that email sits in both my outbox and the recipient's inbox. If others were copied to that email, that same email would exist in other locations as well. Whilst this works well for emails, it does not work if that email has a monetary value. If one could "create" an endless supply

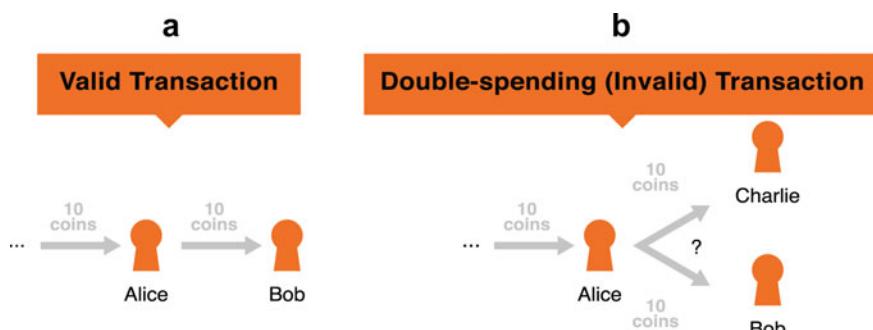


Fig. 9 The double-spend problem. (a) Valid transaction. (b) Double-spending (invalid) transaction. The problem illustrated in this example is: Suppose Alice has 10 coins and then sends all 10 coins to Bob. How can Bob (and other people using the coin) know that Alice has not sent the same 10 coins to Charlie before, without having a bank to verify transactions? (Source Tsung-Ting Kuo, Heyon-eui Kim, and L. Ohno-Machado, "Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications," Journal of the American Medical Informatics Association, September 8, 2017)

of money, then that money would be almost worthless. The way that we've dealt with this issue is by relying on banks or other central authorities to be those trusted intermediaries or bookkeepers, in exchange, of course, for a fee. Using such intermediaries, Alice can only send \$5 if she has it in her account and when she sends it to Bob, she does not have it anymore to send it to someone else.

But these trusted central authorities have an outsized impact. Not only does their presence add a layer of cost to the system, but they also control who can transact via their services and centralises power in the hands of a few. This is why many argue that Bitcoin is the ultimate financial inclusion tool as anyone, anywhere can create a Bitcoin wallet and receive and send Bitcoin to others without an intermediary. All that I need to send Bitcoin to anyone is their public Bitcoin address, anyone can go online and see how many Bitcoins are at a certain Bitcoin address, and every single Bitcoin transaction is public for the world to see. We don't know who is behind a certain address, but we can see every transaction.

The example that I use with my students when I teach this topic is that of a home address and a home key. Imagine a city full of single houses with big windows. Everyone can see what is in a certain house at a certain address, but they cannot enter the house as they don't have the house key. However, they can drop your mail through the mail slot. The Bitcoin public address is like your home address; everyone can see it. Anyone can send you mail but having your home address does not mean they can enter the house. You can give anyone your home address without the fear that they will enter your house and steal your belongings. It's the same with your Bitcoin public address; you can give it to anyone who can send you any amount of Bitcoin.

However, they will not be able to take those Bitcoin back, in the same way that they cannot retrieve a letter after they have thrown it through the mail slot of your door. In our city example, your home key is very important. If anyone gets a hold of that and knows your address, they can enter your house, steal your belongings and even lock you out. The equivalent of your house keys in the Bitcoin network is your private key, which is why you need to guard your private key (similarly to your house keys) very well! However, despite not having the keys to your house, someone who has your address can come and look from the window of your house and see what you have inside. In order to do this, that person needs to know your address. Ironically, that is how the Bitcoin network operates; all wallet addresses are public and anyone can see the balance at certain address. Like precautions that you take with your home windows (e.g., ensuring not much visible from windows,

ensure you have put valuables in a safe), similar precautions can be taken with Bitcoin addresses (e.g., move Bitcoin to other wallets).

This is a simplistic example, but hopefully helps you visualise how the Bitcoin network works. Bitcoin looked to eliminate the necessity of trusted third parties through the revolutionary combination of four previously unconnected technologies: cryptography, decentralisation, immutability, and proof-of-work. We'll discuss each of them in detail in later chapters.¹⁵⁸



2

Bitcoin

1 The Basics of Cryptography and Encryption

To properly understand the significant interest around crypto-assets and claims they have the potential to transform the financial system, we must first learn a bit about the “crypto” part of the name, or the technology that enables these assets to function. Whilst we don’t intend to cover the technical specifics of cryptography and the different encryption techniques in this book (there are numerous sources online as well as academic literature on the topic for those interested), it’s still important to understand the basics of cryptography along with early attempts to use this technology to create novel digital payment systems.

1.1 Early Encryption Techniques

Cryptography, which comes from the ancient Greek words “*kryptos*” (hidden secret) and “*graphein*” (to write) is the practice and study of techniques for secure communications.¹ Encryption is probably the most well-known use of cryptography and is defined as the process of encoding a message or piece of information in such a way that only authorised parties can access it; those who are not authorised cannot.²

The original version of this chapter was revised: Text correction have been updated. The correction to this chapter is available at https://doi.org/10.1007/978-3-030-97951-5_22

Encryption techniques have been employed for centuries. Julius Caesar used basic encryption techniques to inform his generals of his plans by writing messages using letters that were three letters after the letter they represented.³ For example, ABC would be written as DEF. More recently, Nazi Germany encrypted messages using the Enigma machine, which was finally broken by Alan Turing and his team, a decisive turning point in World War II.⁴ There are numerous types of encryptions, with one of the most basic forms called “symmetric” encryption, which refers to an encryption method in which both the sender and receiver share the same key. Let’s use a simple example based on that of Julius Caesar. Imagine Alice and Bob want to send secret messages to each other. They meet before and agree that if Alice writes an “a”, it should be read as “d” and that if she writes “b”, it should be read as an “e”, implementing a “plus 3” rule for all communications between them. In this case, they’re both using the same “key” (the “plus 3” rule). Of course, this method of encryption is not widely used these days (although it was one of the main encryption methodologies known until 1976⁵), as it could easily be “broken” using today’s technology (e.g., running numerous scenarios until one finds out the “plus 3” rule). But there are also practical implications like key management (e.g., if Alice wants to correspond secretly with other friends, she probably has a separate “key” for each so that Bob cannot read a secret message sent by Alice to others).

While this is manageable with only have Alice and Bob, the process becomes increasingly more complicated if you’re communicating with many different parties. In addition, Alice and Bob need to first find a way to communicate with each other that “plus 3” is the magic key. How to do this secretly in the first place is challenging, leading to a classic “chicken and egg” problem. We are greatly simplifying things here, but hopefully this gives you a better understanding of the challenges involved with symmetric encryption.⁶

1.2 Asymmetric or Public Key Cryptography

In a ground-breaking 1976 paper, cryptographers Whitfield Diffie and Martin Hellman proposed the notion of asymmetric (commonly referred to as public key) cryptography, in which two different but mathematically related keys are used—a public key and a private key. The public key, as its name implies, is public and available for anyone to see, but the private key is not intended to be seen by others. A public key is mathematically derived from a private key that anyone can then use to send you a message that only

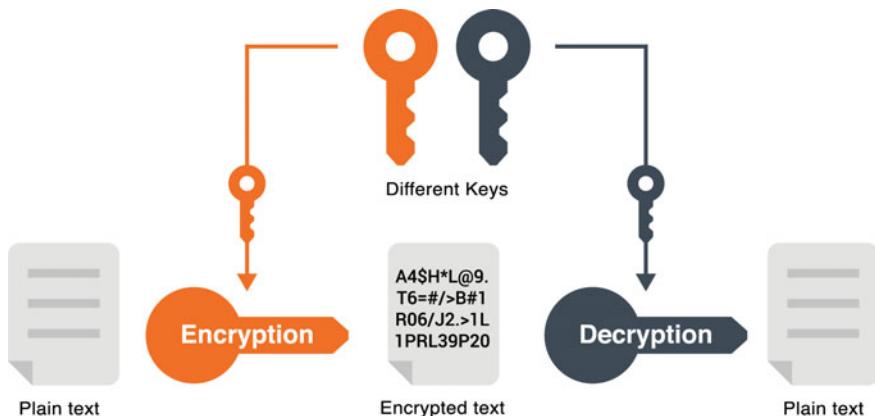


Fig. 1 Asymmetric encryption: public vs private keys (Source Public Domain)

you will be able to decrypt, as only you hold the private key. If anyone intercepts the encrypted message, they won't be able to decrypt it, as they don't have the private key (Fig. 1).

However, for the above to work you need a mathematical algorithm that can generate a public key from the private key. But it's crucial that it's mathematically impossible to do the opposite (i.e., for someone to infer what your private key is by having your public key). Fortunately, there are numerous algorithms that allow you to do just that, of which one of the most widely used is RSA (coined from the surnames of Rivest, Shamir, and Adleman, who first publicly described the algorithm in 1978⁷). Bitcoin uses an algorithm called ECDSA (Elliptic Curve Digital Signature Algorithm) that also allows you to use your private key to generate a public key,⁸ and that public key allows you to generate your Bitcoin address. It's impossible for anyone who has your public key to guess your private key, but more on this later.

1.3 Early Experiments with Cryptocurrencies

The cryptography developments of the 1970s began to shift cryptography from a primarily military-focused discipline to one that was exploring increasingly broader use cases.⁹ In 1985, David Chaum, an American computer scientist and cryptographer, revealed an electronic cash system that used cryptography to ensure anonymity to its users, which Chaum described in an article entitled "Security without identification: Transaction systems to make big brother obsolete".¹⁰ Four years later, Chaum founded DigiCash, an electronic payment company that allowed its users to conduct online transactions in a completely secure and anonymous way by utilising the latest developments of public and private key cryptography.

While his company was ultimately unsuccessful (a good example of being too early), Chaum's work arguably laid the foundation for blockchain and cryptocurrencies today. Interestingly enough, Chaum made a comeback in 2018 with a new project called Elixxir,¹¹ which was followed a year later by Praxxis.¹² I had the opportunity to interview Chaum for an episode of my FinTech Capsule® episodes (available on my YouTube page).¹³ The 1990s saw the rise of the Cypherpunk movement, ushering in the first formal steps towards the creation of cryptocurrencies. Chaum's work had greatly inspired three retired professionals—Eric Hughes, Timothy C. May, and John Gilmore—who were passionate about computer science, mathematics, and cryptography. Using Chaum's studies as a starting point, the trio began discussing these topics during regular meetings in San Francisco, which rapidly evolved into a full movement, the Cypherpunks, which advocated for cyberspace freedom, reaching a broad audience of about 2,000 people by 1997 through the “Cypherpunks Mailing List”.¹⁴

As described in “A Cypherpunk’s Manifesto”,¹⁵ published in March 1993 by Eric Hughes, the goal of the Cypherpunks was to give privacy and freedom back to individuals. To facilitate conversation between individuals and organisations, Hughes suggested creating systems allowing anonymous transactions to occur.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak.—The Cypherpunk Manifesto

As the years went by, the Cypherpunks developed several projects with features that can now be clearly recognised as predecessors to Bitcoin and other cryptocurrencies. The two most notable examples are Hashcash,¹⁶ proposed in 1997 by Adam Back, and B-money,¹⁷ proposed in 1998 by Wei Dai. Hashcash was designed to reduce the impact of email spam by attaching a digital stamp to each email. The stamps essentially required the spammer's central processing unit (CPU) to do some work for the email to be successfully delivered, which as a result would make spam uneconomical, as spammers need the ability to send huge volumes of emails at very little or no cost. B-money, meanwhile, was an essay with two proposals for an anonymous and distributed “scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst

themselves without outside help".¹⁸ Whilst these projects had limited success, each was later referenced in the original Bitcoin whitepaper, showing the distinct influence they had.

2 The Bitcoin Whitepaper

2.1 The Role of Cryptography in Bitcoin

Let's get back to what Satoshi wrote in his whitepaper:

We define an electronic coin as a chain of *digital signatures*. Each owner transfers the coin to the next by digitally signing a *hash* of the previous transaction and the *public key* of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership. The problem of course is the payee can't verify that one of the owners did not double-spend the coin.

Focus for now on the public key, and as we learned earlier, your private key enables you to come up with a public key. But remember, this is a one-way street. Whilst your private key enables you to come up with your public key, it's impossible to use the public key to deduce the private key (except one day with quantum computers, but more on that later). My favourite analogy to explain how a public key is derived from a private key is the one used by Canadian blockchain commentator Don Tapscott in an interview subsequently picked up to comedic effect by U.S. talk show host John Oliver. Tapscott compares the process to Chicken McNuggets, noting that it is easy to turn a chicken into a McNugget, but very difficult to turn the McNugget back into a chicken.¹⁹

What is a digital signature? In the traditional world, one would sign a check or a receipt to make it valid. We know that faking a signature made by hand is ridiculously easy, especially since you always use the same signature and it's somewhat comical that we still ask for handwritten signatures these days. In the crypto space, anyone who can see your public key can verify that the signature was created by the holder of the associated private key without needing to know the private key itself. To continue with our McNugget example, it would be like knowing that a specific McNugget comes from a specific chicken, but without revealing the chicken's secret name. A comical analogy, but hopefully it serves the point, and because the signature is valid for a specific transaction, it cannot be copied and pasted on another piece of data without the signature being invalidated. If one were to take the signature

on the above McNugget and put it on a different McNugget by a different chicken, the signature would be invalid. This is not done by a subjective judgement call, but rather by mathematics.

Moving on to the hash. As mentioned by Satoshi, it's the hash of the transaction that's signed, not the transaction itself. But what exactly is a hash? A hash is an algorithm used in cryptography that takes an input of any size and returns a fixed-length sequence of numbers. This is important as regardless of the length or the size of the data, you will get a fixed size hash. A hash can be generated from any piece of data, but the data cannot be generated from the hash. It only works one way, you cannot guess the input by looking at the hash, and if even a very minor change is made in the data, the hash will be different (Fig. 2).

The SHA-256 (Secure Hash Algorithm) is a good example of an industry standard hash function. Originally designed by the National Security Agency (NSA), it's used in various places in the Bitcoin network. When it comes to Bitcoin transactions, you're in practice using your private key to sign the

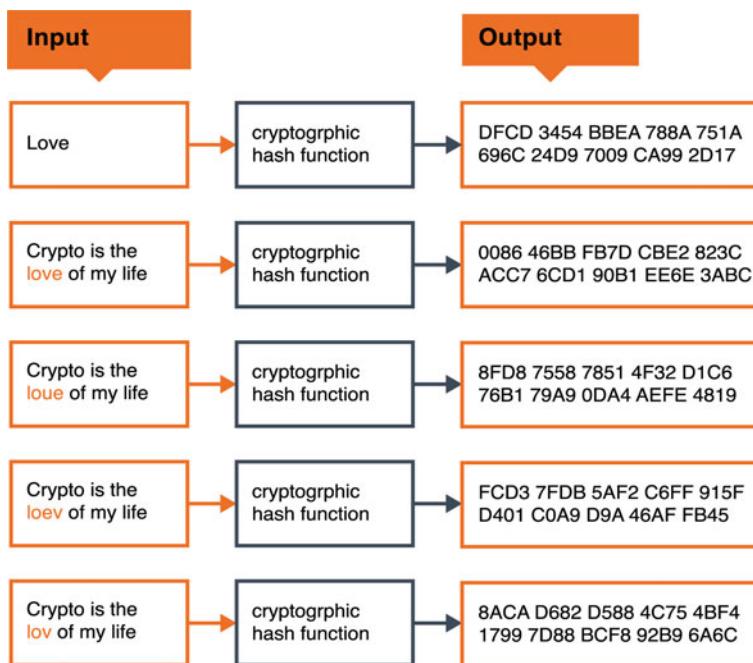


Fig. 2 Outputs of an illustrative Hash function. A hash function takes inputs of any size and creates a random output of uniform size and no relationship to the input; even very similar inputs have very different hash outputs (Source “File:Hash Function Long.Svg - Wikimedia Commons,” Wikimedia Commons, accessed January 1, 2022, https://commons.wikimedia.org/wiki/File:Hash_function_long.svg)

hash of the transaction (not the transaction itself), which enables you to have a small signature even if the underlying data behind the hash is huge. This is what proves ownership to others in the network as they know that it's the person with the right private key who signed the transaction. There are many articles and literature online on hashes and their history for anyone interested.

While the above solves the ownership problem, it does not solve the double-spend issue. As Satoshi writes in his white paper:

The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank. We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions.²⁰

As mentioned, the double-spend issue is dealt with in the traditional world by having banks and other trusted central authorities, but how can we have this in a decentralised world? This is the innovative contribution that Bitcoin made.

2.2 The Role of Decentralisation in Bitcoin

While we could deal with the double-spend issue by having a network of bookkeepers, we would also need a "master bookkeeper" or some type of gatekeeper (a good analogy are standard setters in the accounting profession today or law societies for lawyers). However, this makes the system centralised, so the solution in the Bitcoin network is to allow anyone to be a bookkeeper and to have the same set of books and records as anyone else. These bookkeepers are called nodes. All transactions are broadcast to the various nodes in the Bitcoin blockchain, allowing anyone to see them and update their "books". But then how can we be sure of the order of these transactions? Whilst everyone can see all the transactions, we need to agree on a particular order of transactions. As Satoshi eloquently states:

To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received.²¹

The Bitcoin network does this via blocks. If the Bitcoin network is one massive book, then each block is a page. For everyone to be “on the same page” (no pun intended), the bookkeepers need to know what the last page is and how it reads. It would be like a big book club where nobody moves to the next page until everyone in the group has agreed on what the last page says, or for the Bitcoin blockchain, what each block says (Table 1).

What Is the Bitcoin Taproot Upgrade?

In November 2021, the Bitcoin network went through its first upgrade since 2017. Known as Taproot, the upgrade was poised to deliver greater transaction privacy and efficiency to the network whilst making a huge impact on every participant in the Bitcoin ecosystem, from developers to investors. The Taproot upgrade will improve Bitcoin in several ways, paving the way for:

- **Lower fees:** Since the data size of complex transactions will be reduced, transaction fees will decline proportionally.
- **Improved lightning network efficiency:** Taproot will make transactions on the Lightning Network cheaper, more flexible, and more private.
- **Privacy:** Taproot will enhance Bitcoin’s privacy features by implementing a new digital signature scheme known as Schnorr. Using Schnorr, the Taproot upgrade will add smart contract capabilities to Bitcoin that should strengthen privacy. For example, the transactions that open and

Table 1 Key features of bitcoin compared with traditional finance

	Traditional Finance	Bitcoin
Tabulation	Bookkeeper/Accountant	Nodes
Verification	Auditor	Miner
Qualification	Regulated Intermediaries	Anyone
Compensation	Fees (Fiat)	Fees (Bitcoin)

close payment channels on the Lightning Network would not look much different from normal transactions, thus strengthening privacy.

- **Enhanced smart contract functionality:** With Taproot, Bitcoin will be able to host smart contracts with any number of signatories whilst retaining the data size of a single-signature transaction, laying the technical foundation for DeFi on the Bitcoin network.

In order to implement the Taproot upgrade, a “soft fork” of Bitcoin’s code was required. As we will explore later in this book, a soft fork allows software running the old version of the code to still interact with the upgraded version. The last time such an important soft fork took place was the controversial (and still hotly debated) SegWit fork that took place in August 2017, which resulted in the emergence of Bitcoin Cash. But unlike the SegWit upgrade, which focused on making transactions faster and cheaper, Taproot is focused on much more than reducing fees and improving scalability, aiming to increase privacy and security for the broader network. As was the case with the SegWit fork, the Taproot upgrade is expected to be gradually rolled out over the coming years. It’s important to remember that only two years after SegWit went live, nearly 50% of transactions on the Bitcoin network took advantage of the upgrade. Now, four years later, that figure sits around 80%. This may seem like a slow rate of adoption, but it allows crypto wallets and service providers to opt-in at their own convenience.

Unlike a centralised network that can be changed unilaterally, a decentralised network like Bitcoin requires intensive collaboration, coordination, and, ideally, consensus amongst stakeholders to deploy these changes. In order to ensure that the miners were onboard, a very Bitcoin-esque type of voting took place. As of this May 2021, miners who wished to adopt the upgrade could signal their support by including special data in the blocks they mined, referred to as a “signal bit”. In order to lock in the Taproot upgrade for activation, more than 90% of the blocks in the network were required to show their support by “signalling”, which was reached back in June 2021. The Taproot upgrade ultimately represents a significant part of Bitcoin’s history, laying the foundation for several intriguing use cases and developments down the line.

2.3 The Role of Immutability in Bitcoin

How can we ensure that nobody goes back and can change a page of the book? Satoshi suggests that each new page must contain the hash of all the previous pages.

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be time stamped and widely publishing the hash (...). The timestamp proves that the data must have existed at the time, obviously, to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

As we've seen before, even the most minute changes to a piece of data will result in a different hash. Including the hash of all previous pages on every single page makes it difficult to alter the record, since for someone to change a previous page, he will need to change every single page prior to that page. In the Bitcoin blockchain, a new block (or an official page of the book in our analogy) is created approximately every 10 minutes and added to the chain, ensuring that when any new piece of information is added to the blockchain, it becomes immutable.

But if everyone will be using the same book and nobody will move forward until we have all agreed to the last page's content, then who will decide what that last page will contain? We could have a "master" editor or master book-keeper, but that would make the system centralised once again, defying the purpose of Bitcoin. This is when proof-of-work comes in.

2.4 The Role of Proof-of-Work in Bitcoin

The proof-of-work mechanism is the secret sauce of the Bitcoin network. Satoshi sets it out as follows in the Bitcoin whitepaper:

The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.²²

This process is known as "mining" and involves four separate pieces of data: a hash of transactions on that block, the hash of the previous block, the time, and a number called the nonce. A nonce is a random number separate from the transactions established on that block. A "miner" will take these four variables and hope that the hash output will meet the requirement of the

number of starting zeros, called the golden hash. The miner can begin with a nonce of 0, try a nonce of 1, then a nonce of 2, etc. The more nonces a miner can test, the more chances the miner has to find the “golden hash” that meets the requirements and will allow him to add that block to the Bitcoin blockchain.²³

To be more specific, every miner needs to hash the header of each block in such a way that it is less than or equal to the golden hash (also referred to as the target). The target, at the time of writing, is that the block’s header must be a 256-bit alphanumeric string and must start with eighteen zeros. This difficulty level changes every 2,016 blocks, which translates to about two weeks. For example, it was easier to mine the first-ever block, the genesis block, of the Bitcoin network, as the target only had to start with 10 zeros.²⁴ A miner can achieve this by varying a small portion of a block’s header by trying different digits until he gets the desired result. Finding the correct hash is a matter of luck and trial and error by trying various nonces and getting different hash results. The number of times a hash is being experimented upon is called the hash rate (to be discussed later in this book), and the process is very energy-consuming.

To return to our bookkeeper analogy, the miner would be the equivalent of an auditor determining the correct last page of transactions (the block) and the bookkeepers will use that to add their new transactions until the auditors confirm another page. But for an auditor to determine that his page will become part of the official book, he would need to throw a pair of dice, and whoever gets a double six would be able to add her page to the book. In theory, anyone can become a miner and find the next golden hash; the more different nonces a miner tests, the higher the chances of finding the golden hash and getting new Bitcoin as a reward. The rate at which new nonces are tested is called the hash rate, which is broadly the number of times per second that a computer can run those four variables through a hash function and derive a new hash.²⁵

Miners are compensated and rewarded for their work with Bitcoin if they’re the first one to find the golden hash. That transaction is called the coinbase transaction and is the first transaction of each block. The first rewards for miners were 50 Bitcoin and this amount is halved every 210,000 blocks, which is about four years. For example, the reward went from 50 to 25 to 12.5 to, since May 2020, 6.25 Bitcoin per block.²⁶ The next halving should take place around May 2024²⁷ and the Bitcoin reward amount will continue to be cut in half approximately every four years until the year 2140. After that, Bitcoin miners will only be rewarded with transaction fees, which is why Bitcoin is considered a deflationary currency as the actual inflation rate

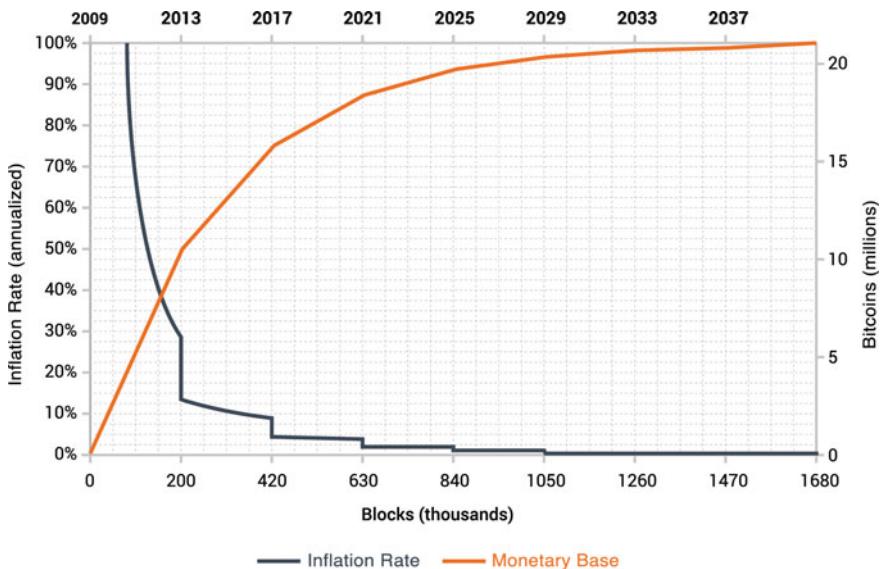


Fig. 3 Bitcoin inflation vs time (Source bitcoinblockhalf.com)

gradually decreases and there is fewer new Bitcoin coming into circulation (Fig. 3).

The purpose of this reward is to compensate miners but also to create new Bitcoin. Following the halving in May 2020, roughly 900 new Bitcoin are created each day (approximately six new blocks per hour \times 6.25 Bitcoin per new block \times 24 hours = 900 new Bitcoin). But this raises an issue: if the secret to getting new Bitcoin is to win at this game of chance, why can't I simply throw a bunch of computers at the problem and increase the mining hash rate? Whilst it may sound appealing, it would cause monetary inflation as it would dramatically increase the supply of Bitcoin, which is why Satoshi added a "self-regulatory" rule in the Bitcoin blockchain where if more computing power is added to the network, the network makes it harder to find the golden hash by adding zeros to the required hash. This is called the "difficulty" and this adjustment is made roughly every two weeks, with a target of miners finding the golden hash in about 10 minutes.²⁸

The difficulty level will constantly adapt. For example, when the hash rate increases (i.e., more people are mining), the difficulty level will go up. Not surprisingly, the level of difficulty is related to the price of Bitcoin, as the more Bitcoin price increases, the more people are interested in mining as the reward is more considerable. Normally, the level of difficulty goes up as the price of Bitcoin goes up and the increased upside in the value of Bitcoin received as a

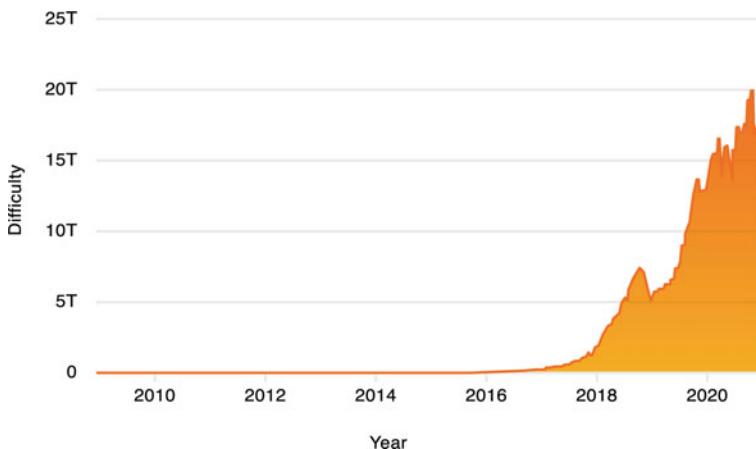
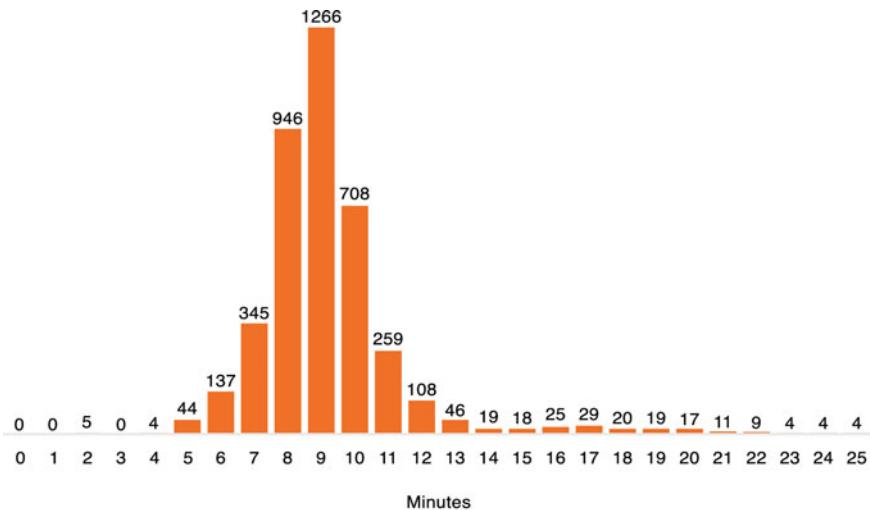


Fig. 4 Level of Bitcoin mining difficulty (Source BTC.com)

reward makes the activity even more profitable, something that we'll discuss later in this book when going in-depth into Bitcoin mining (Fig. 4).

For many years when teaching crypto in my university courses or executive training, I've been using the analogy of Bitcoin mining being the equivalent of someone throwing dice with the hope of getting a double six and being the winning miner. I find it to be very effective as it really shows the element of randomness. I normally invite three students in front of the class, give them a post-it and ask them to note transactions that I say out loud to show them the role of a node. I give them each a pair of dice and ask them to throw them until they get a double six (mining). Once a student gets a double six (the lucky Bitcoin miner), I stick their post-it on a series of blocks borrowed from my kids that I hold in my hand to show how that mined block becomes part of the blockchain (new block on the blockchain). And finally, to show the importance of the difficulty level adjustment, I will give one student a dozen dice and show how much faster they can get a double six compared to their peers with just one pair (more mining machines equals higher chances of finding the golden hash). Approximately every 10 minutes, a new block is added to the chain, which is where the origin of the word blockchain comes from, although it's noteworthy that Satoshi never used the word "blockchain" in the Bitcoin whitepaper (more on this later). As we can see, "The network is robust in its unstructured simplicity. Nodes work all at once with little coordination"²⁹ (Fig. 5).

In theory, anyone can connect to the Bitcoin network, download past blocks, keep track of new transactions, and try to crunch data to find the golden hash, which is a key benefit of the Bitcoin network.³⁰ However,



*Data as of March 2020
Block times greater than 25 min are not featured in this chart*

Fig. 5 Average block confirmation times. Data as of January 1, 2022. Block times of greater than 25 minutes are not featured in this image (Source Coin Metrics)

mining Bitcoin in the pursuit of a golden hash has now become extremely difficult and simply plugging in your laptop and hoping to find the golden hash is very unlikely. The technology used for mining has evolved relatively quickly from CPUs in computers and graphical processing units (GPU) in graphic cards to application-specific integrated circuits (ASIC). To put things in perspective, some of the best ASIC devices available on the market at the time of writing have hash rates of over 50 TH/s, allowing you to crunch data and output a hash 50 trillion times a second.³¹ (Imagine throwing those dice at that speed!) Many of these mining operations are also located in places with cheap electricity, as mining operations today consume a lot of energy. We'll explore Bitcoin and crypto mining later in the book.

3 The Growth of Bitcoin

The first documented purchase of goods through Bitcoin can be traced to May 2010. On May 22, Bitcoin enthusiast Laszlo Hanyecz posted online a receipt of his successful Bitcoin transaction: two pizzas for 10,000 Bitcoin, the equivalent of US\$41 at the time.³² Less than a decade later, those 10,000 Bitcoin are now worth hundreds of millions, arguably making it the most expensive pizza order ever. May 22 is now celebrated by many in the global

crypto community as “Bitcoin Pizza Day”. A fun fact is that when Laszlo posted his initial offer of 10,000 Bitcoin for two pizzas, he didn’t get any offers, so he posted another message wondering whether the amount of 10,000 Bitcoin was too low. The entire message trail is available online on Bitcointalk.³³

Where does the Bitcoin Logo Come From?

Have you ever wondered where the Bitcoin logo comes from and who developed the concept? And why did they settle on such a vivid shade of orange? The story of the Bitcoin logo has twists and turns, but it’s somewhat fitting for the crypto space and its passionate community, a saga filled with rivalries, factionalism, and competing sets of logos

The earliest iteration of the Bitcoin logo can be traced back to the digital asset’s enigmatic creator, Satoshi Nakamoto, and featured a rather minimalist design, nothing more than a “BC” emblazoned over a gold coin. When this was released in 2009, users on the popular forum Bitcointalk seemed split on the concept, with some arguing that the adoption of a logo was entirely unnecessary and was antithetical to the true spirit and ethos of the budding cryptocurrency movement. They maintained a logo skirted uncomfortably close to centralisation, and one year later, Satoshi unveiled a new design, dumping the “BC” in favour of the now-ubiquitous “B” with vertical strokes. Whilst this symbol was better received than their first version, some Bitcointalk users remarked that it nevertheless too closely resembled the Thai baht symbol and could lead to confusion, despite the Thai baht only having one vertical stroke as you see in the image below

By the end of 2010, however, Bitcoin’s logo would evolve into something much more easily recognisable today and can be traced back to user “bitboy” on Bitcointalk. Vividly rendered and slightly askew, bitboy managed to completely transform Bitcoin’s visual identity in a single swoop. Comments appeared to suggest that the logos for Mastercard and Visa heavily inspired the design, with bitboy remarking:

The irony is as much as I hate [Mastercard] and [Visa], it is all about perception when it comes to consumer confidence and behaviour. Lol.

Yet whilst bitboy’s bright orange logo proved to be a hit, many within the Bitcoin community continued to maintain that the logo was self-defeating. Rather, a currency like Bitcoin, they argued, should be represented by a universal symbol like \$, €, or ¥. Supporters of this argument eventually pushed for the adoption of B, which is featured in multiple alphabets around the world. For example, B is used as a phonetic symbol to represent and transcribe the sound [β] and is a letter of the alphabets of the Rade, Jarai,

and Katu languages of Vietnam. Obviously, this parallel symbol didn't gain any traction, with bitboy's neon, off-kilter "B" growing in popularity over the years, helping to drive both the adoption of Bitcoin as a digital currency and store of value along with a surge of demand for Bitcoin-themed merchandise and apparel. It's another fun piece of the history of money!

Over the last decade, Bitcoin steadily began gaining momentum, experiencing a vital boom at the end of 2013³⁴ when its price rose to about US\$1,000. But just when things seemed to be taking off, the price began to fall and continued to experience a steady decline, plummeting back to about US\$200 over the next two years. Those were difficult times for the Bitcoin community due to many public events, including the association with the Silk Road marketplace arrests, as well as the hack of a Bitcoin exchange called Mt. Gox.³⁵ However, the usage of Bitcoin increased with the number of confirmed daily Bitcoin transactions almost doubling every year reaching over 100,000 by 2015.³⁶

What is Silk Road and its Connection to Bitcoin?

The "Silk Road" marketplace, founded in 2011 and shut down by the FBI two years later, was an online platform founded by Ross Ulbricht.³⁷ The website essentially used Bitcoin for money laundering transactions, drug sales, and illegal activity. Designed as a free and open marketplace, Ulbricht's platform used Tor, a network that ensures the anonymity of its users' data and Bitcoin was the primary form of currency facilitating these transactions. At its peak in early 2013, Silk Road accounted for nearly 20% of all Bitcoin activity. Eventually, the website was shut down after the FBI caught up with the network, and its founder sentenced to two life sentences and 40 years without parole. The story of the arrest by law enforcement has been well documented in the media and in a documentary,³⁸ and is probably worthy of a Hollywood movie.³⁹ To this day, many believe the sentence disproportionate and have launched a campaign to support him⁴⁰

Whilst the Bitcoin community had nothing to do with Silk Road (in the same sense that the Federal Reserve is not associated with crime because drug dealers use U.S. dollars), this was seen as one of the main uses of Bitcoin by the media and to the general public, and unfortunately led to a negative perception of Bitcoin and other crypto-assets. However, and as we will discuss later in this book, it's unwise to conduct illegal transactions using Bitcoin, because whilst transactions can be difficult to trace back to their user, all transactions are recorded in the Bitcoin ledger (unlike cash).

There are numerous examples in the media of academics (and of course, law enforcement) successfully identifying individuals who sent Bitcoin for such purposes,⁴¹ and numerous crypto traceability firms (e.g., Chainalysis, Elliptic, Ciphertrace) have made a business of this.⁴² However, these solutions didn't exist during the years of Silk Road, potentially giving a false sense of security to the Silk Road operators and clients. In many recent cases, like the case of a paedophile ring in Asia in 2019, the visibility of Bitcoin transactions was the main reason the criminals were even apprehended.⁴³ Today the usage of Bitcoin in 'dark web' transactions represents less than 1% of transactions of total Bitcoin transactions (down from 30% in 2012).⁴⁴ I often joke that if someone wants to buy drugs or conduct any illegal activity, they should use cash and not Bitcoin, as chances are very high they'll eventually get caught with the tools we have today (and that are improving every year), as we'll discuss later.

The Mt. Gox Scandal

Mt. Gox, a former Tokyo-based Bitcoin exchange that allowed people to trade Bitcoin for cash, launched in 2010 and met its end four years later after it shut down, filed for bankruptcy protection, and eventually faced liquidation. The exchange was originally built to trade the fantasy-based game cards Magic: The Gathering, resulting in the abbreviation "Mt. Gox" from "Magic: The Gathering Online eXchange". By 2013, it was handling around 70% of the world's Bitcoin trading when it was hacked for US\$473 million⁴⁵ in a breach that was a massive setback for the momentum Bitcoin had been gathering. Not only did the hack have adverse effects on the price of Bitcoin, but it also had a far-reaching impact on the broader crypto ecosystem as well. With so much having gone wrong with Mt. Gox, it's safe to say that it was not built with top-class security and governance frameworks in mind. By 2014, Mt. Gox halted all withdrawals and ended up filing for bankruptcy protection.⁴⁶ The court proceedings on Mt. Gox are still ongoing at the time of writing

Following these events, the tide started slowly turning in favour of Bitcoin and the broader crypto ecosystem. In the early days of crypto-assets, those who dabbled in cryptocurrency were a niche group of individuals, ranging from experienced cryptographers and geeks to developers and libertarians. It's important to mention the role that the libertarian movement played in the growth of Bitcoin in the early days. Whilst many with a cryptography or

technology background were attracted to Bitcoin due to its technical features, a significant portion came from the libertarian circles in the United States and beyond.

How Did I Discover Bitcoin?

A question I often get asked is how I first discovered Bitcoin. I first learned of Bitcoin in 2013 and organised my first Bitcoin event in March 2014. At the time, I was living in Hong Kong and working for the Swiss investment bank UBS. I was already very passionate about the future of finance, the changes that were starting to disrupt finance and what would then be known as FinTech. As one of my many “side roles”, I was also the President of the Armenian Community of Hong Kong and China. In late 2013, we were in the process of revamping our website and my volunteer CTO was a fellow Armenian living in Hong Kong named Raffi. Unbeknownst to me, he’d been mining Bitcoin since 2011, when Bitcoin was \$30, before selling them when the price hit \$300, thinking he had done great by multiplying his investment by 10 in the matter of months. At the end of one of the endless negotiations on pricing with the developers for the new website of the Armenian Community of Hong Kong and China, Raffi asked if they accepted Bitcoin. At the time, I remember being angry at him as I thought it was a stupid question after what was a great negotiation, but it made me curious and I started researching the topic.

I wanted to know whether others were also interested in Bitcoin and were at least as curious as I was on the topic. An opportunity would arise a few weeks later, in January 2014, after reading an article in Hong Kong’s South China Morning Post newspaper about this young French banker called Aurelien Menant, who had just left a French investment bank to launch one of Hong Kong’s first crypto exchanges, Gatecoin. I got in touch with Aurelien and we met for coffee in Hong Kong’s iconic IFC building, hitting it off and agreeing that more people needed to hear about Bitcoin. I was then co-chair of the Financial Services Committee of the Canadian Chamber of Commerce and used that opportunity to organise an event in March 2014 called “Bitcoin: Disrupting Financial Transfers” where I invited Aurelien to be guest speaker (in what was his first-ever public keynote). I had fallen into the crypto rabbit hole and have been passionate about the space since. I left UBS in 2015 to focus exclusively on FinTech and have been focused 100% on crypto since 2017 when I launched the crypto team at PwC (which is another story all together).

The landscape started to change quickly in 2015 and 2016 as more and more individuals became interested in cryptocurrencies, from university students day trading in their dorm rooms to early adopters who chose to invest a portion of their diversified portfolio in this new asset class. The year 2017 will be remembered as a game-changing year for Bitcoin and the broader crypto ecosystem.⁴⁷ Bitcoin's price hit US\$10,000 in November 2017—a new high that would have been unthinkable only a couple of years back. But the frenzy continued, with Bitcoin's price reaching nearly US\$20,000 towards the end of December 2017. Suddenly, Bitcoin was being discussed regularly on media platforms like Bloomberg and CNBC, which generated massive amounts of global buzz in the crypto space (Fig. 6).

Many retail and institutional investors also started paying attention to and becoming more and more involved in crypto-assets. People began discussing Bitcoin at the dinner table and family gatherings. For example, U.S.-based exchange Coinbase opened over 100,000 new accounts over the 2017 Thanksgiving holiday,⁴⁸ and demand was so high that many exchanges had to stop taking on new clients or were flooded with requests, and crypto exchange Binance opened 250,000 new accounts in just an hour after it reopened its platform in 2017.⁴⁹ All this activity led to more acceptance of Bitcoin with merchants as well, with the online travel booking platform Expedia allowing



Fig. 6 Historical price of Bitcoin (October 2013–January 2022). The value of bitcoin has appreciated significantly but has also exhibited extreme volatility (Source “BTC-USD Historical Prices | Bitcoin USD Stock - Yahoo Finance,” Yahoo! Finance, accessed January 1, 2022, <https://finance.yahoo.com/quote/BTC-USD/history/>)

users to book some hotels via Bitcoin and Microsoft allowing users to buy content from Windows and Xbox stores with Bitcoin.⁵⁰ Professional services firms, from law firms to accounting firms, started setting up specific crypto teams. My favourite development (and one that my colleagues and I were involved in) was to have PwC's Hong Kong office accept its first Bitcoin payment in 2017 for advisory services.⁵¹ The year 2018 was a different story as the price of Bitcoin and many other crypto-assets fell substantially in what would come to be called the "crypto winter". Bitcoin closed the year at slightly over US\$4,000, far from the highs it saw in 2017, reviving the debate between Bitcoin believers and its sceptics. For example, Nobel laureate Nouriel Roubini gave a presentation at a U.S. Senate Committee in which he referred to Bitcoin as the "mother of all scams".⁵² Others took a more nuanced view; Christine Lagarde, who was then managing director of the International Monetary Fund, mentioned that it could change how people save and invest. Meanwhile, CFTC Chairman Giancarlo went in front of the Senate Banking Committee and said that "we owe it to this new generation" to give Bitcoin and virtual currencies more attention after seeing his own children's interest in Bitcoin. His opening remarks, which would later earn him the nickname "Crypto Dad", read as follows:

It strikes me that we owe it to this new generation:

To respect their enthusiasm about virtual currencies with a thoughtful and balanced response, not a dismissive one.

To crack down hard on those who try to abuse their enthusiasm with fraud and manipulation.

To thoroughly educate ourselves – and the public – about this new innovation.

To make good policy choices and put in place sound regulatory frameworks to reduce risk for consumers."⁵³

Only 32% of Millennials Own Stocks. But 17% Own Bitcoin?

According to a 2021 survey by Gallup almost half of Americans (45%) do not own any stocks.⁵⁴ Various factors like household income, education, and race all play a role in the likelihood of owning stocks, but one interesting variable that pops out is age: over two-thirds of millennials do not own any stocks (Table 2).

These figures ultimately illustrate that nearly half of all Americans missed out on the stock market rally following the record levels of quantitative easing during the COVID-19 pandemic, leaving most gains in the hands of older,

Table 2 Stock ownership among key U.S. demographics

Stock Ownership Among Major U.S. Subgroups, 2021	Yes, own stock %	No, do not %
U.S. adults	55	45
Men	58	42
Women	52	47
18-29	32	68
30-49	59	41
50-64	66	33
65+	58	41
Non-Hispanic White adults	64	36
Non-Hispanic Black adults	42	58
Hispanic adults	28	72
Postgraduate	85	14
College graduate only	77	23
Some college	54	45
No college	33	66
\$100,000+	84	15
\$40,000-\$99,999	65	35
<\$40,000	22	77
Republicans	61	37
Independents	51	49
Democrats	56	44

whiter high-earners. But whilst stock ownership is going down, the situation seems to be the opposite for crypto. From 2018 to the end of 2019, the number of Americans who owned cryptocurrencies nearly doubled from 7.95% to 14.4%, an 81% increase over a single year according to research from Finder⁵⁵ (Fig. 7)

Unlike traditional stocks, crypto seems to be the favourite of millennials, with 17.21% of millennials claiming to own crypto and only 2.24% of baby boomers saying the same. I guess age matters when it comes to love for digital assets.

The year 2018 also saw institutional players enter the crypto space. Fidelity Investments, which administers more than US\$7 trillion in client assets, announced a new and separate entity called Fidelity Digital Asset Services to provide crypto custody and execution and Nomura formed a partnership with France's Ledger to provide custody to its institutional clients.⁵⁶

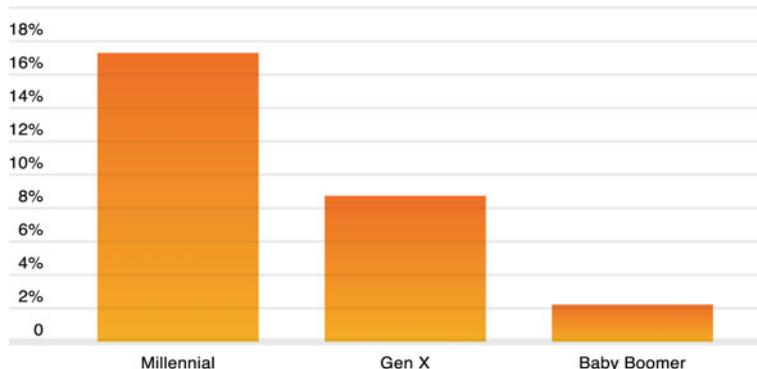


Fig. 7 Levels of crypto ownership by generation (Source Richard Laycock and Catherine Choi, "A Rising Number of Americans Own Crypto," Finder, June 14, 2021)

The year 2019 saw the crypto industry witness the thawing of the “crypto winter” and the beginning of the “crypto spring” with the price of Bitcoin recovering to over US\$10,000. Numerous institutional announcements took place, from J.P. Morgan announcing its JPM Coin⁵⁷ to Julius Baer looking to offer access to its clients.⁵⁸ However, the earthquake in 2019 would be Facebook announcing the launch of its Libra cryptocurrency,⁵⁹ becoming a catalyst and putting crypto-assets on the agenda of every policymaker, financial institution, and regulator.

Perhaps catalysed by this development, China’s central bank, the People’s Bank of China, announced that it was looking at launching its digital currency electronic payment (“DCEP”), commonly referred to as the digital yuan, something it had been researching as early as 2014.⁶⁰ These two developments are covered in detail later in this book.

By the time 2020 came around, most expected that the industry would continue its gradual evolution. However, COVID-19 and the subsequent economic crisis ironically acted as a massive catalyst for Bitcoin and the entire crypto ecosystem. Whilst Bitcoin fell in the first half of the year, even falling under US\$5,000 in March 2020, it quickly rebounded and hit its then all-time high of nearly \$20,000 later in the year.

What Are the Patoshi Patterns?

Due to the public nature of the Bitcoin blockchain, we can analyse the patterns of the very early Bitcoin miners. One pattern that stands out (called the Patoshi Pattern) is attributed to Satoshi and was developed by blockchain researcher Sergio Demian Lerner.⁶¹ The evidence is centred around something called the ExtraNonce. The ExtraNonce is not part of the Bitcoin protocol, in that it is not part of the consensus rules, nor is there a formal specification about how to interpret the field. The ExtraNonce is an area in the coinbase transaction (i.e., a new Bitcoin that is just mined) which can vary after several hashing attempts to provide extra entropy (i.e., randomness) for miners, once the standard nonce in the block header has been used up.⁶² The individual behind that Patoshi pattern (perhaps Satoshi Nakamoto himself) is estimated to have between 700,000 to 1.1 million Bitcoin, of which 99.9% are unspent. In other words, they have never moved since the time they were created.⁶³ The crypto world got excited in May 2020 when 50 Bitcoins that were mined in February 2009, a month after Bitcoin's launch, were transferred to another wallet. This news caused the market to fall, with many fearing that Satoshi could be dumping some Bitcoin. However, whilst these Bitcoins belong to a very early Bitcoin miner, it is unlikely that they belong to Satoshi, based on an analysis of his mining patterns.

The mystery behind Satoshi continues...

The unprecedented levels of quantitative easing from central banks worldwide to fight the economic consequences of the COVID-19 pandemic generated interest from retail and professional investors for inflation-resistant assets, including Bitcoin. Whilst many compared the 2020 Bitcoin rally to the 2017 rally, there were key differences between the two. For example, whilst retail FOMO (fear of missing out) drove the 2017 bull run, the 2020 rally was largely driven by institutional investors. A wave of hedge funds had shown significant interest in entering the crypto space, from Renaissance Technologies and Tudor Investment Corporation to Guggenheim, and in addition, highly visible figures from the investment world, like Stanley Druckenmiller and Ray Dalio, became quite vocal about crypto and even monetary historian Niall Ferguson came out in favour of Bitcoin. Meanwhile, sell-side financial firms began to actively cover the asset class, with Citibank predicting that Bitcoin could pass US\$300,000 by December 2021⁶⁴ and Deutsche Bank predicting that CBDCs would eventually replace cash⁶⁵ with JPMorgan gradually coming around to crypto, and financial institutions and hedge funds increasingly interested in digital assets.

By 2020, there were several regulated ways for hedge funds and other institutional investors to gain exposure to Bitcoin and digital assets, most of which were not available three years ago during the 2017 rally. One example involved the Bitcoin futures listed on the Chicago Mercantile Exchange (CME) in December 2017. By mid-2020, Bitcoin futures on the CME hit a record high. The CME was an exchange with which most buy-side firms were familiar and already trading other assets, and even though CME futures are cash settled (vs “physical” Bitcoin settled), this metric still provided the market with a good barometer of which way the institutional winds were blowing. Another significant example comes from Grayscale Investments, which offered investors a way to gain access to Bitcoin via a listed instrument with its funds surpassing \$10 billion in AUM towards the end of 2020. This was significant, as over 80% of new capital for Grayscale products was reportedly flowing in from institutional investors (Fig. 8).

In addition to this new wave of hedge funds, several companies were now adding Bitcoin to their treasuries and yet whilst institutional players seemed to be driving part of the 2020 rally, the role played by retail investors should not be wholly disregarded. After all, whilst there were only around 6 million people with accounts at crypto exchanges in 2016, the number was over 100 million by 2020 based on data from the University of Cambridge,⁶⁶ another critical factor when explaining the 2020 rally was that it had never been easier to buy Bitcoin.

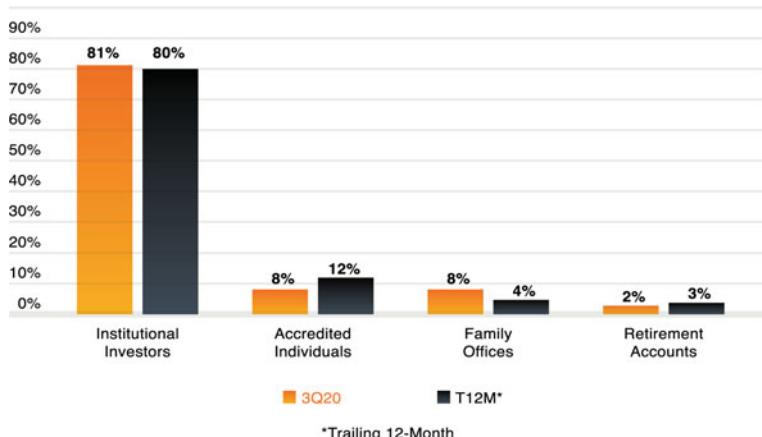


Fig. 8 Grayscale investor profile by type. Institutional investors continued to be the primary source of investment capital in 3Q20 (81%), in line with the investor flow over the T12M (80%). Notably, family offices were a much larger portion of inflows during 3Q20, representing over 8% of the total (Source “Q3 Digital Asset Investment Report,” Grayscale, 2020)

Why are Athletes Falling in Love with Digital Assets?

The year 2021 saw a newfound surge of interest in the cryptocurrency space from some of the top athletes on the planet. The highest profile example of this intersection between sports and crypto came when NFL superstar and seven-time Super Bowl champion Tom Brady revealed that he wanted to get paid in Bitcoin, Ethereum, and Solana. This is hardly Brady's first foray into the crypto space, with the quarterback and his wife, Gisele Bündchen, taking an equity stake in FTX in June whilst signing on as global brand ambassadors for the exchange. Joining Brady is NBA icon Steph Curry, who made quite the splash with his 55 ETH purchase (equivalent at the time to \$180,000) of one of the wildly popular Bored Ape Yacht Club NFTs. Another professional athlete who was an early pioneer in the cryptocurrency world is arguably current Washington Wizards guard Spencer Dinwiddie, who announced in 2019 that he was looking to raise \$13.5 million by tokenising the first year of his three-year, \$34.5 million contract with the Brooklyn Nets.

This outside-the-box approach to professional athlete contract negotiations would provide cashflow to players whilst allowing accredited investors the opportunity to bet on certain players and fans to show support for their favourite athletes. Whilst this idea hit roadblocks with the NBA, it generated a lot of buzz and since then, Dinwiddie has raised \$7.5 million for a token-based app, Galaxy, that allows creators and celebrities to raise money with tokens and interact directly with fans via video messages, online classes, video calls, and fan club subscriptions. Dinwiddie's unorthodox thinking was shortly followed by Lionel Messi when he inked his new contract with Paris St. Germain. The contract contains a provision that allows Messi to receive part of his salary in the French club's fan token, with trade volumes of the PSG token topping out at a whopping \$1.2 billion in trading volume whilst rumours swirled around Messi's pending arrival in Paris.

Top-tier cryptocurrency companies have also become more aggressive in landing sponsorship contracts with professional sports leagues, with FTX securing the naming rights to Miami Heat's arena in a \$135 million deal, followed by the exchange coming to terms with Major League Baseball on an agreement to have umpires throughout the sport wear FTX patches as part of their uniforms. And speaking of uniforms, both StormX and Crypto.com have made major forays into the NBA, with StormX and the Portland Trail Blazers launching a redesigned jersey with the StormX logo and Crypto.com signing a similar deal with the Philadelphia 76ers, so two perennially playoff-bound teams will be displaying prominent advertisements for each firm for seasons to come. Ultimately, sports and crypto are becoming increasingly more intertwined and who knows what the next several years will bring?

In November 2020, PayPal removed its waitlist, allowing 286 million American users to buy, sell, and trade crypto seamlessly and securely, and was reportedly buying 70% of new Bitcoins being mined.⁶⁷ Even though individuals buying crypto via the PayPal app could not transfer their BTC outside the app, PayPal would still need to hedge those client funds, thus generating additional demand on Bitcoin and other cryptocurrencies, and with Cash App reportedly buying the other 40% of new Bitcoin mined,⁶⁸ this could have contributed to the upward pressure on the price of Bitcoin. Finally, the massive levels of quantitative easing (QE) in 2020 generated interest not only from institutional investors but also from the broader public, as the effects of printing record amounts of new money on the value of their cash holdings were being increasingly discussed, not to mention the need to hedge against inflation. By the end of 2020, a consensus had emerged amongst many large financial institutions that Bitcoin was here to stay, and as U.S. bank Wells Fargo mentioned in a December 2020 report, “fads don’t last 12 years”.⁶⁹

The year 2021 would become another game changer for the crypto ecosystem with developments taking place in every corner of the industry and certain new verticals, like decentralised finance or non-fungible tokens (NFT) emerging from the shadows. Many public events would also take place, from Tesla buying \$1.5 billion dollars of Bitcoin on its balance sheet and El Salvador making Bitcoin legal tender to the launch of the first Bitcoin ETF in the U.S.

4 Retail Adoption of Bitcoin

Many different organisations have been trying to accurately determine just how many crypto users there are throughout the world. For example, in 2020, Cambridge University estimated the number of global crypto users at around 100 million⁷⁰ (Fig. 9)

Of course, this was before the incredible bull market of early 2021 that brought crypto-assets back to the forefront, with a report from Crypto.com stating that the total number of global crypto users hit 221 million in June 2021⁷¹ (Fig. 10)

The fascinating thing to consider is that it only took four months in early 2021 for the global crypto population to double from 100 to 200 million. Meanwhile, although Bitcoin drove growth earlier in the year, altcoin adoption by May led to a massive surge in crypto users, from 143 million at the end of April to 221 million in June. Altcoin adoption was likely spurred by the influx of new users interested in tokens like Dogecoin (DOGE) and Shiba

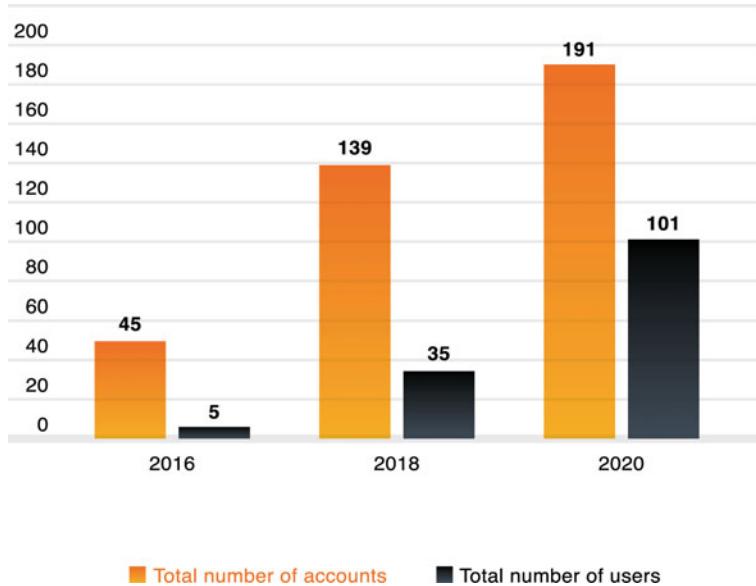


Fig. 9 Total number of crypto-asset users and accounts (Source "3rd Global Cryptocurrency Benchmarking Study," Cambridge Center for Alternative Finance, 2020)

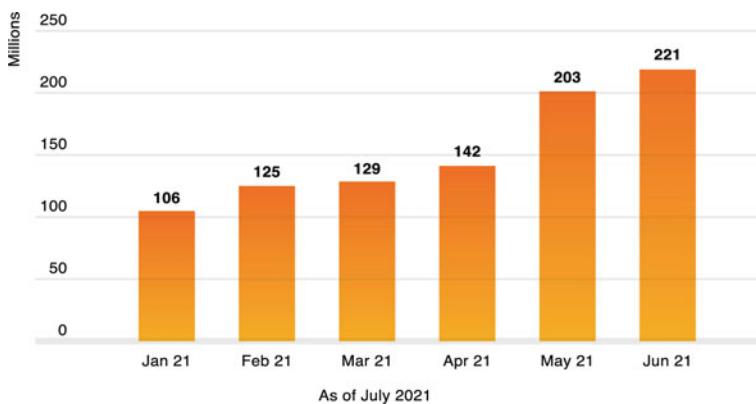


Fig. 10 Global crypto market size over time (Source "Measuring Global Crypto Users: A Study to Measure Market Size Using On-Chain Metrics," Crypto.com, July 2021)

Inu (SHIB), amongst others, contributing to Bitcoin dominance going from almost 70% to 50% (Fig. 11).

Crypto ownership is important, as it demonstrates how quickly adoption is taking place, and in addition, many believe that the Bitcoin usage rate can have an impact on its price. These reports provide a glimpse into just how quickly crypto adoption is taking place at the global level and whilst

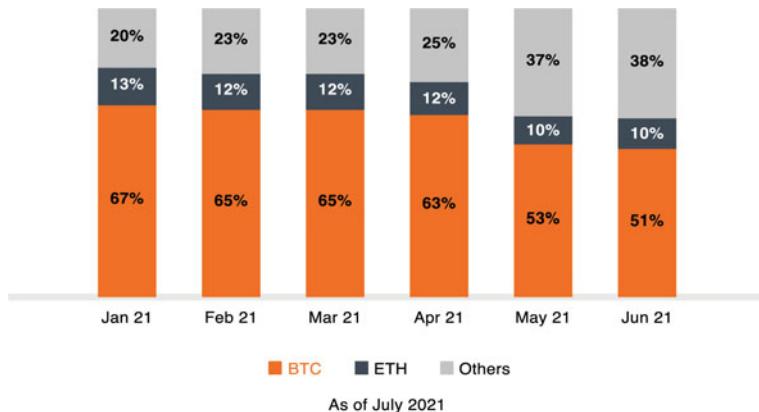


Fig. 11 Percentage of crypto-asset ownership by asset type (Source "Measuring Global Crypto Users: A Study to Measure Market Size Using On-Chain Metrics," Crypto.com, July 2021)

Table 3 Levels of crypto adoption by country

Country	Score	Rank	Rank of individual weighted metrics feeding into index			
			On-chain value received	On-chain retail value received	Number of on-chain deposits	P2P exchange trade volume
Ukraine	1	1	4	4	7	11
Russia	0.931	2	7	8	5	9
Venezuela	0.799	3	19	14	15	2
China	0.672	4	1	1	95	53
Kenya	0.645	5	37	11	57	1
USA	0.627	6	5	6	39	16
South Africa	0.526	7	12	9	41	10
Nigeria	0.459	8	14	7	112	3
Colombia	0.444	9	25	18	61	4
Vietnam	0.443	10	2	2	44	81

Bitcoin has become a global phenomenon, some countries are seeing higher adoption than others. To get to the bottom of this mystery, Chainalysis did an in-depth analysis to study geographical trends in cryptocurrency adoption, usage, and regulation⁷² with on-chain crypto value received, retail value transferred, number of deposits, and P2P exchange trade value metrics used in the report. Which countries came out on top according? Ukraine, Russia, and Venezuela (Table 3).

Both Russia and Ukraine share several factors that typically suggest higher rates of crypto adoption and usage. Trust in government and traditional

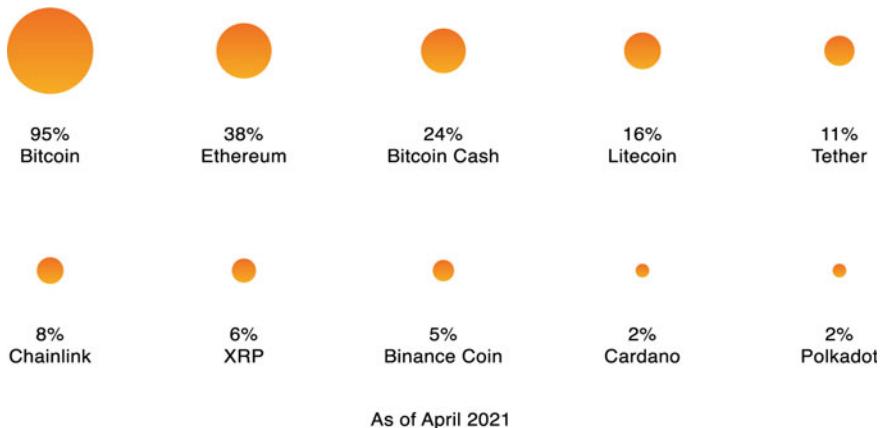


Fig. 12 Most commonly held crypto-assets in the U.S. (Source “The State of U.S. Crypto Report,” Gemini, 2021)

banks is low, whilst consumers in both markets have high familiarity and comfort with e-money and electronic payments. Banks in particular face a lack of trust, with one study finding that 56% of Russians don’t trust banks.⁷³ Ukrainians don’t seem to trust banks either; in recent years, the Ukrainian government has reportedly declared more than 90 banks insolvent, representing roughly 30 per cent of the banking sector’s total assets. Venezuela, on the other hand, is in a situation on its own. With the economic situation deteriorating and the bolivar plunging in value amidst hyperinflation, more and more citizens are turning to crypto to preserve their savings.

The data is interesting in developed markets as well. A survey conducted by crypto exchange Gemini about Americans and their crypto habits in the spring of 2021 showed just how rapidly the American crypto landscape is shifting. The survey splits its focus between current crypto investors and “non-coiners”, or those with no crypto holdings at all. Of the non-coiners, the survey finds that nearly two-thirds classify themselves as “crypto curious”, a strong indication they want to learn more about the space and may plan on participating in the near future.⁷⁴ Yet what’s most fascinating about these non-coiners is the demographic aspect. For instance, whilst only 26% of current crypto holders are women, women account for more than half of the “crypto curious”. Bitcoin is by far the leader when it comes to general awareness of the different types of assets; whilst 95% of the “crypto curious” had heard about Bitcoin, and view Bitcoin and crypto as synonymous with one another, only slightly over a third of those surveyed had heard of Ethereum (Fig. 12).

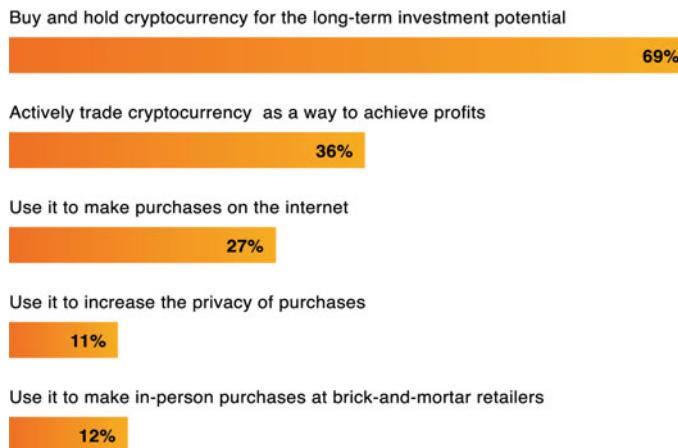


Fig. 13 Key factors behind crypto ownership in the U.S. (Source “The State of U.S. Crypto Report,” Gemini, 2021)

On the other end of the spectrum, most current crypto investors stated that they buy and hold crypto because of its long-term investment potential. Slightly over a third classify themselves as active traders and a minority use Bitcoin and the like as a means of exchange (Fig. 13).

All in all, survey results seem to confirm the growing mainstream appeal of cryptocurrency, with a rapidly expanding appetite for digital assets amongst several key demographics, signalling crypto’s move from “insider status” to something for everyone.

Do the Financially Literate or Illiterate Own More Bitcoin?

An interesting report published by the Bank of Canada mentions that 47% of Canadians have a high level of financial literacy, 35% are at a medium level, and 18% of Canadians show low signs of financial literacy.⁷⁵ The report shows that the more financially literate Canadians were more likely to have heard of Bitcoin and other cryptocurrencies, with 93% of the most financially literate expressing familiarity with digital assets as opposed to only 72% of the low financially literate group. But in a somewhat interesting twist, as financial literacy increased, the likelihood of crypto ownership decreased, with 8% of Canadians in the low level holding crypto compared with only 4% from the high level. Time will tell which camp is right, I guess.

The data is somewhat similar when we look at the UK as well. In the first half of 2021, the UK regulator, the Financial Conduct Authority, conducted an interesting survey that captured how the British population views crypto.⁷⁶ The report is full of fascinating takeaways. First, 78% of adults reported that they had heard of cryptocurrency, a 5% jump over the past year, and unsurprisingly, Bitcoin is the most recognised crypto-asset amongst the public and a whopping 2.3 million adults across the UK hold some form of cryptocurrency, constituting a 0.5% jump. Specifically, we see the median holdings hover around £300, a noteworthy rise from the previous £260, and the typical profile of crypto users in the UK are men over the age of 35. As far as learning about crypto goes, most respondents replied that they first heard about crypto from online news followed by friends and family, whereas new users mainly heard about it via traditional media. When browsing online for crypto resources, Reddit and other online forums have become the main source of research. As for motives behind investing in crypto, most respondents specified that speculation was the driving interest, followed by portfolio diversification. As for how users in the UK acquire their crypto, most respondents confirmed that they continue to use exchanges for their crypto needs, paying for their assets with their disposable income. Interestingly, British consumers have a habit of checking their balances daily, with a significant jump from 13 to 29%, and half the crypto users covered in this survey plan to buy even more crypto in the months and years ahead.

5 Bitcoin as Legal Tender?

The crypto space witnessed a ground-breaking milestone in 2021, with El Salvador becoming the first country in the world to officially recognise Bitcoin as legal tender. The world first caught wind of this development in June 2021, when the President of El Salvador, Nayib Bukele, revealed that he would propose a new law that would make Bitcoin legal tender in the country. Three days later, the law was voted in by a supermajority in the Salvadoran Congress, receiving 62 out of 84 votes, finally coming into force in September 2021. To celebrate this momentous milestone, the country purchased 400 Bitcoin whilst each citizen throughout the country received \$30 worth of BTC in a government-backed digital wallet. Despite a few hiccoughs when the law went into effect, El Salvador's decision to elevate Bitcoin to legal tender status could be an interesting game changer.

El Salvador is a small country of 6.4 million people, over 20% of the population live in poverty whilst 70% remains unbanked,⁷⁷ and around 16% of

the country's GDP consists of remittances coming from abroad, primarily from the United States⁷⁸ What really stands out about this news is that El Salvador is actually a dollarised economy, meaning that the legal tender used every day is not a local currency, but the U.S. dollar. It's one of the few countries in the world in this sort of situation, but it's hardly alone. In fact, Ecuador, Timor Leste, Palau, Micronesia, and several other small countries all rely on the dollar. This development may have an important impact, with several parties benefiting from this forward-thinking move. The new law reinforces Bitcoin's legitimacy, as this is the first time Bitcoin has been recognised as legal tender. Japan came close in 2017 when they recognised Bitcoin as an asset and as a means of payment, but not as legal tender, which has a specific legal definition.

No one stands to benefit more from this law than El Salvador itself, and whilst this development is still sending shockwaves throughout the broader crypto space, there are still several practical issues worth considering. First, if financial inclusion or reducing the cost of remittances was the goal, then why focus on Bitcoin and not stablecoins? El Salvador already uses U.S. dollars and most remittances come directly from the United States. Wouldn't the use of U.S. dollar stablecoins be a better idea as it would have allowed users to avoid the conversion process between dollars and Bitcoin on both sides of the transaction, as well as not expose users to Bitcoin price fluctuations? Let's also not forget the educational efforts needed to explain Bitcoin to the masses in a country that is 70% unbanked. However, it appears that with the levels of quantitative easing and rising fears of inflation, the government saw their embrace of Bitcoin as strategic. Although the excitement hasn't yet worn off, there are a lot of counterparties displeased by this move. As mentioned before, El Salvador relies heavily on remittances from the United States, meaning that this new law could present problems between local banks in the country and their U.S. correspondent banks. Since the law was passed, numerous actors in the global financial sphere ranging from the IMF and the World Bank to JPMorgan and Fitch have subtly tried to pressure Bukele's government into reversing course, citing concerns over macroeconomic stability and Bitcoin's energy consumption as reasons to drop this experiment. The bond rating agency Moody's took things even further when they downgraded the country's rating weeks after the law was voted in.

As for the law itself, the devil will be in the details. For example, the text of the law stipulates prices may be expressed in Bitcoin, taxes can be paid in Bitcoin, and exchanges in Bitcoin will not be subject to capital gains tax, just like any other legal tender. Another important consideration to note is

that in addition to legal tender, merchants throughout the Central American nation will be required to accept Bitcoin as a means of payment if customers opt to use the cryptocurrency in lieu of the dollar. For accounting purposes, meanwhile, the U.S. dollar will be used as the reference currency. Another interesting thing to consider is whether this development will have a snowball effect. We're already seeing countries from around the region, from Panama and Paraguay to Brazil and Argentina, toying with their own progressive Bitcoin ideas, not even including Cuba, which recently confirmed that it will recognise and regulate cryptocurrencies such as Bitcoin, citing "reasons of socioeconomic interest". Time will tell if the decision from El Salvador is just a blip in the history of Bitcoin or an important catalyst in the broader history of money.

What does Legal Tender mean?

Many countries have recognised Bitcoin as an asset or a currency, but what makes El Salvador's recognition of BTC as legal tender different? In 2017, Japan recognised Bitcoin as a means of payment, but they didn't go so far as to call it legal tender. After all, legal tender has a very narrow technical meaning that has no use in everyday life. It means that if you offer to fully pay off a debt to someone in legal tender, they can't sue you for failing to repay. In the United States, the Coinage Act of 1965 states, "United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues".⁷⁹ If you owe a debt to a creditor, then the Coinage Act stipulates that U.S. coins or banknotes are a legal means of payment. But the catch is that there is no federal statute that mandates private businesses or organisations, not to mention individuals, must accept U.S. coins and banknotes for goods or services. Private businesses can set their own policies on what they will and will not accept. A metro line could refuse to be paid in pennies, or, commonly, smaller businesses could refuse large banknotes over a certain amount. The UK is an interesting case in point, where legal tender changes depending on where you are in the country. In England and Wales, Royal Mint coins and Bank of England notes are legal tender, but in Scotland and Northern Ireland, only Royal Mint coins have that designation. There are even restrictions on coins, with the smaller 1-pound and 2-pound coins only used as legal tender for a debt of up to 20 pounds. Everyday means of payments like cheques, debit cards, and contactless e-payments are not legal tender.

Satoshi's Final Message on the Blockchain

On April 23, 2011, Satoshi mentioned in one of his last emails that he has “moved on to other things”.⁸⁰ At the time, Bitcoin was still in its early days. In the summer of 2008, bitcoin.org was registered as a domain name, and that fall, Satoshi’s ground-breaking white paper was released to the public.⁸¹ Months later, the Bitcoin network emerged after Satoshi mined the very first block and around the time his message was released, Bitcoin’s price was still hovering around \$1. In the past decade, Bitcoin has evolved from a niche, close-knit, word-of-mouth project to a global phenomenon, drawing the attention of governments and the biggest corporations, banks, financial institutions, and investors on the planet. The fact that we haven’t heard from Satoshi whilst all this has been unfolding only deepens the mystery.

As far as the context of his final message is concerned, we don’t even know what prompted it. Some theorise that Satoshi’s parting words were a response to an article that appeared in PC World that focused on Wikileaks and its adoption of Bitcoin as a means of navigating its way around a financial blockade imposed by Bank of America, Visa, Mastercard, PayPal, and Western Union.⁸² In response, Satoshi posted the following message on Bitcointalk⁸³:

It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet’s nest, and the swarm is headed towards us.

Others believe it was linked to the fact that Gavin Andresen, one of Bitcoin’s early contributors, was about to attend an event put together by an organisation linked to the CIA. Satoshi wrote in response to that news on April 26, 2011:

I wish you wouldn’t keep talking about me as a mysterious shadowy figure, the press just turns that into a pirate currency angle. Maybe instead make it about the open-source project and give more credit to your dev contributors; it helps motivate them.

Soon after, his final message would appear on Bitcointalk, warning of the risks of a DDoS attack. Whether we ever hear from the enigmatic Satoshi again remains to be seen, but in any event, his name will be forever remembered when it comes to the history of money and finance

We have passed the point of no return with Bitcoin and broader crypto-assets and they are here to stay, but the reality is that there are still specific challenges and roadblocks that need to be overcome before Bitcoin and other crypto-assets become mainstream. We’ll address some of these in the coming pages.

6 Bitcoin as Company Treasury

The role of the treasury in any large company is to manage the firm's cash and other assets and ensure it has the money to manage day-to-day obligations, from paying salaries to buying required goods, whilst also helping develop its longer-term financial strategy and policies. It has been incredible to watch as many companies start to hold Bitcoin and other crypto-assets as part of their treasury, but why are they doing so and how? Let's investigate step by step.

First, when analysing this topic, it's important to draw a distinction between crypto companies and non-crypto companies. Let's start with the crypto companies. It's perhaps not surprising to see crypto companies add Bitcoin as part of their balance sheet, since these are firms involved in crypto, so one would expect them to hold Bitcoin as part of their treasury. For example, crypto exchange Coinbase stated they hold Bitcoin in their treasury as part of their public filings and many other crypto companies like Chainalysis, which does crypto compliance, announced they're now holding Bitcoin on their balance sheet. There are also other companies related to crypto that have Bitcoin as an important part of their strategy. A good example is the mobile payments company Square, which first announced it had purchased over 4,000 Bitcoin in October 2020. The press release that accompanied Square's first Bitcoin purchase went so far as to say that the company viewed crypto as "an investment for economic empowerment".

But what is most interesting is companies not involved in crypto buy Bitcoin as part of their treasury. A good example is electric carmaker Tesla. In February 2021, the New York-listed Tesla announced that it had bought \$1.5 billion of Bitcoin; those 43,000 Bitcoin are worth over \$2.5 billion as of Q4 2021. Another example is Asian gaming giant NEXON, which is listed on the Tokyo Stock Exchange and cited its \$100 million purchase of the digital asset earlier this year as part of a disciplined strategy for protecting shareholder value and maintaining the purchasing power of its cash assets. Let's not forget Asian tech company Meitu, which is listed in Hong Kong and which bought \$40 million of Bitcoin in early 2021, stating in their press release they were buying Bitcoin because cryptocurrencies provide "diversification to holding cash".

The reality is that there are many more companies buying Bitcoin as part of their treasury, but the reality is that only public companies need to make such disclosures and thus why we know about them and can discuss them publicly. The big question is why are these companies all holding Bitcoin? The most common answer is that firms are worried about the risk of inflation,

hyperinflation, and currency devaluation following record levels of quantitative easing we've seen, especially from the COVID-19 global pandemic. These firms deem it prudent, and to a certain extent as part of their fiduciary duty, to put a portion of cash holdings or diversified portfolio in Bitcoin to hedge against such risks. Time will tell if we experience a major inflationary event over the coming years, but if we look at history, such inflationary and hyperinflationary events have happened time and again, as it even occurred when people were using primitive forms of money, like cowrie shells discussed in Chapter 1. They originate from the Maldives, so the supply was limited, but when Europeans started bringing shiploads full of cowries, hyperinflation ensued.

It has also happened when empires started to issue their own currency. In 64 CE, the Roman emperor Nero, thinking nobody would notice, started debasing the denarius, their currency at the time, by reducing the amount of silver and gold in the coins, gradually leading to the collapse of the Roman Empire. It happened to the Chinese in the twelfth century, who had by then invented paper notes, when the overprinting of money from emperor Kublai Khan led to rampant inflation and the collapse of the Khan dynasty. It happened to Spain and Portugal in the sixteenth and seventeenth centuries when the record levels of gold and silver brought from America resulted in rampant inflation; for example, between 1500 and 1600, it's estimated that prices in Spain rose by 400%. It's happened to some modern empires as well. During the French Revolution in the 1790s, the French simply printed more money as they needed to fund the war and their various initiatives. Inflation was so rampant that the price of the ink that would be used to print the banknotes was worth more than the value of the banknotes themselves.

In the eighteenth century, it happened in the United States. In 1775, the U.S. Congress issued the Continental to finance the American Revolutionary War against Great Britain. However, it soon lost its value (thus the American expression "not worth a Continental") and Congress stopped issuing it in 1780. Inflation happened dozens of times in more recent history, with the twentieth century alone having over 50 episodes of hyperinflation from post-war Germany and Hungary to more recent cases in Venezuela or Zimbabwe. Whilst many previous cases of hyperinflation in history were linked to physical war with countries printing money to pay for the war effort, many would argue that this is not too dissimilar to what we're seeing today with the exception that we're trying to fight a global pandemic. The argument of many firms buying Bitcoin is that due to unprecedented levels of quantitative easing, it is prudent to hold some Bitcoin as part of a diversified basket of currencies and assets to hedge against such potential risk.

This is in addition to other reasons firms may have for being optimistic about the future of Bitcoin and its price, from increasing adoption globally to greater regulation. However, whilst this may be a prudent move, there are always risks involved. For example, Bitcoin is still a very volatile asset, so any company adding Bitcoin to their treasury needs to be comfortable with that. Bitcoin is also a new asset and many executives, especially some with more traditional experience, will not necessarily be familiar with it. Ultimately, education is needed to ensure they understand the asset and are comfortable with it. In some countries, there are regulatory considerations as well. In China, for example, buying Bitcoin is simply not allowed. There are also tax and accounting considerations, from the way Bitcoin is characterised from an accounting perspective to ongoing tax uncertainty in some countries. Ultimately, businesses will need to make their own decisions on the pros and cons of adding such an asset to their treasury based on their circumstances. The good news is that it's now definitely possible and there are many easy ways for them to do so if they move forward, from using crypto brokerage firms to crypto exchanges, so don't be surprised to see more companies begin holding Bitcoin and other crypto-assets as part of their treasury in the years to come.

7 Challenges Facing Bitcoin

Despite its many innovations, Bitcoin is not perfect, and I often compare it to the Model T's automobile engine, designed by Ford Motor Company in 1908. Whilst revolutionary at the time, it was relatively slow (about 40 miles per hour),⁸⁴ not much faster than the running speed of a horse. Also, the engine was inefficient, and it was highly energy-intensive and noisy, but we've come a long way since then to today's Tesla electric cars. The crypto industry is going through the same evolution from the Model T to the Tesla but compressed into a dozen years.

How Many Times Has Bitcoin Been Declared Dead?

Bitcoin has been declared “dead” so many times, there’s a website that keeps track. Bitcoin’s “death” can be tracked to Bitcoin Obituary, a parody website that collates news articles and blogs. The digital asset was declared dead nine times in 2021 and 14 times in 2020, but the highest number of “deaths” recorded (124) were in 2017, when its market cap hit \$100 billion for the first time. Interestingly, the first time it was declared dead was when it was worth \$0.23. Bitcoin has even been declared dead numerous times in 2021,

when in January, 82-year-old investor Jeremy Grantham said on Bloomberg that the asset has nil value⁸⁵ (when Bitcoin's price was around \$33,000) and that February, when Bitcoin was worth over \$52,000, Nouriel Roubini argued that Bitcoin's fundamental value is zero.⁸⁶ This drastic divergence of opinions is something we should continue to expect for the coming years, which only makes following this space even more exciting.

Bitcoin currently faces many challenges. For example, its price remains volatile and whilst volatility is great for speculators and traders, it's unsuitable for an asset that can be used as a store of value. People buy blue-chip stocks or gold in part because of their stability. Many hope that as Bitcoin adoption increases and the number of institutional investors grows, volatility will decline, but that's not the case yet. Volatility is also an obstacle to having more widespread acceptance, such as from retail investors or merchants (although, as we will see later, Bitcoin is probably not the best cryptocurrency for everyday payments, in the same way that you wouldn't pay for coffee using bars of gold today). Another issue is legal, regulatory, and especially tax clarity; it's challenging for an asset to gain mainstream acceptance if investors don't know the tax impact for any gain or loss and one needs to have certainty on legal and regulatory frameworks before putting his life savings in that asset.

The good news (as will be discussed later in this book) is that many governments, regulators, and tax authorities are addressing these issues. Many milestones have been reached, but unfortunately this doesn't happen overnight.⁸⁷ Whilst initiatives have been undertaken to solve this matter using hard forks (e.g., Bitcoin Cash), soft forks (e.g., Segregated Witness), or layer 2 solutions (e.g., Lightning Network), this is still an outstanding issue. Thankfully new blockchains have come along that provide alternatives when it comes to scalability and payments.

Bitcoin also faces serious ecological challenges, as mining consumes an incredible amount of energy. As of November 2021, it was estimated that the Bitcoin network was devouring over 180 TWh of electricity annually, which is equivalent to the electricity consumption of Thailand.⁸⁸ This is due to the proof-of-work consensus mechanism, which, as we explored in detail earlier, requires a lot of electricity. This is probably not scalable in any sort of sustainable way, especially as we collectively try to reduce our carbon footprint. The good news is that whilst Bitcoin and some earlier cryptocurrencies use proof-of-work, many of the second-generation cryptocurrencies use other consensus mechanisms (e.g., proof-of-stake) that are much more environmentally friendly. In addition, an ever-increasing percentage of global

Bitcoin mining takes place using renewables and, in many cases, Bitcoin mining can even make renewable energy production more sustainable. We'll explore Bitcoin mining later in the book.

8 The Bitcoin Lightning Network

One of the biggest challenges with the Bitcoin network is that it is not suitable for smaller payments. A new block is created only once every 10 minutes, and transactions can be quite pricey, thus making it unsuitable for smaller transactions. It would be like going to Starbucks and trying to pay with a bar of gold. Enter the Lightning Network. The Lightning Network is a second-layer protocol that paves the way for off-chain Bitcoin transactions, or transactions that are not recorded on the Bitcoin blockchain, whilst allowing transactions that are very fast and cheap. The Lightning Network traces its history back to 2015 when two researchers, Thaddeus Dryja and Joseph Poon, released their paper "The Bitcoin Lightning Network"⁸⁹ with proposals based on arguments about payment channels made by none other than the mysterious Satoshi Nakamoto.

Fast forward six years later, and the Bitcoin Lightning Network has gained a lot of popularity and traction. A lot of this attention stems from the rollout of El Salvador's Bitcoin Law, where, on October 1, 2021, El Salvador's President, Nayib Bukele, claimed that over 2 million Salvadorans had been onboarded to the Chivo digital wallet. Whilst there's no direct correlation between the number of Chivo users and the number of active Lightning users, every wallet holder in the country now can send and/or receive Bitcoin through smartphones using the Bitcoin Lightning network.

How exactly does the Lightning Network work? The Lightning Network enables the creation of a peer-to-peer payment channel between two parties, like between a customer and a shop owner.⁹⁰ Once everything is up and running, the channel lets each party send an unlimited amount of transactions that arrive instantaneously and with almost no fee. In a way, the network acts as a mini ledger for users to pay for smaller goods and services, such as a cup of coffee, without impacting the broader Bitcoin network. In order to set up a payment channel, the sender must lock a certain amount of Bitcoin onto the network.⁹¹ She can then start sending Lightning Network transactions up to the amount of Bitcoin locked. The two parties then can transfer funds between themselves using smart contracts indefinitely, all without the need to record these on the main Bitcoin network. Since every transaction

doesn't need to be approved by the main Bitcoin network, the use of the Lightning Network significantly speeds up transaction times.

Let's look at a practical example.

In Figure 14, we can see that Bob and Alice each chose to fund a side of the channel with 1 BTC. This allows Alice and Bob to start sending payments to one another. First, Alice pays Bob 0.5 BTC, which is deducted from Alice's side of the payment channel and credited to Bob's side of the channel.⁹² After this transaction has been completed, Alice now has 0.5 Bitcoin on her side whilst Bob has 1.5 Bitcoin. Suppose Bob wants to send 0.25 Bitcoin back to Alice. Seeing as how he has sufficient funds in his balance, Bob can send that quarter of a Bitcoin over to Alice, who now has 0.75 Bitcoin,

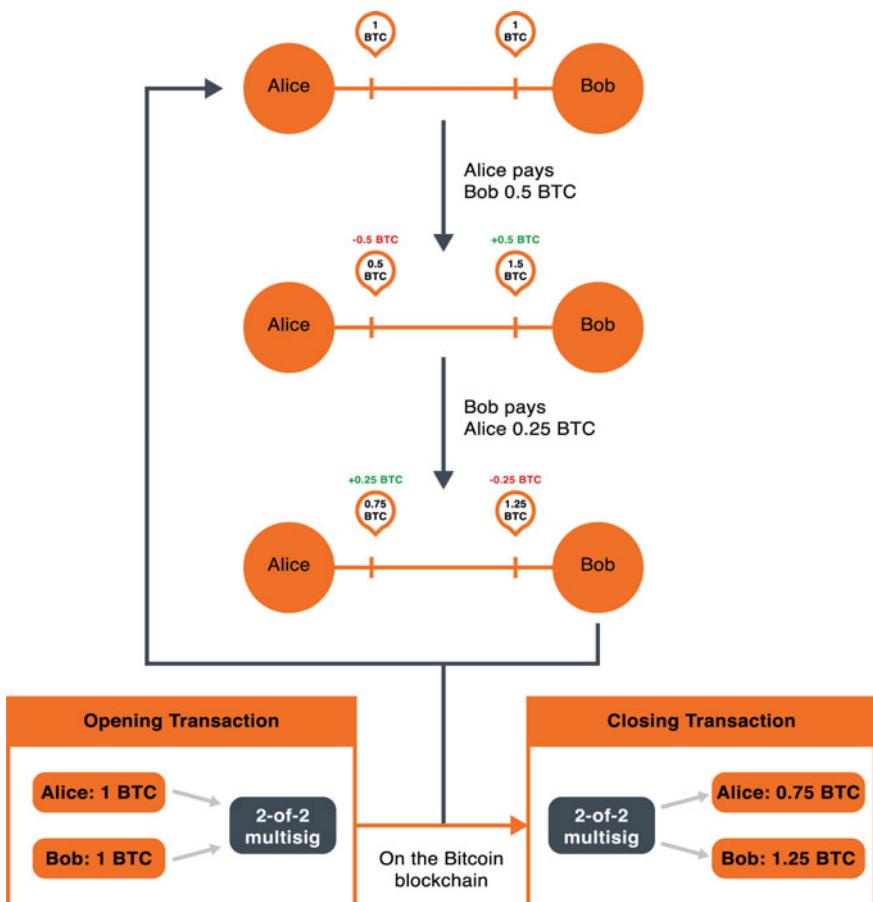


Fig. 14 Illustration of payment channels on the bitcoin lightning network (Source "The State of Lightning," Arcane Research, October 2021)

bringing Bob's total down to 1.25. This back-and-forth process could theoretically continue forever. Now suppose Alice no longer needs to have this payment channel with Bob, leading her to shut things down. Whilst Bob cannot prevent Alice from doing so, he can block her from sending false information to the Bitcoin mainnet blockchain. If Alice attempts to send in a final ledger that shows more than 0.75 Bitcoin on her side of the channel, Bob could easily dispute this, showing how she only had 0.75 Bitcoin remaining after their final transaction. In fact, the Lightning Network has a protocol in place to prevent people from attempting to steal Bitcoin using false and/or misleading statements.⁹³

For instance, if Alice sends incorrect information to the network and Bob proves this information to be false, all funds in the payment channel would immediately be sent to Bob, meaning Alice would lose her 0.75 Bitcoin. In a different scenario, Alice and Bob both agree to close the channel and Alice doesn't try to pull a fast one on the network. In this case, both sign off on a closing statement that shows how much Bitcoin each has. As each party initially locked 1 BTC, the correct closing amount is distributed between the parties.

What about a scenario where both nodes are not connected to each other? This is important as not every node will be connected to every other node on the Lightning Network. This is when the routing mechanism comes in. The act of routing is what makes a transaction between two unconnected parties possible, all through a series of payment channels. For instance, suppose that Alice wants to pay her friend Charlie over the Lightning Network. Unfortunately, Alice doesn't have a direct channel set up with Charlie, but Bob does via John and Sara. The magic of the blockchain allows Alice to send a payment to Bob with the expectation that he will then relay the payment to Charlie via John and Sara, and for the trouble, Bob, John, and Sara will even receive a small fee (Fig. 15).

The routing process is made possible by what is known as Hashed Time-Locked Contracts (HTLC), a specific type of Bitcoin transaction that functions as a smart contract.⁹⁴ HTLCs allow Alice to promise to pay a small fee to Bob only if Bob can prove that he has sent Alice's funds to John and so on. Once Alice and Charlie complete their transaction, they can close the channel. All the channel's information is consolidated into a single transaction, which is then sent to the Bitcoin mainnet for recording. Consolidating all the tinier transactions into one ensures that small payments don't clog up the Bitcoin network at once; rather, simplifying them into a single transaction makes it easier and less time-consuming for the nodes to validate. If it

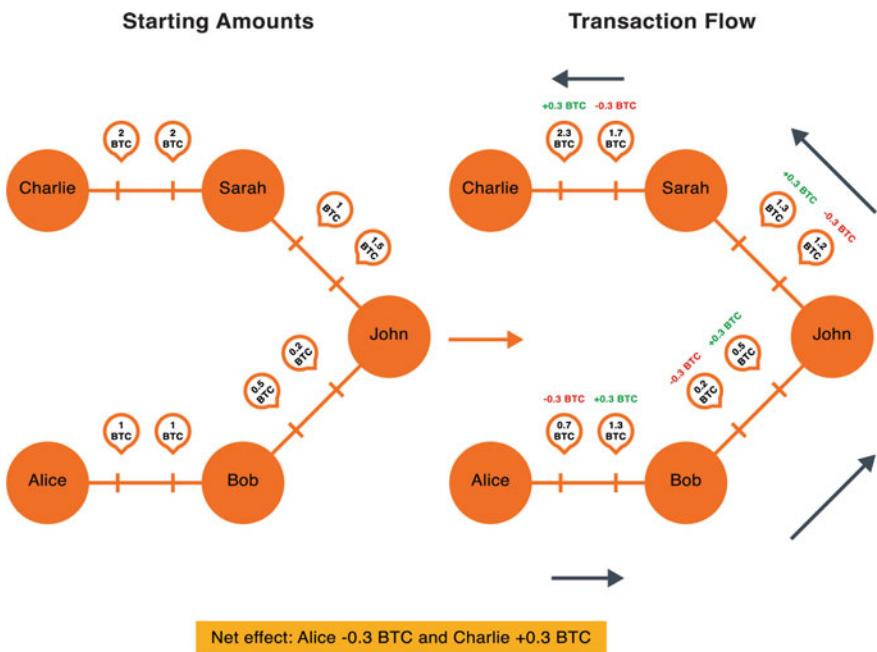


Fig. 15 Illustration of payment channels on the bitcoin lightning network (Source "The State of Lightning," Arcane Research, October 2021)

weren't for the existence of payment channels, in fact, all these small transactions could have a harmful impact, congesting the network and grinding validation times to a halt. Ultimately, what's important to remember is that the Lightning Network provides very significant benefits⁹⁵:

Instant Payments: Without having to worry about block confirmation times, parties can send payments to one another instantaneously, with payment speed measured in increments of milliseconds to seconds. The Lightning Network is capable of being used anywhere in which instant payments are needed, from retail point-of-sale terminals to device-to-device transactions.

Micropayments: The Lightning Network offers the ability for users to send funds all the way down to 0.00000001 Bitcoin without any custodial risk.⁹⁶

Scalability: Transactions conducted on the Lightning Network are not recorded on the blockchain and do not require any delegation of trust or ownership, meaning users can engage in an unlimited number of transactions. The Lightning Network is thus capable of millions to billions of transactions per second.

Low Cost: Because transactions are settled off-chain, fees on the Lightning Network are remarkably low, making the network an attractive option to use for some emerging new use cases, like remittance payments.⁹⁷

Ultimately, the Lightning Network addresses some issues (slow transaction times, scalability) that have affected the Bitcoin network, facilitating instant, low-cost payments between people anywhere in the world. For instance, the technology behind the Lightning Network paves the way for smaller transactions and micropayments to a degree that was never possible before, and if not for the Lightning Network, users would still be stuck paying exorbitant fees for basic transactions whilst waiting several minutes before the transaction is validated. Meanwhile, because the Lightning Network exists as a layer on top of the Bitcoin network, it can take advantage of Bitcoin's security protocols. For example, users can opt to use the Bitcoin network for larger transactions and the Lightning Network for smaller payments without needing to worry about security in either case, and in addition, the Lightning Network offers users the ability to conduct their transactions in private, meaning that observers can't look at each individual payment.

Yet whilst the Lightning Network obviously offers several tempting advantages, there are downsides to be aware of. In order to use the Lightning Network, users first need to find a compatible wallet. Whilst finding a wallet is not difficult by any stretch, funds need to come from a traditional Bitcoin wallet and as the initial transaction between these wallets has a fee, users wind up losing some Bitcoin along the way. Once funds have arrived in the Lightning Network wallet, users need to lock their Bitcoin before creating a payments channel. Meanwhile, if either the sender or the recipient in the payments channel decides to pull any of the funds, they need to close that channel and receive the Bitcoin back before being using it. In other words, it's currently impossible to simply withdraw a bit of the funds without closing the entire channel. Moving Bitcoin back and forth between wallets is, undoubtedly, an annoying and often stressful experience. The fact that this is a prerequisite to using the Lightning Network could lessen the appeal for newer, more casual users. However, there are some wallets that can handle both on and off-chain payments without the need for fees, and if we've learned nothing else about the crypto space over the past decade, it's that bottlenecks tend to be corrected over time.

9 Proof-of-Stake

As discussed above, whilst proof-of-work is an ingenious way to operate the Bitcoin network, it's not energy efficient. There are numerous debates in the crypto community as to whether there are other consensus mechanisms that could be used to validate and verify transactions, and one of the most discussed is proof-of-stake. However, it's important to understand that in addition to proof-of-work and proof-of-stake, there's a constant flow of new consensus mechanisms being developed (e.g., proof-of-weight, delegated proof-of-stake, proof of activity, byzantine fault tolerance).

As we've seen, under a proof-of-work system, miners compete to win a game of chance to have the opportunity to verify all the transactions in the next block. The winner is rewarded with a certain amount of Bitcoin, the block is shared with everyone, and miners then move to try to solve the next block.⁹⁸ In a proof-of-work mechanism, the more hashing power one has, the more chances she has of "winning" at that game of chance and mining the next block. Proof-of-stake has a couple of major differences with proof-of-work, including better energy efficiency; a lower barrier to entry as there's no need for specialised equipment; and it's easier to achieve decentralisation.

Proof-of-stake differs entirely from proof-of-work as the right to mine the next block is determined not by winning at that game of chance, but rather by your share or "stake" in that crypto-asset. Forgers (the proof-of-stake equivalent of a miner) are chosen to build blocks based on their stake in a currency and the age of that stake within the blockchain's network. For instance, let's say you hold 100,000 of Crypto X, so you would be more likely to create the candidate block than someone with 1,000 of Crypto X. Also, if you had held your stake for a year, you'd have a greater chance to be chosen than someone who has been holding it only for a month.⁹⁹

A good analogy of proof-of-stake is to imagine that someone's odds of winning the lottery increase based on the number of lottery tickets you buy and for how long you have been buying those lottery tickets. In theory, anyone could stake a predetermined amount of a cryptocurrency (by locking it following a predetermined mechanism) and become a validator. For example, the Ethereum 2.0 proof-of-stake mechanism requires only 32 ETH to become a validator. For most proof-of-stakes, the bigger the size of their stake, the higher are the chances that it will be selected as the validator to forge the next block.

However, proof-of-stake mechanisms have features to ensure that not only the wealthiest in the network are favoured.¹⁰⁰ For example, some proof-of-stake will have a mechanism that when a validator has forged a block, their

coin age is reset to zero and they must wait a certain period before being able to forge another block. For anyone interested in learning about the different types of proof-of-stake mechanisms, there's a lot of material online as this just a simple example of a proof-of-stake mechanism as there are many variants. One trait that some proof-of-stake currencies have is that all coins are created at the launch of the currency and their number is fixed. Therefore, rather than receiving new coins as rewards (as is the case for Bitcoin miners), forgers (as they're called in proof-of-stake ecosystems) receive transaction fees.¹⁰¹ To validate transactions and create blocks, a forger must first put their own coins (and reputation) at stake. If a forger validates a fraudulent transaction, they lose their holdings, as well as future rights to participate as a forger. Forgers are therefore incentivised to validate only correct transactions.¹⁰² It's worth noting that whilst Ethereum will migrate to proof-of-stake under its Ethereum 2.0 roadmap (discussed later in this book), it will continue to issue new ETH, although at a lower rate than under its proof-of-work consensus mechanism, based on its under its "Minimal Necessary Issuance" policy.¹⁰³

There is tremendous debate in the crypto community on the pros and cons of each consensus mechanism. Whilst proof-of-stake has clear environmental benefits, in that it does not consume as much electricity as proof-of-work, many would argue that it's less democratic than proof-of-work as it gives an advantage to those who already hold the currency and have held it for a long time. On the other hand, proof-of-work may itself be considered undemocratic due to the high level of capital required to mine cryptocurrencies like Bitcoin. There are always discussions in the crypto community about improving or amending either proof-of-work or proof-of-stake, and there is much material online on the developments on this topic for anyone who might be interested.



3

Ethereum

Ethereum's currency, Ether (ETH), has become the second biggest crypto-asset after Bitcoin based on its market capitalisation. The Ethereum community has arguably become an important element of the global crypto ecosystem. At its core, Ethereum intends to be a decentralised world computer where every node runs a copy of the Ethereum Virtual Machine (EVM).¹ The underlying idea was to utilise aspects of Bitcoin technology and combine it with the capabilities of smart contract technology, so that this combination would lead to a platform that could sustain not only the money or medium of exchange use case that was developed by Bitcoin, but also to add programmability to money, introducing conditional logic to the equation that would open up a world of possibilities with regards to decentralised financial applications and products, and additional decentralised applications.²

1 History of Ethereum

Ethereum was invented in 2013 by Vitalik Buterin who wrote a whitepaper on the topic.³ Born in Russia and raised in Canada, Buterin attended the University of Waterloo before dropping out when he received the Thiel Fellowship, allowing him to focus on Ethereum. Ethereum was formally

The original version of this chapter was revised: Text correction have been updated. The correction to this chapter is available at https://doi.org/10.1007/978-3-030-97951-5_22

announced to the public in early 2014 at a Bitcoin conference in Miami. Ethereum was funded via a presale that took place from July 2014 to September 2014, a total of 42 days. The price of ether was initially set to a discounted price of 2000 ETH per BTC, when BTC was worth around US\$500, and stayed that way for 14 days before linearly declining to a final rate of 1337 ETH per BTC. 60 million Ether were created for the presale, of which 80% was available for purchase, with 20% (or 12 million) being retained by the Ethereum Foundation’s “development fund” which consisted of early contributors to the project and developers.⁴

The presale ended with ~31,000 BTC (equivalent to ~\$18.3 million at that time) being raised by the Ethereum Foundation and that ETH was not usable or transferable until the launch of the genesis block which occurred on July 30, 2015.⁵ Whilst the Ethereum platform is like Bitcoin in many ways, in that it is blockchain-based and permissionless, there are also some important technical differences, including its monetary policy. Unlike Bitcoin which has a fixed total supply of 21 million Bitcoin, Ethereum does not have a fixed supply and instead uses a monetary policy that focuses on minimum issuance to secure the Ethereum network.⁶ For example, Ethereum’s current yearly network issuance of new ETH (or inflation rate) is approximately 4.5% with 2 Ether per block and an additional 1.75 Ether per uncle block (we will explain uncle blocks later) being rewarded to miners. And, unlike Bitcoin where a new block is mined every 10 minutes or so, a new block is mined in the Ethereum blockchain every 12–15 seconds.⁷

2 How Is Ethereum Different?

Also, whilst both Bitcoin and Ethereum currently use proof-of-work, the Ethereum network is moving to a proof-of-stake consensus mechanism in its Ethereum 2.0 upgrade expected to take place from 2020 to 2022.⁸ One of the most important distinctions is that the Ethereum network can also run smart contracts⁹ and decentralised applications (dApps).¹⁰ As we will see later in this book, smart contracts are self-executing contracts with the terms of agreement written directly in the line of code.¹¹ In the Ethereum context, a good example is the ERC-20 smart contract standard which provides a common set of features for how the contract will function in the Ethereum ecosystem.¹² A good analogy is a regulatory handbook with templates that a lawyer can use to draft a contract. The ERC-20 standard was used by most companies doing an initial coin offering (ICO) (which we’ll explore in more detail later on in the book) in the 2017–2018 frenzy and has contributed greatly to the growth of the Ethereum network and ETH in recent years.

The Ethereum community is generally seen as strong and continuously working on enhancing functionalities, from scalability to new smart contract standards. The Ethereum network has been updated numerous times since it launched, with upgrades like Homestead (2016), the DAO fork (2016), Byzantium (2017), and Constantinople (2019),¹³ but the biggest upgrade in the history of the network is Ethereum 2.0. As mentioned, the Ethereum blockchain originally used a proof-of-work consensus mechanism but is expected to be fully transitioned to proof-of-stake by 2022. However, the Ethereum proof of work consensus mechanism recognises “uncle blocks”, which is something the Bitcoin blockchain does not do. Uncle blocks are created in Ethereum blockchains when two blocks are mined and submitted to the ledger at roughly the same time. To better understand this, we can go back to how a blockchain works. A blockchain is formed as miners (the ones rolling the figurative dice) add new blocks to the chain, thus lengthening the blockchain. The miner who is first to add the new block to the blockchain is rewarded with a block reward, which is the case in both the Bitcoin and Ethereum blockchains. However, it is possible that two blocks are generated at the same time. This is particularly an issue with the Ethereum blockchain as unlike the Bitcoin blockchain, a new block is added every 12–15 seconds. This results in a temporary and unsettled state of the blockchain network as the various nodes try to build a consensus about which of the newly identified blocks to continue with and which one to reject.

In the Bitcoin blockchain, the rejected block is called an orphan and is simply disregarded. The miner does not get any type of reward for that block. However, in the Ethereum blockchain, these are called “uncle blocks” and are still rewarded, although with a lower reward amount. This uncle block receives 87.5% of its base reward, and the nephew that includes the stale block receives the remaining 12.5%. Transaction fees, however, are not awarded to uncles.¹⁴ This was a design choice in the Ethereum blockchain and was put in place to ensure the security of the network despite having short intervals for new blocks.

For most readers, the above should be enough, but if you want to geek out, keep reading. Uncle blocks are achieved by implementing a protocol called GHOST (“Greedy Heaviest Observed Subtree”) which is an innovation first introduced by Yonatan Sompolinsky and Aviv Zohar in December 2013. The motivation behind GHOST is that blockchains with fast confirmation times suffer from reduced security due to a high stale rate because blocks take a certain time to propagate through the network. For example, if miner A mines a block and then miner B happens to mine another block before miner A’s block propagates to B, miner B’s block will end up wasted

and will not contribute to network security. Furthermore, there is a centralisation issue: if miner A is a mining pool with 30% hash power and B has 10% hash power, A will have a risk of producing a stale block 70% of the time (since the other 30% of the time A produced the last block and so will get mining data immediately) whereas B will have a risk of producing a stale block 90% of the time.

Thus, if the block interval is short enough for the stale rate to be high, A will be substantially more efficient simply by virtue of its size. With these two effects combined, blockchains which produce blocks quickly are very likely to lead to one mining pool having a large enough percentage of the network hash power to have de facto control over the mining process.¹⁵ The Ethereum blockchain solves this issue by including stale (uncle) blocks in the calculation of which chain is the “longest” and provides block rewards to stakes. A stale block receives 87.5% of its base reward, and the “nephew” that includes the stale block receives the remaining 12.5%. Transaction fees, however, are not awarded to uncles.¹⁶

Ethereum implements a simplified version of GHOST which only goes down seven levels. There are two main reasons for this. First, unlimited GHOST would include too many complications into the calculation of which uncles for a given block are valid. Second, unlimited GHOST with compensation as used in Ethereum removes the incentive for a miner to mine on the main chain and not the chain of a public attacker.¹⁷ Lastly, whilst Bitcoin has a concept of transaction fees to compensate miners for each block, Ethereum uses a concept of “gas” which is the fee you need to pay to perform a particular transaction, which varies depending on the nature of the transaction.

2.1 What Is the Concept of “Gas” on the Ethereum Blockchain?

ETH is required to transact on the Ethereum network and if the Ethereum blockchain is a nice sports car, ETH is the gas that allows it to run, and gas is paid in ETH. Every transaction that occurs on the Ethereum network requires a set amount of gas, which is the unit used to measure the computational power required to process a transaction. To process a transaction and include it in a block, miners expect to be compensated for this task, which is accomplished by setting the gas price for every transaction, equal to 1 unit of gas, denominated in gwei (1 ETH = 1,000,000,000 gwei). For example, when you simply send ETH from one account to another, this costs 21,000

gas. If you were to set a gas price of 1 gwei, this transaction would cost 0.0000021 ETH.¹⁸

Another way to look at it is that gas prices are denoted in gwei, which itself is a denomination of ETH as each gwei is equal to 0.000000001 ETH (10^{-9} ETH). For example, instead of saying that your gas costs 0.000000001 ether, you can say your gas costs 1 gwei.¹⁹ This process creates a fee market using gas prices where users decide how much they are willing to pay for each unit of gas. Due to the gas block limit, the fee market almost always determines what order transactions are mined in because miners looking to profit will select the transactions with the highest fees.²⁰ A couple of elements become critical for each transaction:

- **Gas:** Unit for how much computation work is done.
- **Gas Price:** How much you're willing to pay per gas for work (in gwei)
- **Transaction Cost:** Gas used * Gas Price
- **Gas Limit:** Maximum gas you will pay for a certain transaction
- **Gas Block Limit:** Maximum gas allowed in a certain block

At the time of writing, Ethereum is one of the most important blockchain communities. For example, Solidity (the coding language for the Ethereum blockchain) is reportedly twice as popular as the next blockchain coding language,²¹ and the implementation of Ethereum 2.0 will be critical to watch over the coming years. One of the best examples of the changes occurring were the London Fork and the EIP-1559 Upgrade in August 2021. Such upgrades have become necessary, as the number of transactions on the Ethereum network has increased significantly since its launch. The most important component of the London upgrade is known as EIP-1559 (EIP stands for Ethereum Improvement Proposal), as it significantly revamps how Ethereum fees are paid. Under the current approach described above, miners receive fees for processing transactions in a supply and demand auction format. But if the network has a bottleneck, fees can quickly skyrocket. For example, in the first half of 2021 alone, average gas fees on the Ethereum network have ranged between \$4 all the way to \$44.

This level of unpredictability is obviously not ideal, as volatility in crypto markets can make it challenging for users to plan for an appropriate level of fees for input so the transaction goes through. Even when a transaction fee is an input by a trader, there are no guarantees, as market conditions can quickly change, and users may need to wait a significant amount of time for confirmation. EIP-1559 addresses this by separating the fee into two components: the base fee and the priority fee.²² The base fee is adjusted up and down

by the protocol based on network congestion. When the network exceeds a certain target per block gas usage, the base fee increases slightly. Likewise, when capacity is below target, it decreases slightly. Because these base fee changes are constrained, the maximum difference in base fee from block to block is predictable, allowing wallets to auto-set the gas fees for users in a highly reliable fashion.

Then there's the priority fee, which some have been calling a "tip" to the miners.²³ For most users, the base fee will be estimated by their wallet and a small priority fee will be automatically set. Users can also manually set the transaction maximum fee to limit their total transaction costs. An important aspect of this fee system is that miners only get to keep the priority fee, as the base fee is always burned (i.e., it is destroyed by the protocol). Whilst the upgrade was welcome news to users, many Ethereum miners are not happy with this upgrade. Ethereum miners in the current proof of work consensus mechanism are rewarded by block rewards and transaction fees, but transaction fees have made up a significant percentage of their revenues until this upgrade and reaching as high as 50% in early 2021.²⁴ Most in the crypto ecosystem would agree that the EIP-1559 change is generally positive for the Ethereum network in the long term, as it fixes the high and unpredictable gas fee problem. Whilst it may not reduce the average gas fees for transactions on the Ethereum blockchain, it will at least make them more predictable and less prone to volatile swings.

Separately, many have been pointing out that the base fee being burned may positively impact the price of Ethereum as it reduces the supply and may even make ETH a deflationary currency. Miners are rewarded by block rewards and transaction fees, but transaction fees have made up a significant percentage of their revenues until this upgrade and reaching as high as 50% in early 2021.²⁵ Most in the crypto ecosystem would agree that the EIP-1559 change is generally very positive for the Ethereum network in the long term, as it fixes the high and unpredictable gas fee problem. Whilst it may not reduce the average gas fees for transactions on the Ethereum blockchain, it will at least make them more predictable and less prone to volatile swings.

Whilst a valid argument, it will be difficult to know what the supply will be, as we don't know today how much ETH will be burned via base fee transactions since the future volume of transactions is unknown, but it can be meaningful. In the three months since the London fork in August 2021, and at the time of writing, over \$3 billion worth of ETH had already been burned.²⁶

How Did the London Fork Get Its Name?

The launch of Ethereum's London Fork in the summer of 2021 was truly a historic day for the crypto space. But you may have asked yourself, why is it called the London fork? How did it get its name? These Ethereum updates are named after the order of the cities in which the DevCon conferences have been held, which are major conferences for Ethereum developers around the globe. A previous upgrade was named Berlin and the name of upgrade (London) was the next city on the DevCon list. Following this logic, we can expect a Shanghai upgrade in the coming years. Mystery solved!

3 What Is Ethereum 2.0?

At the time of writing this book, the Ethereum network is undergoing a massive new revamp, with all new changes set to culminate in Ethereum 2.0. Launched in 2015, the Ethereum network quickly became a victim of its own success and began to suffer from a variety of scalability issues, but the new upgrades should ultimately result in a more scalable, more secure, and more sustainable Ethereum network. Yet what makes Ethereum 2.0 different from Ethereum 1.0 as described above? There are three distinct phases to Ethereum 2.0.

The first stage of the new network rollout will see the introduction of the Beacon Chain, launched on December 1, 2020. It was more of a subtle shift than a radical revamp, and users and developers might not even notice the change, but the new chain will help coordinate the wider network and lay the foundation for a proof-of-stake concept in the broader Ethereum ecosystem. The shard chains, or the second phase of the Ethereum 2.0 rollout, is expected to launch in 2022. “Sharding” is a common concept in computer science, referring to the process in which a database is essentially split up to spread the load around to multiple systems, thus decreasing network traffic and congestion and significantly increasing transactions per second through the creation of new “shards” or chains.

Not only is this important for scalability reasons, the introduction of “sharding” will continue to make the network as decentralised as possible. Rather than taking the opposite direction and investing in powerful computers with massive databases that can handle the traffic, this new network of decentralised validators will only need to store data for the individual chain, or “shard”, that they are validating, rather than the entire

network. In the third phase, the Ethereum mainnet will ultimately merge, or “dock”, with the Beacon Chain at some point in 2022, allowing for staking on the entire network and will see the end of energy-intensive mining. This last phase is critical, as it will bring together proof-of-work, which will continue to run on the Ethereum mainnet in the meantime, and proof-of-stake, used on the Beacon Chain and shard chains.

This will mark the end of proof-of-work for Ethereum, and the full transition to proof-of-stake. Ultimately, the end of proof-of-work will usher in a more sustainable, environmentally friendly Ethereum, significantly reducing both the computing power and energy consumption needed to run the network whilst reaching the full scale, security, and sustainability outlined in the ETH2 vision.



4

The Emergence of New Blockchains and Crypto-Assets

Although Bitcoin was the first cryptocurrency, there are now (at the time of writing) over 15,000 different cryptocurrencies. Whilst Bitcoin is seen as the mother of all cryptocurrencies, many others that have followed made tweaks, some minor, some major, that made that particular asset more suitable for specific purposes. One of the fascinating ways crypto-assets differ from more traditional financial instruments is that anyone can create them (whether this is legal to do so is another question to be discussed later in this and subsequent chapters). All that's needed is a bit of technical know-how and a community of people who believe the crypto-asset you've created is, or could, have some value (Table 1).

It's important to understand that most cryptocurrencies or tokens can be separated into Layer 1 and Layer 2 solutions.

Table 1 Top 20 crypto-assets by market capitalization (January 2022)

1	Bitcoin	11	Shiba Inu
2	Ethereum	12	Crypto.com Coin
3	Binance Coin	13	Litecoin
4	Solana	14	Polygon
5	Cardano	15	Uniswap
6	XRP	16	Algorand
7	Polkadot	17	Chainlink
8	Dogecoin	18	Bitcoin Cash
9	Avalanche	19	Decentraland
10	Terra	20	Axie Infinity

What's the Difference Between Layer 1 and Layer 2 Solutions?

Congestion on the Ethereum network and volatile swings in gas fees have thrown the topic of Layer 1 and Layer 2 ecosystems back into the spotlight. What's the difference between the two? And what do Layer 2 solutions have to do with scaling? To start, Layer 1 blockchains are the foundational blockchains that provide infrastructure, including many of the big-name projects we've come to associate with the crypto ecosystem: Bitcoin, Ethereum, Solana, Avalanche, Algorand, and the like.¹

What's Layer 2 then? Layer 2 is essentially a catch-all term for any project that is built on top of a Layer 1 solution. Many current Layer 2 solutions, for example, are designed to help solve the vexing issue of scalability, with a separate execution layer that inherits the security and decentralised features of the Layer 1 network it's running on top of but allowing for better scalability.² Layer 2 solutions allow us to take some of the transactional burdens off the Layer 1 foundation and shift it to Layer 2, which then takes care of the bulk of processing responsibilities, ultimately reporting back to the primary chain to finalise transaction results.³ As we discussed in Chapter 2, Bitcoin is a Layer 1 blockchain and the Bitcoin Lightning Network is a Layer 2 solution designed to improve speed and scalability challenges on the Layer 1 Bitcoin network.

Ethereum, in particular, has been heavily affected by scalability issues, particularly as more users and developers than ever interact with DeFi and NFT platforms tied to the Ethereum ecosystem. This has led a number of different projects (like Polygon, Arbitrum, and many others) working towards scaling up by handling and processing transactions off the primary, base Ethereum Layer 1 blockchain. There are numerous ways that these Layer 2 solutions operate and Zero-Knowledge and Optimistic Rollups (which we'll explore in more detail later in this book) are good examples.

Meanwhile, the gradual convergence of gaming and crypto has resulted in a surge of interest in blockchain-based games like Axie Infinity. Without Layer 2 solutions, decentralised, metaverse-based games on Ethereum that depend on instant transactions wouldn't make sense today. This may be solved with Ethereum 2.0, but in the interim, Layer 2 solutions can help.

1 Examples of Cryptocurrencies and Tokens

It goes without saying that from the 15,000 cryptocurrencies and tokens that exist at the time of writing, some are more popular or more commonly discussed than others. In the pages below, we'll introduce and summarise the key features of some coins and tokens. I included these coins or tokens based on subjective criteria including market cap (e.g., ADA, AVAX, BNB); notoriety (e.g., DOGE, SHIB); unique features (e.g., ALGO, HBAR, IOTA, MATIC, XTZ); differentiating features (e.g., XMR, ZEC); longevity (e.g., LTC); or interesting history (e.g., BSV). Inclusion in this list is by no means an endorsement or any investment advice. Rather, it's to highlight a particular feature that I find interesting from an intellectual perspective, thus allowing you to better understand the broader crypto ecosystem.

Listed in alphabetical order, these coins or tokens are not static assets but rather part of a continuously evolving ecosystem, meaning several of these projects may have added new features or made improvements by the time you read this. Nonetheless, I believe it's helpful to enable you to better understand the particularities of each.

1.1 Algorand (ALGO)

The Algorand blockchain is a Layer 1 blockchain founded by Turing award winner and MIT professor Silvio Micali that launched in 2019. It tries to

differentiate itself with four attributes. The first is speed, as it can process and settle transactions in less than four seconds. The second is scalability, as it allows for thousands of transactions to happen without an increase of fees, and third is security, leveraging its pure proof-of-stake consensus mechanism (different from traditional proof-of-stake consensus as the selection of the validator is random). There is no forking of the Algorand blockchain, and finally Algorand is carbon neutral, since it's using pure proof-of-stake. There's a total supply of 10 billion tokens, of which 60% are in circulation.

1.2 Avalanche (AVAX)

Launched after the foundation of Ava Labs in 2018 by several professors from Cornell University with extensive backgrounds in cryptography, Avalanche concluded its initial coin offering (ICO) in 2020 in less than 24 hours, hauling in \$42 million.⁴ Designed to address some of the limitations of older blockchain platforms, including transaction speeds, centralisation, and scalability, Avalanche's unique consensus protocol promises low latency, low fees, high throughput capabilities, and resistance to 51% attacks in addition to being eco-friendly as it uses a proof-of-stake consensus mechanism.⁵

The network's speed is one of its advantages. For instance, unlike Bitcoin and its seven transactions per second average (or Ethereum and its 14 transactions per second average), Avalanche can process up to 4,500 transactions per second but also provides almost instant finality (instead of waiting for several blocks of 10 minutes as in the Bitcoin blockchain for example).⁶ The platform is built around Avalanche's native utility token, AVAX, which is used for everything from paying network fees to staking in exchange for yield. There's a hard cap of 720 million AVAX, of which about one-third are in circulation.

1.3 Binance Coin (BNB)

BNB is a cryptocurrency created in June 2017, launched during an ICO and initially issued as an ERC-20 token. BNB was designed as an asset to function within the Binance exchange and its broader ecosystem. It has several uses including trading fee discounts (initially of 50% and then reduced to 25%), unique participation rights to IEO or other listings, and a currency for trading pairs as well as uses on other third-party platforms.⁷ Following the launch of Binance Chain in May 2018, BNB has pivoted to become the native asset of Binance Chain and Binance Smart Chain (Ethereum compatible and allows to build Dapps), working similarly to ETH for the Ethereum

blockchain.⁸ At the core of the token economics of BNB, there's a quarterly burn mechanism based on revenues of the Binance platform that pivoted to an auto-burn mechanism in December 2021.⁹ From its initial maximum supply of 200 million, burns are expected to continue until the supply reaches 100 million,¹⁰ which is why many believe that BNB is de facto a security and should be regulated as such.

1.4 Bitcoin Cash (BCH)

Bitcoin Cash (BCH) was born as a result of the Bitcoin hard fork in August 2017. Bitcoin Cash aims to solve scalability problems of Bitcoin with an increased block size of 8 MB, compared to Bitcoin's 1 MB, which provides faster and cheaper transactions. It's intended to be used as a payment system and many supporters believe that it more closely resembles the ideology of what Satoshi wanted to accomplish. The goal for Bitcoin Cash is to become "sound money that is usable by everyone in the world".¹¹ Being a fork of Bitcoin, Bitcoin Cash also uses a proof-of-work consensus mechanism and like Bitcoin, has a total supply of 21 million BCH.

In November 2018, BCH was hard forked for a second time and split into Bitcoin ABC and Bitcoin SV. The first camp, supported by entrepreneur Roger Ver and Jihan Wu of Bitmain, promoted the software entitled Bitcoin ABC (short for Adjustable Blocksize Cap), which would maintain the block size at 32 MB. The second camp led by Craig Steven Wright and billionaire Calvin Ayre put forth a competing software version Bitcoin SV, short for "Bitcoin Satoshi Vision", which increased the block size limit to 128 MB.

Bitcoin ABC became the dominant chain and inherited the BCH ticker, as it had more hash power and most nodes in the network. BCH had its most recent halving in April 2020, when its block reward was reduced to 6.25, from 12.5. The Bitcoin Cash network has scheduled protocol upgrades twice a year, in November and May, required for all node operators. Rather than a specific block height, the upgrades are based on a timestamp to better enable businesses to prepare for the upgrade at a particular estimated date. The Bitcoin Cash community has set out a roadmap of technical improvements it aims to implement over the coming years including enabling Bitcoin Cash to scale from ~100 Tx/s to over 5,000,000 Tx/s.¹²

1.5 Bitcoin SV (BSV)

Bitcoin SV (Satoshi's Vision) was born from the hard fork that split Bitcoin Cash into two different digital currencies in November 2018: Bitcoin SV and Bitcoin ABC (that became BCH) and Bitcoin SV. Bitcoin SV claims a strict adherence to Satoshi Nakamoto's vision for the original Bitcoin¹³ and its proponents claim that BSV was created to restore the original Satoshi protocol, keep it stable, and enable it to massively scale. On its official website, it claims that "unlike other Bitcoin projects, only Bitcoin SV has the plan for a stable protocol and plan for massive on-chain scaling to become the world's new money and the global public blockchain for enterprise."¹⁴ Bitcoin SV has been controversial especially due to one of its biggest proponents, Craig Wright, who has been claiming for many years that he is Satoshi Nakamoto.¹⁵ Like Bitcoin, Bitcoin SV has a total supply of 21 million BSV and uses a proof-of-work algorithm.

1.6 Cardano (ADA)

Cardano was born following a public token sale from September 2015 to January 2017 and which launched in September 2017. There is no single white paper for Cardano; rather, there are several academic papers.¹⁶ Named after the Italian Renaissance mathematician, Gerolamo Cardano, the Cardano protocol sees itself as a next-generation blockchain, implementing the Ouroboros protocol (named after the ancient symbol depicting a dragon eating its own tail) and claiming to be the first peer-reviewed, verifiably secure blockchain protocol.¹⁷

Ouroboros focuses on two things. First is security; Ouroboros features mathematically verifiable security against attackers and is guaranteed to be secure so long as 51% of the stake—in the case of Cardano, ADA—is held by honest participants, achieved through random leader selection. Then come incentive mechanisms that reward network participants for their participation and can either be operating a stake pool or delegating a stake in ADA to a stake pool. Rewards (in the form of ADA) can be earned by completing either of these activities.¹⁸ To go a bit deeper, Ouroboros processes transaction blocks by dividing chains into epochs, which are further divided into time slots. A slot leader is elected for each time slot and is responsible for adding a block to the chain. To protect against any adversarial attempts to subvert the protocol, each new slot leader is required to consider the last few blocks of the received chain as transient: only the chain that precedes a prespecified number of transient blocks is considered settled. This is also

referred to as the settlement delay and is the mechanism through which the ledger is securely passed between participants.¹⁹

The Cardano roadmap has been organised into five eras: Byron, Shelley, Goguen, Basho, and Voltaire. Each era is centred around a set of functionalities to be delivered across multiple code releases. Whilst the eras of Cardano will be delivered sequentially, the work for each era happens in parallel, with research, prototyping, and development often in progress all at once across different development streams.²⁰ There are also a handful of core entities in the Cardano ecosystem: IOHK, the Cardano Foundation, and Emurgo and each has a distinct role: IOHK develops the technology, the Cardano Foundation is responsible for supervising development and promoting Cardano, and Emurgo drives commercial adoption. The ADA token is named after Ada Lovelace, a 19th-century mathematician who is recognised as the first computer programmer and was the daughter of poet Lord Byron. There's a total supply of 45 billion ADA, of which around 60% are in circulation.

1.7 Chainlink (LINK)

Founded in 2017, Chainlink has built what is known as a decentralised oracle network, which allows blockchains (like Ethereum, for instance) to securely interact with off-chain data feeds and payment methods. Chainlink is a decentralised network of nodes that provides data and information from off-blockchain sources to on-blockchain smart contracts via oracles. This process, along with extra secure hardware, eliminates the reliability issues that might occur if using only a single centralised source.²¹ Chainlink fixes this issue by leveraging a reputation contract, an order matching contract, and an aggregating contract.²² The native token is an ERC-20 token called LINK used to pay Chainlink node operators for their work, and node operators also use LINK to stake in the network; node operators must deposit LINK with Chainlink to demonstrate commitment to the network and incentivise good service.²³ There's a total supply of around 1 billion LINK tokens with half in circulation.

1.8 DASH (DASH)

Dash (combination of “Digital” and “Cash”) was launched in 2014 by founder Evan Duffield under the name Xcoin and then Darkcoin before settling on its current name. It's intended as a payment system with the goal of enabling anyone, anywhere in the world to make quick, easy, and

cheap payments at any time without going through a central authority. It also has a privacy option allowing you to send DASH anonymously using what is called a PrivateSend option. It uses proof-of-work (with an additional proof-of-service performed by the masternodes) and has a total supply of 18.9 million with approximately 55% in circulation.²⁴

1.9 Dogecoin (DOGE)

Dogecoin was launched in 2013 by IBM software engineer Billy Markus and Jackson Palmer, a marketer at Adobe, with the duo seeking to create a new cryptocurrency that was instant, fun, and free from traditional banking. Ironically, the initial thought behind Dogecoin was that it was a joke, a reaction to the overwhelming number of altcoins popping up in the market. After a whilst, the pair felt that their new venture could potentially reach a broader range of people than Bitcoin, all whilst steering clear of some of the pitfalls and controversies that plagued so much of the early wave of ICOs.

Even if you're not that familiar with Dogecoin, you would undoubtedly recognise the iconic token, with Dogecoin featuring the face of the Shiba Inu dog from the widely shared and iconic "Doge" meme as its logo. The meme originated on the cultishly popular turn-of-the-millennium comedy website Homestar Runner, with one of the characters misspelling "dog" as "dope". Over the years, the joke took on a new life, popping up on Reddit and Tumblr before transforming into its own blog. And whilst Dogecoin has many of the features of other cryptocurrencies like Bitcoin (e.g., decentralised, peer-to-peer), there are some notable differences as well. First, whilst the initial goal was to have a fixed supply of 100 billion DOGE, the founders scrapped that plan in 2014 to change it to 5 billion new DOGE coins being mined each year. This is different from other cryptocurrencies like Bitcoin, where there will only be a fixed supply of 21 million Bitcoin ever. Second, the Dogecoin consensus mechanism is more like that of Litecoin than that of Bitcoin, using a proof-of-work mechanism but with scrypt technology that basically makes it impossible to mine with traditional Bitcoin SHA-256 mining machines. Also, Dogecoin's block time is 1 minute, as opposed to Litecoin's 2.5 minutes or Bitcoin's 10 minutes.

The third most prominent difference between the two coins comes down to utility. For instance, whilst other cryptocurrencies have more traditional uses as either a store of value or as a means of payment, Dogecoin was primarily designed as a tipping system in which users can quickly use Dogecoin to tip anyone around the world for good content or good service, in any amount they choose. The final difference between DOGE and BTC is

apparent when you look at their respective communities. Although there is no inherent value in Dogecoin when viewed from traditional metrics (e.g., total supply, usage), there is a strong and vocal Dogecoin community, based mainly on Reddit, with many believing this is what gives Dogecoin its edge. In recent years, for example, the community has raised funds for projects like sending a team to the Olympics, building a well in Africa, and even sponsoring a Dogecoin logo on an official NASCAR. Throughout 2021, a series of pumps occurred when celebrities and business tycoons started getting invoked, from Snoop Dogg to Gene Simmons, but no one has been a more vocal advocate of Dogecoin than Elon Musk, repeatedly tweeting about it and sending the price of the coin higher, all whilst providing the Internet with some classic memes. At the time of writing, there's a total supply of over 130 billion DOGE which increases each year.

1.10 Eos

Introduced in May 2017, the EOS platform was developed by the company Block.one, its white paper was authored by Daniel Larimer and Brendan Blumer. EOS was launched following a year-long ICO in 2017 that allowed it to raise a mind-blowing \$4 billion dollars. A total of 200 million (20% of the tokens) were distributed during a five-day period, 700 million more (70%) distributed over the rest of the year, and 100 million (10%) held in escrow for Block.one. The EOSIO blockchain platform is an open-source platform designed for enterprise-grade use cases and built for both public and private blockchain deployments. Its native token is EOS and it's positioned as being different from other blockchains on several items. First, it's focused on decentralised applications (dApps) and a focus on transaction speed and block confirmation times. Second, it operates using programming languages with which developers are already familiar like C++, Java, and Python. This allows developers the ability to build applications without the need to learn a new language, and it's also focused on enterprise use cases and is customisable to suit a wide range of business needs across industries. The most controversial element of EOSIO is probably its delegated proof-of-stake (DPoS) consensus mechanism.

What Is Delegated Proof-of-Stake?

Delegated proof-of-stake (DPoS) is a consensus algorithm invented by Dan Larimer in 2013 and originally to power BitShares, Larimer's first blockchain project and then used for his second project, Steem, and finally for EOS.²⁵

DPoS is a system in which a fixed number of elected entities (called block producers or witnesses) are selected to create blocks in a round-robin order. Block producers are voted into power by the users of the network, who each get votes proportional to the number of tokens they own on the network (their stake).²⁶ Alternatively, voters can choose to delegate their stake to another voter, who will vote in the block producer election on their behalf.²⁷ The block producers are those responsible for creating and signing new blocks. They're limited in number and are elected by the voters.

The block validators in DPoS refer to full nodes that verify that the blocks created by block producers follow consensus rules and any user can run a block validator and verify the network. This is different from the definition of validator in the Ethereum 2.0 proof of stake where validators are the ones creating the blocks.²⁸ The major difference between delegated proof-of-stake and "regular" proof-of-stake is that in a regular proof-of-stake, anyone with tokens can become a validator and participate in the consensus mechanisms by validating transactions and adding blocks to the blockchain. However, in delegated proof-of-work, token holders only get to vote for the block producers they prefer who will in turn be able to validate transactions and participate in the consensus mechanism and be rewarded for doing so.

In the case of EOS, there are 21 block producers. Each holder of EOS stakes their tokens and then casts their votes in a continuous election for their chosen block producer. They can vote for up to 30 block producer candidates and change their votes at basically any time. The top 21 candidates with the most tokens staked in their favour have responsibility for validating transactions.²⁹ Critics have pointed out that this makes the system centralised; however, Dan Larimer acknowledges that sacrificing a bit of decentralisation is needed in order to achieve speed.³⁰ For example, at the time of writing, the EOS network can process up to 4,000 transactions per second.³¹ Other critics have mentioned that many block providers were based in China,³² and still others have mentioned that there are widespread cases of vote buying with block producers giving a kick-back to token holders who vote for them.³³ EOS has a total supply of 1,021,208,059 EOS, of which around 91% are in circulation.³⁴

1.11 Hedera Hashgraph (HBAR)

Launched in August 2018, Hedera sees itself as a third-generation public ledger to be used for a multitude of use cases from payments and tokenised assets to identity and fraud prevention.³⁵ Capable of supporting smart

contracts and decentralised apps (dApps), Hedera enables over 10,000 transactions per second, a 3–5 seconds finality, very low fees (around \$0.0001), and minimal energy consumption.³⁶ The Hedera network is unique as whilst a DLT, it's not technically a blockchain but rather a hashgraph. It uses the asynchronous Byzantine Fault Tolerance (aBFT) and is patented.³⁷ Whilst the consensus algorithm is not open source, it is “open review”, meaning anyone can verify there are no backdoors in the code and no license is required to build Hedera applications.³⁸ What may come as a surprise is that Hedera is owned and governed by a broad consortium of major corporations, including Google, IBM, Boeing, LG, T-Mobile, and others that compose the Hedera Global Governing Council. Its native token is called HBAR. It is used to pay for fees and for staking to secure the network. There's a total fixed supply of 60 billion HBAR which were minted at the launch of the network and placed in the Hedera Treasury account with about one-third in circulation.

1.12 IOTA (IOTA)

IOTA conducted its token sale in 2015 and launched its mainnet in 2016. IOTA is unique as it does not use blockchain, but rather a different distributed ledger technology called Tangle, a directed acyclic graph (DAG)-based ledger, where each new transaction is verified by two random nodes that have previously requested a transaction. There are no transaction fees or miners and as the network gets bigger, the faster transactions can be confirmed. IOTA's focus is to be the transaction settlement and data layer for the Internet of Things (or The Internet of Everything).³⁹ The lack of transaction fees makes it ideal for machine-to-machine transaction between IoT devices. IOTA is used as a native currency within the IOTA network and can be used for peer-to-peer payments. You'll often see it quoted as MIOTA, which is a unit of IOTA. It's bought directly on almost all stock exchanges, and the price of IOTA is usually quoted in MIOTA. The “M” stands for mega, so one million. Thus, 1 MIOTA is equivalent to 1,000,000 IOTA.⁴⁰ It has a total supply of 2.8 billion IOTA that are all in circulation.

1.13 Litecoin (LTC)

Litecoin is described as a “peer-to-peer Internet currency that enables instant, near-zero cost payments to anyone in the world”.⁴¹ The cryptocurrency was created by Charlie Lee, a former Google employee, in 2011, shares many features with Bitcoin, and is often considered as “Silver” to “Bitcoin's

Gold”, mainly because of its larger supply (84 million Litecoins) and speed to generate blocks (four times faster than Bitcoin). Like Bitcoin Cash, it’s intended to be used as a payments system. Whilst it also uses a proof-of-work consensus mechanism, it uses a different algorithm called Scrypt and was developed in response to the centralisation of mining power of ASIC machines. The algorithm initially had CPU mining as its only objective; however, shortly after the debut came the first software tools for GPU mining, and a year later, towards the end of 2013, the first Scrypt-based ASICs arrived, decrying the failure of the objectives set by this algorithm.⁴² Whilst still possible today to mine Litecoin using consumer grade hardware such as GPU, in practice Litecoin mining is, similarly to Bitcoin, dominated by large miners.⁴³ There’s a total supply of 84 million Litecoins of which around 80% have been issued.

1.14 Monero (XMR)

Monero is a private cryptocurrency that hides the sender, amount, and receiver in each transaction by using a combination of privacy technologies including ring signatures, ring confidential transactions (RingCT), and stealth addresses. It also doesn’t have a hard block size limit; instead, the block size can increase or decrease over time based on demand.⁴⁴ It has become the go-to cryptocurrency for dark web transactions. Monero is an Esperanto word that means “coin” and initially was called “Bitmonero”, which translates to “Bitcoin” in Esperanto. After the community decided to fork from the original maintainer, “bit” was dropped in favour of simply “Monero”.⁴⁵ Monero has a fixed emission rate, not a set maximum supply, and has a block reward of 1.16 XMR per block with the average block interval being around 2 minutes. However, as of May 2022, the block reward will be changed to 0.6 XMR per block indefinitely.⁴⁶ It uses proof-of-work, and the current supply is around 18 million XMR.

1.15 Polkadot (DOT)

The Polkadot whitepaper⁴⁷ was published in 2016 and a token sale was conducted in October 2017. The Genesis block of the Polkadot network launched in May 2020, as a proof-of-authority network before becoming proof-of-stake in June 2020. Polkadot is an open-source project funded by the Web3 Foundation, founded by Gavin Wood, a co-founder of Ethereum. A primary use case for Polkadot is enabling interoperability between chains,

regardless of features or status as a private or public chain. Polkadot's core consists of a unique concept called "parachains",⁴⁸ or parallel chains, blockchains that can perform fast transactions⁴⁹ due to their sophisticated design. These chains eventually connect to a network known as the Relay Chain,⁵⁰ which is the central hub of the entire Polkadot network, ultimately responsible for security, interoperability, and governance. Finally, the Bridge Chain⁵¹ connects the Polkadot ecosystem to other blockchains that don't use Polkadot's protocols, like Ethereum. Whilst some may view Polkadot as a serious rival, or even threat, to Ethereum, others view each network as complementary to one another. DOT is the native token of the Polkadot network in a similar way that Ether is the native token of the Ethereum blockchain. DOT serves three key functions in Polkadot (i) to be used for governance of the network, (ii) to be staked for the operation of the network, and (iii) to be bonded to connect a chain to Polkadot as a parachain.⁵² DOT is an inflationary currency (designed to be around 10%) so there is no maximum cap and its supply increases depending on the percentage of DOT staked (there's around 1 billion DOT supply at the time of writing).

1.16 Polygon (MATIC)

Polygon launched as Matic Network in 2017 before rebranding to Polygon in February 2021 and aims to solve scalability issues of Ethereum whilst benefiting from Ethereum's advantages. It offers a core component called Polygon SDK which allows developers to build and connect layer 2 infrastructure like optimistic or ZK-Rollups.⁵³ Polygon's native token, MATIC, is an ERC-20 token used to pay for fees on the Polygon network and for staking. It has a maximum supply of 10 billion tokens of which around 70% are in circulation.

1.17 Ripple (XRP)

XRP is a digital asset built for payments and is the native digital asset on the XRP Ledger—an open-source, permissionless and decentralised blockchain technology that can settle transactions in 3–5 seconds. XRP can be sent directly without needing a central intermediary, making it a convenient instrument for bridging two different currencies quickly and efficiently.⁵⁴ It's important to understand the difference between XRP, Ripple, and RippleNet. XRP is the currency that runs on a digital payment platform called RippleNet, which is on top of the distributed ledger database called

XRP Ledger. Whilst RippleNet is run by a company called Ripple, XRP Ledger is open source. Originally, the XRP Ledger was called “Ripple” for the way the technology allowed payments to ripple through multiple hops and currencies. For the native asset built into the ledger, the creators chose the ticker symbol “XRP” from the term “ripple credits” or “ripples” and the X prefix for non-national currencies in the ISO 4217 standard.⁵⁵ Payments move across the XRP ledger in three seconds (way faster than ETH or BTC) and the platform is scalable, able to handle over 1,500 transactions per second.

Established in 2012, the technology is open sourced and consumes less energy than other cryptocurrencies due to its unique consensus mechanism called the XRP Ledger Consensus Protocol, different from the more widely used proof-of-work or proof-of-stake mechanisms.⁵⁶ Without going into too much detail, it’s useful to understand that the XRP Ledger processes transactions in blocks called “ledger versions” or “ledgers” for short. Each ledger version contains three pieces: (i) current state of all balances and objects stored in the ledger; (ii) set of transactions that have been applied to the previous ledger to result in this one; and (iii) metadata about the current ledger version, such as its ledger index, a cryptographic hash, that uniquely identifies its contents, and information about the parent ledger that was used as a basis for building this one.⁵⁷ Each ledger version is numbered with a *ledger index* and builds on a previous ledger version whose index is one less, going all the way back to a starting point called the *genesis ledger*. Each new “block” in the XRP Ledger contains the entirety of the current state, so you don’t need to collect the entire history to know what’s happening now.

The main job of the XRP Ledger Consensus Protocol is to agree on a set of transactions to apply to the previous ledger, apply them in a well-defined order, then confirm that everyone got the same results. When this happens successfully, a ledger version is considered *validated*, and final. From there, the process continues by building the next ledger version.⁵⁸ The core principle behind the XRP Ledger’s consensus mechanism is that a little trust goes a long way. Each participant in the network chooses a set of validators, servers specifically configured to participate actively in consensus, run by different parties who are expected to behave honestly most of the time. Anyone can operate a validator and there are at the time of writing over 150 validators active on the XRP ledger, operated by universities, exchanges, businesses, and individuals.⁵⁹ This list is sometimes called a Unique Node List, or UNL⁶⁰ and as the network progresses, each server listens to its trusted validators³; if a large enough percentage of them agree that a set of transactions should occur and that a given ledger is the result, the server declares a consensus. If

they don't agree, validators modify their proposals to more closely match the other validators they trust, repeating the process in several rounds until they reach a consensus.⁶¹

Like Bitcoin with its 21 million maximum hard cap, there is a maximum of 100 billion XRP (with about 47 billion in supply). To protect the XRP Ledger from being disrupted by spam and denial-of-service attacks, each transaction must destroy a small amount of XRP. This transaction cost is designed to increase along with the activity load on the network, making it very expensive to deliberately overload the network. Every transaction must specify how much XRP to destroy to pay the transaction cost with the current minimum transaction cost required by the network for a standard transaction being 0.00001 XRP (10 drops). There's no need to worry about running out of XRP, as at the current rate of destruction, it would take at least 70,000 years to destroy all XRP, and XRP prices and fees can be adjusted as the total supply of XRP changes.⁶²

1.18 Shiba Inu (SHIB)

Shiba Inu traces its roots back to August 2020, when an anonymous developer known as Ryoshi published a whitepaper on what he hoped would emerge as a “dogecoin killer.” In the whitepaper,⁶³ Ryoshi wrote that Shiba Inu was “an experiment in decentralised spontaneous community building.” They also reference the chaos and fallout from the 2021 showdown between day traders and hedge funds over meme stocks like GameStop and AMC as being foundational moments in the coin’s development: As far as technical specifics go, Shiba Inu operates on the Ethereum network and contains several unique characteristics. For example, the Shiba Inu community has three different types of tokens: SHIB, LEASH, and BONE. SHIB is the foundational currency of the Shiba Inu ecosystem, with a supply of 1 quadrillion tokens. Some 50% of those SHIB were sent to Vitalik Buterin, who then donated one billion SHIB to several charities, including India COVID-Crypto Relief Fund, before burning 90% of his supply (worth over \$32 billion today).

LEASH is another currency geared towards being a “DOGE killer.” The initial idea was for its price to be tied to that of dogecoin. However, those plans were subsequently dropped and there are only 107,647 LEASH tokens in existence. BONE is a governance token and with 250 million tokens, BONE allows the community to vote on what tokens can be used on ShibaSwap, the decentralised exchange launched by the community. The Shiba Inu community is involved in fun and charitable initiatives, like

supporting dog shelters.⁶⁴ The rise of SHIB has been fascinating to watch; whilst the SHIB token doesn't have any particular competitive advantage when it comes to technology, what gives it strength is the power of its community, as we've seen in the case of dogecoin.

1.19 Solana (SOL)

Solana⁶⁵ is an open-source public blockchain that supports several DeFi solutions and protocols, including the development of decentralised applications (dApps) and smart contracts. Solana's native token SOL can be used to pay transaction fees and for staking, like the role that ETH plays in the Ethereum blockchain. Each SOL can be subdivided into fractional SOLs, which are called lamports, named⁶⁶ after American computer scientist and Turing Award winner Leslie Lamport. Each lamport⁶⁷ has a value of 0.000000001 SOL. Solana traces its history⁶⁸ to November 2017 when Anatoly Yakovenko published a whitepaper⁶⁹ describing Proof-of-History,⁷⁰ a new technique for keeping time between computers that don't trust one another. Drawing from his professional experience designing distributed systems at companies like Qualcomm and Dropbox, Anatoly realised that a reliable clock can ultimately make network synchronisation a simple task and increase speed.

As big-name decentralised blockchains like Bitcoin and Ethereum struggled to scale up beyond a few transactions per second worldwide, whilst Visa easily achieved 65,000 transactions per second at peak times, Anatoly saw an opportunity for Solana. Without a clock, he believed that the Bitcoin network, for example, would never evolve into the top-tier global payment system or global supercomputing system that its proponents claimed it could be. The project was initially dubbed Loom,⁷¹ but this quickly resulted in confusion with another project known as Loom Network and the name was changed to Solana, a nod to Solana Beach, a small town north of San Diego, where Anatoly and initial founders lived and surfed for three years whilst working for Qualcomm. When the network launched, 500 million SOL were created with just under 300 million in circulation.⁷²

There's a predefined inflation rate of 8% annually,⁷³ decreasing by 15% year-over-year, reaching a long-term fixed inflation rate of 1.5% annually. As for infrastructure itself, there are a few distinct features that differentiate Solana from other blockchains. First is its focus on speed, with Solana claiming to have 400 millisecond block times and handling over 50,000 transactions per second, with the blockchain's infrastructure capable of reaching the upper bound levels of 710,000 transactions per second.⁷⁴ The second factor is its consensus mechanism. Unlike other blockchains,

Solana uses a proof of authority consensus⁷⁵ that combines proof-of-history with proof-of-stake relying on a Byzantine Fault Tolerance (BFT) mechanism called Tower Consensus. A third major difference are fees, with Solana having an average transaction fee of less than \$0.01 (\$0.00025).⁷⁶ Finally, unlike other blockchains like Ethereum that are exploring Layer 2 or sharding solutions, on Solana, all transactions take place on Layer 1, which is a big benefit when it comes to speed and scalability.

What Is the Proof-of-History Consensus Mechanism?

Proof-of-history is another consensus mechanism that has been gathering attention, especially following a surge of interest in Solana in 2021. Traditional blockchains like Bitcoin synchronise data on blocks and a transaction cannot be processed until a certain duration, known as a “block time”, has passed. In the Bitcoin blockchain, this occurs roughly every 10 minutes or so. Nodes must communicate back and forth to establish the time, thus requiring a significant amount of processing power and time to be dedicated to determining the correct chronological order of messages and transactions. The longer it takes to reach consensus, the slower the process of adding new blocks becomes because the next block cannot be verified and added to a blockchain until the current one is confirmed.

The popular way to get around this issue is to tag each block with a wall clock timestamp, also called a Unix Time or Epoch time, systems for describing a point in time that reflects the number of seconds that have passed since the Unix epoch, which was arbitrarily set at 00:00:00 UTC on 1 January 1970, with each day treated as if it contains exactly 86,400 seconds. But proof-of-history (PoH) is slightly different. In proof-of-history,⁷⁷ the leader nodes essentially “timestamp” the blocks with cryptographic proofs that some duration of time has passed since the last proof. The idea is that all the data hashed into that proof will have taken place before the proof was even generated. This allows cryptographical verification of the passage of time between two events, and due to this mechanism, PoH allows us to break blocks into smaller batches of transactions called entries, which are sent to validators (in charge of verification for the PoH consensus algorithm) in real time, before any notion of block consensus, thus making the entire process significantly faster.

PoH then chains these entries from nodes together to provide a relative chronological order of events not dependent upon local clocks or timestamps. To accomplish this, a network node is selected as the leader node and placed in charge of generating a PoH sequence optimised for maximum efficiency and throughput. In the Solana PoH model, the leader node is chosen by proof-of-stake elections. It's important to understand that PoH technically⁷⁸ never

sends a block, but rather uses the term to describe the sequence of entries that validators vote on to achieve confirmation. In addition, by processing⁷⁹ transactions optimistically, there's no time lag between when the most recent entry is received and the time when the node can vote. This optimistic processing technique came to light in 1981 and is known as an Optimistic Concurrency Control, which can be applied to blockchain infrastructure when a cluster votes on a hash that represents the full ledger up to some specific block height. For example, in Solana's PoH, it's implemented by using the last entry's PoH hash. In the event consensus isn't reached, a node will simply roll back its state. It will be interesting to see if the rise of Solana will generate more awareness of this consensus mechanism.

1.20 Stellar (XLM)

Launched in 2014, Stellar is an open-source network for currencies and payments and has processed 450 million operations made by over four million individual accounts. It uses its own Stellar consensus protocol and currency called Lumens and wants to allow people (especially in emerging markets) to make payments with traditional currencies whilst using the efficiency of a cryptocurrency network to lower costs and speed up processing. The Stellar network also allows the easy creation of stablecoins.⁸⁰ The network has a native currency called Lumens used to pay transaction fees and required minimum balance.⁸¹ but the inflation mechanism was ended by community vote in October 2019 and in November 2019, the overall lumen supply was reduced to 50 billion lumens in existence, with no more lumens created. Nearly 20 billion lumens are in the open market whilst the Stellar Development Foundation supports the growth and development of the broader Stellar Network.⁸²

1.21 Tezos (XTZ)

Tezos was proposed in a position paper in 2014 by Arthur Brietman and conducted an ICO in 2017 that raised \$230 million.⁸³ Tezos aims to be an open-source platform for assets and applications that can evolve by upgrading itself, offering a platform to create smart contracts and build decentralised applications for a wide range of use cases from payments and CBDCs to tokenisation and DeFi. The upgrade of the network is done by a self-amendment process that allows Tezos to upgrade itself without having to

fork the network into different blockchains and by allowing all stakeholders to participate in governing the protocol. Proposed amendments accepted by stakeholders can even include payment to individuals or groups that improve the protocol in order to encourage robust participation and decentralisation of the maintenance of the network.⁸⁴

It uses a proof-of-stake consensus mechanism and “baking” to secure the network, which is the act of signing and publishing blocks to the Tezos blockchain. Bakers are a crucial component of the proof-of-stake consensus mechanism by ensuring that all transactions in a block are correct, that the order of transactions is agreed upon, and that no double-spending has occurred. Bakers validate all transactions and add them to the blockchain. If a baker behaves dishonestly, the protocol has a built-in mechanism that can cause them to lose their security deposit.⁸⁵ Bakers earn a block reward of 16 XTZ (or tez, the native currency of the Tezos network) for baking a block. In addition to the Baker, 32 Endorsers are randomly selected to verify the last block that was baked and endorsement rewards can be up to 2 XTZ. Block rewards are funded via newly issued coins with an annual inflation rate of 5.5%.⁸⁶ The native currency tez or XTZ is required to pay for fees or to become a baker and there are around 900 million tez issued at the time of writing.⁸⁷

1.22 Tron (TRX)

Launched in 2017, TRON is a decentralised blockchain platform for supporting smart contracts and high throughput and sees itself as a future operating system which will allow developers to deploy their own decentralised applications.⁸⁸ Founded by Justin Sun, who previously served as the chief representative for Ripple in the Greater China area,⁸⁹ TRON uses a 3-layer architecture (Storage layer, Core layer and Application layer) and uses the proof-of-stake consensus model. It can allegedly process 10,000 transactions per second,⁹⁰ and a total of 27 “super representatives” are responsible for validating blocks on the network chosen through a voting system that allows users to vote based on the tokens they hold. Tron’s native currency is called the Tronix or TRX and is used to pay content creators and developers to access their applications. Miners earn TRX by providing data storage space to network users. TRX was initially an ERC-20 token on the Ethereum network before migrating to the TRON mainnet in June 2018. There’s a total supply of 100 billion TRX of which around 70% are in circulation.

1.23 Vechain (VET)

VeChain conducted a token sale in 2017 and aims to tackle some of the supply chain management issues using blockchain technology, focusing on supply chain management solutions for enterprises and integrating with Internet of Things (IoT) devices to ensure transparency, traceability, efficiency, and cost reduction. There are two tokens in the VeChain ecosystem: the VeChain Token (VET) and VeChainThor Energy (VTHO). The former is used to relay value across VeChain's network, whilst the latter is utilised as "gas".⁹¹ VeChain initially launched an ERC-20 VEN token before launching their own mainnet (the VeChain Thor blockchain) and swapping VEN for VET tokens at a rate of 1 VEN for 100 VET. At the time, the token was an ERC-20 on Ethereum. The team later discarded VEN in favour of VET when they launched a mainnet version of the VeChainThor blockchain and a token swap allowed holders to swap VEN for VET at an exchange rate of 1:100. VEN is no longer an active token.⁹² There's a total supply of around 86 billion tokens of which 75% are in circulation.

1.24 ZCash (ZEC)

Created in 2013, ZCash is a privacy protecting digital currency that was a fork of the original Bitcoin protocol. Originally known as "Zerocoin", ZCash uses a form of zero-knowledge proof called zk-SNARKs that allows it to provide a privacy option. ZCash has a public blockchain to show transactions, but hides the amount, sender, and recipient addresses by encrypting transaction metadata rather than making it publicly available, as Bitcoin does. ZCash offers two types of addresses: shielded and transparent. Shielded addresses are not visible and transactions between shielded addresses don't reveal address, transaction amount, or contents of the encrypted memo field. However, transparent addresses and transactions between them are publicly viewable on the ZCash blockchain, in the same way that Bitcoin addresses are viewable.⁹³ ZCash addresses are either private (z-addresses) or transparent (t-addresses), with private z-addresses starting with "z" and transparent t-addresses starting with "t".

Between these two types of addresses, there are four transaction types. A Z-to-Z transaction appears on the public blockchain, so it's known to have occurred and that fees were paid. But addresses, transaction amount, and the memo field are encrypted and not publicly visible as it leverages zero-knowledge proofs.⁹⁴ The owner of an address may choose to disclose z-address and transaction details with trusted third parties—to comply with

audit or compliance for example—using view keys and payment disclosure.⁹⁵ A T-to-T transaction works just like Bitcoin: the sender, receiver, and transaction value are publicly visible. It's important to note that the two ZCash address types are interoperable; funds can be transferred between z-addresses and t-addresses. It also offers encrypted memos, available for shielded transactions, allowing the sender to include relevant information to the receiver, completely encrypted. Owners of shielded addresses can disclose transaction details for regulatory compliance or auditing and the owner can disclose all incoming transactions and the memo field but doesn't have access to the sender address unless identifying information is included in the memo field. ZCash is also expected to eventually support full viewing keys that reveal all transaction values in and out of the address.⁹⁶ Unlike other projects, ZCash is run by a private for-profit company and 10% of the monetary base goes to the founders. As ZCash was a fork of Bitcoin, it kept the same monetary supply of 21 million tokens and uses proof-of-work but has differences like using 1.25-minute blocks and a halving of the reward (currently 3.125 ZEC) halving every four years.⁹⁷ Out of the total supply of 21 million ZEC, approximately 60% are issued.



5

The Technology Behind Bitcoin: Blockchain

Before considering the emerging role that crypto-assets are playing in the financial ecosystem, it's vital to take a moment to consider the broader impacts of the technical innovations showcased in the Bitcoin whitepaper. This chapter will focus on how the broader application of this technology—typically referred to as blockchain—is shifting how the financial services community considers the architecture of the systems that enable financial transactions, and we'll investigate the characteristics and challenges facing blockchains and explore several possible use cases.

1 Defining the Characteristics of a Blockchain

To the surprise of many, the term “blockchain” is not even mentioned once in Satoshi’s white paper. The closest Satoshi comes to saying blockchain is via references to “blocks are chained” or “chains of blocks”.¹ However, the idea of having blocks and linking them in a chain using cryptographic functions is the basis of the Bitcoin network, and why the birth of blockchain is attributed to Satoshi.

Where Does the Name Blockchain Come From?

If Satoshi never used the term “blockchain” in the Bitcoin whitepaper, where did it come from? Whilst some claim that the term “block chain” (used separately) can be found in some cryptography mailing lists around 2008,² the term did not enter the mainstream until about 2015. According to some researchers, a few media articles in late 2015 catalysed the use of the term “blockchain”.³ One was in *Bloomberg Markets* titled “Blythe Masters Tells Banks the Blockchain Changes Everything”⁴ featuring Blythe Masters, who was a respected financial innovator who played a big role in developing the credit default swaps markets. The other was in the October 31, 2015 issue of *The Economist* titled “The Trust Machine”, which featured blockchain and used the term blockchain throughout the piece.⁵ Google searches for the term “blockchain” are reported to have risen over 70% in the days following the release of these articles.⁶ Since then, the term has been widely used and was finally added to the Merriam-Webster dictionary in March 2018⁷

It's also important to clarify that there is no single blockchain. For example, the Bitcoin blockchain is completely different from the Ethereum blockchain, not to mention the Solana or Algorand blockchains. They may all achieve the same goal, but each has its own rules, coding languages, purpose, etc. A good analogy would be VHS and Betamax cassette formats or HD-DVD vs. Blu-ray formats. Both allow you to watch a movie, but the way each operates is different.

A more modern analogy could be Apple iOS vs. Google Android operating systems. Both allow you to use your smartphone in new and innovative ways, but each function slightly differently. However, unlike operating systems or cassette formats, where there were often two or three competing systems, there are now hundreds of blockchain networks. There may only be a handful of blockchains that become widely adopted amongst large developer communities, applications, and users in the future, but others believe that the key lies in having solutions that enable interoperability between blockchains or inter-blockchain communications.⁸ Whilst it is difficult to know how the future will unfold, this is an area worth keeping an eye on. Although each blockchain contains different features and attributes, there are several characteristics that most blockchains typically share⁹:

- **Decentralised and transparent:** There is no central database or central authority, and each participant maintains a copy of the ledger. Users can check on any transaction that has taken place at any time on the blockchain. The degree of decentralisation varies from blockchain to

blockchain, in that some like the Bitcoin blockchain, are very decentralised, whereas others like EOS are more centralised.

- **Consensus-driven:** All participants share and update the ledger after reaching a consensus and agreeing on the validity of transactions. Whilst true of most major blockchains, there are other ways to achieve consensus, as we have previously seen, including proof-of-work and proof-of-stake as two of the most common consensus mechanisms.
- **Immutable:** Once data is added to the blockchain, it cannot be altered, thanks to the use of the cryptographic techniques we discussed earlier.

There are exceptions to the above, but being decentralised, consensus-driven, and immutable are common characteristics across most blockchains, with the biggest fundamental distinction between different blockchains is whether they are public or private, which we will discuss shortly.

What's the Difference Between Blockchain and Decentralised Ledger Technology?

The terms Distributed Ledger Technology (DLT) and blockchain are often used interchangeably, but there is an important distinction. DLT is simply a decentralised database managed by various participants.¹⁰ Blockchain, on the other hand, is a type of DLT with a specific set of features that consists of having blocks form a chain. One way of looking at it is that DLT is the generic umbrella term and blockchain is a sub-category, whilst another way is that all blockchains are DLT, but not all DLT is a blockchain. A car is a type of vehicle in the same way that blockchain is a type of DLT,¹¹ and there are now numerous DLT networks not using blockchain (e.g., IOTA, Hashgraph)¹²

2 Differences Between Private and Public Blockchains

If you want to start a passionate debate between blockchain aficionados, bringing up the topic of private vs. public blockchain is a sure-fire way to get things going (Table 1).

The main distinction between public (also called permissionless) and private (or permissioned) blockchain is who can participate in the network, like the difference between the internet (open to many) and an intranet (set

Table 1 Key distinctions between public (permissionless) blockchains and private (permissioned) blockchains

		Read	Write	Commit	Example	
Blockchain types	Open	Public permissionless	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Sovrin
Closed	Consortium	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger	
	Private permissioned ('enterprise')	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries	

*Requires significant investment either in mining hardware (proof-of-work model) or cryptocurrency itself (proof-of-stake model).

up by a company for its own private use). A public blockchain network is completely open, meaning anyone can join and participate. Anyone can become a “bookkeeper”, add blocks to the blockchain, and conduct transactions. Bitcoin, Ethereum, and Litecoin are examples of public blockchain networks. On the other hand, a¹³ Hyperledger Fabric (Linux Foundation), Corda (R3), and Quorum (Consensys) are examples of private blockchains.

These private blockchains came about when some businesses realised they liked the utility of Bitcoin’s blockchain but were not comfortable (or in certain cases not allowed by law) to be as open with the information they wanted to place on a distributed ledger.¹⁴ Whilst we could go on for hours covering the pro and cons of each (there are many articles online for anyone interested in this topic), the reality is there are uses for both public and private blockchains and both are likely to coexist for the foreseeable future, each with its own set of use cases.

3 Challenges of Blockchain

Blockchain technology is not a panacea that will solve all the world's problems, and whilst it has many unique advantages, it also has some downsides:

- **Anonymity:** One of the things that makes public blockchains, such as the Bitcoin blockchain, unique is that they allow anyone to join the system and conduct transactions. However, whilst every transaction is traceable, it's difficult to know who's behind a given movement of funds. Whilst this may present positive factors, including the elimination of unreasonable censorship, it can prove a challenge when it comes to complying with regulatory frameworks (e.g., financial institutions) that require those institutions to know who their counterparties are. This is why certain industries have opted to use private blockchains where the identity of participants is known and, in many cases, each participant needs to be vetted by the others before being admitted.
- **Quality of Information:** Whilst the data on a blockchain is immutable, it does not necessarily mean that it is accurate, and the same principle of “garbage in, garbage out” applies as with any other database.
- **Interoperability:** The blockchain industry is still, relatively speaking, in its infancy, and there are no dominant established industry standards for its technology infrastructure. Most blockchains today operate in a standalone universe with little interoperability with other blockchains. Whilst efforts are being made to address this, we are still a couple of years away from reaching a solution that enables full interoperability.
- **Mass Adoption:** Blockchain is still new technology, most people and enterprises are in the early days of the learning curve, and it is unlikely that any large enterprise will move their entire database onto the blockchain anytime soon. This adoption will take some time, and there will be a day when people will be able to conduct transactions faster and more efficiently without knowing that the backend they're using is a blockchain, like how we today turn on our Wi-Fi and surf the web without really knowing the various internet protocols operating in the background.
- **Legal Uncertainty:** Current regulatory frameworks and requirements—particularly in highly regulated industries like financial services and healthcare—were not drafted with blockchain technology in mind. Basic legal concepts ranging from customer data protection to more recent data privacy requirements like the “right to be forgotten” mandate a detailed review in a blockchain context.

Whilst the above challenges may appear daunting, many individuals and groups around the globe are already working to address these issues. The blockchain ecosystem is growing at an astonishing pace, and the interest in the space from large corporates and financial institutions has increased exponentially in recent years. The financial services industry has been actively involved in the blockchain space, usually experimenting with permissioned and private blockchains via various consortiums, allowing financial institutions to experiment with blockchain whilst operating in private environments, including Hyperledger Fabric (Linux Foundation), Corda (R3), Quorum (Consensys), and the Ethereum Enterprise Alliance, each consortium with its own set of particularities.

How are Blockchain Consortiums Organised?

Blockchain consortiums come in different forms and shapes, but are generally organised around three primary parameters:

- **Technology:** These are generally open-source protocols with related technology platforms and developer communities. The Hyperledger ecosystem, managed by the Linux Foundation, and R3's Corda network are two such examples
- **Industry:** For the most part, a group of related industry actors come together to explore certain blockchain-based use cases whilst addressing some common industry pain points. The B3i consortium in the insurance industry, which is owned by 21 insurance market participants, is an example¹⁵
- **Geography:** Different blockchain initiatives focus on a specific geographic region or country. The Alastria network in Spain, in which companies from the banking, energy, and telecommunications sectors come together, is an example¹⁶ as is the China Blockchain-based Service Network (BSN)¹⁷

As excitement about the potential of blockchain continues to grow and pressure increases for firms to demonstrate engagement with the technology, there's a risk that organisations may be pursuing pilots and proofs of concept that are unlikely to deliver long-term value or scale to production. In fact, a November 2017 report published by Deloitte found that out of a total of 26,000 blockchain projects launched in 2016 (that had made contributions to the public code repository GitHub), only 8% remained active.¹⁸

Things have improved since then and whilst it's nigh impossible to keep track of all production deployments around the globe, in 2019 it was estimated that there were hundreds of live blockchain networks that were being

used in production environments across a variety of sectors and industries.¹⁹ As in many other verticals within the FinTech industry, there has been a lot of innovation theatre that has taken place in the blockchain space, and whilst the promise of blockchain technology may be large, long-term success will require participants to avoid innovation theatre and focus activities on use cases with strong potential to develop into production.

What is Blockchain Innovation Theatre?

Blockchain innovation theatre refers to cases when financial institutions or other organisations get involved in blockchain proofs of concept or consortiums purely from a marketing perspective, with no real intention or strategy on how they can integrate the technology into their business. This phenomenon happens very frequently in the FinTech world, where young companies are radically different animals from incumbent financial institutions, with completely different cultures and values. Attempts at partnership within the confines of the traditional incumbent organisation often fail and for this reason, many incumbents have elected to set up internal innovation teams and labs with the objective to learn how to effectively collaborate with FinTechs. These labs are a new kind of physical or virtual environment, a designated team or an initiative created by companies with a mission to serve as a focal point for innovation programs, research, and/or design activities, and will scan the market for new technologies or start-ups, meet with the teams, and potentially run proofs of concept to test their technology. The end goal is to be able to integrate some of these start-ups or their technology into existing systems.

Yet for all their popularity, such labs face a litany of problems. The creation of a lab is not the same as clear executive vision and a deep commitment of resources to the transformation of an organisation. A lab may be created simply for marketing and public relations reasons, or to point to when shareholders ask questions about the institution's strategy for addressing FinTech disruptors. Labs created in this way are typically not granted a meaningful budget and have limited authority to challenge the entrenched interests of product owners and other mid-level executives across the organisation. This is frustrating not only for the FinTech start-ups who risk spending considerable time and resources on proofs of concept with no scope to scale across the organisation, but also for the incumbent organisations' innovation teams who do not feel empowered. Given these issues, it's not surprising that innovation teams in incumbent financial institutions tend to see high rates of turnover.

Indeed, even when strong support and clear direction exist for innovation lab teams, their work can face significant resistance from within the institution. The aim of a lab is to develop capabilities that will give the institution a

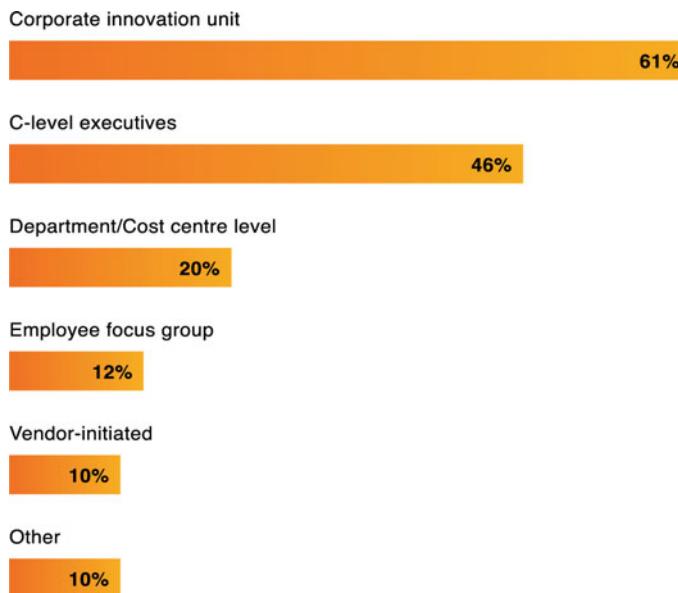


Fig. 1 Who initiates blockchain projects at the enterprise level? (Source “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)

competitive advantage in the long term, but the immediate economic impact of many lab projects is often not measurable. This creates tension with many staff and executives responsible for “business as usual” operations, whose buy-in is essential to the project’s success, but whose performance is measured on a quarterly or annual basis. Thus, the FinTech innovation efforts just become theatre, much as was true for FinTech, and unfortunately, has also become the case with blockchain technology

However, data suggests that many of the innovation units at financial institutions have been successfully driving blockchain initiatives within their organisations, and even more positively, the C-suite has been the driver behind enterprise blockchain initiatives in nearly half of surveyed organisations²⁰ (Fig. 1).

4 Use Cases of Blockchain

As this book is about crypto-assets and not blockchain specifically, we won’t go down the rabbit hole of all the different blockchain use cases in various

industries. I could write an entire new book on each industry and how blockchain can help, and anyone interested to find out more can simply Google blockchain and “insert industry” and you’ll undoubtedly find a series of whitepapers or analyses written by consulting firms or start-ups (Fig. 2).

Whilst not the focus of this book, it’s important to at least touch upon the obvious use cases that are being tackled in the broader financial services space. Given that the existing financial system is built on a complex network of trusted third parties and hub and spoke systems, it’s no surprise that discussions of the potential use cases of blockchain have generated innumerable ideas and so it should not come as a surprise that the finance and insurance industry represent almost half of all the blockchain use cases and live networks (Fig. 3).

A few finance use cases that are frequently cited include clearing and settlement, trade finance, KYC, and cross-border payments. There have been numerous experiments trying to leverage blockchain for clearing and settlement, which is basically the cumbersome process that takes place behind the scenes after someone buys a financial instrument or transfers funds. A 2017 report from Accenture estimated that this process costs financial institutions over US\$30 billion a year and that using blockchain could help save nearly a third of costs, or around US\$10 billion a year.²¹ However, changing the “pipes”, especially when it comes to an infrastructure that has numerous legacy layers and is global and full of high stakes, is not easy. It may take years, if not decades, before we see blockchain replacing the existing infrastructure,

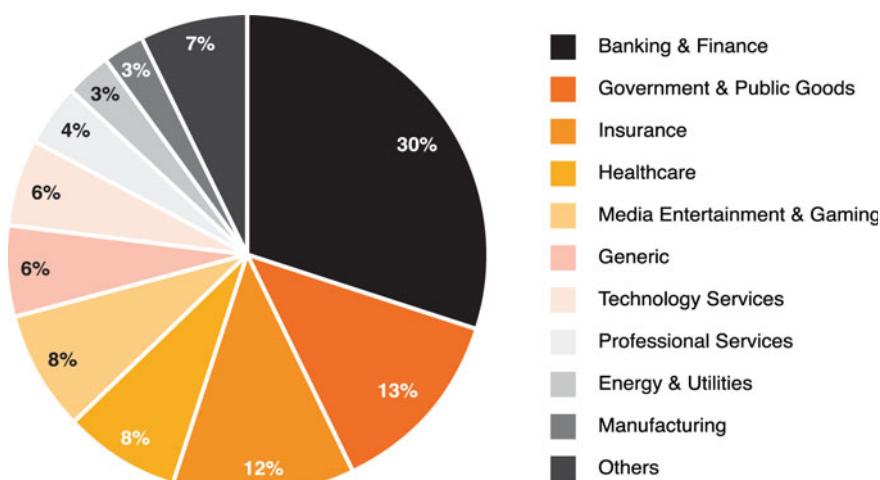


Fig. 2 Frequently cited blockchain use cases by industry (Source “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)

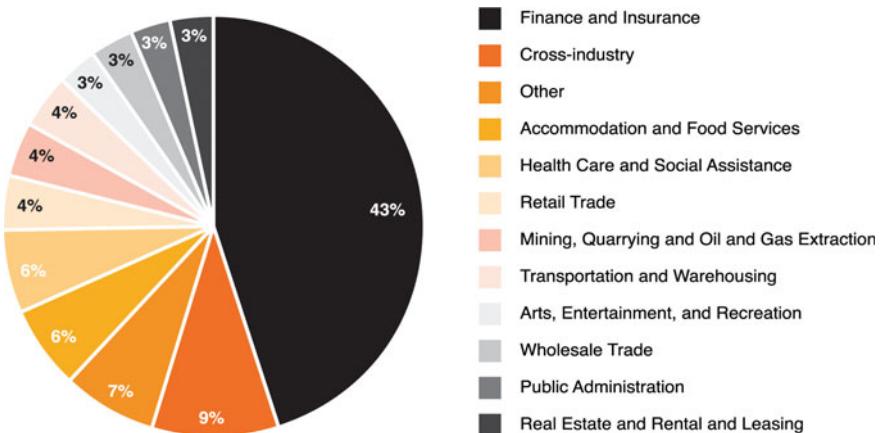


Fig. 3 Frequently cited blockchain use cases by sector (Source “3rd Global Cryptotasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020 [33])

and why we may see an entire parallel ecosystem of tokenisation or tokenised securities arise first (more on that later). The trade finance industry, worth over \$10 trillion per year, is another textbook example of how blockchain can help, in that there are many manual and cumbersome steps in a simple transaction of a Canadian importer buying a container of goods from China (Fig. 4).

There are also numerous use cases specific to the insurance industry, from smart contracts in episodic insurance to basic claim processing. For example, insurance group AXA has started to implement blockchain smart contracts to offer “direct and automatic compensation to policyholders whose flights are delayed”.²² If a policyholder purchases flight delay insurance on AXA’s new platform “fizzy”, the transaction—or insurance contract—is recorded on the Ethereum blockchain. The smart contract is directly linked to global air traffic databases, so if a delay of two or more hours is recorded in air traffic systems, policyholders will automatically receive their compensation. There are also numerous use cases outside of financial services or insurance in industries ranging from food and drugs to government and identity. For example, there are now a variety of experiments focused on how to use blockchain for food safety and provenance, particularly useful in countries like China and India where counterfeit goods, including food and drugs, are still way too common.

In another example, a great deal of research has been done on how blockchain-based land registries can harness smart contract technology to not only establish land titles, but to also automatically transfer land ownership

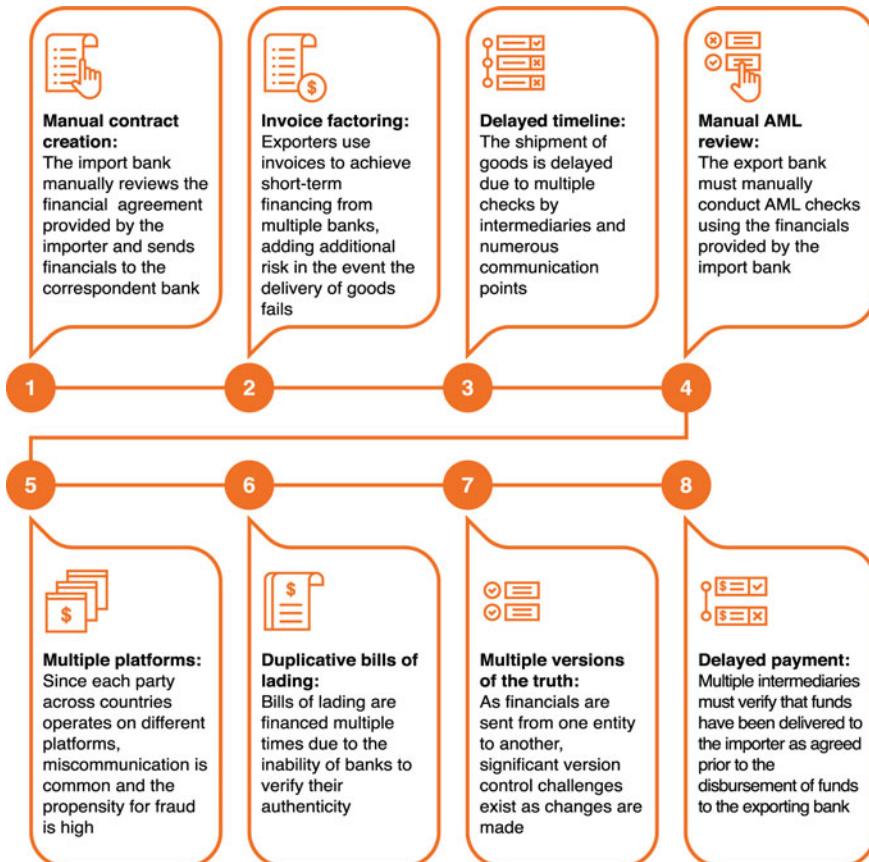


Fig. 4 Current challenges with traditional trade finance (Source Soumik Chatterjee, Vikas Singla, and Matthew Lam, "How Blockchain Can Reshape Trade Finance," Deloitte, December 9, 2019)

and hamper fraudulent transactions.²³ Using this technology could cut transaction times between land buyers and sellers substantially,²⁴ and according to a report by the United Nations Development Programme, in a country like India where corruption, lack of information, and the inability to verify transactions have led to a loss of confidence in the system, this technology could be a real game-changer in enhancing the reliability of land recognition.²⁵

Why are We Still Using Chops?

If you thought that chops (or seals and stamps) had gone the way of other outmoded tools like pagers and fax machines, you'd be wrong. Many countries

across East Asia still use chops for business or regulatory purposes. In Hong Kong, where I spent many years of my professional life, I never cease to be amazed that corporate chops were still required for many types of documents, from contracts to purchase orders. On one occasion, I was getting a haircut when a delivery arrived, and the courier did not want to leave until my hairdresser had put the company chop (a stamp that can be easily copied five minutes later) on the delivery receipt. But Hong Kong is not alone. Japan is notorious for its widespread use of its signature Hanko chops in nearly every aspect of life, but the seemingly unending lifespan of the Hanko may finally be nearing a close, with Japan's former Prime Minister declaring war on these chops to further digitise the nation.²⁶ After all, this inefficient practice has been blamed for causing delays in the transfer of vital information and for forcing individuals to physically show up at offices during the pandemic just to stamp a document²⁷

Ultimately, it's ridiculous that in 2021, with all this technology at our fingertips, that these chops are still required. Given how easy it is to forge a chop (not to mention traditional signatures), this outdated form of authentication raises serious concerns aside from its inherent inefficiency. As the use of blockchain becomes more mainstream, we'll hopefully start to realise the uselessness of not only chops, but other "authenticity" mechanisms like wet signatures



6

Cryptocurrencies

The diversity of crypto-asset projects currently being pursued by innovators, combined with the relative newness of this ecosystem, make the accurate categorisation of crypto-assets a challenging task. No useful and sufficiently detailed framework is likely to either establish mutually exclusive categories or be collectively exhaustive in categorising the full universe of crypto-assets. Several conceivable approaches exist for categorisation, with the simplest likely to categorise crypto-assets based on easily measurable factors such as the specifications of their underlying technical protocols, size of their active user communities, or market capitalisation. However, whilst definitive, such categorisations provide little value for those wanting to understand the appropriate legal treatment of a given token or consider the appropriate valuation methodology.

A more complex approach might be to use an existing industry classification system and assign tokens to categories based on the industry that they most closely align to. In such a system, a token designed to support traceability of supply chain provenance would be categorised separately from one designed to establish a network for the monetisation of artistic content. Another way of thinking about the categorisation of assets would be to consider the rationale that a token holder would have for possessing a given token and categorising crypto-assets accordingly. For example, tokens intended to be redeemed in exchange for access to cloud computing services

The original version of this chapter was revised: Figure and text correction have been updated.
The correction to this chapter is available at https://doi.org/10.1007/978-3-030-97951-5_22

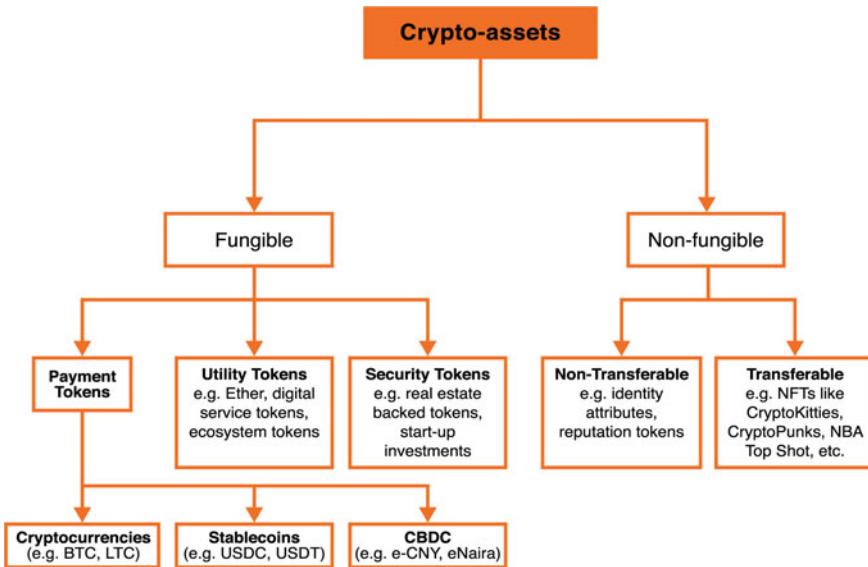


Fig. 1 Our proposed taxonomy of crypto-assets used in this text classifies tokens based on fungibility and intended usage

would be categorised differently from those representing loyalty rewards or those serving as speculative investments into a newly created business.

The taxonomy in this book draws on multiple sources to present a simplified view of crypto-assets based primarily on intended usage and functionality.¹ When I wrote my last book titled “The Future of Finance”, I presented the first version of the below taxonomy. Not surprisingly, the crypto industry has grown so much since then, and at that time, Bitcoin was still a fringe asset, Facebook had not announced Libra, and CBDCs were only discussed in academic symposia. The table is the amended version that I believe reflects the current state of the crypto-assets ecosystem and which I will use to better explain crypto-assets overall, but I expect this taxonomy to evolve with the industry over the coming years (Fig. 1).

Cryptocurrency, Virtual Currency, Digital Asset, or Crypto-Asset?

Just what exactly are we to call this new asset class? Crypto-assets? Virtual currencies? The possibilities go on and on. To try to answer this question, the OECD looked at the evolution of the terminology by regulators from 2013 to today. From 2013–2014, the asset class was primarily referred to as either Bitcoin or virtual currency, whilst from 2015–2017, the terms cryptocurrency and digital currency began to gain popularity² (Fig. 2).

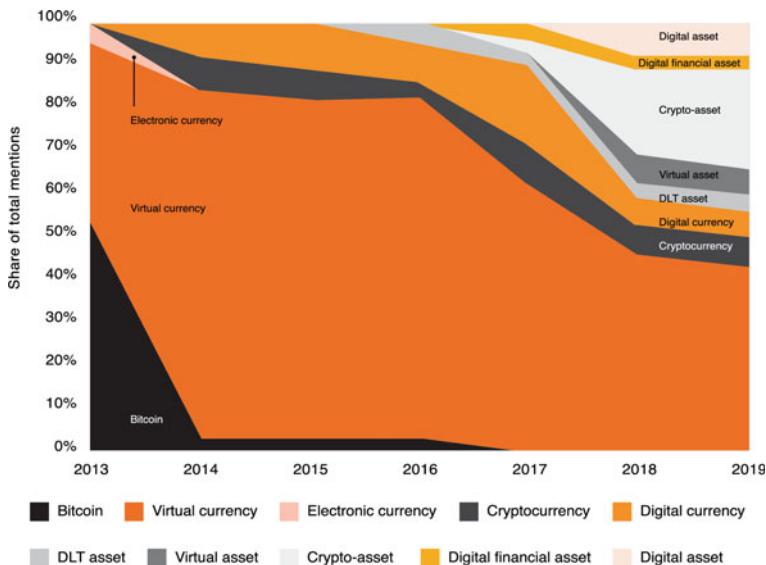


Fig. 2 Evolution of crypto terminology used by regulators (Source OECD [2020] “Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues,” OECD, Paris, www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emergingtax-policy-issues.htm)

Since 2017, the terms digital asset and crypto-asset, in addition to virtual currency, have gained greater prominence, though the jury is still out. Terminology like this may sound trivial, but it is nonetheless a practical difficulty for many practitioners in this space, having run across this issue with this book when I had to decide what term to use, settling finally on crypto-asset

1 Fungible and Non-fungible Tokens

The first major distinction that we need to consider is whether a token is fungible or non-fungible. A fungible token is a token of a crypto-asset that is functionally identical to and interchangeable with any other token of that crypto-asset. For example, any given U.S. dollar or a given share of Apple common stock is interchangeable with any other. If I promise to give you a dollar, you don’t really care what the serial number is or what year it was minted; all you care is that you receive a genuine U.S. dollar. The vast majority of crypto-assets in existence today are fungible, so, for example, if I

promise to give you a Bitcoin, you don't care when that Bitcoin was mined as any Bitcoin is identical in its characteristics, usefulness, and valuation.³ Although, as we will see later in the book, one can argue that Bitcoin used for nefarious activities or by bad actors is worth less than a "clean" or "virgin" Bitcoin. This is a problem that doesn't exist with fiat currencies as fiat money is, despite what many may think, more difficult to track than Bitcoin and most cryptocurrencies.

What is a Virgin Bitcoin?

As we saw earlier in this book, Bitcoin and most cryptocurrencies are easily traceable. In the case of the Bitcoin blockchain, all transactions are public. Whilst this has many benefits (e.g., law enforcement or data analytics), it has the counter-effect that the history of any fraction of a Bitcoin remains forever. There is no "delete history" function. For example, when I deposit \$100 in cash in a bank, the bank has no idea where that \$100 bill was beforehand, perhaps used in a bakery or a strip club. The person who is depositing it may potentially know where he directly got it from, but it's unlikely that he'll know anything more than that. With Bitcoin, we could easily go through the entire history of that Bitcoin and see if at any time in its existence it has passed by a wallet that is known to be used by nefarious actors. Whilst it's not my fault that the Bitcoin that I'm holding was used in a dark-net transaction 15 transactions ago, or many years hence, there is an element of the currency being tainted.

This is one reason why many institutional investors have been trying to buy newly mined Bitcoins directly from miners or the OTC trading desks that service them. According to some news reports, there is a premium of 10–20% for such coins,⁴ and financial institutions or more traditional investors may sometimes prefer these virgin coins to regular coins. Ironically, in addition to buying them from Bitcoin miners (or OTC brokers who service them directly), another way to buy virgin coins is from law enforcement. Law enforcement will often seize Bitcoin and other cryptocurrencies as part of their various investigations. For example, venture capitalist Tim Draper bought around 30,000 Bitcoin from the U.S. Marshalls in 2014 (then worth around US\$600 per Bitcoin). These coins were initially seized from the Silk Road dark-net marketplace investigation, and that \$18 million purchase is now worth over a billion dollars. A more recent example was in November 2020 when the U.S. government seized 69,369 Bitcoin when each Bitcoin was worth around \$15,000. These will be eventually auctioned off, and although they're directly linked to criminal activities, the fact that they're being sold by the U.S. government cleans them up, meaning they become virgin again and may command a premium.

Within the category of fungible tokens, there are three high-level sub-categories: tokens intended to be used to facilitate payments (including cryptocurrencies, stable coins and central bank digital currencies); tokens intended to be redeemed for a consumable service (utility tokens); and tokens intended to serve as investments in financial assets/securities (security tokens). From the fungible token category, the broader payment token space has exploded in prominence in recent years, from stable coins to CBDCs, and we will discuss each of these categories over the coming pages.

Non-fungible tokens are tokens of a crypto-asset that are not interchangeable as each has unique properties, the equivalent of a passport or a land title in the physical world. In the crypto world, non-fungible tokens most often refer today to collectibles (from the early day CryptoKitties and Punks to the more recent Bored Apes and Beeple pieces—all of which will be discussed in this book). Within the category of non-fungible tokens, there are two broad sub-categories: tradable tokens and non-tradable tokens. Tradable tokens are “alienable” and can be transferred to a new owner. For example, I can own an NFT of a CryptoKitty that is for all intents and purposes unique, but I can transfer it to someone else. In comparison, non-tradable tokens are inalienable and thus not transferable between owners (e.g., digital identity).

In the pages that follow, we’ll provide a brief explanation of each of these token categories along with examples. However, it’s important to bear in mind that the universe of crypto-assets is at a nascent stage, and if these assets are to gain large-scale adoption, each category will likely need to expand and change, and new dimensions of categorisation will need to be considered.

2 Payment Tokens

A payment token is a crypto-asset whose features are intended to serve as a medium of exchange, a store of value, and a unit to account for a broad array of transactions. In other words, they are cryptographic tokens that use blockchain technology to secure transactions and to control the creation of monetary units or units of value, aiming to serve a function like that of traditional fiat currencies and associated payment networks (e.g., debit/credit networks, PayPal, Venmo, remittance networks). However, it’s important to understand that many payment tokens (the best example being Bitcoin) are probably perceived by most people today as stores of value rather than units of exchange for payments (although that was the original purpose proposed by Satoshi). All things being considered, I still believe there are benefits to keeping such assets in the broader payment tokens category.

At the current stage of the development of crypto-assets, we can categorise payment tokens into three sub-categories: (i) cryptocurrencies, (ii) stable coins, and (iii) central bank digital currencies. We'll discuss each one of the above in detail over the coming pages, and whilst the structure of each payment token is different, they tend to share several general characteristics⁵:

- **Global and always available:** You can transfer or receive cryptocurrencies 24 h a day, 7 days a week, 365 days a year. Crypto markets don't sleep.
- **Cryptographically secure:** Blockchain networks use a combination of public and private key cryptography, which are secure and unbreakable based on the technology available today. However, as discussed in this book, there's still a risk that the holder of the token's private keys will be stolen, allowing a malicious actor to steal its funds. Whilst blockchain has many benefits, we shouldn't rule out the idea that a central bank could in theory issue a central bank digital currency in the future not based on blockchain, but rather on a different centralised platform.
- **Fast:** Whilst some payment tokens such as Bitcoin have slower processing times than domestic payment systems (e.g., debit and credit card networks), most payment tokens offer significantly faster processing times for most cross-border transactions.
- **Inexpensive:** Transferring cryptocurrencies is (almost) free or with very low fees depending on how each blockchain is designed and what type of transaction fees or gas it charges. However, the fees may increase significantly during times of high demand of the network.
- **Irreversible:** Once a transaction has been executed, it is impossible to reverse as no central authority exists to override past transactions. Transactions can only be functionally reversed through a second, mutually agreed upon transaction between counterparties that mirrors the first transaction. In this way, systems very much resemble the use of physical cash.
- **Pseudo-anonymous or anonymous:** Most payment tokens operating today provide some level of anonymity to users (another similarity with the use of physical cash). In the case of Bitcoin and many similar systems, users have pseudo-anonymity, meaning that whilst transactions are public and traceable, the counterparties in a payment transaction are identified only by a unique string of numbers and letters (their public key) making it difficult to identify the beneficial owner of any given token (unless using some specialised traceability software). In other cases, such as for privacy coins like 'Monero', additional features have been added to create "true" anonymity. We shouldn't exclude the idea that a central bank that would

issue its own digital currency would be able to have access to transaction or identification data that would otherwise not be accessible to the broader public.

Despite their unique characteristics and benefits, payment tokens are still facing challenges in achieving mass market adoption. Some of these challenges include:

- **Poor Usability:** Despite some improvements, sending and receiving crypto-assets is still not a very user-friendly process and the use of public keys and crypto wallets is difficult to understand for the average person. Usability improvements are likely to continue, as is public understanding of crypto-assets, but is unlikely to occur overnight. Even in the case of transformative technologies like the internet, broader public adoption is a process that occurs over many years, if not decades.
- **High Volatility:** Some type of payment tokens (e.g., cryptocurrencies like Bitcoin) exhibit high volatility when compared to fiat currencies. Whilst this may be desirable for speculators and traders, it creates serious challenges for both consumers and merchants seeking to use the asset as a unit of account and a means of exchange. It's important to note that this is not (or should not be) a problem faced by stablecoins or central bank digital currencies.
- **Irreversibility:** Whilst the irreversibility of crypto-asset transactions may be desirable in some instances, it's also a source of customer concern. If you lose your bank PIN or make a wrong transaction, you can always call the bank to get help. If you lose the private keys or transfer to an incorrect crypto address, those crypto-assets are gone forever. There is no universal customer support helpline for crypto-assets!

3 Cryptocurrencies

As we have seen previously, money can be anything that can serve as a

- **Store of value:** allowing people to save and use it later
- **Unit of account:** providing a common base for prices
- **Medium of exchange:** allowing the buying and selling for something else⁶

As we've discussed, cryptocurrencies may very well be considered money. I can buy Bitcoin to store wealth to buy a house one day; I can price items in BTC; and I can buy and sell items using Bitcoin. In March 2018, the term "cryptocurrency" was added to the Merriam-Webster dictionary and defined as "any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralised system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions".⁷ Whilst most cryptocurrencies are indeed decentralised, it is important to highlight the distinction with any centralised cryptocurrencies.

3.1 Decentralised Cryptocurrencies

A decentralised cryptocurrency is one that generally meets the characteristics of decentralisation including that there's no central authority; it's peer-to-peer, distributed, and anyone can participate from becoming a miner to creating an address, or making a transaction. As we've seen earlier, Bitcoin is a good example of a decentralised cryptocurrency, where the rules governing the Bitcoin network are transparent and anyone can get involved. A large number (if not the vast majority) of cryptocurrencies are designed to be decentralised (e.g., Bitcoin, Litecoin) although there is a risk that, at times, it becomes more centralised.

A good example is in the early days of cryptocurrency. In the early days of Bitcoin, Satoshi was probably one of the only Bitcoin miners. Satoshi and some others could have colluded and come together to commit a 51% attack, which would enable them to take control of the Bitcoin network. Whilst this could have put an end to the Bitcoin network as trust would have been lost, that was a theoretical risk. In practice, though, that wouldn't be logical as it would have resulted in the loss of the Bitcoin that they hold, thus defeating the purpose of the attack in the first place.

However, there are always fears that an 'in principle' decentralised cryptocurrency could become gradually centralised over time. Stocking with the Bitcoin example, in the early days, anyone with a laptop could become a Bitcoin miner, but today Bitcoin mining is conducted by professional mining farms, and it would be very difficult for anyone to take over the network. For example, until the summer of 2021, 65% of Bitcoin mining globally took place in Mainland China (with the vast majority in Sichuan province).⁸ In theory, these Chinese miners could have come together to collude and commit a 51% attack, which would enable them to take control of the Bitcoin network. The reality is that they would have no incentive to do so as

that would destroy the value of the very same Bitcoin they're trying to mine. Others argue that whilst Bitcoin at its core is decentralised, most users are using centralised intermediaries like crypto exchanges or custodians, which defeats the purpose of decentralisation.⁹

3.2 Centralised Cryptocurrencies

A centralised cryptocurrency is one that does not meet the characteristics of decentralisation listed above (no central authority, peer-to-peer, distributed, or that anyone can participate). Some types of cryptocurrencies are by design centralised, with most stablecoins and central bank digital currencies good examples (although there are exceptions there as well, from DeFi stable coins to decentralised CBDCs, but more on those later.). For example, a stablecoin issuer, which can be a for-profit company or a foundation, could be responsible for ensuring that the stablecoin will operate as it says it does, or a central bank could determine who has the right to have a wallet on its network to access its central bank digital currency.

Some argue that the design features of some cryptocurrencies make them inherently centralised although they may have been designed or marketed as being decentralised. A good example is the EOS token discussed earlier in the book. The EOS blockchain uses only 21 block producers that verify the various transactions in its delegated proof-of-stake consensus mechanism. In comparison, there are thousands of Bitcoin nodes. The EOS blockchain is designed that way and sacrifices decentralisation to enable faster transactions. Another example is the NEO blockchain, which only has seven consensus nodes; the NEO Foundation has a considerable number of votes.¹⁰

There are also the centralised arguments. The example above of the concentration of Bitcoin miners is a good example when it comes to mining concentration, and another example could be price and power centralisation where the issuer of a cryptocurrency still holds most of the tokens and could in theory manipulate the price. For example, the company behind XRP, Ripple Labs, still holds more than half of all XRP tokens.¹¹ Many would argue that some level of centralisation (or a sacrifice of a bit of decentralisation) is required to make the network more scalable. Others would disagree and argue that it's important to sacrifice a bit of scalability in order to have increased security and decentralisation. This is the problem of the blockchain trilemma and bringing this question up at a gathering of crypto aficionados is certainly entertaining as it often inflames a viral debate between individuals (Fig. 3).

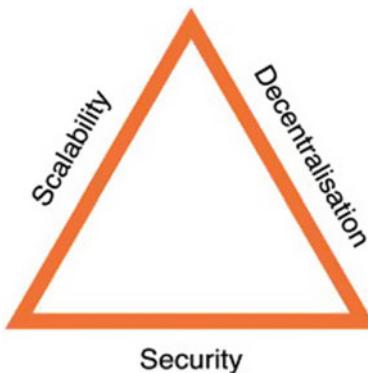


Fig. 3 The blockchain trilemma

What is the Blockchain Trilemma or Impossible Trinity?

Economists often talk about the Impossible Trinity, which is the economics theory that it is impossible to ensure a fixed exchange rate, free capital flows, and an independent monetary policy, all at the same time.¹² The blockchains and crypto community often talks about the blockchain impossible trinity or blockchain trilemma, which is the theory that it is impossible to have security, scalability, and decentralisation, all at the same time. For example, the Bitcoin network may be secure and decentralised, but this makes it not very scalable with only a handful of transactions per second. In contrast, a platform like NEO or EOS may be less decentralised, but able to process thousands of transactions per second as it's more centralised. In recent years, many new blockchains have appeared, from Avalanche to Algorand, that claim to address the blockchain trilemma and enable blockchains to operate in a way that is secure, scalable, and decentralised.

3.3 Privacy Coins

One category of cryptocurrencies worth discussing are privacy coins, unique cryptocurrencies that protect the privacy of their users by shielding their identity and the origin of their transactions, with popular examples including Monero and, to a lesser extent, Zcash and Dash. Unlike Bitcoin and most cryptocurrencies, privacy coins enable users to leverage blockchain technology and send each other transactions without tracing those transactions back to them. Each privacy coin has its own technical mechanisms to enable this, with Monero using a three-prong approach to privacy using ring signatures,

which hide the true output (sender), RingCT which hides the amounts, and stealth addresses, which hides the receiver.¹³ Unlike Bitcoin and most cryptocurrencies, privacy coins enable users to leverage blockchain technology and send each other transactions without tracing those transactions back to them. Each privacy coin has its own technical mechanisms to enable this, with Monero using a three-prong approach to privacy using ring signatures, which hide the true output (sender), RingCT which hides the amounts, and stealth addresses, which hides the receiver.¹⁴

Privacy coins have always been controversial not only in policy and regulatory circles, but also the broader crypto community. For example, many argue that privacy coins need to be banned, the argument being that if the end user is not traceable, then it can create a money laundering or terrorism financing risk. This is why many countries and exchanges ban the trading of privacy coins on crypto exchanges. Others believe that privacy coins are almost a fundamental right and in many cases are essential in certain countries where freedom of expression and freedom of speech are at risk and tracing the transactions could allow government to clamp down on those who oppose them. In addition, many argue that privacy coins provide the same level of privacy that users enjoy today when using cash, but also when using the banking system, at least when it comes to third parties. For example, a 2020 paper by law firm Perkins Coie made this argument as to why we may need to re-explore the thinking of banning such privacy coins.¹⁵ For example, existing cash and non-crypto payment systems already provide relatively high levels of privacy to retail users. Whenever individuals pay for something in cash or, to a slightly lesser extent, with debit or credit cards, the details of that purchase are only apparent to the parties of the transaction. Third parties are not privy to these details.

A popular example of the sense of privacy afforded to modern transactions is a simple donation, be it to a charitable cause or even to a political campaign. Such donations, especially of the political sort, can be a touchy subject, but thanks to different layers of privacy, donors don't have to worry about nosy neighbours or others snooping around asking questions. Without such protection, Perkins Coie argues, donors could be susceptible to harassment, lowering the likelihood of them donating to causes they believe in. Just as it is with individuals, financial privacy is critical when it comes to businesses, since a lack of privacy would allow every one of your competitors to outflank you moving forward, simply based upon your transaction history. The argument is that an absence of the sense of privacy we've come to expect would be greatly damaging to both businesses and individuals alike.

In its report, Perkins Coie also argues that maintaining commercial privacy is critical for protecting the status quo of domestic and international business operations. Since the adoption of cryptocurrencies will continue to expand, businesses need to find a way to utilise this innovative and still-evolving technology without having to sacrifice traditional privacy protections. To draw a parallel to the value that privacy coins provide, Perkins Coie makes an analogy with internet protocols. During the early internet era, most websites used HTTP, or the Hypertext Transfer Protocol, to move data from a web server to a browser so that users could view webpages. The important thing to remember about HTTP is the data being sent to the browser from the server is not encrypted, which makes the data susceptible to theft and exploitation. To deal with that issue, HTTPS, or Hypertext Transfer Protocol Secure, was developed in the early 1990s. By using new layers of security to authenticate websites and protect the privacy of data as it moved between server and browser, HTTPS provided much better insulation from potential MITM, or “man-in-the-middle”, attacks (Fig. 4).

Broad commercial use of encryption software, however, initially faced significant opposition from both the U.S. government and law enforcement agencies. Until 1996, encryption software was subject to significant export regulations administered by the U.S. Department of State. These 1990-era battles, now known as the “Crypto Wars”, were later settled, with arguments and protests centred around constitutional and economic rights paving the way towards public access to encryption software. Mass access of encryption software cleared the field for rapid growth of HTTPS and other types of encryptions over the ensuing decade, with significant public, private, and commercial benefits attached. In recent years, organisations from Google to the White House have called for even more encryption, urging every website owner to switch from HTTP to HTTPS and requiring every federal website to run through a secure connection.

The gist of this analogy? Whilst regulators and law authorities were initially extremely sceptical and outright resistant to any new layers of encryption back in the 90 s, acceptance and adoption gradually followed, with protection and encryption now the norm, not the outlier. The question is whether privacy coins will follow a similar path (Fig. 5).

Perkins Coie argues that just as HTTPS meaningfully improved on HTTP, privacy coins represent the next generation of cryptocurrency transactions. Whilst privacy coins certainly pose AML risks, the argument is that effective management and monitoring of those risks through VASPs, as part of a risk-based AML system, should result in the public benefits of privacy coins outweighing their costs.

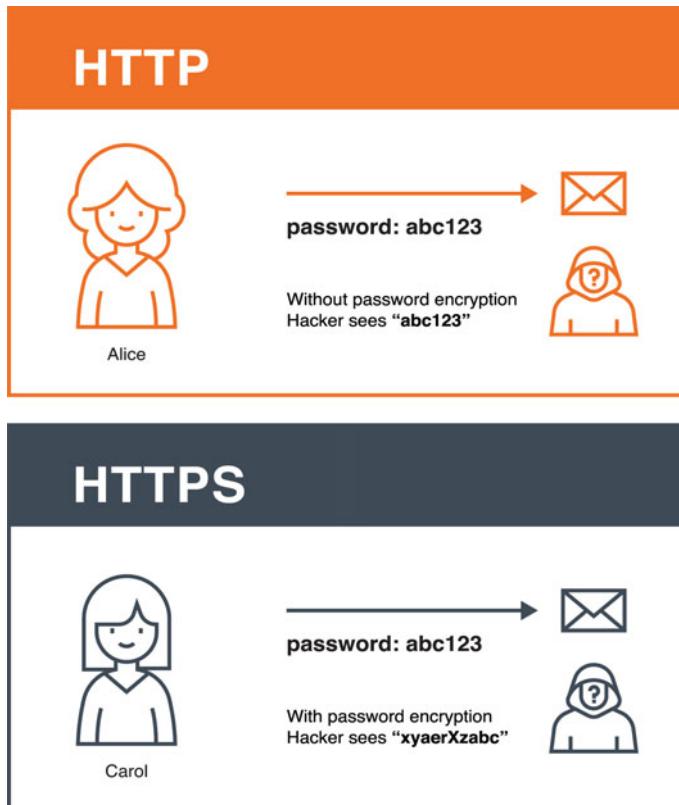


Fig. 4 Comparison between HTTP and HTTPS (Source “HTTP vs HTTPS: The Difference and Everything You Need to Know,” SEOPressor, November 21, 2019)

These include:

- **Enhanced Due Diligence:** Strengthening due diligence on VASP customers who want to use privacy coins for transactions can protect against money laundering. Additional layers of protection (from requiring the privacy coin holder to prove the source of their funds to mandating that customers provide basic sorts of contact information) could reduce some of the risks.
- **Limitations on Types of Customers and Geographies:** Both the types and geographic locations of privacy coin customers are big factors in AML risk through VASPs. By differentiating and sorting customers into different categories and focusing on where a transaction is coming from, VASPs could reduce the risk associated with certain customer types.

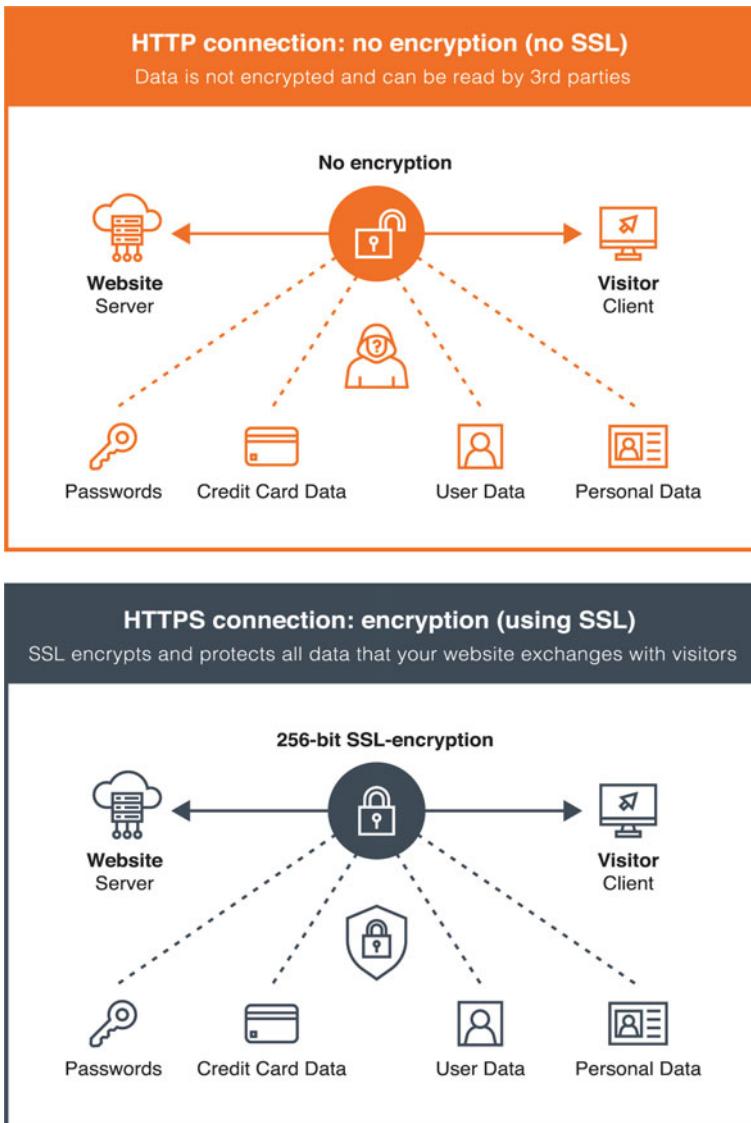


Fig. 5 Benefits of HTTPS and SSL (Source "HTTP vs HTTPS: The Difference and Everything You Need to Know," SEOPressor, November 21, 2019)

- **Ongoing Transaction Monitoring:** VASPs could require certain key details like name, contact information, and purpose of transaction before processing certain purchases made with a privacy coin. Such information would provide more transparency and could potentially deter illegal activity from taking place.

Ultimately, whilst privacy coins like Monero are often associated with money laundering and other sorts of cybercrime, the desire for privacy and protection lends itself to debate on the role that privacy coins may play when it comes to the future of money. But privacy coins are an area of focus for regulators and policymakers, especially after some reports emerged that over 45% of dark-net markets are now supporting Monero, making the coin a cryptocurrency of choice amongst the criminal community. The game changer here will be whether law enforcement is able to trace such privacy coins, where towards the end of 2020, we learned that U.S. authorities were launching a grant for companies that could help them trace privacy coins. Stemming from that announcement, crypto traceability firm CipherTrace announced that it had filed its second Monero tracing patent application.¹⁶ This is an area worth following over the coming years.



7

Stablecoins

A stablecoin is a payment token whose value is linked to that of a reference asset outside the crypto-asset ecosystem, generally a fiat currency like U.S. dollars or euros. Typically, the stablecoin token will be backed in whole or in part by its reference asset with a promise from the issuer that it can be redeemed for that asset at any time. An imperfect analogy would be the early forms of paper notes issued by a bank or central bank that were backed by gold. These notes often promised to pay the bearer the equivalent in gold when presented to a bank, as carrying a piece of paper accepted as being worth a specified amount in gold was more practical than carrying gold itself. At any time, the bearer could go to a bank, present that piece of paper, and receive the gold equivalent instead. The same is true for stablecoins.

Many payment tokens such as Bitcoin may not currently be suitable for cross-border transfers or day-to-day purchases given their high volatility or transaction fees. Stablecoins help address this problem, making it easier for individuals to pay for goods denominated in a fiat currency using crypto-assets and to make cross-border transfers without fear of volatility. There are numerous use cases for stablecoins, and we'll focus on two: one used by traders and one used by the public.

Stablecoins provide many benefits for traders and enable them to move away from volatile crypto-assets into a stablecoin without the need to leave the crypto ecosystem. This is not dissimilar to a trader of traditional stocks

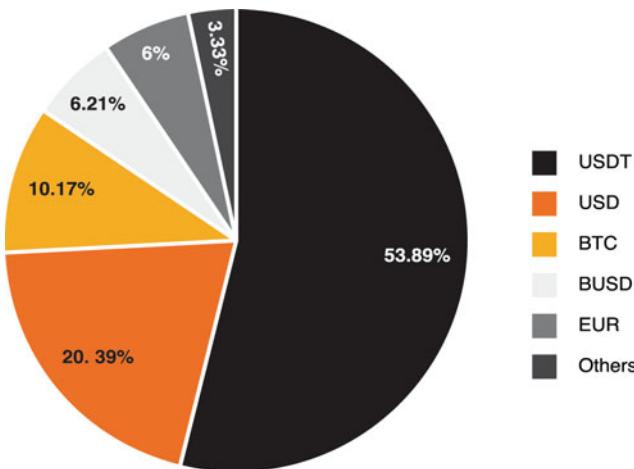


Fig. 1 Share of trade volume by market pair denomination (Jan 2022) (Source The Block Crypto, 2022)

or bonds who might respond to significant market volatility by liquidating a portion of her holdings to be kept in treasuries until markets stabilise. Given the high volatility of crypto-assets and the traditional difficulties many stakeholders face in accessing fiat money via traditional financial institutions, a stablecoin can serve as a desirable “safe-haven” asset.¹ Such a stablecoin would also be useful when trading certain crypto pairs where there is not much liquidity between those pairs. For example, in January 2021, most trading pairs were with the Tether stablecoin, USDT (Fig. 1).

Another benefit of stablecoins is their use by the public, with cross-border payments a great example. Today, the average global cost for sending money across borders is 7%, frankly an embarrassment today when we can send an email or picture to the other side of the world for free or a negligible fee.² The amounts are not small; each year, over \$550 billion is sent by 250 million migrant workers. Whilst the average fee of sending money between two G7 countries can be less than 2% (which is arguably still high), the cost for sending to or from emerging markets is often double digits.³ This is a great use case for stablecoins that allow two users to send money to each other around the world, instantaneously, 24/7, and for almost no fee. This is the problem that Facebook wanted to tackle when it launched Libra, later renamed Diem, in June 2019, a development that we will explore shortly (Figs. 2 and 3).

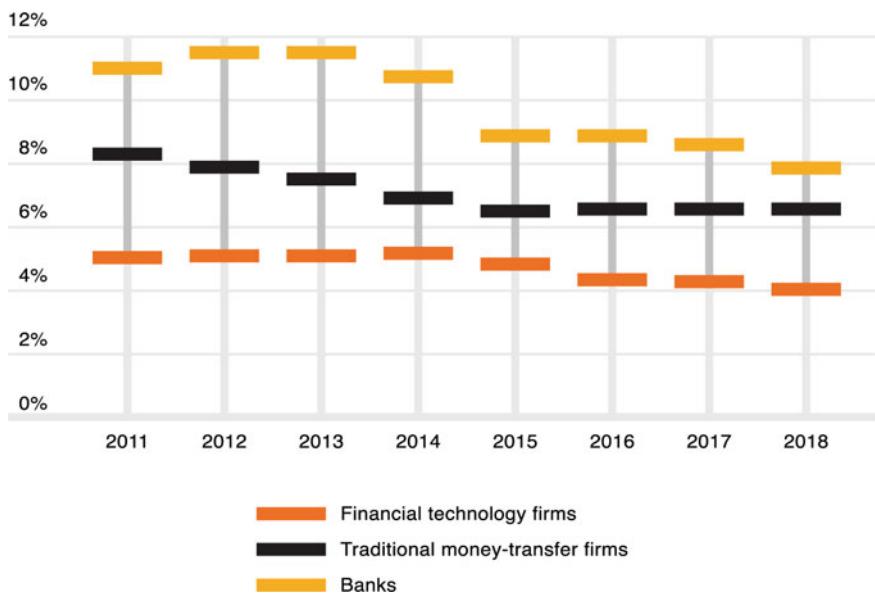


Fig. 2 Average cost of sending remittances (Source FXC Intelligence; World Bank; The Economist, April 13, 2019)

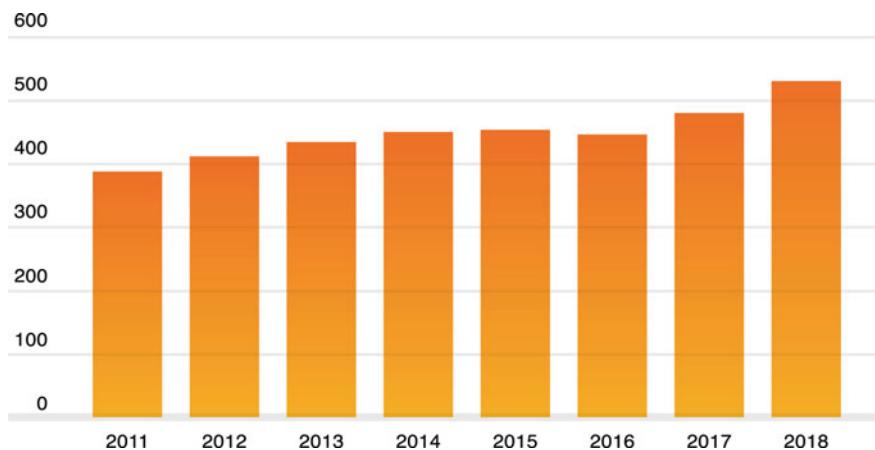


Fig. 3 Global remittances to developing countries (Source FXC Intelligence; World Bank; The Economist, April 13, 2019)

It should be noted that not all stablecoin tokens choose to use a fiat currency as their reference asset, with some instead using a physical commodity, frequently gold. Stablecoins of this type are less common than those pegged to fiat currency and add a level of complication to our taxonomy, because they may serve a dual function, straddling the categories

of payment instrument and investment instrument. As a result, unlike other payment tokens, they may be considered a security by regulators. Whilst the type, design, and purpose of stablecoins are fast-changing, we can categorise them into three general buckets: fiat-collateralised, crypto-collateralised, and non-collateralised.

1 Fiat-Collateralised Stablecoins

Fiat-collateralised stablecoins generally have a fixed face value in fiat currency that enables the holder to redeem the stablecoin on demand for that amount.⁴ For example, anyone who has a US\$1 stablecoin should be able to go to the issuer of that stablecoin and redeem US\$1 in fiat currency. Fiat-collateralised stablecoins are by far the most popular type of stablecoin in the market. The issuer of such fiat-collateralised stablecoins is expected to hold an off-chain, real-world fiat currency and issue a token that represents such a unit generally with a 1:1 ratio. This gives comfort to the holder that there is a corresponding asset or reserve for which the stablecoin can be redeemed.⁵ Redemptions of these tokens for dollars held in reserve is what inspires trust in this system. If a token owner cannot convert into the fiat currency, either because the fiat reserve is not there (or only partially there), or for any other reason, all faith and the peg would be lost.⁶ This is why for fiat-backed stablecoins, trust in the issuer is paramount, and why over the past few years, we've seen stablecoin issuers try to position themselves as being more reputable by making operations more transparent, working with reputable providers or trying to get regulated.

How Do Stablecoin Issuers Make Money?

Whilst we're seeing increased usage of stablecoins, it's worth looking at what the incentives are for those considering issuing them. It's important to remember that historically speaking, whoever is issuing a currency has some benefits. Historically, this was called seigniorage (coming from the French word *seigneur* meaning lord), the difference between the face value of the money and the cost to issue it. For example, if it costs 5 cents to produce a \$1 dollar note, then the issuing entity is making 95 cents of seigniorage on each \$1 banknote. It's the same principle for central banks when it comes to the treasury bills that they issue. In modern finance and economics, in addition to governments, commercial banks also play a role as they can create money by generating loans with deposits that they hold via the principle of fractional

banking as they don't need to hold only a small percentage of reserves for all the activities.

The reality with stablecoins is much simpler. Whilst issuing stablecoins can be a fun activity, an entity would only do so if there are clear benefits, including generating revenues, from that activity. Stablecoin issuers generate revenues in two main ways.

- **Short-term investing in safe assets like treasuries and money market funds:** A stablecoin issuer generally has the right to invest its reserves into safe, liquid, and short-term investments like treasuries or money markets for example. Whilst the interest rate on such products is low (as is the risk), this can become quite lucrative for a stablecoin with large reserves
- **Issuance and redemption fees:** A stablecoin issuer can charge a fee each time that a token is issued (issuer receives fiat and issues a token) or is redeemed (issuer receives the token and provides fiat). This generates revenues for the issuer when there are lots of inflows or outflows from fiat-to-crypto ecosystems. Also, such activity may be done by firms trying to arbitrage the price of a stablecoin with the value of their underlying fiat currency. For example, if a 1 USD stablecoin is trading at 99.8 cents, someone can buy that stablecoin and return it to the issuer in order to receive its 1 dollar in fiat. However, the arbitrage opportunity must be worth it. For example, the stablecoin Tether charges a fee of 0.1% of the issuance or redemption of stablecoins and charges a US\$150 verification fee⁷

There are also other activities that may take place like market making but the above two are generally the main sources of revenue for any issuer.⁸

Consequently, the stablecoin market for fiat-backed issuers is now separated into two main categories: regulated and non-regulated issuers.

1.1 Regulated Fiat Stablecoins

There are several regulated stablecoin issuers globally. Many of the stablecoins issued in the United States are issued by entities that are licensed as trust companies under the New York Banking Law. The issuers of the Paxos Standard (PAX), the Paxos Trust Company or the issuers of the Gemini Dollar (GUSD), the Gemini Trust Company, are good examples. Both these firms hold the dollar deposits of their customers in omnibus accounts at third-party banks with the intention that they be eligible for Federal Deposit Insurance Corporation (FDIC) “pass-through” deposit insurance. Other well-known

stablecoin issuers operating in New York, like Circle, are not banks or trust companies but have obtained a BitLicense from the New York Department of Financial Services and maintain U.S. dollars in segregated accounts with third-party banks, on behalf of and for the benefit of, stablecoin holders.⁹

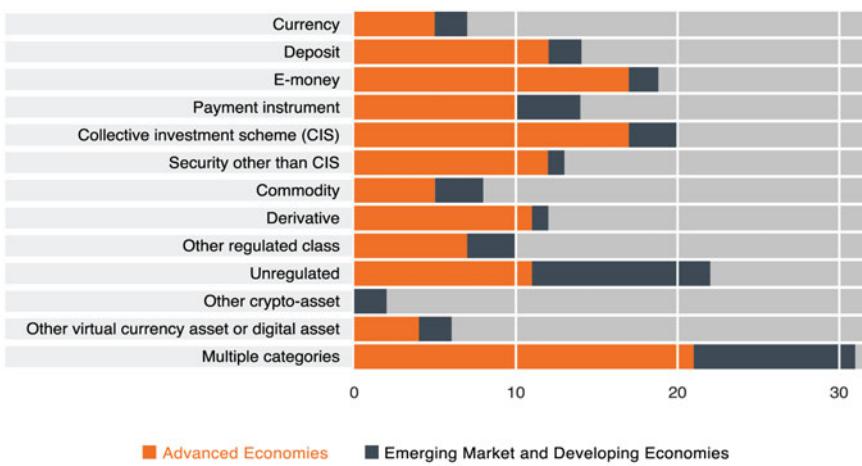
A big development took place in 2018 when crypto firms Coinbase and Circle founded the CENTRE Consortium, which is a “joint venture aimed at establishing a standard for fiat on the internet and providing a governance framework and network for the global, mainstream adoption of fiat stablecoins”.¹⁰ The USD Coin (USDC) became the first fiat stablecoin implementation from CENTRE, and Circle and Coinbase the first commercial issuers of USDC. The growth of regulated stablecoins has been quite impressive in recent years, growing from less than \$5 billion to over \$30 billion dollars in total assets in the year 2020 before surpassing \$100 billion by mid-2021. Regulated stablecoins have grown as well, with USDC going from half-billion in assets at the start of 2020 to over five billion at the end of the year and \$20 billion by mid-2021.

Another major milestone occurred at the start of 2021, when the U.S. Office of the Comptroller of the Currency (OCC) mentioned that banks can now use stablecoins to conduct their payment activities.¹¹ Such a clarification can have a big impact over the coming years as it reduces further the potential hurdles that traditional financial institutions may have in embracing not only stablecoins but also the broader digital assets space.

Why is Classifying Stablecoins so Challenging?

Whilst we classify stablecoins into three categories, fiat-collateralised stablecoins (both regulated and non-regulated), crypto-collateralised stablecoins, and non-collateralised stablecoins, the process is more difficult for global and national policymakers that need to integrate them into an existing legal classification (e.g., e-money, collective investment scheme). Whilst stablecoins can be simple at first glance (it is ultimately a digital token backed by fiat currency), “fitting” them in a legal framework can indeed be more challenging. For example, whilst they can be seen as a digital currency, their value is entirely pegged to a certain fiat currency, and whilst seen as a fiat equivalent, they operate entirely on blockchain rails. Whilst they are asset-backed, they’re not a security, making classifying stablecoins a challenge for policymakers.

A recent survey from the FSB highlighted the approaches taken by various jurisdictions. For example, whilst stablecoins fall in multiple categories in most jurisdictions, most advanced economies consider them as e-money or collective investment schemes whilst most emerging or developing economies consider them as e-money or simply as unregulated instruments (Fig. 4).



Total number of responses: 40 including 22 from advanced economies (AEs), and 18 from emerging market and developing economies (EMDEs)

Fig. 4 Why classification of stablecoins is so difficult (Source “Regulation, Supervision, and Oversight of Global Stablecoin Arrangements: Final Report and High-Level Recommendations,” Financial Stability Board, October 13, 2020 [48])

However, the good news is that most jurisdictions surveyed by FSB agree that the existing regulatory frameworks will need to be changed in the future to accommodate stablecoins,¹² and as stablecoins become more mainstream over the coming years, expect to see increased focus from regulators on this topic.

1.2 Non-regulated Fiat Stablecoins

As their name implies, unregulated stablecoin issuers are not regulated in the traditional sense, but aside from that, they’re identical to other regulated stablecoins when it comes to purpose and issuance. The most prominent example of a non-regulated stablecoin is “Tether”, which aims to maintain a constant value of one U.S. dollar and is by far the largest stablecoin in the market at the time of writing. Launched in 2014, Tether was one of the first and most popular stablecoins in the crypto ecosystem, existing as digital tokens built on most of the large public blockchain networks from Ethereum and Algorand to EOS and Tron. Tether also supports some major currencies including U.S. dollars (USD), euros (EUR), and the offshore Chinese yuan

(CNH). Whilst not regulated, it has over \$100 billion worth of supply at the time of writing in mid-2021, more than any other stablecoin.

There have been numerous allegations against Tether over the years, but the three most important ones are that its tokens are not fully backed by reserves; that its reserves were used to cover the shortfall of Bitfinex (a related crypto exchange); and that Tethers have been used to manipulate the price of Bitcoin.¹³ Let's start with the first one, the allegations that its tokens are not backed which have lingered because it 's not regulated. Tether tried to address this by having a law firm confirm that the U.S. dollar balances are indeed in accounts owned or controlled by Tether at its bank,¹⁴ and Tether also started publishing its balances on its website.¹⁵

The following is an excerpt from the Tether website:

Every Tether token is always 100% backed by our reserves, which include traditional currency and cash equivalents and, from time to time, may include other assets and receivables from loans made by Tether to third parties, which may include affiliated entities (collectively, "reserves").¹⁶

This statement raised several issues in the eyes of those who doubt the claims of Tether. Whilst most would expect Tether to hold all reserves in cash or cash equivalents, the fact that the company may include other assets or other receivables could be a concern in case of a black swan event and users (or exchanges) start redeeming their Tether tokens for the underlying cash. Many believe that a stablecoin issuer should not be in the business of speculating or using those assets backing the stablecoin for other purposes. In early 2020, Tether came under the spotlight again and Tether's bank, Deltec, based in the Bahamas and supposed to hold reserves backing each Tether token, had to confirm that every Tether is backed by reserves and that their reserves are more than what is in circulation.

The second allegation is that Tether reserves were used to cover losses at a sister company, the crypto exchange Bitfinex. This became public in April 2019 when the NY Attorney General issued a court order alleging that the team behind crypto exchange Bitfinex, who shares a parent company with Tether (called iFinex), used funds from Tether to cover up \$850 million in losses following challenges that Bitfinex had with a Panamanian bank.¹⁷ The matter was being litigated until a settlement with the NYAG was reached in early 2021.¹⁸

The third allegations are that Tethers were used to artificially pump the price of Bitcoin. This theory entered the mainstream following publications from a study by professors John M. Griffin from the University of Texas and Amin Shams from Ohio State University.¹⁹ The academics concluded that

Tether was used during the 2017 Bitcoin boom to manipulate the Bitcoin price and that this was attributable to an account crypto exchange Bitfinex and that Bitfinex must have been aware, something that was subsequently denied by Bitfinex.²⁰

Despite these concerns, the reality is that Tether is by far the biggest and most widely used stablecoin, and it seems these concerns have not been an obstacle to Tether's growth. In spring 2021, Tether disclosed the composition of its reserves backing its stablecoin, as it tried to demonstrate that its consolidated assets exceeded its consolidated liabilities.²¹ Considering the dominant role that Tether's USDT plays in the global stablecoin supply, this was an area of focus for many. The most interesting part of the report was the composition of Tether's reserves, with 76% of Tether's reserves being cash or cash equivalents. However, 65% of those cash or cash equivalent reserves were commercial paper, on which there was no information. Whilst Tether was criticised for not being more transparent, the reality is that none of Tether's regulated peers offer any additional information. Regulated exchange Gemini publishes an independent report by its accountants in which only basic information is provided and the same goes for Tether's rival USDC, which only publishes a basic monthly reserve account.

Whilst there have been many challenges with Tether, many would argue that there are practical reasons with Tether being the biggest stablecoin. For example, Tether is the only stablecoin that offers a U.S. dollar stablecoin but without a U.S. nexus. All other U.S. dollar stablecoins are either regulated by U.S. regulators or are based in the United States. This provides a nexus for U.S. authorities of all sorts to either freeze or seize such assets when they see fit, and for many crypto traders, especially those in Asia, this could be an important consideration. Another more practical reason is that Tether is by far the stablecoin most used in trading pairs, and any serious trader in the crypto space needs to inevitably use USDT, with this dominant advantage difficult for any newcomer to easily dislodge (Fig. 5).

2 Crypto-Collateralised Stablecoins

Crypto-collateralised stablecoins are backed by other cryptocurrencies, and are becoming increasingly popular, especially with the rise of Decentralised Finance, or Defi, discussed in detail in other chapters of this book. The stability mechanisms of such crypto-collateralised coins may seem complicated at first glance, but the logic behind them is like any other asset that's collateralised, from a mortgage on a house to a securities portfolio loan.

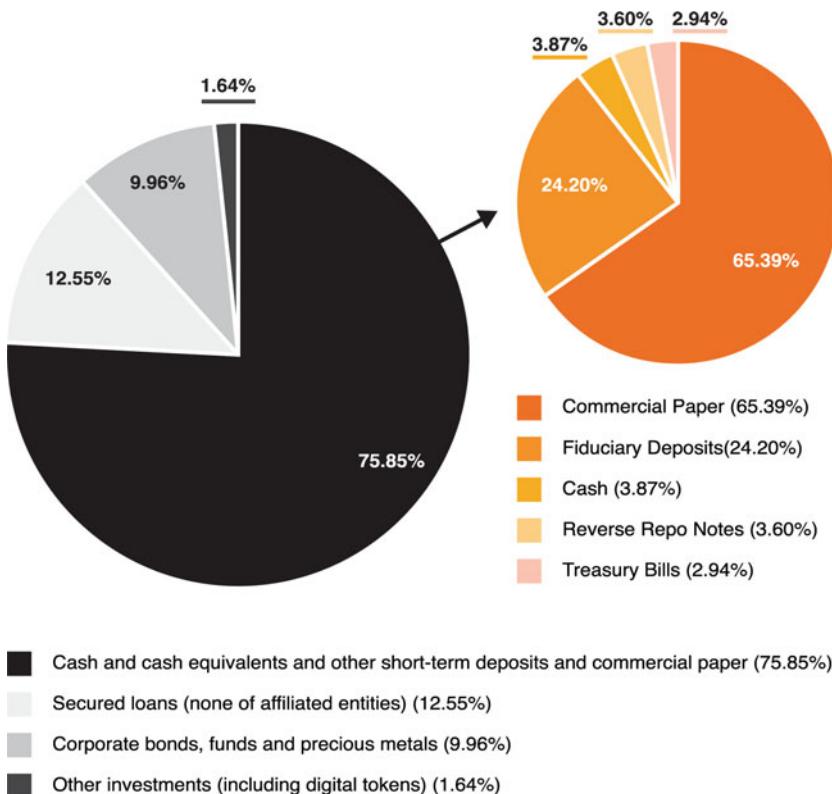


Fig. 5 Breakdown of Tether's reserves (Source "Tether Reserves Breakdown as of March 31, 2021," Tether Holdings Limited, May 13, 2021)

The crypto stabilisation mechanism of such coins typically involves over-collateralisation, such as requiring 200% collateralisation or US\$2 worth of ETH for every US\$1 worth of stablecoin issued, building in a buffer against downward price swings and protecting the peg from being breached. If the collateral value sinks past some threshold, say the ETH's value goes from US\$2 to US\$1.50, the system requires you to liquidate the stablecoin and get your ETH back or simply add more collateral. Of course, the more stable the collateral (e.g., the price of ETH does not fall), the more stable the stablecoin mechanism will be.²² One of the most popular crypto-collateralised stablecoins at the time of writing is the Dai issued by MakerDAO, launched in December 2017, and it is worth looking at how a Dai is created. I'll go step by step and simplify some notions to ensure that the mechanism is understood.

To start, 1 Dai is worth US\$1. For any fiat-collateralised stablecoin described above, you can send US\$1 from your bank to the issuer and the issuer will in exchange send you a US\$1 stablecoin (in practice, there

are issuance fees and minimum amounts). However, a crypto-collateralised stablecoin like the Dai is backed by ETH and in order to receive a Dai, you need to send ETH to a collateralised debt position (CDP), which is a smart contract in the Maker ecosystem. Once you've sent your ETH to the CDP, you'll be able to receive Dai, with the number of Dai you receive depending on the amount of ETH that you sent, and the level of collateralisation required. For example, if the collateralisation level is 150%, then to obtain 100 Dai, I need to send US\$150 worth of ETH, meaning that each Dai is backed by 1.5 ETH. As each Dai is worth US\$1, you can use it for anything you want from online purchases and trading or simply swap it for another stablecoin or withdraw your Dai for fiat currency via an exchange. Your collateralised ETH will be held in the CDP until you "return" your 100 Dai at which point the Dai will be destroyed and you will receive your ETH back. There is a cost for borrowing such Dai using your ETH as collateral (in the same way that you need to pay interest when you get a mortgage from a bank with your house as collateral). This fee is called the Stability Fee, and when you "return" your Dai, you also need to pay this stability fee.²³

The way the stability fee works is relatively straightforward. If the price of Dai goes up (i.e., trading for US\$1.02 meaning that there is more demand for Dai than people are creating it using CDPs), then the stability fee needs to go down and acts as a mechanism to encourage users to create more Dai. For example, if a Dai trades consistently above US\$1, this means that demand is outweighing supply and market participants are willing to pay a premium to purchase Dai. If this happens too consistently, it signifies a need to lower the Stability Fee to incentivise more Dai creation (i.e., becomes "cheaper" to borrow Dai).²⁴ If a Dai trades consistently below \$1, this means supply is outweighing demand and the market is flooded with too much Dai. If this happens too consistently, it signifies that the Stability Fee needs to be raised to slow down Dai creation (e.g., make it "more expensive" to borrow Dai),²⁵ not dissimilar in theory with how a central bank tinkers with interest rates. The rate of the stability fee is determined by a vote of the MKR token holders (more on this below) and varies from close to 0% to almost 20% depending on some of the factors above.²⁶ For example, in the summer of 2021, following a sharp fall in crypto prices, the stability fee fell to less than 5% as demand for Dai stablecoins was lower.²⁷

If the price of ETH rises, then the Dai becomes simply more collateralised. The obvious risk with the Dai is that the value of the collateralised ETH falls. In such a case, a user can add more collateral by locking in more ETH (like a margin call in the physical world). If you don't and the value of the collateral falls below a certain predetermined threshold, then the CDPs will liquidate

your ETH (like a foreclosure in a traditional mortgage). In such a case, a penalty fee also needs to be paid. In the event of a black swan event, say a major hacking or security breach, there is the possibility to trigger an emergency shutdown (previously called the global settlement) where Dai holders will be able to redeem the ETH collateral directly.

Whilst the entire system is decentralised, there is still a type of governance on the platform achieved by the Maker tokens (MKR). Anyone can acquire MKR which gives certain voting rights on topics like the savings rate or the liquidation ratio, and the value is driven by demand as the stability fee is paid using MRK tokens. MKR token holders also have the power to “pull the plug” in the event of an emergency shutdown.²⁸ The downside for MKR token holders is that in the event of an emergency shutdown, if there is not enough collateral to cover all the Dai issued, then additional MKR tokens could be issued and auctioned off to pay the difference (thus negatively impacting via inflation the value of the existing MKR tokens).

Although the Dai is an interesting innovation at the intersection of crypto-assets, traditional lending, and decentralised finance, it still has flaws. For example, due to the underlying volatility of ETH, a lot of collateralisation is required, which does not make it very capital efficient, though this situation should improve with time as volatility in crypto-assets goes down. In addition, crypto-collateralised stablecoins like Dai are still not easy to use for people who don’t have crypto experience or who are not familiar with using digital wallets or smart contracts. Separately, the entire MakerDAO mechanism is quite complex (as you have seen above) which makes it difficult for an average user to fully understand (although we can argue that many use fiat money without understanding even basic economics and monetary policy principles). However, crypto-collateralised stablecoins like Dai are experiencing tremendous growth due to the interest in decentralised finance and are an area worth following over the coming years.

3 Non-collateralised Stablecoins

Whilst we’re still in the experimental stages of non-collateralised stablecoins and such coins have not been very successful so far (and in some cases deemed in breach of regulations), it’s worth discussing them to ensure you have a full picture of the various approaches. Non-collateralised stablecoins do not have any assets backing them up and instead rely on mathematical mechanisms, with price stability achieved by algorithmically increasing or contracting the

coin supply to offset changes in coin demand.²⁹ If a non-collateralised stablecoin is pegged to US\$1 dollar, and the price of the stablecoin goes above US\$1 (e.g., because many people want to buy it), then new coins are issued to devalue the coin. Similarly, if the price of the stablecoin goes below US\$1 dollar (e.g., because people don't want to hold this stablecoin anymore), then existing coins are burned or removed to reduce the availability and increase the value of the coin back to US\$1.

Instead of having a fixed or pre-set supply schedule like most cryptocurrencies, non-collateralised stablecoins alter the equation by having a fixed price peg and flexible supply, not too different conceptually from how central banks approach price stability and inflation-targeting mandates by influencing money supply.³⁰ However, the major difference with other stablecoins is that the coins are not collateralised, either with fiat currency or with some form of crypto-asset. Whilst issuing new coins or inflating the system is not necessarily a challenge, decreasing the supply of available coins is more of a challenge: Whose coins can be burned? Is this process imposed, or can coin holders volunteer? What incentive would a coin holder have to turn in and burn their coins?

Basis is an example of a non-collateralised stablecoin experiment that wanted to tackle this problem.³¹ If a Basis is trading for more than \$1, then new Basis coins would be created and distributed, and if Basis is trading for less than \$1, then bond tokens would be created and sold in an open auction to take out coins in circulation. Such bond tokens cost less than 1 Basis, and they have the potential to be redeemed for exactly 1 Basis when Basis is created to expand supply, incentivising speculators to participate in bond sales and thereby destroying Basis in exchange for the potential that bond tokens will pay out in the future.³²

Whilst it launched to a lot of fanfare having raised US\$133 million from some of the most prestigious Silicon Valley and crypto investors (e.g., Andreessen Horowitz, Lightspeed, Stanley Druckenmiller, Bain Capital, Polychain Capital), it had to shut down after running afoul of U.S. securities regulations (as such bonds could be considered securities) with capital needing to be returned to investors.³³ Whilst several legal and technical challenges remain, we should expect to see more experimentation over the coming years on non-collateralised stablecoins. For example, the Fei protocol is one that is attempting to provide a non-collateralised stablecoin leveraging decentralised finance,³⁴ and one project that has received much attention is Terra, a decentralised and open-source public blockchain protocol for algorithmic stablecoins.³⁵

It's important to remember that the Terra coins are technically backed by Luna, which is another cryptocurrency, but we still classify it as non-collateralised as it is not backed by fiat currency as in the case of USDC. The Terra protocol is a decentralised and open-source public blockchain protocol for algorithmic stablecoins based on a whitepaper issued in April 2019. Using a combination of open market arbitrage incentives and decentralised oracle voting, the Terra protocol creates stablecoins that aim to track the price of any fiat currency. The Terra protocol runs on a proof-of-stake blockchain, in which miners need to stake a native cryptocurrency Luna to mine Terra transactions. It's important to understand that the protocol has two main types of tokens:

- **Luna:** The Terra protocol's native staking token that absorbs the price volatility of Terra. Luna is used for governance and in mining, and users stake Luna to validators who record and verify transactions on the blockchain in exchange for rewards from transaction fees.
- **Terra:** These are stablecoins that track the price of fiat currencies, with users minting new Terra by burning Luna. Stablecoins are generally named for their fiat counterparts, with the U.S. dollar stablecoin called TerraUSD, or UST. TerraSDR is the flagship currency, given that it exhibits the lowest volatility against any one fiat currency and TerraSDR is also the currency in which transaction fees, miner rewards and stimulus grants are denominated.³⁶

Luna and Terra are intertwined due to a process of expansion and contraction.³⁷ Let's start with expansion. When the price of Terra is high relative to its peg, supply is too small and demand too high, so the protocol incentivises users to burn Luna and mint Terra. The new supply of Terra makes its pool larger, balancing supply with demand. Users mint more Terra from burned Luna until Terra reaches its target price, and the Luna pool gets smaller in the process, increasing the price of Luna. For example, if 1 UST is trading at 1.01 USD, users can trade 1 USD of Luna for 1 UST. The market burns 1 USD of Luna and mints 1 UST. Users can then sell their 1 UST for 1.01 USD, profiting 0.01 USD through arbitrage, adding to the UST pool. This arbitrage continues until UST price falls back to match the price of USD, maintaining Terra's peg.

The process is the opposite in the context of a contraction. When the price of Terra is too low relative to its peg, supply is too large and demand too low. The protocol incentivises users to burn Terra and mint Luna, and the decrease in Terra's supply causes scarcity, so the price of Terra increases. More Luna is

minted from burned Terra until Terra reaches its target price, and the Luna pool increases and lowers in price. For example, if 1 UST is trading at 0.99 USD, users can buy 1 UST for 0.99 USD. Users then can trade 1 UST for 1 USD of Luna. The swap burns 1 UST and mints 1 USD of Luna. Users profit 0.01 UST from the swap. This arbitrage continues, and UST is burned to mint Luna until the price of UST rises back to 1 USD.³⁸

4 Facebook's Libra (Meta's Diem)

In June 2019, a bombshell took place in the global financial world as Facebook announced it was launching Libra, having a significant impact on the development of stablecoins and central bank digital currencies.³⁹ Whilst it can be argued that it is simply another fiat backed and regulated stablecoin, it's worth understanding the different reiterations of Libra/Diem as they have had a direct impact on the development of the broader stablecoin ecosystem. Facebook changed its name to Meta in November 2021 and Libra changed to Diem. Whilst the project would reportedly ultimately fail, its impact on the development of the crypto ecosystem was so fundamental that it is worth spending some time to understand what the team behind Diem was trying to achieve. To make it easy for readers, I'll use the terms (e.g., Facebook/Meta, Libra/Diem) as they were called in the period we are referring to.

Whilst the broader vision of Libra was to enable universal access to financial services, one of its more immediate and practical goals was to tackle cross-border payments. As it set out in its whitepaper:

Moving money around globally, and in a compliant way, should be as easy and cost-effective as — and even safer and more secure than — sending a message or sharing a photo, no matter where you are, what you do, or how much you earn.⁴⁰

The Libra announcement singlehandedly catalysed the development of central bank digital currencies and brought the topic of digital currencies to the top of the agenda for any financial services executives. Its potential impact was so significant that it forced policymakers as well as regulators and central bankers to quickly analyse its potential impact not only on the existing financial and payment infrastructure, but also the future of money more broadly.

The fact that it was brought forward by Facebook was also a factor. Whilst many crypto start-ups had proposed solutions over the years that tried to tackle cross-border payments using cryptocurrencies or stablecoins, the fact

that it was proposed by Facebook, the biggest social network worldwide with over 2.5 billion worldwide users was material.⁴¹ Facebook (including WhatsApp) could become one of the biggest players in the global financial ecosystem, and not only did existing financial institutions know that, but also policymakers, regulators, and central bankers. The initial idea of Libra was so bold that it had to be watered down into a more lightweight version, so it's worth spending some time to understand what the original Libra proposal was (let's call it Libra 1.0), how it then changed to a stablecoin model (let's call it Libra 2.0), and finally how it was rebranded to Diem.

4.1 Libra 1.0

The original Libra announcement in June 2019 outlined a bold idea: to create a new global digital currency and financial infrastructure with the unit of currency called "Libra". The key objective was to provide billions of people with access to a low-volatility cryptocurrency that could serve as a low-friction medium of exchange on an international basis and support new digital-native use cases such as micropayments. The way Facebook was trying to tackle this was the creation of a new currency called the Libra that could in theory compete with the U.S. dollar or other major currencies.

Libra 1.0 was designed to be a stable digital cryptocurrency that would be fully backed by a reserve of real assets—the Libra Reserve—and supported by a competitive network of exchanges buying and selling Libra. The Libra Reserves were to be a collection of low-volatility assets, including bank deposits and government securities in currencies from stable and reputable central banks, held by a geographically distributed network of custodians with investment-grade credit ratings to provide both security and decentralisation of the assets. The Libra Reserve was created to support stability and value preservation, meaning that anyone with Libra would have a high degree of assurance they could convert their digital currency into local fiat currency based on an exchange rate. What Libra 1.0 wanted to achieve was to create a new global cryptocurrency that would have all the benefits of cryptocurrencies (e.g., the ability to send money quickly, the security of cryptography, the freedom to easily transmit funds across borders), but with the comfort of its value being stable because it was backed by a basket of global assets.

The fact that Libra was being designed as a new global currency caused a lot of fears with policymakers and, as we will see shortly, forced Libra to change the design into a stablecoin backed by a single fiat currency. The fact that it was supposed to be backed by a basket of currencies also caused some issues as the price of a Libra could vary depending on the value of the

underlying currencies in the basket, which did not make the Libra stable but more akin to a security token that provides exposure to multiple underlying currencies.

Was Libra Similar to the IMF's SDR?

In many regards, the idea of a global currency had been explored decades earlier by the International Monetary Fund (IMF) when it created Special Drawing Rights (SDR) in 1969 as an international reserve asset to supplement its member countries' official reserves. The SDR was created in 1969 as a supplementary international reserve asset in the context of the Bretton Woods fixed exchange rate system. However, the collapse of the Bretton Woods system in 1973 and the shift of major currencies to floating exchange rate regimes lessened the reliance on the SDR as a global reserve asset, but SDR allocations from the IMF can play a role in providing liquidity and supplementing IMF member countries' official reserves, as was the case amid the global financial crisis of 2008.⁴²

The value of the SDR is based on a basket of five currencies—the U.S. dollar, the euro, the Chinese renminbi, the Japanese yen, and the British pound sterling. The SDR serves as the unit of account of the IMF, but the SDR is neither a currency nor a claim on the IMF. Rather, SDRs are a potential claim on the freely usable currencies of IMF members and can be exchanged for these currencies.⁴³ Whilst Libra has some similarities with SDR, both are based on a basket of global currencies and are meant to be global, but the similarities stop there. Unlike SDRs, Libra was meant to be used as a means of payment in everyday transactions and was intended to be used by the retail public, features that the IMF's SDRs cannot do. Also, whilst the SDR is issued by the IMF, a global public institution, Libra coins would be issued via the Libra Association, a not-for-profit entity (which we will discuss further below).⁴⁴

Facebook quickly realised that for Libra to be successful, it would need to be governed by an independent entity where Facebook had limited influence and impact. An independent, not-for-profit membership organisation headquartered in Switzerland called the Libra Association was set up, comprised of diverse organisations from around the world. The Libra Association would be the entity through which the Libra Reserve would be managed, and the association would be the only party able to create (mint) and destroy (burn) Libra. Coins would only be minted when authorised resellers purchased those coins from the association with fiat assets to fully back the new coins. Coins would only be burned when the authorised resellers sold Libra coins to the association in exchange for the underlying assets. This process was not new

and was largely like how other regulated stablecoin providers had been already operating.

Facebook also knew that since Libra needed to address a global audience, the Libra blockchain needed to be open source, designed so that anyone can build on it, unlike the closed ecosystems of Facebook, Instagram, or WhatsApp. Facebook believed that such a model would enable new product innovation and additional entrants to the ecosystem, lowering the barriers to access and cost of capital for everyone and facilitating frictionless payments for more people. This allowed Facebook to try to demonstrate that it would not try to access the user's data, but that was easier said than done. Facebook was heavily criticised for many years, and especially following the 2016 U.S. Presidential elections, for having access to too much of its users' data, knowing well that unless it could prove that it would not have access to users' data, the Libra project would never succeed which is why having an open-sourced Libra Blockchain governed by the Libra Association would be the way to go.

Although Facebook would be the initial driver for the Libra initiative, its actual role within the association would be the same as in any other member (at least in theory). Facebook would have its own app on the Libra Blockchain called Calibra, a regulated subsidiary of Facebook to ensure separation between social and financial data and to build and operate services on its behalf on top of the Libra network. The response from the traditional financial establishment was fierce and negative. U.S. politicians were particularly opposed to the idea as there was fear it could threaten the hegemony of the U.S. dollar. Members of the U.S. Congress wrote letters to the CEOs of some companies involved from Day 1 like Visa and Mastercard, stating that if they do not back off from Libra, they may be investigated. Even then U.S President Donald Trump got involved, tweeting against Libra and stating: "We have only one real currency in the USA, and it is stronger than ever, both dependable and reliable. It is by far the most dominant currency anywhere in the World, and it will always stay that way. It is called the United States Dollar!" Libra became an important topic of discussion not only by policy-makers and regulators, but also from the broader public, with the number of searches of the term "Libra" increasing exponentially at that time.⁴⁵

4.2 Libra 2.0

On April 16, 2020, the Libra Association published version 2.0 of the whitepaper (Libra 2.0), introducing some significant changes to the original plan, namely that it would drop the idea of the Libra global currency and that

it would instead introduce stablecoins.⁴⁶ In the original whitepaper, a multi-currency Libra coin was introduced as a new global digital currency, causing issues with many central banks and policymakers globally worried that it could interfere with monetary sovereignty and monetary policy if the Libra network reached significant scale and a large volume of domestic payments were made in the Libra coin. Whilst many thought Libra could resist the pressure, in the end it could not.

To address this pressure, Libra 2.0 mentioned that the Libra coin will not be a separate digital asset anymore, in what was a major shift from Libra 1.0. It would rather simply be a digital composite of some of the stablecoins available on the Libra network, defined in terms of fixed nominal weights, like the Special Drawing Rights maintained by the IMF. This was a major shift that would give comfort to policymakers as in practice no new currency was being created, but Libra went a step further to give comfort to global policymakers and announced the launch of single-currency stablecoins including Libra USD, Libra EUR, Libra GBP, or Libra SGD. Each stablecoin would be fully backed by cash or cash equivalents, as well as short-term government securities denominated in that currency. The Libra Association also mentioned clearly that it intends to work with regulators, central banks, and financial institutions around the world to expand the number of stablecoins available on the Libra network and to explore technical, operational, and legal requirements to access direct custody. It made clear that if central banks or regulators in a region without a corresponding single-currency stablecoin have concerns about currency substitution, then the Libra Association would work with them to make a specific stablecoin available on the Libra network.

Libra 2.0 also sought to reassure policymakers on some of the concerns around the reserves. It emphasised that each stablecoin on the Libra network will be fully backed by a reserve of high-quality liquid assets (Libra Reserve) and provided details about the specifics. For example, at least 80% of the reserve would consist of short-term government securities issued by sovereigns that have very low credit risk (e.g., A+ S&P rating and Moody's A1 rating or higher) and whose securities trade in highly liquid secondary markets. The remaining 20% would be held in cash, with overnight sweeps into money market funds that invest in short-term (up to one year's remaining maturity) government securities with the same risk and liquidity profiles. The Libra 2.0 whitepaper also stated that the Libra Reserve would be audited on a regular basis by independent auditors, and the results of those audits made public to demonstrate that all stablecoins and Libra Coins in circulation are fully backed by matching assets in the Libra Reserve. The Libra Association would also publish on its website daily the then-current composition of the Libra

Reserve and the then-current market value of the assets in it. In order to appease the fears of regulators, Libra 2.0 also put tremendous emphasis on compliance, with almost 25% of the Libra 2.0 whitepaper focused on the topic.⁴⁷

The whitepaper describes a range of compliance considerations from how the Libra Association will create a comprehensive compliance programme and set mandatory standards to how it will conduct due diligence and distribute coins. In addition, Libra 2.0 makes it clear that the Libra blockchain is designed in a way that will provide public verifiability, meaning that anyone can audit the accuracy of all operations. When the Libra 2.0 whitepaper was issued, the Libra Association announced that it had submitted an application to the Swiss Financial Market Supervisory Authority (FINMA) for a payment system license.⁴⁸ The Libra Association also said it welcomes the oversight and control over the Libra coin by a group of regulators and central banks, or by an international organisation such as the IMF, under the guidance of FINMA, which could oversee and control the weights and components to minimise volatility. Conscious of the public scrutiny of the potential outsized role of Facebook, the Libra 2.0 whitepaper also seeks to clarify the respective role of the various parties. One of the main concerns regulators have had with Libra from the beginning was to understand who could participate. A major concern of regulators was that bad actors, from terrorist groups to money launderers, may leverage the network to commit illegal acts. For this reason, the Libra 2.0 whitepaper clarified the four types of participants that could participate in the network:

- **Designated Dealers:** Commit to making markets within tight spreads and will be able to accommodate high volumes of trading.
- **Regulated VASPs (Virtual Asset Service Providers):** Consist mainly of exchanges and custodial wallets that are registered or licensed as VASPs in a Financial Action Task Force (FATF) member jurisdiction.
- **Certified VASPs:** Including VASPs that have completed a certification process approved by the Libra Association.
- **Unhosted Wallets:** Including all other individuals and entities seeking to transact or provide services through the Libra network.

In the Libra 2.0 whitepaper, the Libra Association reiterates that it is an independent membership organisation headquartered in Geneva, governed by the Libra Association Council, which is composed of one representative per Libra Association member, with each member entitled to one vote. Whilst Facebook and its wallet Calibra were mentioned multiple times in the original

whitepaper, there was no mention of Calibra in the Libra 2.0 whitepaper. Facebook was mentioned only once, specifically to clarify that whilst Facebook teams played a key role in the creation of the Libra Association and the Libra Blockchain, they have no special rights within the Libra Association. In the Libra 2.0 whitepaper, the Libra Association also described that it is the parent of Libra Networks (Libra Networks), which will be the entity directly responsible for operating the Libra payment system, minting and burning Libra Coins, and administering the Libra Reserve. Libra Networks would not directly interface with consumers but will instead partner with a select number of designated dealers to extend liquidity to consumer-facing products, such as wallets and exchanges. The Libra 2.0 whitepaper set out that Libra Networks is the only party able to create (mint) and destroy (burn) stablecoins:

Stablecoins are only to be minted when Designated Dealers have purchased those coins from Libra Networks with fiat assets to fully back new coins. Stablecoins are only burned when the Designated Dealers sell stablecoins or Libra Coins to Libra Networks, in exchange for the underlying assets. Designated Dealers will have a contractual right to sell stablecoins to Libra Networks at a price equal to the face value of the underlying fiat currency".⁴⁹

Does Libra Compete with CBDCs?

A major concern from central banks around the world is that of stablecoins. Whilst stablecoins are growing at a rapid rate, central banks are fully aware that Libra could accelerate the trend, which is why CBDC activity has been catalysed since the announcement of Libra. But there is an argument that a stablecoin of a certain currency is a direct competitor of a CBDC of that currency. For example, a U.S. dollar stablecoin is a direct competitor to a digital dollar that could one day be issued by the U.S Federal Reserve. For this reason, the Libra Association also opens up to CBDCs.

In the Libra 2.0 whitepaper, the Libra Association states that it hopes that as central banks move towards developing central bank digital currencies (CBDC), these could be directly integrated with the Libra ecosystem, removing the need for Libra Networks to manage the Libra Reserves and thus reducing credit and custody risk. For example, if a central bank develops a digital representation of the U.S. dollar, euro, or British pound, the Libra Association could replace the applicable single-currency stablecoin with the CBDC. It also hopes to collaborate with central banks on issues such as direct custody of cash or cash equivalents and short-term government securities or

the integration of the Libra payment system with CBDCs. This would reduce credit and custody risk, streamline the operations of the Libra Reserve and provide additional comfort to Libra Coin holders.

It remains to be seen how Libra could or would interact with CBDCs, but this is a natural conflict that we should expect, not only for Libra, but also for stablecoins more broadly.

4.3 Diem

As part of its efforts to show that it is coming in line with the wishes of policymakers, the Libra Association hired many senior individuals from the traditional banking world, including HSBC's former Chief Legal Officer as CEO.⁵⁰ In December 2020 it announced that it was rebranding Libra to Diem, which means "Day" in Latin, to denote that it was a new day for the project.⁵¹ Interestingly, a couple of months earlier, Facebook had also changed the name of its wallet from Calibra to Novi, inspired by the Latin words "novus" for "new" and "via" for "way".⁵² In a perhaps surprising move, Diem announced in May 2021 a strategic shift to the United States and that it would move Diem's primary operations from Switzerland to the United States⁵³ There has been a lot of speculation as to why this was the case, but it's probably safe to assume that the U.S. authorities were not happy to see an organisation with U.S. roots launching a U.S. dollar stablecoin from Switzerland. However, following a string of departures, it was reported that Meta was finally abandoning the project in January 2022.⁵⁴

Regardless of the outcome it is important to understand that the launch of Libra/Diem had a fundamental impact on the development of the crypto ecosystem. It acted as a catalyst for a range of policy discussions, CBDC experimentation and, most importantly, a global discourse on the future of money.



8

Central Bank Digital Currencies

Whilst Central Bank Digital Currencies (CBDC) have been discussed in academic and other circles since 2014, they really became front and centre following the announcement of Libra in June 2019. In this chapter, we'll discuss what CBDCs are, the various types of both wholesale CBDC and retail CBDC and some implications not only on the financial services ecosystem but also on the future of money. This is a fast-moving space and by the time you read this, new developments will have taken place, but this information should provide you with the foundation to understand any new developments.

To start, what is a CBDC? A CBDC is best defined as a new form of digitised sovereign currency, generally conceived to be equal to physical cash or reserves held at the central bank. It is central bank money, or a component of the monetary base and a direct liability of the central bank.¹ CBDC could constitute a third and new form of central bank money in addition to the two existing components of central bank money: physical cash (coins and bills) and reserves held at the central bank by financial institutions with access to the central bank's deposit facility.²

The original version of this chapter was revised: Figure placement have been updated. The correction to this chapter is available at https://doi.org/10.1007/978-3-030-97951-5_22

Isn't the Money in My Bank Account Central Bank Money?

The short answer is no. Today there are two forms of central bank money. The first is physical cash, either coins or bills, that you hold in your wallet. The second are the reserves held at the central bank by financial institutions. The money that you have in your bank account or use via your favourite payment app is not central bank money. The assets you hold there are, to simplify, accounting entries on the books of the bank or payment firm. This is the basic of what's called fractional banking which allows commercial banks to create money by being able to take those deposits and lend them out. What's exciting about CBDC is that they will allow the creation of a third form of central bank money, akin to a digital banknote, and an exciting development in the future of money.

All of this begs a fundamental question: why are central banks even interested in CBDC? I often mention in my keynotes that if you're a central banker and you love decentralised cryptocurrencies like Bitcoin, then you're crazy. It would be like a taxi driver being excited to see Uber come into their market. However, unlike the taxi industry that tried in many countries to stop ride-sharing companies like Uber or Lyft to enter their markets, central bankers were smarter, realising that there are many features of cryptocurrencies that they can benefit from if they were the ones issuing the digital currencies.

Are Banknotes Sexist?

Despite my undying passion for cryptocurrencies, I still can't help but love good old paper banknotes. Anyone who has stopped by my office in Hong Kong has seen my wide-ranging paper banknote collection, from my Zimbabwean \$100 trillion bill to the demonetised Indian 500-rupee banknote. My biggest hobby growing up was stamp collecting, and in fact, I still have my collection at my parents' place in Canada. Despite all the benefits of digital currencies (and the vast potential of non-fungible tokens), I believe that it will be difficult to recreate the visual beauty of so many of these banknotes. A



Fig. 1 Most commonly used colors on banknotes (Source Salman Haqqi. "A Visual Guide to Banknotes Around the World," Money, May 4, 2020)

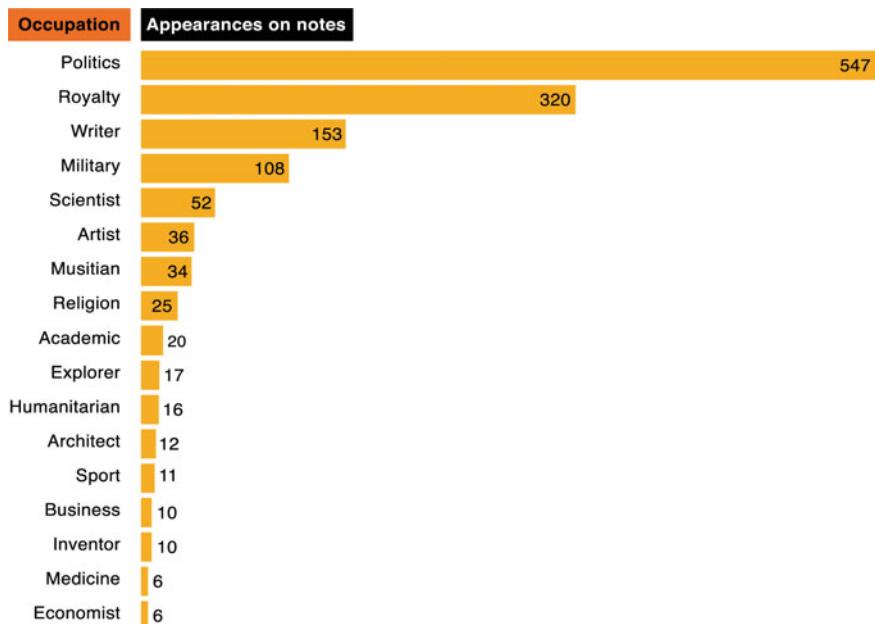


Fig. 2 Most commonly used figures on banknotes by profession (Source Salman Haqqi. "A Visual Guide to Banknotes Around the World," Money, May 4, 2020)

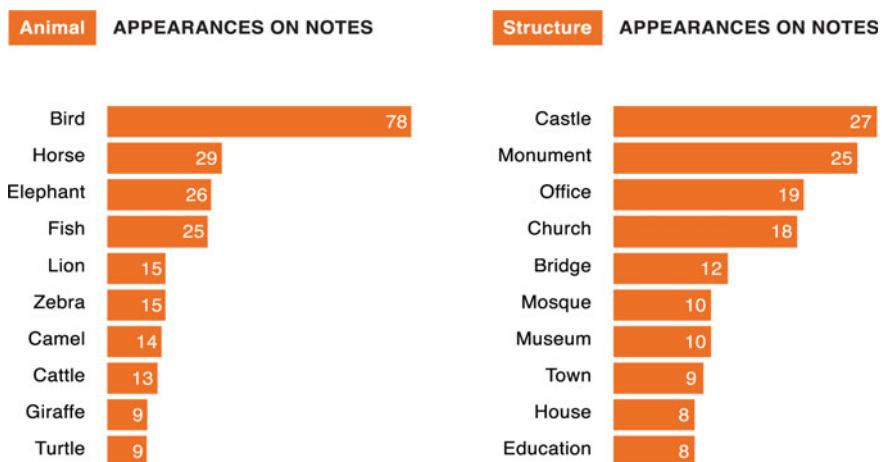


Fig. 3 Most commonly used animals and structures on banknotes (Source Salman Haqqi. "A Visual Guide to Banknotes Around the World," Money, May 4, 2020)

study analysed banknotes from over 150 countries and found some very interesting takeaways.³ For example, the most widely used colour on banknotes today is green (Fig. 1).

The United States used the colour green for its dollar in the 1860s as an anti-counterfeiting measure to prevent photographic knockoffs, since the cameras of the time could only take pictures in black and white, and many other countries would follow suit. The analysis of over 1,300 banknotes revealed that politicians and royalty are the most common figures depicted⁴ (with Queen Elizabeth II clinging to the title of most popular figure, with her visage featured on 45 different note designs across 11 countries.) (Fig. 2).

Somewhat ironically, economists only figure on six banknotes around the world, but also, sports figures appear more than inventors or pioneers in science and medicine. Meanwhile, birds and castles are the most common animal and structure to appear on banknotes around the globe (Fig. 3).

It's important to note that there is a serious lack of gender representation on banknotes, with only 7% featuring a female figure.⁵ This is an area that needs to be improved, with only the United Kingdom, Denmark, and Jersey having a balanced or women-favoured representation on banknotes.⁶

1 Benefits for Central Banks

There are numerous benefits for central banks in CBDCs, particularly retail CBDCs (Fig. 4).

The first is better visibility of economic activity in a country with CBDCs being fully traceable by a central bank or law enforcement. Whilst today Bitcoin and other cryptocurrencies are traceable using some of the tools in the market, it would be even easier for a CBDC issued by the central bank. Whilst this raises some concerns, to be discussed in detail later, there are clear benefits for a central bank or for policymakers. Today policymakers trying to



Better Visibility
of Impact of
Monetary Policy



Curtailing Black
Economy and
Tax Evasion



Combating
Money
Laundering



Embedding
Monetary Policy
in CBDC



Alternative to
Existing
Payments
Systems

Fig. 4 Benefits of CBDCs

understand the economic activity in a certain sector or region and must rely on general estimates or outdated data, because it takes time to gather information from various sources to be aggregated, cleaned, analysed, and presented in a digestible format. An economy that operates on a CBDC could provide live visibility to policymakers on the exact economic activity in the restaurant sector in a certain region or the exact economic output from a certain city. Of course, this assumes that the entire economy is using a CBDC, but as we will see later, that's probably going to happen in the not-so-distant future.

A second benefit is that it allows a good fighting chance against the black economy and tax evasion. In numerous countries, both developed and emerging, many businesses will prefer to accept cash payments as such transactions are not easily traceable, which makes it easier if someone wants to under-report revenues to pay fewer taxes or to avoid paying social security or complying with other administrative procedural requirements. This is a serious problem around the world, and according to estimates from the World Bank, the weighted average size of the shadow economy (as a percentage of "official" GDP) is 38.4% in Sub-Saharan Africa; 36.5% in parts of Europe and Central Asia; and 13.5% in high-income OECD countries.⁷ If such a problem could be tackled, it would be beneficial for many countries.

Another big advantage is the fight against corruption and money laundering. Today, cash is by far the most private means of payment. It is not surprising that criminals, drug dealers, and illicit businesses prefer to operate in cash. When you see a drug ring or a corrupt politician get busted on TV, you often see piles of cash. If the economy becomes CBDC-based, then corruption using cash becomes almost impossible as transactions are traceable. Whilst corruption will probably always exist in other ways, corruption with money becomes difficult. For example, the (UNODC) estimates that between 2 and 5% of global GDP is laundered each year. That's approximately between 800 billion to 2 trillion dollars each year.⁸ CBDCs probably give us for the first time a fighting chance against this serious international challenge. United Nations Office on Drugs and Crime (UNODC) estimates that between 2 and 5% of global GDP is laundered each year, approximately 800 billion to 2 trillion dollars each year.⁹ CBDC give us for the first time a fighting chance against this serious international challenge.

There are many other policy benefits as well and these are linked to what is called programmable money. In short, blockchain technology enables us to leverage smart contracts and other inherent features of blockchain technology to do things with money that are impossible today. For example, central banks could in theory directly impose negative interest rates on CBDC directly, something that is obviously not possible with cash banknotes (but possible

indirectly when the cash is deposited in a bank account). Similarly, they could also make certain injections of new CBDC that need to be spent or else expire. One can imagine such a tool being useful if a government is trying to kick start an economy, as was the case after the COVID-19 pandemic where many governments, like the United States, were doing handouts to their citizens but with no way to force people to spend that money. In a similar way, whilst we still have over a billion people around the world who are unbanked, a large percentage of them may have a smartphone which can easily host a digital wallet. Whilst there is an entire suite of other benefits that exist, like a CBDC network working as a back-up to the existing systems in place, the reality is that there are many benefits for central banks and policymakers. Finally, CBDC could provide an alternative to existing payment systems, that whilst not perfect, do work, and a CBDC payment system could allow us to have a system not only more efficient but also more effective. We shouldn't be surprised that a 2021 BIS survey of central banks found that 86% are actively researching the potential for CBDC, 60% were experimenting with the technology, and 14% were deploying pilot projects.¹⁰

Can Commercial Banks Print Banknotes?

Today, banknotes around the world are issued by central banks. Some central banks outsource the actual printing of the banknotes to private companies like De La Rue in the United Kingdom or Canadian Bank Note Company in Canada, but the actual issuance is done by the central bank and those banknotes are a direct liability of the central bank. There are few exceptions to this rule, including Hong Kong, Macau, and the United Kingdom. In Hong Kong, three commercial banks issue banknotes, HSBC, Standard Chartered, and Bank of China. In Hong Kong's history, there have been eight note-issuing banks in total.¹¹ The Government, through the HKMA, has given authorisation to these three commercial banks to issue banknotes in Hong Kong, accompanied by a set of terms and conditions agreed between the Government and these three note-issuing banks. Banknotes are issued by the note-issuing banks, or redeemed, against payment to, or from, the Exchange Fund in U.S. dollars, at a specified rate of US\$1 to HK\$7.80 under the Linked Exchange Rate System.¹² The only exceptions are the 10 Hong Kong Dollar notes that are no longer printed by commercial banks but rather by the central bank since 2002.¹³

The situation is somewhat similar in Macau where the central bank, the Monetary Authority of Macau, has authorised two commercial banks, the Banco Nacional Ultramarino, S.A. and the Bank of China (Macau) Limited,

to issue banknotes. For issuance or redemption of banknotes, the two note-issuing banks are required to make corresponding payments in Hong Kong dollars to the central bank, at the fixed rate of HKD1 to MOP1.03 under the Linked Exchange Rate system.¹⁴

The situation is a bit different in the United Kingdom. Only the Bank of England issues banknotes in England and Wales, but seven banks in Scotland and Northern Ireland can also issue banknotes, the Bank of Scotland, Clydesdale Bank and The Royal Bank of Scotland in Scotland, and the Bank of Ireland, AIB Group (First Trust Bank), Northern Bank Limited (Danske Bank) and Ulster Bank Limited in Northern Ireland.¹⁵

2 History and Catalysts for CBDCs

Perhaps one of the best-known early conceptual explorations of a retail central bank digital currency is Fedcoin. In 2014 and again in 2016, the Montreal-based economist and blogger JP Koning published papers in which he proposed the idea of “Fedcoin”, which sought to combine the benefits of Bitcoin with the stability that a central bank can offer. As he writes in his 2016 paper:

Bitcoin’s creator envisioned an anonymous payments system without any central points of control. The removal of all central points of control over a currency has the effect of sacrificing price stability, since the absence of an independent entity to ‘back’ the bitcoins in circulation means that their price cannot be managed during periods of fluctuating demand. This price volatility in turn cripples any appeal bitcoins might have to a broader audience. Fedcoin is one solution to the volatility problem. It reintroduces one central point of control to the monetary system by granting a central bank the ability to set the supply of tokens on a Fedcoin blockchain. This allows the central bank to guarantee the one-to-one equivalence between digital Fedcoin tokens and physical banknotes. Even though Fedcoin restores the ‘backing’ point of control over currency, other decentralised features of Bitcoin, such as permissionless validation, may continue to be implemented, the result being that Fedcoin could inherit some of the features of coins and banknotes that Bitcoin has managed to digitally replicate. These include a degree of anonymity, censorship resistance and reusability of tokens.¹⁶

Whilst the paper received support in some quarters, the concept was also widely criticised. For example, the Federal Reserve Bank of St. Louis said

that the call for a “Fedcoin or any other central bank cryptocurrency is somewhat naive”, arguing that once we “remove the decentralised nature of a cryptocurrency, not much is left of it”.¹⁷ The paper further argued that “the distinguishing characteristic of cryptocurrencies is the decentralised nature of transaction handling, which enables users to remain anonymous”. The issue of anonymity is a key point here; a central bank does not require a distributed ledger in order to provide individuals with access to digital payment tokens that are the functional equivalent of physical cash or to enable peer-to-peer transfers of those tokens. That functionality could be offered by a centralised system operated directly by the central bank. In its simplest form, the central bank could do this by permitting citizens to open retail accounts directly with the central bank and enabling transfers between those accounts.

When we think about retail central bank digital currencies, two types of anonymity are important: counterparty anonymity (i.e., not revealing your identity to the recipient) and third-party anonymity (i.e., not revealing your identity to anyone not involved directly in that transaction). For example, a person sending Bitcoin to a public address does not need to reveal his identity to the recipient—meaning these transactions offer counterparty anonymity. He also doesn’t need to reveal his identity to other members of the Bitcoin community, meaning the transaction also offers third-party anonymity, although those transactions are visible and could be traced with the right tools.¹⁸ Policymakers are likely to have serious concerns about enabling any means of payment that provides third-party anonymity, as it could be used to enable tax evasion, money laundering, or the facilitation of other forms of financial crime.

Of course, it’s the case that physical cash is a system maintained by governments that offers third-party anonymity. If one person gives another one a US\$100 bill, nobody can trace that transaction and the central bank will not even know that that transaction has occurred. However, as the Bank of International Settlements notes in a widely cited paper, in the event a central bank cryptocurrency is created, “the provision of anonymity becomes a conscious decision” whereas “the anonymity properties of cash are likely to have emerged out of convenience or historical happenstance rather than intent”.¹⁹

Why are Some Cities Printing Their Own Currency?

Whilst central banks and central governments are normally the ones printing banknotes, there have been some examples of cities printing their own currency. This normally has taken place during an economic crisis like the

Great Depression or during the COVID-19 global pandemic, and many are small towns. One example is the small Italian town of Castellino del Biferno in the Southern Molise region with only 550 residents, which printed its currency called the Ducati that its residents can spend at local shops. The Mexican city of Santa María Jajalpa, a small town of about 6,000 outside Mexico City, also issued a local currency, the Jajalpesos, that can be used as vouchers to purchase food and at designated businesses in the community. The Jajalpesos are backed by the municipality's funds and are traded at par with the Mexican peso, although they are not backed by the Bank of Mexico and are not legal tender.

But it's not just small towns. The Brazilian city of Marica, with 160,000 people and just an hour's drive up the coast from Rio de Janeiro, also has a local currency, the mumbuca. All social benefits and city salaries in Marica are paid in mumbucas and the currency is backed one-to-one by "real" Brazilian real held by Banco Mumbuca, the largest community bank in Brazil, which is funded through the Marica city budget. The currency is accepted almost universally in Marica and businesses are happy to pay the two per cent transaction fee to access its large base of beneficiaries, fees that are subsequently used by the city to fund no-interest loans for local entrepreneurs and homeowners.

This phenomenon is not unique to emerging markets. The small town of Tenino in the U.S. state of Washington, with a population of less than 2,000, decided the best way to support low-income residents hurt by the COVID-19 pandemic was to print money designed exclusively for use in the city. These were minted on a 130-year-old newspaper printer from a local museum and contain the Latin phrase *Habemus autem sub potestate* which translates as "We have this under control". Tenino is capping the amount of the new currency that each resident can accrue at US\$300 per month and residents can use the notes to buy essentials, including food and gas, but cannot use it to buy cigarettes, lottery tickets, or alcohol. Almost every business in town accepts the notes and they can submit redemption requests to the city twice a month to turn the notes into regular dollars. The advent of central bank digital currencies will allow policymakers to quickly get relief funding in the hands of small businesses, the public, and those in need. Until then, you must admire the creativity of some mayors.

There is no doubt that the announcement of Libra by Facebook in June 2019 had a direct impact on the development of CBDC. A true "hockey stick" growth took place afterwards when you look at the number of central banks that started looking at CBDCs and their intensity, as well as Google search data that shows that the general public suddenly became very interested in the topic of CBDCs (Fig. 5).

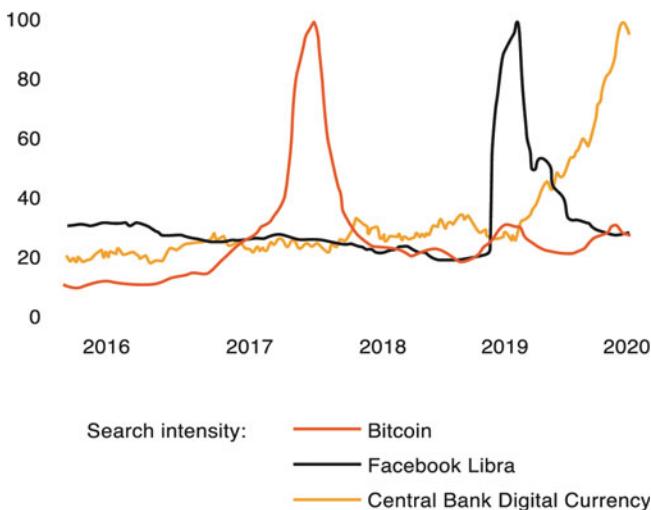


Fig. 5 Google search volumes for bitcoin, Central Bank Digital Currency, and Facebook/Libra (Source Raphael Auer, Giulio Cornelli, and Jon Frost. "Rise of the Central Bank Digital Currencies: Drivers, Approaches, and Technologies." Bank for International Settlements, BIS Working Paper No. 880, August 2020)

This not only generated widespread public interest, but also forced central banks around the world to put this topic at the top of their agendas. In addition, the attitude of central bankers seems to have changed as well. When you analyse speeches by central bankers, the general scepticism seen in 2017 and 2018 has since changed, with the data showing that since the end of 2018, the number of positive mentions of both wholesale and retail CBDC has surpassed negative mentions. The change in the tone of certain central bankers' speeches is interesting. As we say in French, "*juste les fous ne changent pas d'idée*" (only fools don't change their minds) and last time I checked, central bankers were certainly not fools.

The reality is that the same model of CBDC cannot work in Europe as it can in China in that every country and government has different priorities and requirements. For example, many people still oppose the disappearance of cash. In response to a recent survey from the Bank of Canada, almost half of Canadians responded that the loss of physical cash would lead to inconveniences or even outright hardship.²⁰ This is interesting, as 99% of Canadians have access to a debit card and 89% have access to a credit card²¹ (Fig. 6).

This data is like reactions in other countries as well, where right next door in the United States, 60% of Americans are opposed to replacing paper banknotes with digital currency (Fig. 7).

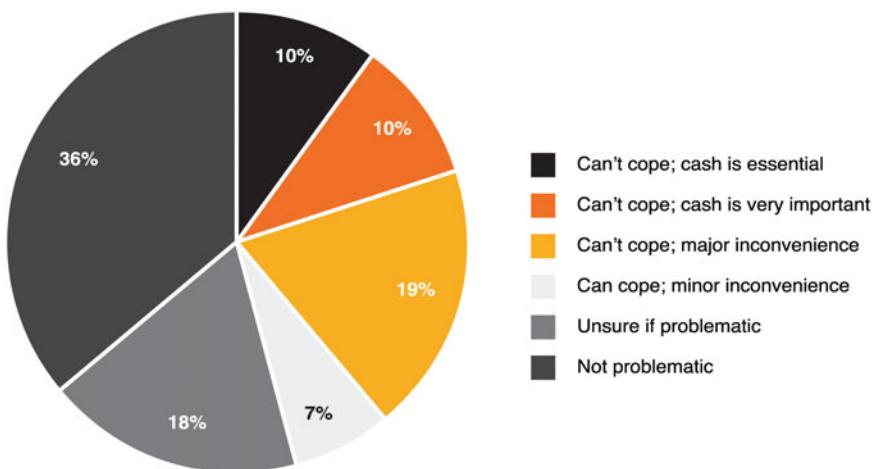


Fig. 6 How Canadians would react to the disappearance of cash (Source: Kim P. Huynh, Gradon Nicholls, and Mitchell W. Nicholson, "2019 Cash Alternative Survey Results," Bank of Canada Staff Discussion Paper 20-8, August 31, 2020)

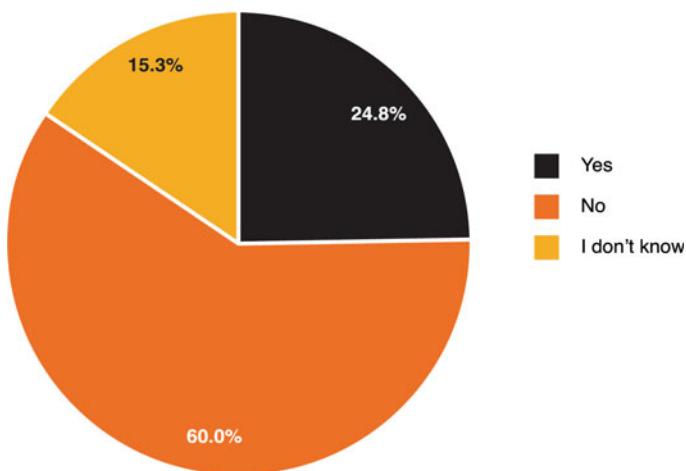


Fig. 7 American views on a potential digital-only dollar (Source "Perceptions and Understanding of Money in 2020," Genesis Mining, 2020)

In most countries, age and level of education plays a role in whether you favour the abandonment of paper currency. In Canada, for instance, people with a high school education in addition to people over 55 tend to be most resistant to the displacement of cash (Table 1).

What people even want in a CBDC varies depending on whom you ask. For example, in April 2021, the EU released the results of a public survey it

Table 1 Responses of Canadian residents to the disappearance of cash by demographic

	Problematic	Not Problematic	Unsure
Overall	46	36	18
Gender			
Male	44	40	16
Female	49	32	20
Age			
18-34	37	45	18
35-54	49	35	16
55+	50	31	19
Education			
High school	52	31	17
College	45	34	21
University	39	46	16
Income			
<\$45,000	52	31	17
\$45,000-\$85,000	47	38	15
\$85,000+	41	39	20
Financial Literacy			
Low	51	32	17
Medium	49	32	19
High	42	40	17

Numbers in percent

conducted on a digital euro.²² The survey was designed to see what Europeans care about when it comes to the topic of a future digital euro and was a record for the EU in terms of participation, with over 8,200 responses received. The most eye-opening fact about how the survey unfolded was that slightly over a third of respondents were under the age of 35. The short and unequivocal answer: privacy, with nearly 4,000 respondents declaring that private payments and transactions were the most important feature for a future digital euro. This preference was uniform throughout the EU member countries but was particularly acute in the case of German respondents. When confronted with a specific choice between an offline digital euro focused on privacy, an online digital euro with innovative features and additional services, and a combination of the two, citizen respondents generally opted for an offline solution focused on privacy.

Both citizens and professionals in the sample generally agreed that the digital euro should be integrated into existing banking and payment solutions. Each type of respondent favoured licensing and oversight of the intermediaries to ensure that digital euro services include appropriate user protections, especially regarding possible misuse of data and concerns about the safety of services related to a digital euro. Notwithstanding the attention to privacy, both citizen and professional respondents support such requirements to avoid illicit activities, and only less than one in 10 are in favour of anonymity. Although many suggest that some identification of users should be facilitated, the privacy of payment data is considered the most important feature, ranging from full privacy of transactions to the possibility that only low-risk small transactions are private.

On the technical side, according to a quarter of the respondents, hardware end-user solutions comprising smart cards or a secure element in devices such as smartphones are the best technical option to facilitate cash-like features. Meanwhile, the results on the impact on the broader economy are interesting, as increased usage of a digital euro could have an impact on financial stability. Most respondents specifically mention the need for either holding limits or tiered remuneration, or a combination of both, to control the number of digital euro in circulation, whilst one in 10 refer to spending limits. About a third of citizen respondents are against the introduction of any tools to restrict the number of digital euro in circulation.

Like public responses, nearly half of merchants (online and physical merchants and merchant associations) are also against any tool that restricts the number of digital euro in circulation. When it comes to cross-border payments, citizen respondents value speed of payments (mentioning that instant payments should be possible), cost, and transparency of exchange rates. Further, an overwhelming majority of respondents stated that the use of a digital euro outside the euro area should not be limited, if safety and security are ensured. Most respondents say they will be ready to support a digital euro by simply adopting it, testing it, or contributing to its design. A quarter of the public (especially respondents 55 and over) say they would not support it, because they're either unwilling or unable to do so. Finally, only a minority would actively oppose the issuance of a digital euro, mainly because they do not believe in the euro area's commitment not to use a digital euro as a tool to enforce deeply negative interest rates and to maintain the availability of cash.

All this is to say that you'll get many different answers depending on whom you ask. To better understand the different considerations, it's worth going into more detail on the type of CBDC. There are different variants of CBDC

**Wholesale CBDC**

A wholesale CBDC is a digital asset issued by the central bank that would be used only between a central bank and financial institutions that have an account at the central bank.

**Retail CBDC**

A retail CBDC is a digital asset issued by the central bank that would be used like a digital extension of cash by the public and companies.

Fig. 8 Key differences between wholesale and retail CBDC

which we will discuss below but that mainly fall in two categories: wholesale CBDC, that would be used to facilitate payments between the central bank and other banks with accounts at the central bank itself and retail CBDC that would be used by the retail public including for retail payments, for example between individuals and businesses, like digital banknotes²³ (Fig. 8).



9

Wholesale Central Bank Digital Currencies

It's worth tackling wholesale central bank digital currencies (CBDC) as they're probably least disruptive when compared to retail CBDCs (or even stablecoins). Wholesale CBDCs relate to the issuance of a CBDC to be used only between the central bank and other entities (mainly financial institutions) which have an account with the central bank for use in interbank payments and securities transactions. These financial institutions could hold wholesale CBDC accounts with the central bank, similarly to the reserve accounts they keep today.¹

To make it easier to understand the wholesale CBDC ecosystem, I like to separate it into three approaches or models that have all evolved as research and experimentation is being conducted in this space. First is the national model, which only focuses on payments within the country; then a cross-border corridor model that focuses on cross-border payments between specific countries; and then the cross-border multi-CBDC model, which is a platform that allows central banks to build a CBDC on it. Let's explore them one by one (Fig. 1).

1 National Model

It is important to mention that in most developed economies today, the interbank payment functionality for domestic payments may not be perfect, but it works well. For example, nearly all central banks of developed economies

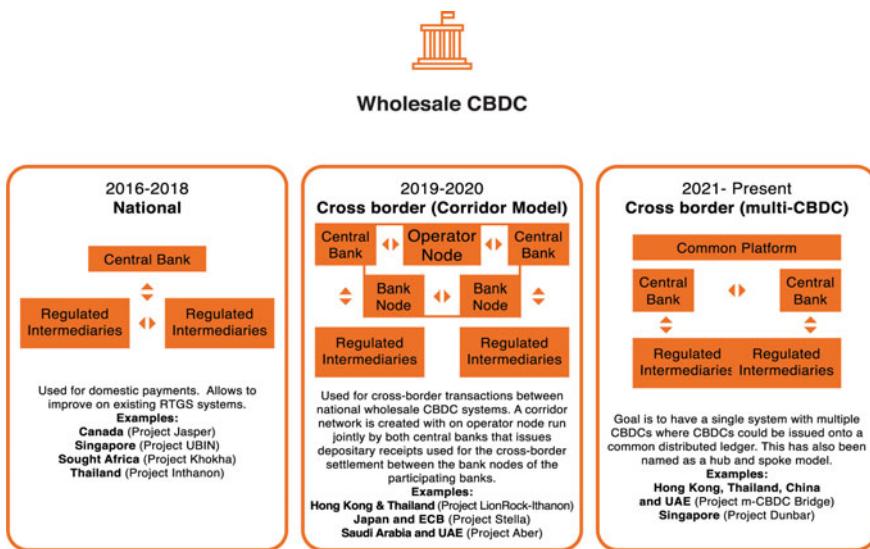


Fig. 1 Different approaches to wholesale CBDC

and many developing ones already have in place real-time gross settlement (RTGS) systems.

RTGS systems affect final settlement of interbank funds transfers on a continuous, transaction-by-transaction basis throughout the processing day. These can be distinguished from older iterations where transactions were made on a deferred basis or at a designated time.² RTGS systems ensure that transfers take place from one bank to any other bank on a “real time” and on a “gross” basis. Settlement in “real time” means a payment transaction is not subjected to any waiting period, with transactions being settled as soon as they’re processed. “Gross settlement” means the transaction is settled on a one-to-one basis without bundling or netting with any other transaction and “settlement” means that once processed, payments are final and irrevocable.³

In addition, many countries have in place some variants of Faster Payments Services (FPS), including those systems providing retail funds transfer in which the transmission of the payment message and the availability of final funds to the payee occur in real- or near-time on a 24/7 or almost around-the-clock basis. These are open systems in which end-users can utilise any number of intermediaries and have immediate clearing between payment service providers of the payer and payee, but the settlement of funds between providers does not necessarily have to occur immediately for every payment. Payee funds’ availability and interprovider settlement can occur either through real-time or deferred settlement. The debiting and crediting of

funds from the payer to the payee occurs at the same time as the debiting and credit of the respective payments service providers. Credit risk is removed, but providers are required at all times to hold sufficient liquidity to settle in real time.⁴ This is why it can be argued that wholesale CBDC for domestic use may not provide additional interbank payment functionality to an economy that already has a well-functioning commercial banking sector and interbank payment system, such as a RTGS system. Such banks can already efficiently transact with one another using reserves held at the central bank in the manner they would with CBDC.⁵ For these reasons, there is not much upside (but lots of risk) for a central bank to seriously explore issuing a wholesale CBDC for domestic payments. It can be argued that the countries that do not have a RTGS system today could look at doing a technological jump and consider a wholesale CBDC instead of a RTGS system, but that is in practice not very likely.

From 2016 to 2018, several experiments were conducted by central banks around the world on the use of blockchain in the development of next-generation RTGS including in Canada (Project Jasper), Singapore (Project Ubin), Japan-Euro Area (Project Stella), Brazil, South Africa (Project Khokha), and Thailand (Project Inthanon). The main purpose of these experiments was to promote central banks' understanding of the DLT systems and their applicability in the existing wholesale financial markets, such as real-time gross settlement systems, delivery versus payment systems, and cross-border interbank payments and settlements systems.⁶ The Bank of Canada and the Monetary Authority of Singapore launched initiatives on wholesale CBDCs with Project Jasper⁷ and Project Ubin,⁸ providing strong evidence that it was possible to use a distributed ledger system to deliver instant settlement.

Nonetheless, these central banks have not taken serious further steps towards implementation because their view is that current technology is not yet able to protect privacy, and these central banks believe that the process of verifying transactions could potentially be faster and most cost-efficient if the verifier is centralised (either through a group of selected commercial banks or a central bank), but then this approach would end up being like the existing centralised system and thus not necessarily superior to the existing system. In addition, their current wholesale payments and settlements systems are already efficient enough, so no strong advantages can be expected from such a wholesale CBDC initiative.⁹

2 Cross-Border (Corridor Model)

Whilst the upside for wholesale CBDC for domestic payments may be limited, there could be an opportunity for wholesale CBDC at the cross-border level, which have several challenges today including¹⁰:

- **High costs:** Series of fees, including foreign exchange and operating expenses, are added at every step of the correspondent banking process.
- **Speed:** Reliance on multiple intermediaries and a mismatch in the operating hours of RTGS systems across different jurisdictions hinders the direct processing of payments.
- **Delays:** Clearing and settlement procedures are sequential processes, and must deal with varying payment standards, availability constraints, guidelines, and regulatory requirements.
- **Lack of transparency:** Lack of network interoperability increases the uncertainty of a payment reaching its destination, whilst payment status in the chain is often unknown.
- **Legacy payments infrastructure challenges:** There are significant technical barriers to improve payment systems like RTGS.

A big reason for these challenges is due to existing correspondent network infrastructure; for a bank to arrange a cross-border transaction, it must either have both parties' currencies in its possession or else have a means of buying the foreign currency required to execute the transaction. Whereas some larger international banks might have the banking license and liquidity required in the respective currency, the vast majority don't, which is why banks have correspondent banking relationships with strategically selected foreign banks that can handle the desired payment. The reason why such networks exist is both the lengthy process of acquiring a banking license in another jurisdiction and the high-cost burden, and these intermediaries are, of course, entitled to a cut of the transaction volume along the way¹¹ (Fig. 2).

Besides the reliance on correspondent banking channels, dependence on the operating hours of the national RTGS systems is often another challenge. This means that there are only small windows of time when systems across different countries are open simultaneously. This results in cross-border payments getting trapped in a country, waiting for the respective RTGS system to open, and thus driving the time lag in cross-border transactions reaching their destination. As if these challenges were not enough, there's always the fact that one can never guarantee that the recipient will receive the whole amount; a transaction might, for instance, be blocked for any reason at one of the steps in the process.¹²

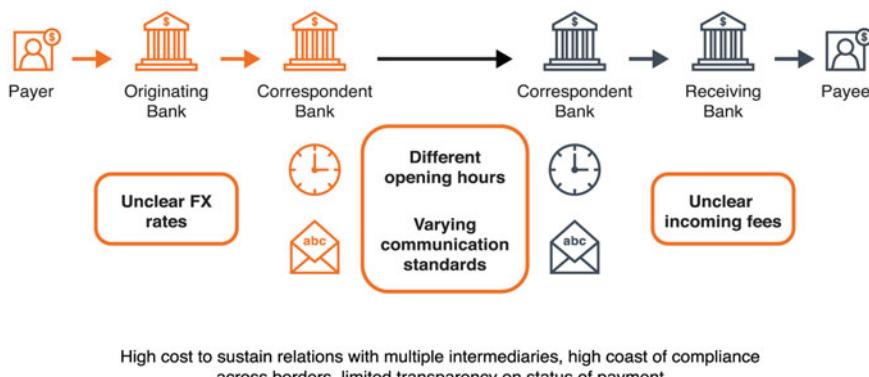


Fig. 2 Bottlenecks in cross-border payments (Source Raphael Auer, Henry Holden, and Philipp Haene, "Multi-CBDC Arrangements and the Future of Cross-Border Payments, Bank for International Settlements," BIS Paper No. 115, March 19, 2021)

There have been recent initiatives to explore whether a wholesale CBDC could improve efficiency in speed and costs for cross-border interbank payments, which may also allow us to bypass the outdated correspondent banking systems and the various challenges related to legacy infrastructure, intermediary operating hours or cut-off times, and other interbank processes discussed above.¹³ Whilst there have been a few experiments using this model, especially from 2019 to 2020, it's worth focusing on two: Project Stella, a joint research project between the European Central Bank and the Bank of Japan and Project Inthanon-LionRock, between the Bank of Thailand and the Hong Kong Monetary Authority.

Project Stella is a joint research undertaking by the European Central Bank and the Bank of Japan first launched in December 2016. Its first two phases focused on processing large-value payments and securities delivery versus payment (DVP) in a DLT environment and in its phase three, the project focused on cross-border payments, with a particular emphasis on a back-end arrangement for cross-border transfers.¹⁴ Project Stella acknowledged that initiatives exist to address current inefficiencies of cross-border payments, whilst safety aspects of transactions across payment ledgers remain a challenge. In view of this, Stella phase three explored whether cross-border payments could potentially be improved, especially in terms of safety by using new technologies. One problem that Project Stella addresses is the issue of credit risk in cross-border transfers, which might arise if a party fails prior to completion of a cross-border transfer.

In this simplified example, Entity A intends to send ¥100 million to Entity C by sending €1 million to Entity B (e.g., an intermediary bank), which has

access to both euro and yen ledgers, and in turn sends ¥100 million on behalf of Entity A. If Entity B fails after the first leg of the transfer is complete (i.e., the €1m-transfer from A to B) but before the second leg of the transfer is complete, Entity A faces the risk of loss of its funds. This risk can be mitigated if the payments are synchronised and funds are locked, but in today's world such synchronisation rarely happens¹⁵ (Fig. 3).

To address this, Project Stella focused on analysing global interoperability based on a protocol for interledger payments being used (i) between a centralised ledger (e.g., a ledger operated by commercial banks or a real-time gross settlement (RTGS) system operated by central banks) and a DLT ledger, (ii) between DLT ledgers, and (iii) between centralised ledgers.¹⁶ Each phase of Project Stella is built on the previous one. For example, Stella phase two identified a new approach for settlement across ledgers through Hashed Timelock Contracts (HTLC) that could potentially allow the mitigation of credit risks through the synchronisation of settlement. Stella phase three expanded the scope of this analysis and investigated the safety and efficiency of five payment methods used in cross-ledger payments. Project Stella proposed the following payment options:

1. **Trustline:** An arrangement between the payer and the payee outside the ledger where the payer promises to make a payment if the payee fulfils a predefined condition. The total amount of payments which has not been settled must not exceed the predetermined maximum amount that the payer can pay without settlement on the ledger.
 2. **On-ledger escrow using HTLC:** Allows conditional transfers which are recorded on the ledger and enforced by the ledger if the payee fulfils a predefined condition.

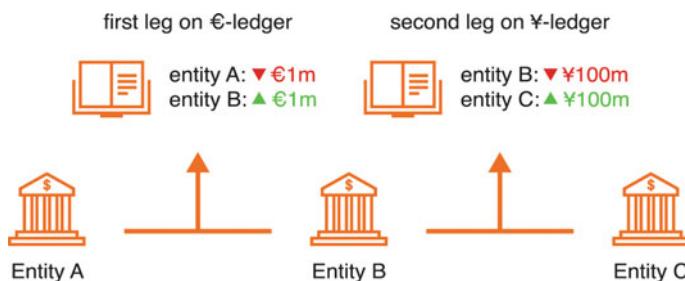


Fig. 3 Credit risk arising from cross-border payments (Source European Central Bank and Bank of Japan, "Synchronized Cross-Border Payments," ECB/BOJ Joint Research Project on Distributed Ledger Technologies, June 4, 2019)

3. **Third-party escrow:** Conceptually like the on-ledger escrow but relies on a third party which is trusted by the payer and the payee rather than on the ledger to enforce the conditional transfers.
4. **Simple payment channel:** An arrangement between the payer and payee using escrowed funds in a shared temporary account on the ledger. Both parties promise to exchange signed claims off-ledger, which represents their entitlement to a specific portion of escrowed funds, if the payee fulfills a predefined condition. Only the final net position of multiple bilateral payments is actually settled on the ledger.
5. **Conditional payment channel with HTLC:** Like the simple payment channel in the sense that both parties exchange signed claims off-ledger, but in addition has an enforcement mechanism by the ledger for the transfers based on whether the payee fulfills a predefined condition.¹⁷

Project Stella concluded that only payment methods with an enforcement mechanism, either through the ledger itself or through a third party, can ensure that the transacting parties who completely satisfy their responsibilities in the transaction process are not exposed to the risk of incurring a loss on the principal amount being transferred.¹⁸ Some of the payment methods explored in Stella phase three, for example, use a smart contract to enforce a conditional payment, whereby funds are temporarily locked until a cryptographic condition for the payment is fulfilled. When the condition is fulfilled, payment of the locked fund is executed. In addition, experiments applying a payment method with HTLC proved the technical feasibility of synchronised settlement between different types of ledgers, including settlement between DLT and centralised ledgers. Project Stella also concluded that from a technical perspective, the safety of today's cross-border payments could potentially be improved by using payment methods that synchronise payments and lock funds along the payment chain.

The other interesting experiment has been between the Hong Kong Monetary Authority and the Bank of Thailand called Project Inthanon-LionRock to explore the application of DLT to increase efficiency in cross-border funds transfers and overcome pain points including inefficiencies, high cost, limited traceability, and complex regulatory compliance.¹⁹ Launched in September 2019, Project Inthanon-LionRock seeks to build a proof-of-concept (PoC) where a THB-HKD cross-border corridor network is set up as a bridge between the Inthanon and the LionRock networks (DLT-based local payment network of each jurisdiction). Built on Corda, R3's blockchain platform, the corridor network is designed to allow Inthanon and LionRock network participants to conduct funds transfers and foreign exchange transactions on

a peer-to-peer basis which helps reduce settlement layers. The cross-border funds transfer process is enhanced to enable real-time transfers and atomic payment versus payment (PvP) settlements, and smart contracts, funds transfers, and foreign exchange transactions are bundled together. The corridor network is designed to enhance banks' foreign currency liquidity management, adopt the liquidity saving mechanism for multiple currencies, and incorporate compliance of local regulations where possible (Fig. 4).

The LionRock-Inthanon experiment was an interesting one. In that model, the central bank is the sole issuer of its wholesale CBDC which is tokenised and redeemed against the issuing central bank. The domestic settlement networks (i.e., Inthanon network and LionRock network) are separated from cross-border transactions since non-resident banks are not allowed to access the domestic network and hold their respective wholesale CBDC and a "corridor network" is introduced for cross-border settlement. Participants in the corridor network are participating banks from the Inthanon network and the LionRock network and to settle transactions in the corridor network, a Depository Receipt (DR) is needed for transferring value amongst all participants in the corridor network. In the corridor network, participating banks

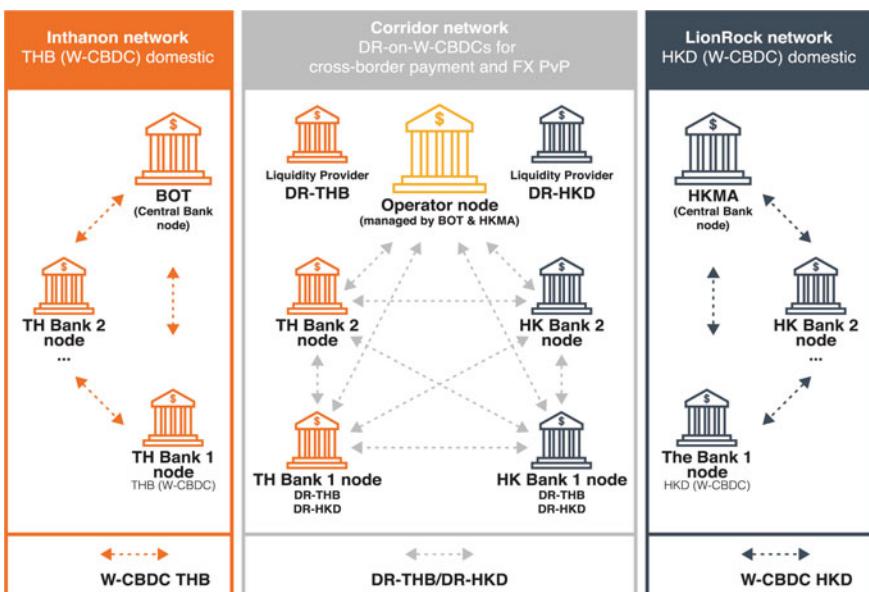


Fig. 4 Key features of project Inthanon and project LionRock (Source Bank of Thailand and Hong Kong Monetary Authority, Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020 [21]), https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf

may hold DR-THB and DR-HKD for cross-border funds transfer and FX PvP transactions, which are performed on a peer-to-peer basis with finality. Liquidity management processes (including Queueing Mechanism, Gridlock Resolution, and Liquidity Provisioning) are on the corridor network in both local and foreign currencies, and compliance with local regulations is considered where possible.²⁰

In the corridor network, the parties involved are the corridor operator node, the central banks, the participating bank nodes, and the foreign currency liquidity providers.²¹

- The corridor operator node is a joint BOT-HKMA body responsible to (i) issue and destroy DR-THB and DR-HKD in response to DR conversion requests by participating banks, (ii) provide gridlock resolution service, and (iii) ensure regulations are complied with.
- Each central bank plays a role in its respective domestic settlement network to facilitate the conversion of wholesale CBDC to DR nominated in its domestic currency and vice versa.²²
- Participating bank nodes in the corridor network (independent of Inthanon/ LionRock): (i) initiate and settle cross-border payments and HKD/THB FX transactions (between the participating banks in the corridor network), and (ii) manage their own liquidity in both local and foreign currencies.²³
- Foreign currency liquidity providers provide foreign currency liquidity when deadlock occurs.²⁴

The biggest challenge that to be addressed is that of liquidity. For example, the biggest cost of any cross-border transaction for a financial institution is the nostro-vostro liquidity cost. The terms *nostro* and *vostro* express the same bank account from different perspectives. *Nostro* refers to a situation when a bank deposits its money with another bank (*nostro*: our money at your bank) whilst *vostro* refers to an account where other banks open an account at your bank (*vostro*: your money at our bank)²⁵ (Fig. 5).

Other central banks have explored this topic as well, with one experiment worth mentioning Project Aber between the Saudi Arabian Monetary Authority (SAMA) and the United Arab Emirates Central Bank (UAECB), a digital currency project for use in financial settlements between the Kingdom of Saudi Arabia and the UAE through DLT. The stated goal was to establish an additional means for the central financial transfer systems of the two countries and enable banks to directly deal with each other in conducting financial remittances.²⁶

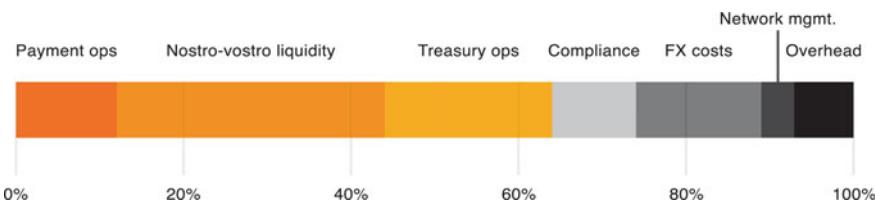


Fig. 5 Cost breakdown per cross-border transaction (Source Bank of Thailand and Hong Kong Monetary Authority, Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020 [21]), https://www.hkma.gov.hk/media/eng/doc/key-functions/financialinfrastructure/Report_on_Project_Inthanon-LionRock.pdf

This idea was taken at the cross-border level with Project Jura between the BIS Innovation Hub, the Bank of France, and the Swiss National Bank, exploring cross-border settlement with two wholesale CBDCs and a French digital financial instrument on a DLT platform. It involved the exchange of the financial instrument against a euro wholesale CBDC through a delivery versus payment (DvP) settlement mechanism and the exchange of a euro wholesale CBDC against a Swiss franc wholesale CBDC through a payment versus payment (PvP) settlement mechanism. These transactions were settled between banks domiciled in France and in Switzerland.²⁷

What About Private Sector Initiatives?

It's important to note that central banks are not the only ones coming up with initiatives and pilots for financial institutions that can provide many of the same benefits as a wholesale CBDC. For example, Ripple claims to have over 300 financial institutions on its RippleNet network,²⁸ focused on achieving four main goals: standardisation, speed, certainty, and cost reduction.²⁹ Another example is SWIFT, which established a new standard for participating institutions, SWIFT gpi (global payments innovation), to improve speed, security, and transparency in cross-border payments across the correspondent banking networks.³⁰ It's still too early to tell if such private sector initiatives will be successful compared to the central bank-led ones.

Whilst these bilateral wholesale CBDCs were successful, the reality is that for such a CBDC to scale, we need a platform that can enable interoperability and for many central banks to work together, which leads to the third and latest version of wholesale CBDC experimentation.

3 Cross-Border (Multi-CBDC) Model

It's not sufficient for a blockchain-based solution to be possible; it must be better than the existing centralised solution and indeed it must be sufficiently better to justify the non-trivial costs of transitioning away from an existing system and developing a new one. The most important consideration for the future success of wholesale CBDCs is interoperability, and central banks and policymakers are fully aware of this, which is why since 2021, the focus has been on exploring models that can make wholesale CBDCs interoperable.

This is particularly important if we want to be able to use CBDCs in cross-border payments. As we saw earlier, the reality is that domestic payments, whilst not perfect, operate reasonably well now in most countries around the globe. But it's a totally different story for multi-currency, cross-border payments, which are significantly more complex than their domestic counterparts. For example, The Economist estimates that the average fee of a cross-border payment globally is 7%, with this figure ballooning to double digits in many emerging economies. Whilst CBDCs could be the answer, if each country develops its own CBDC but they aren't interoperable, then there's no real improvement at the global level. This is why the concept of a multi-CBDC (often shortened to mCBDC) was born with the goal of trying to find a solution to make CBDCs interoperable. Although, as the BIS acknowledges, the concept is still in its infancy, there is very good momentum with three conceptual approaches to mCBDCs today: Compatible CBDC Approach, Linking CBDC Approach, and Multi-CBDC Platform Approach (Table 1).

To fully understand the impact of the above on the future of money, it's important to look at each approach in detail along with some pros and cons.

3.1 Compatible CBDC Systems

The compatible CBDC approach would mean having common technical and common standards, such as message formats, security, and data requirements as well as aligned legal, regulatory, and supervisory standards that could reduce the operational burden of participating in multiple systems. But whilst an interesting idea, it would still require a multitude of privately offered correspondent and clearing services, similar to the cross-border models we have today. Thus, it wouldn't really be moving forward when it comes to fixing the problems of today. In addition, compatibility takes time and such harmonisation efforts take many years. For example, the common messaging standard ISO 20,022 was first introduced in 2004 and is expected to be only rolled

Table 1 Different approaches to multi-CBDC include compatible, interlinked, and single mCBDC multi-currency systems

	Compatible CBDC Systems	Interlinked CBDC Systems	Single mCBDC multi-currency System
Pros	Could be designed with international standards to encourage a wide, diverse group of participants to join	A common clearing mechanism could reduce the number of relationships	Would allow banks in different countries to transact in mCBDC on a single, common platform. Could provide economies of scale in development and maintenance whilst being more technically approachable than several interlinking systems.
Cons	Does not solve the current problem; would still require privately offered correspondent and clearing services Compatibility and harmonization is a lengthy process Incumbent banks with existing large networks and foreign exchange operations would still have a leg up	Connecting 200 central banks around the world would require 20,000 bilateral links Linking payment systems is an extremely complex task Would require a scalable, secure and resilient operating infrastructure whilst coordinating a huge number of stakeholders and participants	Questions on governance, ownership and risk management need to be addressed Would require a scalable, secure and resilient operating infrastructure whilst coordinating a huge number of stakeholders and participants

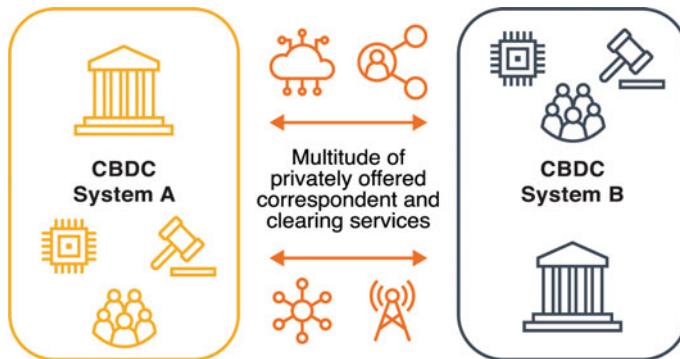


Fig. 6 Compatible CBDC approach (Source Raphael Auer, Henry Holden, and Philipp Haene, "Multi-CBDC Arrangements and the Future of Cross-Border Payments, Bank for International Settlements, BIS Paper No. 115, March 19, 2021)

out by SWIFT towards the end of 2022. Even when such initiatives have central bank or political support, they can take many years like the Single Euro Payments Area (SEPA) that took decades (Fig. 6).

However, being able to design such a model from scratch could have benefits. It could be designed with international standards in mind and encourage a diversity of private participants to ensure choice and competition. However, the reality is that many of the challenges of the current

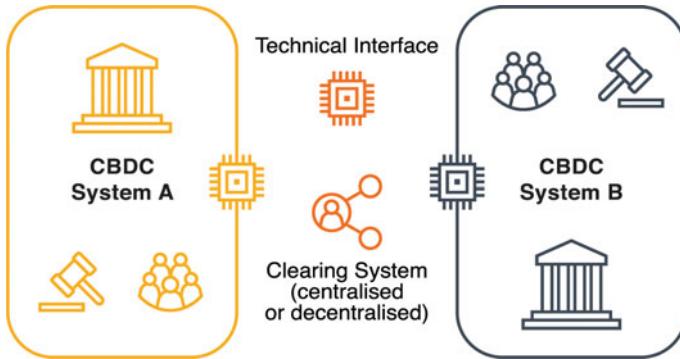


Fig. 7 Linking CBDC approach (Source Raphael Auer, Henry Holden, and Philipp Haene, "Multi-CBDC Arrangements and the Future of Cross-Border Payments, Bank for International Settlements, BIS Paper No. 115, March 19, 2021)

correspondent network system would still exist and incumbent banks with large networks and foreign exchange operations may have an advantage, leading to the concentration seen in correspondent banking networks and their inherent drawbacks. For these reasons, it's unlikely that such a model would be ideal (Fig. 7).

3.2 Interlinked CBDC Systems

The second approach, that of linking CBDC systems, is doable but also very complex. Linking payment systems is a difficult task, often requiring complex compatibility measures. Payments have been compared to the "plumbing" of the financial system; an analogy the BIS makes for linking systems is connecting water pipes with different pressures or flow rates. Simply joining them together will not work. Valves and controls are required: contractual and operational arrangements are the equivalent for payment systems. Linking CBDCs can take various forms and some of them have been explored already like having a shared technical interface (explored in Project Stella by the ECB and Bank of Japan in 2019) or a common clearing mechanism (explored by Singapore and Canada in 2019).

But none are easy to implement. Setting up a real link not only involves ensuring a scalable, secure, and resilient operating infrastructure but also coordinating the many stakeholders and participants involved (which would multiply with each CBDC added). For example, connecting all the world's 200 central banks would require nearly 20,000 bilateral linkages. Historically, these types of initiatives have never worked, as they require not only the right mix of incentives for participants to use the system safely and efficiently,

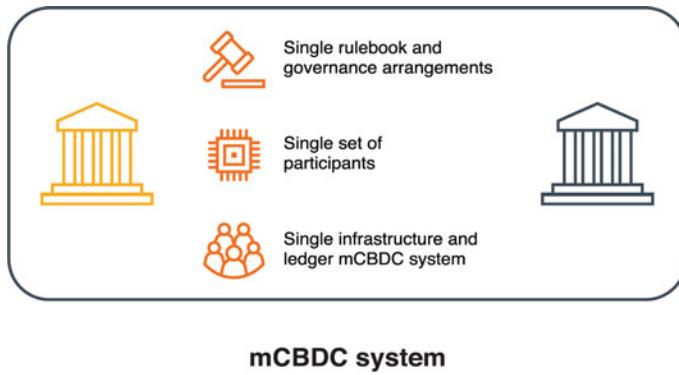


Fig. 8 Single mCBDC arrangement (Source Raphael Auer, Henry Holden, and Philipp Haene, "Multi-CBDC Arrangements and the Future of Cross-Border Payments, Bank for International Settlements, BIS Paper No. 115, March 19, 2021)

but also significant investment in broader coordination to introduce compatibility. Even with the above, the chances of success have been historically limited and thus, it's unlikely that such a model would work (Fig. 8).

3.3 Single mCBDC Multi-Currency System

The final and probably most promising approach is to have a single system with multiple CBDCs where CBDCs could be issued onto a common distributed ledger. This has also been named a hub and spoke model, in which central banks issue their CBDCs on a single common platform and participants on the network could directly transact using the different CBDCs. This could potentially provide economies of scale in development and maintenance whilst being more technically simple than interlinking distinct systems. Multiple systems for different use cases could exist, for example, with a retail CBDC system focusing on higher volume, low-value cross-border payments and a wholesale CBDC system focusing on higher value, real-time payments.

The idea of a common platform has already been successfully deployed all over the developed world, providing those economies with clear, tangible benefits.³¹

Whilst such a model will take a lot of time and effort to set-up and there are numerous challenges along the way, it can enable scalability and provide genuine tangible benefits in fixing one of the biggest challenges that we have today in global finance.

Yet a single mCBDC system, regardless of the approach chosen, raises a number of challenges for central banks. One of the biggest challenges of

creating an international platform for cross-border payments involves the question of governance and ownership.³² After all, in a domestic setting, the central bank is the natural, trusted authority, responsible for issuing and guaranteeing the domestic currency. How would that work on an international level?

Central banks tend to have a strong preference to maintain complete control over their respective currencies. Hypothetically, an international wholesale settlement platform could allow banks from various countries to transact in a variety of different currencies issued by different central banks on a common platform, and could enable possibilities and complexities not previously available (e.g., through additional monitoring to detect illegal activity).³³ There are two initiatives of a mCBDC using a common platform worth exploring. First is Singapore, which has been working for many years on wholesale CBDC models, namely via Project Ubin³⁴ with the latest reiteration Project Dunbar,³⁵ which also explores mCBDC models. Whilst the initiative has put forward many interesting ideas, one great contribution is explaining how the CBDC stack can be unbundled into 4 distinct components³⁶ (Fig. 9).

- **Wallet:** External client application used by banks, corporates, or retail. Customers connect to the platform and initiate a transaction or check their balance
- **CBDC:** Currency issued by the central bank on the decentralised platform.

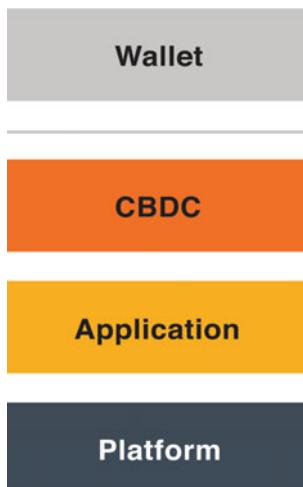


Fig. 9 What does a CBDC stack look like? (Source "Multi-CBDCs: Designing a Digital Currency Stack for Governability," Monetary Authority of Singapore, April 21, 2021)

- **Application:** Decentralised application that provides functionalities of the digital currency, including issuance, transfer, and redemption. The decentralised application could also connect with other external applications to provide other functions, such as transaction monitoring or reporting.
- **Platform:** Blockchain base where the digital currency application operates (e.g., Ethereum, Corda).

If we use the stack example, we see that the level of control and responsibility over the currency increases as we move from the bottom platform level to the top CBDC level. Whilst the issuance of a CBDC will likely remain the sole purview of central banks, the platform and application that the stack relies on could theoretically be cooperatively owned by the central banks and other actors. Meanwhile, the technology required to unbundle a digital currency stack could open the doors for new types of governance and implementation models (Fig. 10).

In this example of a CBDC stack, a group of central banks could agree to collectively monitor and manage the decentralised platform, which would simplify connectivity issues for each actor involved on the network. Ideally, participants on the platform would then have ease of access and ability to transact with a variety of digital currencies. Further, the central banks who issue the CBDCs could set up access controls to approve or deny which parties are privy to data on the digital currency. But arguably the most advanced project at the time of writing is the mCBDC Bridge initiative³⁷ (later renamed mBridge), led by the BIS Innovation Hub³⁸ in partnership with the Hong Kong Monetary Authority, the Bank of Thailand, the People's

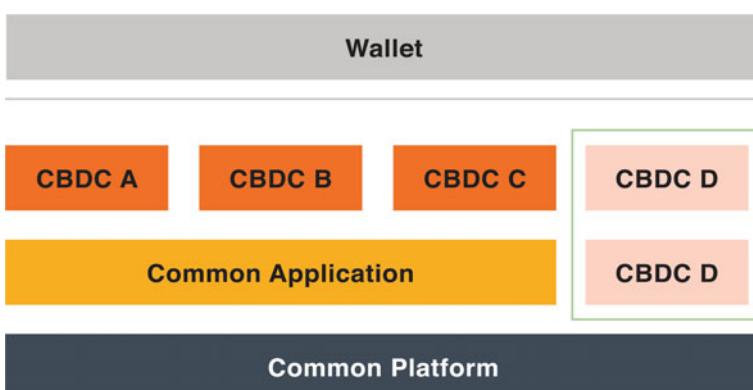


Fig. 10 What does a CBDC platform look like? (Source "Multi-CBDCs: Designing a Digital Currency Stack for Governability," Monetary Authority of Singapore, April 21, 2021)

Bank of China, and the Central Bank of the United Arab Emirates. In its prototype released in September 2021, it proposes a 3-layer solution of a mCBDC multi-currency system:

- **Layer 1:** Core layer that contains the blockchain ledger where data persists and the smart contract logic that implements functionality is programmed.
- **Layer 2:** Back-end application layer that provides identity, access, and routing functions into layer 1 along with wallet signing, key management, and off-ledger FX services.
- **Layer 3:** Front-end layer that provides the interface into the core systems and can take on different forms depending on the end-user and the desired functionality.³⁹

The prototype demonstrated a substantial improvement in cross-border transfer speed from multiple days to seconds, as well as the potential to reduce several of the core cost components of correspondent banking. I highly recommend reading the September 2021 report for anyone interested in this topic.⁴⁰ There's no doubt that the future of wholesale CBDCs will happen via multi-CBDC platforms, and by the time you're reading this, there will hopefully be new experiments or initiatives that will build on the research already undertaken.



10

Retail Central Bank Digital Currencies

A retail central bank digital currency is a digital payment token issued by a central bank. In many ways, such a token would be identical to a stablecoin whose reference asset is the currency issued by that central bank, but unlike a stablecoin, this token would be issued and fully backed by the central bank (like a traditional fiat currency), and as such, it would be easier for users to have faith in its stability. This can be much more transformative than a wholesale CBDC discussed earlier that simply makes the central bank clearing and inter-bank operations more efficient. A retail central bank digital currency would be effectively the equivalent of a banknote, but in digital form, so would simply be a digital banknote in a digital wallet. Moreover, it could be transferable from person to person without a commercial bank or payment service provider as an intermediary, like how one can transfer a \$1 bill from one person to another. Whilst we set out some of the benefits of CBDCs earlier, it's when you think about retail CBDCs that the benefits for policymakers become obvious¹ including these potential benefits:

- **Efficiency in retail payments:** Potential to provide efficient cross-border retail transactions with reduced cost and speed for users.
- **Reduced financial risk due to enhanced monitoring:** Potential to improve financial data transmission and reporting to central banks.

- **Reduction of money laundering or other illicit payments:** Improve traceability of payments relative to physical cash (e.g., to reduce illicit activity).
- **Cost reduction:** Potential to reduce costs and frictions associated with cash management.
- **Strengthens monetary policy:** Potential to improve monetary policy transmission and effectiveness depending on interest rate policies. For example, a retail CBDC may be allowed to put in place a negative or positive interest rate directly on the CBDC or even to conduct helicopter money if needed.²
- **Financial stability:** Provide a safe-haven public option for savings, with lower risk of default than storing savings with commercial banks.
- **Financial inclusion:** Allows anyone to transact especially as usage of cash decreases.
- **Increased competition:** Potential to reduce perceived outsized market power of large private payment service providers in certain markets. Can challenge commercial banks' market power over retail deposits, pressuring banks to increase interest rates or offer better financial services to depositors.
- **Access to central bank money:** Despite rapid decline of usage and availability of cash in certain markets.
- **Rise in consumption:** Recent paper from the Bank of Canada showed that introducing a central bank digital currency could lead to an increase of up to 0.64% in consumption for Canada and up to 1.6% for the United States³

Can We Implement Interest Rates Directly to CBDCs?

Many academic papers have been written on whether CBDCs could be a tool to strengthen monetary policy due to the ability to impose positive or negative interest rates on the CBDC itself. This is of relevance as many countries in recent years have had their interest rates close (or in some cases under) the zero-lower bound. The zero-lower bound is a macroeconomic problem that occurs when the short-term nominal interest rate is at or near zero, causing a liquidity trap and limiting the capacity that the central bank has to stimulate economic growth.⁴ Imposing negative interest rates on CBDCs is a topic that's often discussed, with economists and academics arguing that if digital cash is used to completely replace physical cash, this could allow interest rates to be pushed below the zero-lower bound. By overcoming the zero-lower bound and therefore freeing negative interest rate policies of current

constraints, a world with only digital central bank money would allow for strong monetary stimulus in a sharp recession and/or financial crisis, avoiding recession, unemployment, and/or deflation, but also the need to take recourse to non-standard monetary policy measures with more negative side effects than negative interest rate policies.⁵

Several authors have argued that CBDCs widen the range of options for monetary policy, since variable interest rates on CBDCs would provide for a new, non-redundant monetary policy instrument that would improve the overall effectiveness of monetary policy. For example, a CBDC regime can contribute to the stabilisation of the business cycle by giving policymakers access to a second policy instrument that controls either the quantity or the price of CBDC in a countercyclical fashion. Some even argue that interest on CBDCs would simplify monetary policy as the central bank would use the interest rate paid on these accounts as its main policy tool.⁶ In other words, it's technically possible to implement directly interest rates in a CBDC, but the effects of whether that will be positive or negative remains to be seen.

The introduction of a retail CBDC has some serious downside considerations as well, including the following:

- **Disintermediation of banks:** A retail CBDC could be seen as a true risk-free asset and may cause a bank run with depositors converting their commercial bank deposits to CBDCs. As the ECB mentions in a recent report, “If households substitute banknotes with CBDC, then central bank and commercial bank balance sheets do not really change. However, if households substitute commercial bank deposits with CBDC, then this would imply a funding loss for commercial banks and could lead to ‘disintermediation’ of the banking sector”.⁷
- **Acceleration of bank runs in times of crisis:** In the event of a systemic banking crisis, holding risk-free central bank issued CBDCs could become vastly more attractive than bank deposits. There could be a sector-wide run on bank deposits, magnifying the effects of the crisis.⁸
- **Less risky methods are in place to reduce counterparty risk:** Strong monitoring of existing banks could provide the safety needed. For example, where a strong deposit insurance system is already in place, retail CBDCs would probably not provide added value in terms of offering a safe-haven option for retail savings. On the economic policy side, there may be alternatives such as negative nominal interest rates on reserves or fiscal policy measures such as tax rebates aimed at subsidising households.

- **Increase funding costs:** A drop of deposits with banks could in turn reduce the size of their activities and revenues potentially increasing funding costs as well.
- **Upside limited upside for domestic retail payment in most countries:** Main benefactor to be cross-border payments that may not be as relevant for a large portion of the population.
- **Cybersecurity:** Any retail CBDC would be a target for rogue actors.
- **Data privacy:** Depending on the design of the CBDC (more on this later), serious data privacy debates will need to take place as many would be afraid of a potential “Big Brother” scenario.

One important design consideration that comes up about retail CBDCs is the debate between token-based issuance and account-based issuance. Whilst likely that retail CBDCs will eventually have features of both token-based and account-based designs, it's worth taking the time to explain the differences and their potential impact.

1 Token-Based Issuance

A token-based retail currency (sometimes called a digital token currency or value-based digital token) is issued by the central bank and held by the owner in digital wallets of various kinds and like physical cash, represents a “token” or object of stored value that is digital fiat money and that can be directly transacted by owners who are either known or pseudonymous. Because token-based CBDCs centre on the token object rather than the holder's identity (particularly related to transaction validation), it can arguably afford greater anonymity and fewer user-identity requirements than account-based CBDC (which we will see below).⁹

To simplify, you can think of a token-based issuance as like banknotes but in a digital format. The reality is the very few central banks are considering purely token based systems, in the same way that no economy today relies purely on cash banknotes. There are some benefits to having a token-based model, where a token-based retail CBDC may be preferred if the central bank seeks to design a CBDC that is widely accessible like cash, potentially allowing foreign citizens and entities of various kinds to use it and not requiring user identification. If user identities are not required, and the CBDC can be sent to anyone with a suitable digital wallet, then a wider audience could employ the digitised sovereign currency. This could potentially support policy goals related to widening access to central bank

money and an efficient means of retail payments, and anonymity and transaction privacy could also be stronger.¹⁰ If banknotes are no longer accepted for retail payments, assuming that neither consumers nor retailers want to continue using paper banknotes, such token-based retail CBDCs could be a good replacement.¹¹ Another big benefit is that a token-based model enables payments to be made offline (to a certain extent) which could be useful in areas where internet access is not optimal and can help when it comes to financial inclusion efforts.

However, there are downsides as well. For example, a universally accessible CBDC without identity requirements would increase the risk that CBDCs could be used for illicit activity and conflict with most know-your-customer (KYC), anti-money laundering (AML), and countering the financing of terrorism (CFT) requirements. As a result, token-based CBDCs for wallet holders who are non-identified parties may be more suitable if restricted to small-value transactions. In addition, without strict user-identity requirements, it might also be more difficult to restrict usage to certain types of participants or within state borders with token-based CBDC. All else being equal, accessibility is both easier to scale and more difficult to control in the token-based CBDC concept.¹² One other consideration for a token-based model is that a “hardware” aspect for payments is almost essential to be able to enable offline payments.

Why is a CBDC Considered a “Risk-Free” Asset?

The risk profile of the money that we hold differs depending on how we are holding it and in particular against whom we have a claim. For example, if I hold one dollar at a bank, I have a claim for my dollar against the bank (either a retail or commercial bank for example). However, if I’m holding a CBDC issued directly by the central bank (e.g., a direct token-based issuance), I have a claim against the central bank which is in practice the state.

This has significance for the money’s credit and liquidity risk. Depositing my dollar with a commercial bank has some inherent risks as the commercial bank can go bankrupt. It is, in theory, impossible for a central bank to go bankrupt as they can always meet their obligations by simply “printing” more money. Central bank money is thus seen as a risk-free asset and at the same time a means of payment. Even if money held at banks has been made safe with the aid of legislation and a state deposit guarantee, it is not risk-free in the same way that central bank money is. Whilst many countries have in place deposit insurance, these only cover up to a certain amount and it may take some time for you to claim your funds back. This is why money held

at banks is not as certain or as liquid as central bank money, and thus is not considered a “risk free” asset.¹³

Sweden's central bank was one of the first to study the practical impact of a token-based CBDC (or value-based retail CBDC as the Riksbank, the Swedish Central Bank, calls it). This initiative is often referred to as Report 2 or the 2018 initiative (compared to the account-based initiative that is referred to as Report 1 or 2017 initiative, to be discussed below).¹⁴ Sweden is a good use case as the usage of cash is one of the lowest in the world. Whilst in the euro area the value of cash as a percentage of GDP is just over 10%, in Sweden the figure is just over 1%. Since 2008, the value of cash in circulation has declined by around 50% and half of the retailers in Sweden believe that they will stop accepting cash as a means of payment by 2025.¹⁵ This data was collected before the COVID-19 pandemic which further reduced the usage of cash.

The Riksbank had an interesting dilemma with many important considerations¹⁶:

- **Reduction of the role of the Central Bank:** Since 1904, the Riksbank has had a monopoly on issuing cash. If the use of cash continues to decline at a rapid pace, Sweden could be headed for a situation where the role of the state is changed, and all means of payment to which the general public have access are issued and controlled by private commercial agents. For example, apart from the RIX system for payments between financial institutions, the entire infrastructure for the payment market would be in private ownership.
- **Liquidity Risk:** Central bank money has a lower credit and liquidity risk than private bank money. Historically, the possibility to convert money in a private bank to state issued banknotes has been considered fundamental to guaranteeing that confidence in private money is upheld.
- **Reliance on private sector:** If cash disappears, then it would mean that all Swedes must have an account with one of the private agents to be able to store their money electronically, have access to it, and to make payments. Although most Swedes already have a bank card issued by a private bank, there is currently an alternative to this in the form of cash.
- **Risk of Monopoly from Banks:** The characteristics of the payment market mean that monopoly situations can easily arise. Cash currently competes, albeit to a declining extent, with digital means of payment offered by banks, but the fact that there's an alternative means that there's a limit

to how high a charge banks can levy for their payment services before consumers or the trade sector change to cash. If cash disappears and is not replaced by a new state alternative, this limit will no longer apply and banks can raise their charges more easily.

- **Financial Exclusion:** If cash stops working as a generally accepted means of payment, there's a risk that those outside the banking system will be in a situation where they have difficulty making and receiving payments, which in practice means they will have difficulty accessing goods and services.

These are real issues that from a policy perspective the Riksbank must deal with, and which is why Sweden explored issuing a retail token-based CBDC called the e-krona. There were numerous advantages including:

- **Access:** The e-krona could become a modern krona in electronic form as a complement to physical cash and the public would continue to have general access to central bank money.
- **Contingency:** The e-krona could also strengthen emergency preparedness. The private market cannot be expected to take full responsibility for ensuring that payments function in crisis situations. Preparedness, in the form of extensive back-up systems, entails major costs and the private sector cannot be expected to have the same interest as the state in ensuring these systems are in place. In the event of serious crises, when private payment systems may fail, an e-krona could work as an alternative system and thereby increase stability in the payment system as a whole.
- **Neutral and Public Infrastructure:** The e-krona could offer a competitively neutral infrastructure which payment service providers can join and offer services to households and companies, leading to increased competition, innovation, and somewhat lower charges.
- **Financial Inclusion:** There are groups in society that have problems when cash use declines as they find it difficult to use digital payment solutions for one reason or another, including older people, people with disabilities or those who, for different reasons, do not have access to payment instruments other than cash. Since it cannot be expected that the private market fully caters to these groups, the state can choose to take greater responsibility for them.¹⁷

The e-krona proposal sought to address many of the above considerations. To start, the Swedish central bank had a small but important challenge. Legally speaking, a token-based e-krona would be classified as e-money, which is

compatible with the Sveriges Riksbank Act. However, an account-based e-krona can be likened to a deposit, which may require amendments to the Act to ensure Riksbank can issue an account-based e-krona.¹⁸ This is why a token/value-based issuance was considered and as mentioned in the 2018 Riksbank report:

E-krona should always be exchangeable for other forms of Swedish krona, such as cash or money in bank accounts. The e-krona should be broadly accessible to all members of society and can either be held in an account with the Riksbank or comprise a prepaid value that is stored locally on a card or in an app on a mobile phone. Just as in the case of cash, the Riksbank does not itself need to supply e-krona to households and companies, but will instead offer an open infrastructure where other participants can create payment services to offer to the general public. However, this does not rule out the possibility of the Riksbank offering a basic range of services.¹⁹

However, having the central bank interact directly with the end-users of the e-krona is something so different from the status quo it was decided against, and instead, an open architecture was preferred that allows integration with existing ecosystem players. As the Riksbank writes:

The Project proposes that an e-krona platform be based on an open architecture with a standardised interface. This is so that it could be an integrated part of the existing payment system and could interact with other systems, such as clearing institutions (including Bankgirot), the instant payment system and the Riksbank's system for large-value payments (RIX). It is also the opinion of the Project that the Riksbank should not have direct contact with the e-krona's end-users, but that payment service providers and other financial institutions should easily be able to join the platform and supply different services from it.²⁰

Whilst there are many benefits to a token-based CBDC (not dissimilar to the benefits of traditional cash today), the reality is that a retail CBDC would be a combination of a token-based model and an account-based one.

2 Account-Based

The other type of issuance is called account (or register) based which consists of having the CBDC available only in the form of an account that is maintained in a central register maintained by the central bank or an intermediary. A good analogy of an account-based system is if you were only able to use

your traditional bank account with its debit card but never able to use cash banknotes. Whilst an account-based model has many of the benefits of a token-based model, there are some inherent limitations. For instance, like a bank account today, it can only operate online or with internet access which can be a challenge if a main goal is financial inclusion. The reality is that such accounts will be always issued by intermediaries as it's unlikely that a central bank will want to open and manage accounts, conduct related regulatory compliance, and customer-service functions.²¹ Once again, the Swedish central bank was one of the first central banks to do in-depth research on this topic, and in 2017, issued what became known as Report 1 or the 2017 initiative. After analysing the pros and cons of a token-based vs account-based CBDC, Riksbank highlighted future potential of an account-based model (which they call "register-based"):

The Riksbank's preliminary assessment is that a value [token]-based solution has more limited development potential than a register [account]-based system, but secures access to a means of payment issued by the central bank. The advantage of a value-based e-krona is that it could be introduced more quickly than a register-based solution. A value-based e-krona can be seen as a new, more modern, technology-based form of cash. A register-based e-krona is deemed to be a more complex solution, but to have more potential as it can offer a wider range of services aimed at more user groups. It is also easier to broaden and extend a register-based solution (scalability) to adapt to future requirements, but is deemed initially to be more expensive to develop and run."²² (Table 1).

The reality is that the ideal form of a retail CBDC is probably a mix between token-based and account-based models, like what we have today with physical banknotes (token model) and bank accounts (account model). It's likely that most people will still prefer to hold their retail CBDC at an account with an intermediary, but with the ability to have a token-based feature for smaller amounts that can also be done without being online.

3 Forms of Retail CBDC

It's likely that over the coming years, many new proposals will be put forward for retail CBDC platform models. Some may be fully run by the central bank (like many of the current RTGS systems) whilst others may be more open to the private sector playing a role. Regardless, some key features will always be present in any platform including²³:

Table 1 E-Krona properties compared to cash and commercial bank money

Problematic	Cash	E-krona – value based	E-krona – register based	Commercial bank money
Credit risk	No	No	No	Yes*
A store of value	Yes	Yes	Yes	Yes
Payments in real time	Yes	Yes	Yes	No**
Offline function	Yes	Yes	No	No***
Option of anonymous payments	Yes	Yes, possible for card-based solutions	No	No
Physical presence required	Yes	Yes for card, no for app	No	No
Usability	Works without technical aids	Requires e.g. a card reader or special smartphone technology	Can be managed via apps or online	Can be managed via apps or online

*The deposit guarantee does, however, include holdings up to and including EUR 100,000.

**The exception is payments within the same bank and Swish.

***Cards can have an offline function.

Resilience: A critical piece of national infrastructure, it would need to be able to handle hardware and software failures in parts of the CBDC system, or telecom network failures, whilst maintaining continuity of operations and without having a single point of failure that could break the system.

Scalable: Must be able to adapt to sudden peaks in demand and be possible to increase the capacity of the core ledger as demand increases over time.

Secure: Would need to maintain data integrity and be protected from data loss, data theft, and cyber vulnerabilities.

No downtime: Needs to operate 24/7 with no planned downtime.

Speed: Must be able to process and confirm transactions very quickly.

Adaptable: Must be possible to update and upgrade the platform as demand changes or new use cases emerge.

Whilst each central bank considering a retail CBDC may have its unique features and differences, we can group them in five major approaches to the issuance of a retail CBDC: (i) a decentralised approach, (ii) a direct approach, (iii) a synthetic approach, (iv) a platform/hybrid approach, and (v) a two-tiered/intermediated approach (Fig. 1).

I order these from the least likely to the most likely. Whilst some approaches like the decentralised or the direct approach are unlikely to be implemented in practice, it's important to explain their basics as it helps in understanding more advanced models.

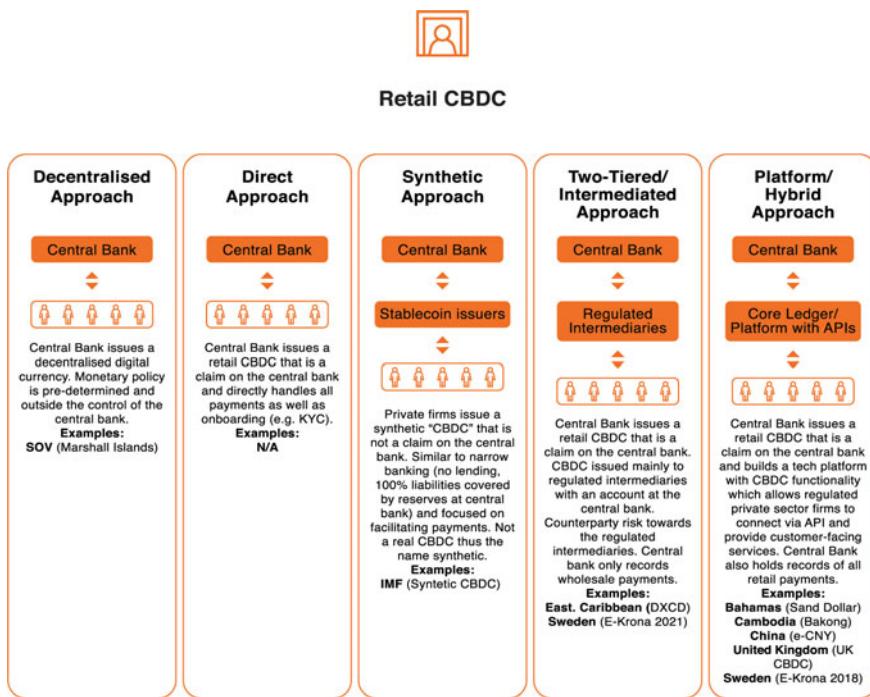


Fig. 1 Different approaches to retail CBDC

3.1 Decentralised Approach

The notion of a decentralised retail CBDC may sound absurd at first glance because it is. Why would a central bank issue a digital currency that is decentralised and where it would relinquish control? Not only would it not benefit from all the potential benefits for a central bank having a digital currency, but it would go one step further and not even have control over it. It's unlikely that we'll see many countries issue a decentralised retail CBDC, but there are exceptions, and a good example is the Republic of the Marshall Islands. In 2018, the Parliament of the Republic of the Marshall Islands adopted the Sovereign Currency Act where it introduced its own national currency called the sovereign (SOV), to be issued in the form of a blockchain-based digital currency, as "legal tender of the Marshall Islands for all debts, public charges, taxes and dues".²⁴

Before analysing the SOV, it's important to understand the particularities of the Marshall Islands as a country. The Marshall Islands is a Pacific Island nation with a population of 50,000 living on 1,100 islands scattered across 750,000 square miles of ocean. Fishing (particularly skipjack tuna used in

canned tuna) and coconut processing (particularly copra, the dried meat of coconuts) are central to the economy. It has a GDP of US\$196.3 million (2016) with a per capita GDP of US\$3,624. Budgetary expenditure accounts for 65.1% of GDP, of which 43.5% are financed by grants, which shows the outsized role the government and external grants play in its economy.²⁵ Like many smaller economies and particularly Pacific Island nations, the Marshall Islands are in danger of losing access to the world's financial systems due to potential discontinuation of correspondent relationships by major banks citing increased regulatory requirements and lack of profitability. Not surprisingly, the cost of remittances is particularly high with fees of over 10% often the case, which is a significant problem in the Marshall Islands, since many citizens work abroad and send money home.²⁶ Due to its size and remoteness, the Marshall Islands does not have a central bank and has never issued its own currency, instead using the U.S. dollar throughout the islands. Most transactions are made using cash, very few people have bank accounts or debit cards, and even the most populated islands only have a small handful of ATMs. Payments across islands are difficult and often done by shipping physical cash with boats.²⁷

These conditions make the Marshall Islands an interesting test case for a CBDC initiative. After careful consideration, the Republic of the Marshall Islands decided to move forward highlighting some key advantages that the SOV provided for the country, including lower transaction fees locally and globally for remittances. It could also not only promote financial inclusion, but also potentially enable the ability to prove digital identities to be used to access government services. Whilst there are numerous countries experimenting with retail CBDCs, what sets the Marshall Islands apart is that the currency would be fully decentralised. At launch, there will be 24 million SOVs, with 100 cents (sovis) per unit, for a total of 2.4 billion sovis in circulation. The total supply of the SOV is set to grow at a fixed rate of 4% annually in line with the estimated growth of world GDP. This rate is immutable and coded directly into the blockchain with no ability to increase or decrease the rate of SOVs to be issued.²⁸

The decision on the rate was made based on the money supply k-per cent rule devised by economist Milton Friedman. According to Friedman, "The stock of money [should be] increased at a fixed rate year-in and year-out without any variation in the rate of increase to meet cyclical needs". Friedman asserted that the most effective way to stabilise the economy over the long term was to grow the money supply by a fixed amount (the k variable) each year, regardless of the state of the economy. Friedman also advised that this constant rate of growth be equivalent to the rate of growth of real GDP.²⁹

The government of the Marshall Islands has taken the conscious decision to relinquish control over this new currency's money supply. Instead, the monetary policy rule is fixed in law and is embedded in a tamper-proof manner on the blockchain, giving users certainty that the government cannot issue additional currency to advance policy objectives.³⁰ It's important to understand that as the country was operating using U.S. dollars already, it didn't have its own currency so in practice it was not relinquishing control of much, and since there's no central bank, issuing authority rests with the finance ministry.³¹

The SOV has a consensus mechanism that is decentralised although with a layer of governance. Block producers are decentralised entities that propose and confirm the blocks of the SOV blockchain in exchange for block rewards in SOV for each block. The SOV Administrative Authority provides approval and licensing for these block producers. Once there are more than 21 total approved entities, anyone who has permission to use the network can participate in selecting block producers in a continuous voting system. By approving more than 21 eligible nodes, the Marshall Islands would allow the community to share in the decision of which entities are trusted to maintain the consensus and governance of the blockchain.³² The Marshall Islands model is unique and it's unlikely that other countries will follow such a model and decide to relinquish control of their monetary policy. However, it's important to understand that such an approach exists and that at least one country is looking at it.

Will the IMF or World Bank Allow the Marshall Islands to Move Ahead with the SOV?

At the time of writing, it's not even clear if the Marshall Islands will be allowed to move forward or that international organisations will put so much pressure that the country will need to back out. For example, the IMF has been critical of the country's plans on its CBDC, and in its 2021 public report said the following:

The issuance of the digital currency SOV as a second legal tender would raise risks to macroeconomic and financial stability as well as financial integrity. The issuance of the SOV could jeopardize the RMI's last USD correspondent banking relationship. This combined with anti-money laundering and combatting the financing of terrorism risks (including those related to the SOV) could disrupt external aid and other important financial flows, resulting in a significant drag on the economy.³³

Such international organisations like the IMF or the World Bank hold an outsized influence on these countries and can apply pressure, from making

aid conditional to simply blocking aid, unless countries comply with their requirements. Unfortunately, the Marshall Islands have very little leverage so time will tell if this moves forward. Another country that has faced similar pressure is El Salvador after it recognised Bitcoin as legal tender; not only did the World Bank criticise the move, they also refused to provide technical assistance, citing environmental and transparency concerns. They also stated that the adoption of Bitcoin as legal tender raises macroeconomic, financial, and legal issues.³⁴

3.2 Direct Approach

A direct approach to retail CBDC is issued by a central bank and that same central bank would handle all payments and all operational requirements like onboarding or KYC. In the traditional banking system, the central bank doesn't handle payments or operational requirements as these are done by regulated financial institutions.³⁵ It's unlikely that any central bank would want to do that and there are also additional considerations. For example, running such a system would remove the central bank from its traditional role of policy to an operational one on which it has no real experience. Also, despite all those central banks may be doing on CBDCs, they don't have the culture and mindset to put forward innovative initiatives like many FinTech firms, payment firms, and even (as shocking as it may sound) traditional financial institutions. Using a direct issuance approach would have the central bank competing against the private sector firms it's supposed to oversee, which would increase the risk of financial instability. Perhaps not a coincidence, there are currently no central banks exploring a direct issuance, but it's important to understand its particularities to better see the differences with some other approaches.

3.3 Synthetic Approach

In a synthetic CBDC (sometimes called “reserve-backed private tokens” or “hybrid CBDC”), the central bank allows financial institutions, electronic money or payment service providers (PSP), or tech firms that do not typically have access to the central bank's deposit facility to hold reserves at the central bank.³⁶ Technically speaking, a synthetic CBDC is not a CBDC for reasons

we'll discuss below, but I believe it's important to add to this list to ensure you have a full picture of the various options regardless of their technical nuances.

The most discussed model of a synthetic CBDC is likely the one proposed by a team at the IMF in July 2019.³⁷ In that paper, the IMF argues that the two most common forms of money today, cash and bank deposits, "will face tough competition and could even be surpassed" and that "central banks will play an important role in moulding this future".³⁸ The IMF recognises the crucial role that central banks play by supervising banks and offering liquidity when needed, but they also democratise the landscape by enabling interoperability. As they write:

Importantly, central banks also settle payments between banks. Otherwise, interbank payments would be expensive, slow, and potentially contentious. Indeed, short of exchanging cash or gold, banks have to extend credit to each other in order to settle payments between themselves and their customers. This is where the central bank comes in. All banks hold accounts at the central bank, and a payment from one to the other is settled by transferring perfectly safe funds (called central bank reserves) from one account to another. Not only does this remove credit risk from inter-bank transactions, it also ensures that payments are interoperable across banks. As a result, no single bank—however large its network—has an advantage in allowing payments among more customers. Interoperability is essential to level the playing field between banks. What if providing a level playing field also meant offering settlement services to e-money providers? What if these firms could also hold central bank reserves, just like large banks, to the extent that they satisfied certain criteria and agreed to be supervised?³⁹

Whilst innovative, this is not a completely new idea and it resembles ideas that are already in force elsewhere, namely licenses to non-bank FinTech firms and narrow banks. Many central banks, from India to Hong Kong, offer certain licenses that allow non-bank FinTech firms to hold reserve balances. For example, Hong Kong's Stored Value Facility (SVF) is a great example of a quite successful programme.⁴⁰ In China, the PBOC asks large tech payment providers like Alipay and WeChat Pay to hold client funds at the central bank in the form of reserves.⁴¹

Narrow banks (unlike fractional banks) are financial institutions that cover 100% of liabilities with central bank reserves and do not lend to the private sector, instead focusing solely on facilitating payments. The running costs and the remuneration of capital is covered by a spread between the narrow bank deposit rates and the rates at which the central bank remunerates the reserves of banks. This has been discussed at various times in the past decades. The Chicago Plan of 1933⁴² is a good example and a more recent example is TNB

(The Narrow Bank) in the U.S. state of Connecticut⁴³ that looked at offering practically risk-free deposits to institutional (non-retail) clients. At the time of writing, TNB is still trying to open a reserve account at the Fed, which is refusing to do so.

It's important to note that, unlike other types of CBDCs, a synthetic CBDC is not a claim on the central bank in the case of issuer default (thus the name synthetic). However, it ensures that central banks can support the provision of a stable and electronic money by a private institution but with strict safeguards and protections for user funds.⁴⁴

Why a Synthetic CBDC is not Really a CBDC

Whilst in the early days of CBDC discussions, we would include synthetic CBDCs as one type of retail CBDC, it's not accurate for a variety of reasons. As the adjective "synthetic" implies, a synthetic CBDC is not a real CBDC as it is not a claim on a central bank and is not central bank money. The fact that private sector payment service providers can issue liabilities matched by funds held at the central bank makes it more akin to narrow banking than a new form of central bank money. Such a synthetic CBDC model also lacks some of the characteristics of central bank money. For example, central banks can expand their balance sheets and create additional liabilities at short notice (what we call more commonly quantitative easing), and by design, a private sector firm in a synthetic CBDC model cannot do that. Whilst important for us to cover the topic of a synthetic CBDC, it's critical to understand that it does not fall within the definition of a retail CBDC, something that the BIS made sure to reiterate in a 2020 report.⁴⁵

One major benefit is that launching such a synthetic CBDC could probably be implemented more quickly than other forms of retail CBDCs. It may also allow central banks to focus on core competencies such as transaction settlement rather than a full suite of retail CBDC components and requirements.⁴⁶ Whilst some countries have experimented with such models, namely Ukraine and Uruguay, at the time of writing, there are no countries that have made public some plans of issuing a synthetic CBDC.

3.4 Two-Tier/intermediated Approach

A two-tiered CBDC (often also referred to as intermediated CBDC) is when the retail CBDC, which is a claim on the central bank, is issued solely via commercial banks or other regulated third parties that have an account at

the central bank. In such a two-tiered issuance, only the central bank can issue and redeem the CBDCs, and commercial banks can only obtain/redeem the CBDC against the debiting or crediting of reserves they hold with the central bank. This is not dissimilar from the existing two-tiered structure that exists today where commercial banks have accounts with the central bank and where the public has a counterparty exposure and risk with the various regulated intermediaries.

Whilst the central bank also needs to build a platform or ledger for the two-tiered issuance, it differs from the platform/hybrid approach in that the central bank only records wholesale payments (so only the payments in retail CBDC taking place between the various regulated entities and not every single retail transaction). In this model, the central bank does not record retail transactions, but only the wholesale balances and the detailed records of retail transactions are maintained by the regulated intermediary.

There are many benefits for such a model:

- Would diminish the need for centralised data collection.
- Would reduce the risk of data security breach due to the decentralised nature of recordkeeping, with the data being spread across many regulated entities.
- Would address privacy protection concerns as would reduce the amount of data with the central bank.
- Would be easier for the central bank as a platform to record only wholesale transactions can be easier to build and maintain than one to record all retail transactions.
- Creates less disintermediation risk and the existing status quo, with whom the central banks are familiar, remains in place.
- Would avoid need for central bank to deal with end-users' challenges from onboarding and account management to customer service and compliance.

There are some additional considerations with such a model:

- Additional safeguards and prudential standards would be necessary, as regulated intermediaries would need to be supervised, although central banks have good experience in this area.
- Whilst the ledger would only record wholesale payments, it still is a massive tech endeavour.

Many believe that, due to the above, such a tiered model may be a practical and reasonable approach and the one we are most likely to see central

banks implement if they decide to launch a retail CBDC. This is particularly the case when you think about increased levels of concern around privacy for retail CBDCs, especially in Europe. On the other hand, the fact that the central bank does not see retail transactions (only wholesale) does not give the full benefits. This type of retail CBDC has seen quite a bit of experimentation so far, with one of the first central banks to conduct such two-tiered issuance experimentation was Sweden with the e-kronor pilot announced in early 2020⁴⁷ (Fig. 2).

In this two-tiered issuance, only Riksbank can issue and redeem e-kronors, like cash today. Participant banks can only obtain/redeem e-kronor against the debiting or crediting of reserves they hold with the central bank in the Riksbank's settlement system called the RIX. The RIX is the centralised payment system in which transfers between accounts of different banks are handled.⁴⁸ The Riksbank does not deal with end-users as all such interaction with end-users is handled by participant banks from digital wallets to mobile apps. As would be expected, the e-krona network is private and only the Riksbank can approve and add new participants to the network. All transactions in the e-krona network occur on a standalone basis separately from the existing payment networks, which can provide added robustness in the event of problems with the existing payment infrastructure. Separately, payments occurring in the e-krona network will take place without the involvement of RIX, but the supply or redemption of e-kronor will be done via RIX.⁴⁹

Riksbank experimented with a two-tiered/intermediated model. As it mentions in its April 2021 report:

The fact that the network is decentralised means that the transactions using e-kronor are registered with the participants in the network involved in the transaction, instead of in a central database. The participants, for instance, banks and payment services providers, run their own nodes in the network and thus have the possibility to request the issue of e-kronor and to exchange them, distribute them and to execute and receive transactions on behalf of end-users connected to them.⁵⁰

One central bank that has implemented a two-tiered/intermediate approach has been the Eastern Caribbean Central Bank (ECCB). The ECCB is the monetary authority for a group of eight island economies: Anguilla, Antigua and Barbuda, Commonwealth of Dominica, Grenada, Montserrat, St. Kitts and Nevis, Saint Lucia, and St. Vincent and the Grenadines. The Eastern Caribbean Central Bank (ECCB) launched its historic DXCD pilot, in March 2019, with the "D" for "digital" added to "XCD", the international currency code for the Eastern Caribbean (EC) dollar.⁵¹

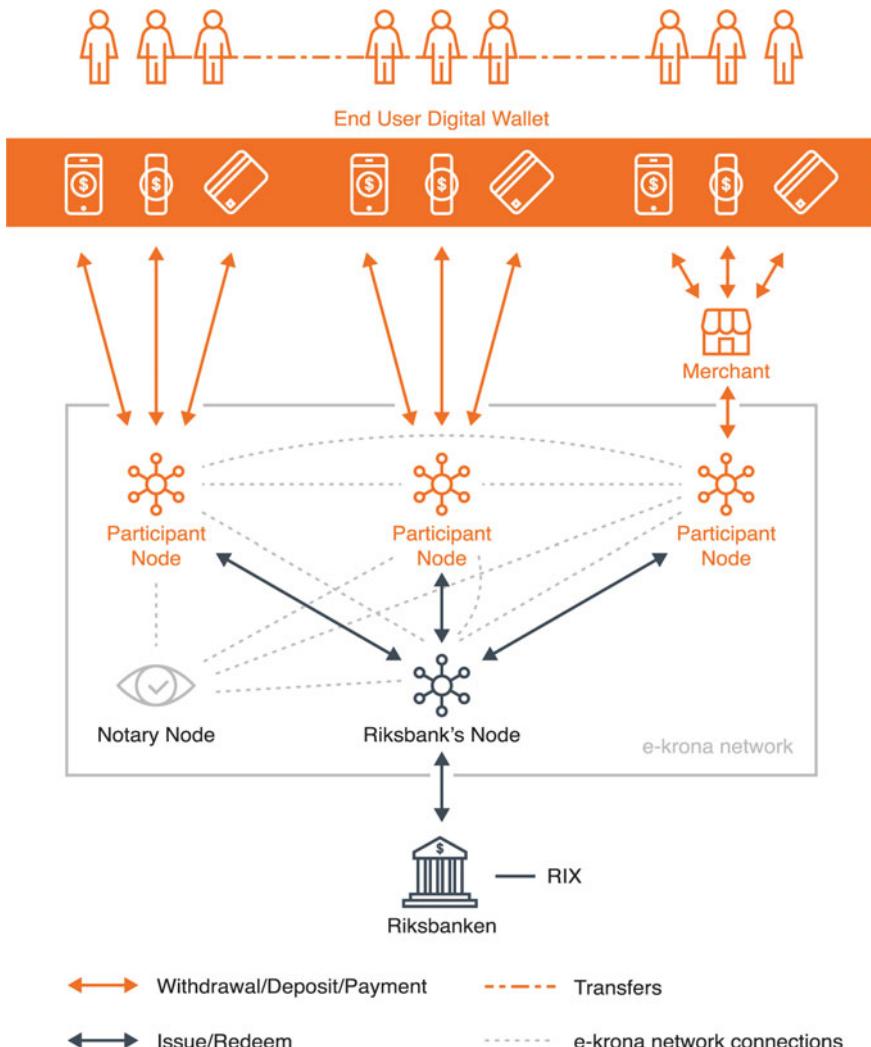


Fig. 2 Conceptual framework for the E-Krona pilot (Source "The Riksbank's E-Krona Project Report 2," Riksbank, October 2018 [4])

The pilot involved a securely minted and issued digital version of the EC dollar—DCash. The objective of this pilot was to assess the potential efficiency and welfare gains that could be achieved from the introduction of a digital sovereign currency, including deeper financial inclusion, economic growth, resilience, and competitiveness in the Eastern Caribbean Currency Union (ECCU). The goal of the ECCB is for DCash to be issued by the ECCB and distributed by licensed bank and non-bank financial institutions in the ECCU. It will be used for financial transactions between consumers

and merchants and person-to-person (P2P) transactions, all using smart devices. When it comes to the data privacy, the ECCB has been clear that it does not have access:

Only the parties participating in a transaction, and their associated financial institutions, have access to that transaction's history. Access to the transaction history on users' phones requires the user to authenticate to the device. Financial institutions use multi-factor-authentication to access any transaction data stored on the backend.⁵²

However, whilst the two-tiered model has many benefits for central banks from a financial stability perspective as that it keeps the existing banks in the mix, the fact that it does not have access to granular transaction level data does not enable the central bank to fully optimise the benefits of a CBDC, like the platform model.

What is the March 2020 Digital Dollar Proposal?

The United States was traditionally seen as a laggard when it comes to CBDCs. This isn't surprising as the United States, with the dollar being the world's reserve currency, could be argued had little incentive for things to change. But sometimes unprecedented times give rise to unprecedented ideas. For example, in March 2020, as the United States was in the middle of dealing with the COVID-19 pandemic, the idea of a "digital dollar" was discussed in both the U.S. House of Representatives and Senate as part of a coronavirus stimulus package. Whilst the proposal of a digital dollar was removed in the final draft of the stimulus package, it brought together many ideas that have been discussed in crypto policy circles in recent years (e.g., FedAccount, Tiered Retail CBDC, Narrow Banking).

The Act provided for the creation of a Digital Dollar, a Digital Dollar Wallet, and a Pass-Through Digital Dollar Wallet to be made available no later than 1 January 2021. A Digital Dollar was defined as (a) "a balance expressed as a dollar value consisting of digital ledger entries that are recorded as liabilities in the accounts of any Federal reserve bank" and (b) an electronic unit of value, redeemable by an eligible financial institution.

What this meant in practice was that the Act allowed (a) member banks to participate using the existing reserve banking system (like other retail CBDC proposals) but also (b) created a token or value-based retail central bank digital currency. The concept of a Pass-Through Digital Dollar Wallet was introduced and defined as "a digital wallet or account, maintained by a member bank or on behalf of a qualified individual, where such qualified individual is entitled to a pro rata share of the pooled reserve balance that the member bank

maintains at any Federal reserve bank". In practice, this was like the "Narrow Banking" ideas that have been discussed in the past (i.e., banks that cover 100 per cent of their liabilities with central bank reserves and do not lend to the private sector) including the idea of a FedAccount. Financial inclusion was clearly a goal as any qualified individual (defined as any individual other than any non-resident alien individual) could require any member bank to have a pass-through digital dollar wallet.

However, it is unlikely that member banks would have been in favour of this (which may have been a reason it did not make it into the final draft). It not only required them to establish and maintain a separate legal entity for these pass-through digital dollar wallets, but also imposed a range of restrictions. For example, these accounts cannot impose any account fees, minimum/maximum balances, overdraft coverage, and cannot be closed or restricted by the member bank based on profitability considerations. However, these accounts need to pay interest, provide functionality, and service levels not less favourable than those that the member banks offer for its existing transactions accounts (including access to debit cards, ATMS, etc.). Member banks would have to cover the cost incurred for this programme except those with assets of less than US\$10 billion where the costs would be reimbursed by the Federal Reserve. Also, non-member banks, like state banks and credit unions, would be able to open such accounts for the exclusive purpose of offering pass-through digital dollar wallets. In practice, this touches on some of the ideas discussed by the IMF in its synthetic CBDC proposal. As mentioned, this proposal was dropped from the final proposal of the stimulus bill, but nevertheless, it demonstrated that even the United States understand the benefits of issuing a CBDC.

3.5 Platform Approach

Another approach to a retail CBDC is called the platform approach (often referred to as hybrid by others, including the BIS).⁵³ Whilst this approach has a lot of similarities with the two-tiered or intermediated model, there is one major difference. In the platform/hybrid model, the central bank also records retail balances on its main ledger (versus recording only wholesale balances in the two-tier/intermediated model.) In such a platform/hybrid model, the private sector onboard all clients; is responsible for enforcing AML/CFT regulations and ongoing due diligence; and conducts all retail payments in real time. However, the central bank also records retail balances, allowing the

central bank to act as a backstop to the payment system.⁵⁴ If any of the intermediaries fail, the central bank has the necessary information, including the balance of every retail client, allowing it to substitute for the failed intermediary and guarantee a working payment system.⁵⁵ The platform approach was first put forward by Sweden's Riksbank in 2018. As the Riksbank described it in 2018:

The Riksbank would supply a platform or technical infrastructure containing an account structure for account-based e-krona and a register that enables the issuing and redemption of value-based e-krona. The e-krona platform in turn needs to be able to interact with various types of system and/or application, namely user applications, external systems, internal support systems and settlement systems.⁵⁶ (Fig. 3)

The Riksbank 2018 proposal of a retail CBDC platform had several components:

- **Core e-krona platform:** Contains central register for holders of e-krona and the regulatory framework and conditions to be applied. The platform has the logic necessary to process and implement different types of payment. The e-krona platform is the central part of the e-krona system that also manages interactions with other systems and participants. Regulatory framework for the e-krona platform owned by the Riksbank and where payments between e-krona users will be settled.
- **User applications/users:** These are applications that can be used to make payments. These can be apps but also IoT devices.

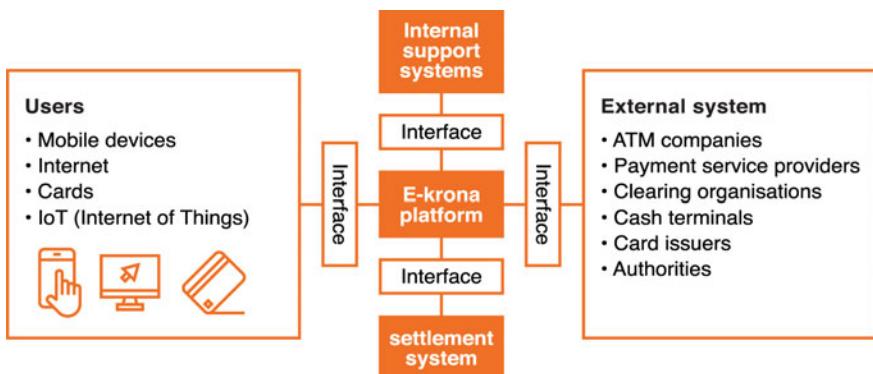


Fig. 3 Platform model design of the E-Krona system (Source "The Riksbank's E-Krona Project Report 2," Riksbank, October 2018 [18])

- **External systems:** These are systems that connect to the core e-krona platform. What type of systems will need to be connected depends on the final design. For example, if e-krona offers services via a card, the platform needs to have a connection to an underlying card infrastructure, such as a card issuer.
- **Internal support systems:** These internal systems enable administrative and various types of control functions, e.g., checks for money laundering and terrorist financing.
- **Settlement systems:** The e-krona platform must be linked to a settlement system for central bank money. It must be possible to move e-krona in and out of the platform smoothly and safely so that there is control at each given point over how many e-krona there are in total on the platform.

In a platform model, the central bank has an important role: to build a platform to which not only banks but non-bank FinTech firms or payment companies can connect. In its March 2020 discussion paper, the Bank of England also put forward the idea of a platform model.⁵⁷ The BoE proposal was that it would build a fast, highly secure, and resilient technology platform (which it called the “core ledger”), which would provide the minimum necessary functionality for CBDC payments. This would serve as the platform on which private sector firms, called Payment Interface Providers (PIP), not just regulated intermediaries with an account at the central bank, could connect in order to provide customer-facing CBDC payment services.⁵⁸

These PIPs firms could build “overlay services” or additional functionality not part of the core ledger, but which could be provided as a value-added service for users. The BoE would impose standards for these overlay services, alongside wider regulation, to ensure they were secure, resilient, and interoperable with the wider CBDC payment system. But if the private sector complies with these standards, they would be free to innovate and come up with payment services for specific use cases using CBDC (Fig. 4).

The BoE’s model has several components⁵⁹:

- **Core ledger:** The core ledger is a database that records CBDC values, and processes payments and transactions made using CBDCs. The core ledger could be limited to the essential features required to enable CBDC payments, making it easier to build a system that is simple, fast, and resilient, and could allow innovation in CBDC payment functionality to happen in the private sector.
- **Application Programming Interface (API):** The core ledger would be accompanied by an API to allow third-party PIPs to securely send payment

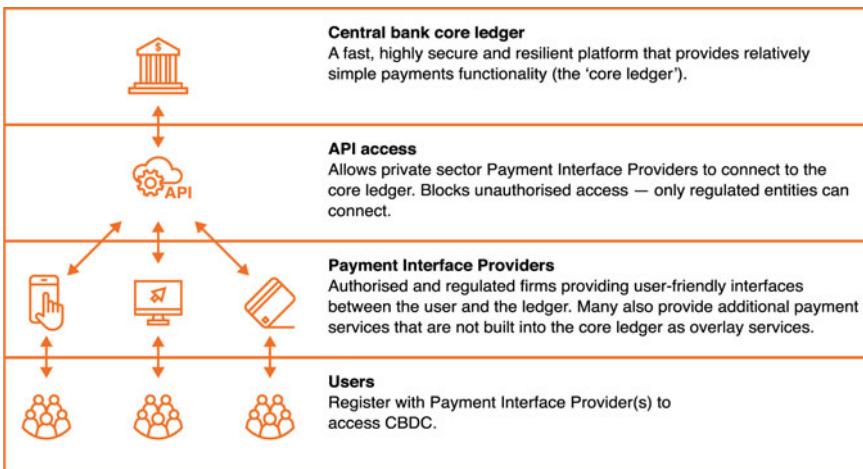


Fig. 4 Platform CBDC model (Source "Central Bank Digital Money: Opportunities, Challenges, and Design," Bank of England, March 2020 [26])

instructions and ask for updates from the ledger. To ensure resilience, security, and integrity, only entities approved by the bank would be able to connect to the core ledger.

- **Payment Interface Providers (PIP):** Would be private sector firms managing all interactions with users of CBDCs and provide overlay services that extend the functionality of CBDCs. The range of services they can provide is broad and can include an interface and the KYC to AML checks and merchant services.

What is also interesting with the BoE proposal is that although the model is fully permissioned, the BoE also mentions that whilst it operates the core ledger itself, it could be open to the possibility of distributing or decentralising aspects of the maintenance of the ledger and processing of transactions.⁶⁰ Another central bank that has taken a platform/hybrid approach is Cambodia with Project Bakong.⁶¹ The National Bank of Cambodia (NBC) began its CBDC work in 2016 with the launch of Project Bakong, named for a temple of the ancient Khmer Empire dedicated to Lord Shiva. The goal of the project was to explore the capacity of digital payment systems to mitigate burdens for banks, to encourage the use of the local currency, the riel, and, most importantly, to enhance financial inclusion.⁶² The NBC concluded that they would need a retail CBDC based on DLT. In 2017, the NBC selected Hyperledger Iroha, as its backbone a blockchain platform commissioned by the Linux Foundation Hyperledger Project.

Without diving into details of Project Bakong, it's important to understand that it would connect all the financial institutions and payment service providers of the country under a single payment platform allowing for fund transfers to be processed on a real-time basis without the need of a centralised clearinghouse. Institutions that are current participants of the country's fast payment system called FAST would be able to interface directly with Bakong without making changes to their existing infrastructure.⁶³ Interestingly, it seems Cambodia chose the platform/hybrid approach where the central bank also maintains a record for all retail transactions whilst KYC is the obligation of participating institutions. As mentioned by the BOC:

Transactions are transparent to validating nodes, which are run by the NBC as a central bank and a regulator, without disclosing the identity of parties involved in performing the transaction. In this sense, Bakong requires participating institutions to manage KYC for their end users or clients. This segregated approach reinforces privacy of users and ensures the public's trust.⁶⁴

One jurisdiction that has done a lot of work on this topic and launched a retail CBDC in late 2020 is the Bahamas with its Sand Dollar.⁶⁵ The Sand Dollar project has four major goals:

- Increase efficiency of Bahamian payments systems through more secure transactions and faster settlement speed.
- Achieve greater financial inclusion, cost-effectiveness, and provide greater access to financial services across all the Bahamas.
- Provide non-discriminatory access to payment systems without regard for age, immigration, or residency status.
- Strengthen the country's national defences against money laundering, counterfeiting, and other illicit ends by reducing the ill effects of cash usage.

It released the Sand Dollar, a digital version of the Bahamian Dollar, via authorised financial institutions with the goal to allow greater flexibility and accessibility for residents that want to participate in financial services via either smartphone (iOS and Android) or using a physical payment card to access a digital wallet.⁶⁶ The Central Bank has been clear on the role it intends to play:

Central Bank of The Bahamas plays a multi-purpose role, including currency issuance, monitoring of holdings and sponsoring a centralised KYC/identity infrastructure. In particular, although the Bank will not provide front-end

customer service, nor directly sponsor digital wallets, it maintains the ledger of all individual holdings of the digital currency.

On a near to medium-term timeline, the bank will promote a centralised KYC register to maintain identification and profile data that would either mandate or allow individuals who do not maintain such information within banks or licensed intermediaries to supply data for the register.⁶⁷ The Sand Dollar also has a tiering mechanism, with two types of wallets for individuals and one for businesses⁶⁸:

Individual Wallet Tier 1:

- \$500 eWallet holding limit, with a \$1,500 monthly transaction limit.
- Government-issued identification is not an enrollment requirement.
- Cannot link to a bank account.

Individual Wallet Tier 2:

- \$8,000 eWallet holding limit, with a \$10,000 monthly transaction limit.
Government-issued identification is required for enrolment.
- Can be linked to a bank account.

Merchant Wallets:

- Holding limit of \$8,000 to \$1,000,000 with unlimited annual transactions. Merchant wallets must be tied to a bank account and produce a Valid business license and a VAT Certificate during enrolment.

The most recent example of a platform/hybrid model is the People's Bank of China with its latest e-CNY tests. If one of the financial institutions or payment firms fail, the PBOC can act as a backstop and as it has the necessary information, it can guarantee a working payment system (probably by having another player or a group of players service those customers).⁶⁹ What really sets this platform/hybrid approach different from the two-tier/intermediated one is the fact that the central bank has access to the full record of CBDC transactions, so the big issue here is privacy. Will citizens be happy that their central bank has access to all the transactions they conduct? Whilst this may work in China, would it be possible in Europe, where privacy is treasured? In addition to the obvious data privacy concerns, this also gives rise to many data governance and data security issues. This is why in the traditional world of finance or in schemes like the FPS, central banks do not hold customer data. It's an area of intense research and experimentation at the time of writing and

I would expect a lot more work to take place on this topic over the coming months and years.

What You Need to Know About China's e-CNY

In the summer of 2021, China's central bank, the People's Bank of China (PBOC), published a progress report that provides several interesting details on its upcoming digital currency, the e-CNY.⁷⁰ Here are the 10 things everyone interested in the future of money should know about the e-CNY.

1. What is the e-CNY?

The e-CNY is the digital version of the fiat currency issued by the PBOC and operated by authorised operators (e.g., commercial banks, licensed non-bank payment institutions). The e-CNY will be a substitute for cash in circulation (M0) and its issuance and circulation will be identical to that of physical RMB (1 e-CNY = 1 physical RMB). The e-CNY will coexist with physical RMB, be a liability of the central bank, and have legal tender status.

2. How will the e-CNY be distributed?

The e-CNY adopts a centralised management model with a two-tier operational system. The right to issue e-CNY belongs to the state and the PBOC lies at the centre of the e-CNY operational system, responsible for issuance and disposal, inter-institution connectivity, and wallet ecosystem management. Additionally, the PBOC is responsible for selecting commercial banks with certain strengths in capital and technology as authorised operators to take the lead in providing e-CNY exchange services. But it's these authorised operators (e.g., commercial banks, licensed non-bank payment institutions), selected by the PBOC, who will circulate the e-CNY to the public.

3. Will physical cash be banned?

No. The PBOC makes it clear that if there is demand for physical RMB, the PBOC will not stop supplying it nor replace it via administrative order. The PBOC reiterates that China is a large country with a vast territory, large population, multiple ethnic groups, and wide differences in regional development and that in such a society, people's payment habits, age, and security needs vary. Therefore, physical RMB enjoys advantages that cannot be easily replaced by other means of payment.

4. What about privacy?

The PBOC mentions that the e-CNY follows the principle of "anonymity for small value and traceable for high value", and that it "attaches great importance to protecting personal information and privacy". The PBOC aims to meet the public's demand for anonymous small value payment services. But at the same time, it wants to guard against the misuse of

e-CNY in illegal and criminal activities, such as money laundering or tax evasion, by making sure that larger transactions comply with AML/CFT requirements.

5. What kind of data will be collected?

The PBOC makes it clear that the e-CNY system will collect less transaction information than traditional electronic payment and will not provide information to third parties or other government agencies unless stipulated otherwise in laws and regulations. Internally, the PBOC will also set up a firewall for e-CNY related information, and strictly implement information security and privacy protocols, such as designating special personnel to manage such e-CNY data, separating e-CNY from other businesses, applying a tiered authorisation system, putting in place checks and balances, and conducting internal audits. Any arbitrary information requests or use will be prohibited. However, the PBOC also mentions in the report that it has set up a framework of big data analysis, risk monitoring, and early warning for e-CNY to enhance the foresightedness, accuracy, and effectiveness of e-CNY management.

6. Will the e-CNY be used for cross-border payments?

The PBOC acknowledges that the question as to whether the e-CNY will be used in cross-border payments and to promote RMB internationalisation has been drawing much attention and makes it clear that although technically ready for cross-border use, the e-CNY is presently designed mainly for domestic retail payments. However, the PBOC explicitly mentions that the internationalisation of a currency is a natural result of market selection and that cross-border payments involve various complicated issues such as monetary sovereignty, foreign exchange policies and arrangements, and regulatory and compliance requirements.

7. What types of wallets will be available?

Both individual and corporate wallets will be available. Transaction and balance limits will be determined depending on the level of KYC, but the PBOC makes it clear that “least-privileged” wallets can also be opened without any KYC to reflect the principle of anonymity but that these wallets can then be upgraded following KYC. Both software and hardware wallets will be available, software wallets through mobile payment apps, SDKs and APIs, and hardware wallets via IC cards, mobile phones, wearables, and other IoT devices. The PBOC also mentions that parent/sub-wallet structures will also be available. Individuals can set payment caps, payment conditions, personal privacy protection, and other functions through sub-wallets. Corporates and institutions can pool and distribute funds and manage finances through sub-wallets.

8. Will the e-CNY work offline?

The e-CNY will share both the features of physical RMB (token-based) such as settlement upon payment and anonymity and the features of electronic payment instruments (account-based), which are less costly, highly portable, highly efficient, and hard-to-counterfeit. Thus, the token-based feature also enables the e-CNY to work offline.

9. What about programmability and security?

In order to encourage “business model innovation”, the e-CNY will allow programmability by deploying smart contracts that will enable self-executing payments according to predefined conditions or terms agreed between two sides. When it comes to security, the e-CNY will adopt a variety of technologies, including digital certificate systems, digital signatures, and encrypted storage to make double-spending, illegal duplication and counterfeit, transaction falsification, and repudiation unfeasible. In addition, a multi-layer security system will initially be established to guarantee that e-CNY has a safe life cycle and that risks are manageable.

10. How advanced are ongoing pilots and when will the e-CNY officially launch?

It's important to remember that the PBOC has been working on e-CNY since 2014, setting up a task force to study digital fiat currency. In 2016, it established its Digital Currency Institute, which developed the first-generation prototype of digital fiat currency and in 2017, upon approval by the State Council, the PBOC began working with commercial institutions developing and testing digital fiat currency. In 2019, the PBOC finally launched its e-CNY pilots in Shenzhen, Suzhou, Xiong'an, and Chengdu to test a range of aspects, including the stability of systems, the usability of functions, the convenience of processes, the applicability of scenarios, and the controllability of risks. In November 2020, the pilot was also extended to Shanghai, Hainan, Changsha, Xi'an, Qingdao, and Dalian. As of June 30, 2021, the e-CNY has been used in over 1.32 million use cases, covering utility payments, catering services, transportation, shopping, and government services. Around 21 million personal wallets and over 3.5 million corporate wallets have been opened, with over 70 million in transaction volumes representing around RMB34.5 billion (US\$5.3 billion) of transaction value. When it comes to the official launch date, the PBOC simply mentions that it “will continue to prudently advance the pilot e-CNY R&D project in line with China's 14th Five-Year Plan, with no present timetable for the final launch”.

As we can see, further experimentation and societal debate is likely required before we can see numerous countries issue their own CBDC as their impact could be quite transformative on not only the economy but broader society.

This is definitely an area to watch in the coming years as it can be argued it's only a question of when, not if, a major G20 central bank will launch its own retail CBDC.



11

Utility Tokens and Social Tokens

1 Utility Tokens

Utility tokens are crypto-assets designed to be consumed and provide a specific utility. For example, a consumer token could be used to access a service, offered by a certain blockchain, which could be cloud storage usage, a loyalty token redeemable for a physical good such as a coffee, or perhaps access to a specific piece of content like an online multi-player video game. These assets can theoretically enable a range of benefits for consumers, allowing them greater flexibility in coordination with the exchange of consumption rights.¹ Perhaps the most well-known example of a utility token in use today is Ether, the native token of the Ethereum blockchain. As we discussed in detail earlier in this book, Ethereum seeks to provide a decentralised and shared world computer where anyone can use Ether tokens, sometimes referred to as “gas”, to run segments of code called smart contracts.

Other blockchains like Solana, Algorand, and Avalanche exhibit similar characteristics, and the best way to explain a utility token is via an analogy. One that I like to use is that of a private club. Imagine a consumer token that is used to pay membership dues in a private club that provides access to a range of facilities including a golf course, restaurant, and steam room. The token provides access to the club but does not confer rights to a portion of the club’s income or a claim on the club’s assets. As the total amount of tokens are limited, if the club is popular and everyone wants to join and use the facilities, then the value of the tokens may go up. However, if nobody wants

to use the private club, the value of those tokens will fall. Another analogy is that of an amusement park. Imagine that someone decides to build a new amusement park where a limited number of tokens are issued that are the only way to pay for entrance fees. These tokens do not confer any other right other than paying for entrance fees, but could also offer some non-monetary benefits like having the right to vote on what new rides the amusement park will open next or what colour to paint the roller coaster. There is obviously no private club or amusement park in the blockchain world (at least not yet!) but this hopefully adds some clarity.

2 When Is a Token a Security?

Every jurisdiction generally has well-defined rules around what is considered a security. In some cases, the definition of a security is set out in legislation and in other cases, it's decided by the courts. Let's examine the legal treatment of this question in two jurisdictions: Hong Kong and the United States. In Hong Kong, if digital tokens offered in an ICO represent equity or ownership interests in a corporation, these tokens may be regarded as "shares". For example, token holders may be given shareholders' rights, such as the right to receive dividends and the right to participate in the distribution of the corporation's surplus assets upon winding up.

Where digital tokens are used to create or to acknowledge a debt or liability owed by the issuer, they may be considered as a "debenture". For example, an issuer may repay token holders the principal of their investment on a fixed date or upon redemption, with interest paid to token holders. If token proceeds are managed collectively by the ICO operator to invest in projects with an aim to enable token holders to participate in a share of the returns provided by the project, the digital tokens may be regarded as an interest in a "collective investment scheme" (CIS). In Hong Kong, shares, debentures, and interests in a CIS are all regarded as "securities". Where an ICO involves an offer to the Hong Kong public to acquire "securities" or participate in a CIS, registration or authorisation requirements under the law may be triggered unless an exemption applies.² In the United States, the question of what is, and is not, a security regulated by the Securities and Exchange Commission is determined by the "Howey Test", a legal framework that emerged from the 1946 case, SEC v. W. J. Howey Co.

This case revolved around a complex set of real estate transactions related to a tract of Florida orange groves. The owner of these groves, the eponymous Mr. Howey, allowed individuals to purchase parcels of land and then lease

the land back to him under a service arrangement where the maintenance of the land and sale of its produce would be fully managed whilst the owner themselves would have no right of entry to the land. Whilst purchasers could make other leasing arrangements, the sales materials advertised the significant profits and superior quality of his services. Most purchasers of land under this agreement were not farmers, and in many cases not Florida residents, but rather professionals with little to no agricultural experience.

The SEC filed an injunction against Howey's corporation arguing that this leaseback arrangement constituted an investment contract and was thus a security. The case was ultimately decided by the U.S. Supreme Court, in which the author of the majority opinion, Justice Frank Murphy, established one of the court's earliest tests to ascertain if a given arrangement constitutes an "investment contract" for the purposes of the Securities Act. Justice Murphy wrote that:

An investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party, it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise.

In other words, the Howey test says an investment contract is a security if it is:

1. An investment of money
2. In a common enterprise
3. With an expectation of profits
4. Solely on the efforts of others

This test has become an important consideration in the minds of both entrepreneurs and investors as they consider whether the sale of their tokens would meet all four of these criteria and thus require registration with the SEC in order to be legally sold in the United States. The Howey Test is a topic that comes up again and again especially as the SEC increases its enforcement cases against token issuers it believes may be distributing tokens to the public. Utility tokens encompass a vast array of potential use cases and should arguably be regulated under whatever consumer protection regulation governs the goods, services, or media being consumed by the user. Unfortunately, whilst regulatory statements to date have largely held this to be true for platforms that *currently* provide access to consumable goods, services, or

media, things could be a little more complicated for those platforms who plan to do so but are not yet operational.

The reason for this is best explained through the previously discussed analogies of the private club or amusement park. Clearly those tokens are not a security, right? It turns out that, at least in some jurisdictions, especially in the United States, it depends on whether the club or amusement park has already been built. In the landmark 1961 case of California Silver Hills Country Club v. Sobieski, a California judge ruled that the use of a membership plan to finance the construction of a new, for-profit country club constituted a solicitation of risk capital and thus required registration as a security issuance. The judge noted that only by a member risking capital alongside other members could the benefits of club membership be created. Interestingly, the conclusion of this case differs from the previously discussed Howey test because even though members of the prospective club do not stand to profit directly from the success of that club, the fundraising scheme is still considered a securities issuance.³

The challenge this poses in the United States to issuing a consumer token is clear. Whilst selling such a token for an existing service likely does not constitute a securities sale, the selling of such a token to fund the creation of a prospective service may well be a securities issuance and therefore subject to much more extensive regulatory scrutiny. This topic has been on the radar of many lawyers operating in the digital assets space due to some recent cases featured heavily in the media on the topic.

A good example was the Hong Kong and Virginia, US-based company, Block.one, that had to pay a US\$24 million civil penalty to settle charges with the U.S. SEC in 2019 for conducting an unregistered initial coin offering (ICO)⁴ According to the SEC's order, Block.one conducted an ICO between June 2017 and June 2018. At that time, Block.one stated it would use the capital raised in the ICO for general expenses, and to develop software and promote blockchains based on that software Block.one's⁵ However, the SEC found that Block.one did not register its ICO as a security offering pursuant to the federal securities laws, nor did it qualify for or seek an exemption from the registration requirements.

Stephanie Avakian, the Co-Director of the SEC's Division of Enforcement, mentioned at the time that "companies that offer or sell securities to U.S. investors must comply with the securities laws, irrespective of the industry they operate in or the labels they place on the investment products they offer".⁶ Block.one paid a US\$24 million penalty without admitting or denying the findings. Whilst one may argue that paying a US\$24 million fine was a bargain considering that Block.one raised around US\$4 billion,

it set the expectation that the SEC was serious about going after crypto firms. Another example happened a few months later with the Telegram case. In 2018, Telegram, the popular messaging app with over 400 million users worldwide, announced that it was working on a next-generation blockchain platform called TON and a cryptocurrency named Gram. TON was designed to share the principles of decentralisation pioneered by Bitcoin and Ethereum but claimed to be vastly superior in speed and scalability. When integrated with Telegram, TON aimed to revolutionise how people store and transfer funds and information.

Telegram ended up raising around US\$1.7 billion in 2018 by way of a private sale that also included U.S. investors.⁷ However, the SEC determined that Telegram's unregistered offering of digital tokens called "Grams" violated federal securities laws. In October 2019, the SEC filed a complaint⁸ against Telegram, alleging that the company had raised capital to finance its business by selling approximately 2.9 billion Grams to 171 initial purchasers worldwide. The SEC sought to preliminarily enjoin Telegram from delivering the Grams it sold, which the SEC alleged were securities that had been offered and sold in violation of the registration requirements of the federal securities laws. On March 24, 2020, the U.S. District Court for the Southern District of New York issued a preliminary injunction barring the delivery of Grams and finding that the SEC had shown a substantial likelihood of proving that Telegram's sales were part of a larger scheme to unlawfully distribute the Grams to the secondary public market. The judge not only blocked the delivery of Grams to its initial purchasers but later clarified that the ban also applied globally including for non-US-based investors, although \$1.27 billion of the US\$1.7 billion of the funds raised to finance the development of the TON came from overseas-based investors. Both parties finally reached a settlement in June 2020. Telegram agreed to return more than \$1.2 billion to investors and to pay an \$18.5 million civil penalty, without admitting or denying the allegations in the SEC's complaint.⁹ This would prove fatal to Telegram token plans. In May 2020, weeks before the settlement with the SC became public, Telegram's CEO would announce that the messaging app's active involvement with TON was over.¹⁰

This was an unfortunate development which put an end to one of the biggest and most interesting blockchain development projects globally that could have a big impact due to its scale. This event also reignited not only the debate regarding the extraterritorial reach of U.S. regulations but also pushed some global players to avoid U.S. markets, a practice that was already increasingly common, and also reignited the debate around decentralisation

and reinventing how we view money. As Telegram's CEO wrote in ending his letter:

I want to conclude this post by wishing luck to all those striving for decentralization, balance and equality in the world. You are fighting the right battle. This battle may well be the most important battle of our generation. We hope that you succeed where we have failed.

The Telegram development also reignited the debate around the negative effect regulations can have on innovation in the field of crypto if new ideas and business models cannot take off.

What was the SEC's Token Safe Harbour Provision?

One idea proposed in early 2020 (and posted on GitHub) by an SEC commissioner, Hester Pierce, was that of a Token Safe Harbour. Pierce has a great understanding of the crypto ecosystem and was even nicknamed "Crypto Mom". (Fun fact: Commissioner Hester Pierce was the first person to receive a copy of my last book "The Future of Finance", as I was meeting her just 10 minutes after I received the first hard copies in my hands.)

The safe harbour originally proposed in February 2020 sought to provide network developers with a three-year grace period within which, under certain conditions, they can facilitate participation in and the development of a functional or decentralised network, exempted from the registration provisions of the federal securities laws. Based on feedback from the crypto community, lawyers, and members of the public, the proposal was amended in April 2021 to address concerns especially in relation to investor protections.

First, to enhance token purchaser protections, the safe harbour proposal now requires semi-annual updates to the plan of development disclosure and a block explorer. Second, in response to concerns about the lack of clarity at what happens at the end of the three-year grace period, the safe harbour proposal now includes an exit report requirement. The exit report would include either an analysis by outside counsel explaining why the network is decentralised or functional, or an announcement that the tokens will be registered under the Securities Exchange Act of 1934. Third, the exit report requirement provides guidance on what outside counsel's analysis should address when explaining why the network is decentralised.

The guidance is not a bright-line test, but rather attempts to strike a balance between providing a manageable number of useful guideposts whilst maintaining sufficient flexibility for the facts and circumstances of each network to be considered in the analysis. Whilst at the time of writing, this Token Safe Harbour is not adopted yet, there is a lot of optimism that it will,

especially from Gary Gensler, who became SEC Chairman in April 2021. Whilst Chairman Gensler had a long career as a banker (he was a partner at Goldman Sachs) and as a regulator (he led the CFTC from 2009 to 2014), he also has been a Professor of the Practice of Global Economics and Management at the MIT Sloan School of Management and has been heavily focused on blockchain and crypto in recent years. Time will tell if the optimism is justified...

Efforts to clarify the regulatory landscape for utility tokens in the United States and abroad are underway, but in many jurisdictions, there's no clear timeline to the delivery of regulatory guidance. It should therefore be expected that treatment will differ from region to region, and that in many jurisdictions, regulatory uncertainty regarding utility tokens will persist for the foreseeable future.

3 Social Tokens

One interesting type of crypto-asset that has started to gain serious steam as of 2021 has been social tokens. But what exactly are social tokens? Social tokens (sometimes referred to as community tokens) are tokens backed by the reputation of an individual, brand, or community. These social tokens have various uses, from giving access to special content from an individual (e.g., a newsletter, special content, unique merchandise) to broader use in a community (e.g., ability to vote on governance decisions or new initiatives). As these tokens are often limited in supply, the more the community grows, the more valuable they may become due to potential increased demand. This in turn provides an incentive for community token holders to see the community can grow and succeed.

There have been a number of factors behind the rise of such social tokens. One main one is that they give content creators more control over how they can monetise their work. For example, it is well documented how artists or content creators only get a fraction of the fees that large platforms, from Spotify and YouTube to Facebook and Instagram, generate off their work. Second, this is part of the broader trend of the “ownership economy”, an idea that crypto can enable a better distribution of value.¹¹ Rather than a platform’s inner circle of founders and investors pocketing the value, users can earn most of the value generated from their collective contributions, and like many other developments in recent months, COVID-19 acted as a catalyst to

this phenomenon. The virus forced many small brands and creators to rethink how they engage with their fans and followers. We can see the impact of this in everything from the rise of Patreon, Substack, and Bandcamp to the more paywalled content on Twitch and YouTube.

What makes social tokens so powerful is that they are directly or indirectly linked to the growth in NFTs as well. It can be argued that whilst an NFT is the first step that a celebrity or artist can take when issuing a unique collectible or piece of art, social tokens can be the natural next step. The Grammy-winning artist RAC is a good example. He issued an NFT which could be redeemed for a limited-edition cassette tape. After the success of this first experiment, he then launched a token¹² that gave access to limited-edition perks and content. In addition to individual content creators, many public personalities, from rappers to artists and athletes, have jumped on the bandwagon in recent months. Social tokens are not only intertwined with NFTs but also the broader metaverse and Web 3.0 developments, with more on that later in this book.



12

Security Tokens

Security tokens (or investment tokens) are instruments whose primary function is to serve as a financial investment for the holder of the token and thus are considered securities (or in some cases commodities) under most regulatory regimes. These can include both instances where pre-existing physical assets or legal rights (such as a bond or a share of stock) are “tokenised” on a blockchain, and instances where new investment opportunities are created that are native to the crypto-asset ecosystem (including a significant number of ICOs that have security like features). We’ll explore both in this chapter.

1 What Is Tokenisation?

Tokenisation consists of issuing digital tokens on a blockchain where each token represents an underlying real life or digital asset. For example, imagine a large office tower in downtown New York City, on sale at the price of \$100 million dollars. Unless you’re an individual or a company with lots of money, like a private equity fund or a pension fund, buying such a large asset on your own is practically impossible. This is why many large assets have what we call an illiquidity discount, as they are not that easy to sell and there are only a few buyers who can afford to pay for it.

Tokenisation consists of taking this one, large \$100 million asset, then dividing it into 1 million shares that would each cost \$100, with each share represented by a digital token on a blockchain. This kind of an arrangement

has many benefits. First, it enhances liquidity because more people can buy an asset that costs \$100 than something that costs \$100 million and there is likely to be more activity, more buying and selling, of the tokens of that asset. This not only helps in what is called price discovery, as it allows us to better reflect the price of an asset but is a win-win for both the asset owner and potential buyers as it provides for more liquidity. Second, it provides access to people. To remain in the real estate example, I'm sure many readers have looked at buying a house, but you don't always have enough capital to put the down payment together and may need to save for years before having enough cash. With tokenisation you still need to save for that one lump sum, but at least you have a chance to have access and exposure to the real estate market earlier by buying the \$100 tokens, where at least you're buying assets and aren't left entirely out of the market.

The third benefit is cost. Tokenising such large assets into smaller pieces was not economically feasible before the rise of blockchain technology, as the costs and operational headaches didn't outweigh the benefits. For example, the closest thing we have today to tokenisation in the real estate space is something called a Real Estate Investment Trusts (REIT), products listed on major stock exchanges around the world. REITs let you buy into a select set of real estate assets by buying a share of that REIT. But such products do have downsides: they are expensive to put together and only provide exposure to a set number of assets that the REIT manager and trustee have included. Blockchain technology changes that, as it allows tokenisation of any asset for a fraction of the price. Another benefit is access, in that you could, in practice, tokenise any asset of value and give people access to assets previously unavailable. Some have already started tokenising pieces of art that were previously only available to the very wealthy. This has already begun with paintings by Andy Warhol and Pablo Picasso being tokenised and made available to the broader public who can buy a fraction of a painting and, although they cannot hang it in their living room, they get the economic exposure to the painting, with such assets traded on regulated exchanges around the world.

This doesn't only apply to real-life assets and can be even more easily applicable to digital assets. For example, in March 2021, the artist Beeple sold an NFT for US\$69 million dollars. It's important to understand that as that piece of art was digitally native in the form of a NFT, it's even easier to tokenise it and automate all activities. For example, whilst very few can afford to pay US\$69 million dollars for a piece, many more could afford 1/100,000th of that if it was tokenised. The beauty is that if the painting is sold again, each one of the 100,000 token holders will automatically receive its share of the selling price.

Of course, tokenisation goes beyond real estate or art as it allows us to transform many of the outdated aspects of finance today. For example, consider company shares. Today when you buy or sell a public company stock, there are several operational processes that take place behind the scenes like clearing and settlement, to shareholder voting and other corporate actions. For example, finding who the shareholders are of a certain stock today is not as straightforward as you might expect, complicating basic processes like shareholder voting and dividend payments. The beauty of tokenised blockchain assets is that you always know who the shareholders are, and you can pay dividends instantaneously using digital assets. For example, there is nothing that stops you from moving away from annual or quarterly dividends and moving towards monthly, daily, or even hourly dividends as blockchain technology now enables.

Tokenisation is probably even more impactful for SMEs, whose access to capital is archaic and often still paper based. If we were to tokenise private company stock, by having each stock represented by a digital token on a blockchain, we could dramatically reduce the costs of issuance, trading, and ownership of such assets. Smaller companies could tokenise their shares and offer it to investors and the process would cost a fraction of what it costs for a company to go public via an IPO and more user-friendly than the archaic term sheets with wet signatures still in use today. We're still in the very early days of the broader tokenisation movement and whilst the technology is already quite advanced, a lot remains to be done to educate investors and issuers alike on what tokenisation is and its potential benefits.

2 Tokenisation of New Investment Instruments

In addition to facilitating payment or providing a utility function, crypto-assets can act as investment instruments for the formation of capital around a new venture. For example, a promising start-up seeking funding from investors might choose to sell equity in the form of a security token. In theory, this could enable the firm to involve fewer intermediaries in the raising of capital, give early-stage investors access to improved liquidity, streamline corporate actions like dividends, and even democratise access to investments in the start-up, allowing average people to purchase small stakes, where usually only venture capitalists or the very wealthy could make investments.

This is a compelling narrative, but unfortunately, implementing it is a good deal more complicated. In most jurisdictions, before a security can be

sold to the general public, it needs to be registered with the relevant regulatory authorities, a typically lengthy, costly, and complex process which is designed to protect small-time investors saving for retirement. Regulators are concerned that average people who lack specialised training in investments and lack sufficient funds to endure a significant financial loss without experiencing financial hardship, may be persuaded by promises of vast returns to invest in high-risk or poorly conceived ventures. Fortunately, for those wishing to raise capital via the sale of newly created security tokens, “private placement” exceptions exist in most jurisdictions, allowing securities to be sold to some types of investors and the public without the same onerous registration requirements placed on securities issuances, if certain requirements are met.

The most common of these requirements is ensuring that the security is issued only to “accredited investors”, also sometimes called “professional investors”. These are individuals deemed sufficiently sophisticated and wealthy enough to understand and evaluate the risks of their investments and to endure consequences if the investment fails to meet expectations. Requirements to be considered an accredited investor differ from jurisdiction to jurisdiction, in some cases being determined by income and in others by liquid net worth, but if the token offering limits marketing only to such individuals it will likely be exempt from registration, or subject to less onerous requirements.

Based on these exemptions, many crypto companies have decided to offer tokens only to professional and/or accredited investors, even if they themselves do not consider the token a security. Given existing regulatory uncertainty, this limits their exposure to regulatory action if the regulator comes to a different conclusion. This strategy was particularly common in the United States where the previous SEC chairman stated publicly that the commission viewed most ICOs as securities and with the high-profile enforcement cases against firms like Block.one or Telegram we discussed earlier.¹

Whilst such an approach solves some problems, it also creates new ones. For example, most token ecosystems require a critical mass of users to be sustainable. If funds are raised from a broad community of retail investors, it could create a natural base from which to build user engagement. By contrast, building such an ecosystem with only professional investors and not regular end-users can be a challenge. Restrictions on public ownership may also limit the value of a token to accredited investors, limiting the range of potential buyers for the tokens in secondary markets. This is one of the drivers behind the Token Safe Harbour proposal put forward by SEC Commissioner

Hester Pierce discussed earlier. Despite these challenges, nothing stops a start-up from raising funds via a security token offering, with a good example FinTech company Figure Technologies that raised over US\$100 million in such a manner.²

3 Tokenisation of Pre-existing Investment Instruments

In addition to facilitating the creation of tokens that act as new investment instruments, blockchain technology enables the “tokenisation” of existing investment instruments. This is another way of saying that legal rights to the underlying instrument are represented by an entry in the distributed ledger of a blockchain network, allowing the asset to be freely traded between network participants via updates to the distributed ledger. In some cases, features such as the distribution of dividends and voting rights might also be handled via the blockchain and in all other ways, the instrument continues to have the same properties as if it were traded on a more traditional centralised exchange or through a peer-to-peer “over-the-counter” (OTC) arrangement.

Theoretically there is no limit to the assets that could be tokenised, including financial instruments such as equities, bonds, and derivatives or commodities like gold, silver, wheat, or even orange juice. In practice though, these instruments are already actively traded on longstanding exchanges around the world, making it difficult for blockchain-based solutions to displace their network effects (at least in the near term). However, there have been interesting developments in recent months with the tokenisation of traditional financial assets. For example, many organisations from the Bank of Thailand and the Union Bank of the Philippines and even organisations like the European Investment Bank or the trading firm Olam International, have issued blockchain-based bonds, with the BIS Innovation Hub in Hong Kong and the Hong Kong Monetary Authority looking at tokenising green bonds for the retail investing public.³

Where blockchain can potentially be more disruptive is in assets with existing markets that are informal, disconnected, or inefficient. Gold and oil are highly standardised products that are actively traded and have global prices, but markets for less standardised assets like fine art or diamonds are not, nor are those for large assets, like large pieces of real estate, often sold as a bloc. As a result, these assets can suffer from an “illiquidity discount” where the price of the asset is negatively affected by their inability to be easily bought and sold. Advocates argue that tokenisation of these assets would facilitate

improved liquidity by increasing asset transparency and reducing the cost of price discovery.⁴

For example, one could tokenise the shares of a holding company that owns a piece of real estate, an asset that has traditionally suffered from significant illiquidity. Instruments for doing this already exist in traditional markets, most notably REITs that offer investors exposure to fractional assets; however, these organisational forms are expensive to establish and are typically only used for very large properties. If blockchain networks for fractional ownership of tokenised real estate could be deployed cheaply and at sufficient scale, it could enable the sale of fractional ownership in a much smaller asset, such as a personal home.⁵

A recent example of real estate tokenisation in action is the Aspen Digital Security Token, which enables investors to own an indirect equity stake in the St. Regis Aspen Resort in Colorado.⁶ Others have been involved as well, including Latin American investment banking giant BTG Pactual issuing the ReitBZ token on the Tezos blockchain backed by Brazilian real estate and enabling investors to get exposure to this asset class. Tokenisation may also serve a purpose in the case of certain kinds of funds. Accredited and institutional investors will often allocate money to venture capital and private equity funds in addition to their more traditional allocations to stocks and bonds. The underlying assets that these private equity and venture capital funds invest in are highly illiquid, so the fund will typically require allocations to be “locked in”, often for years at a time. Sales of the end investors’ capital are possible today in “secondary markets”, which lack liquidity and transactions often require extensive paperwork. Tokenisation may also bring liquidity to assets that are otherwise illiquid.

A good example was the NBA’s Brooklyn Nets guard Spencer Dinwiddie looking to tokenise his \$34 million contract. The project was structured as a bond sale that raised the contract’s upfront value and allowed Dinwiddie access to the capital. The security token holders would in turn receive payouts as the season progressed.⁷ Having marketplaces of tokenised secondary sales may make it easier for investors to buy and sell such fund units. It may also allow individuals holding large allocations of private stock (for example, the founding team of a fast-growing start-up) to more efficiently realise sales of that stock prior to an initial public offering (IPO). Additionally, tokenisation of physical assets can also enable fungibility of assets that are not fungible in the physical world. For example, in the physical world an expensive painting generally can only have one owner, but when tokenised, ownership can be distributed more easily amongst many individuals. In June 2018, fractional ownership of Andy Warhol’s painting “14 Small Electric Chairs” was sold

using a blockchain platform that allowed buyers to each own a fraction of the painting.⁸

However, it's important to temper our excitement for such solutions. The tokenisation of an existing investment instrument on a blockchain will not in and of itself automatically create more liquidity or investor interest. There are many traditional marketplaces that have not been successful in delivering those improvements. Instead, arguments in favour of such systems rely on uncertain assumptions that tokenising the asset on a blockchain would expand the pool of possible investors, by creating greater asset transparency, greater connectivity across regions, or resolving specific issues of mistrust between buyers and sellers. It's also important to remember that the successful design of any such token would be highly complex, in some cases requiring embedded features such as disclosure requirements, transfer or ownership restrictions, corporate actions, etc.

There are also some potential benefits from a CSR perspective, as tokenisation could enable a broader component of the public to access assets that would be otherwise not easily accessible. The best example could be in the tokenisation of real estate assets. In many cities around the world, Hong Kong, London, or New York for example, it's extremely difficult for young people to get started on the real estate ladder as it takes many years before being able to gather the down payment amount required, if they even get there in the first place. Tokenisation of real estate could enable young people to gradually buy small tranches of real estate assets allowing them to gradually gain exposure.

Pro Athletes Tokenising Their Contracts?

We mentioned earlier in the book about how intertwined crypto and sports are becoming. Often that's in the context of advertising or NFTs, but it's also happening when it comes to security tokens. Former NBA Brooklyn Nets guard (and current Washington Wizard) Spencer Dinwiddie announced in 2019 that he was looking to raise \$13.5 million by tokenising the first year of his three-year, \$34.5 million contract. Such a solution would provide cash flow to players whilst allowing accredited investors the opportunity to bet on certain players and fans to show support for their favourite athlete. The NBA, perhaps unsurprisingly, forbade Dinwiddie from moving forward with his project.

Undeterred, Dinwiddie has continued to advocate for his proposal, arguing that democratising contract ownership not only maximises talent acquisition but also enhances fan engagement. Following the COVID-19 pandemic,

NBA players recently agreed to a 25% salary withholding, even though one-third of their players live paycheque-to-paycheque. Whilst Dinwiddie did not wind up getting his way in his new contract, this discussion nevertheless transformed not only the world of professional sports, but also the financial structures that bolster social media influencers and popular entertainers. The tokenisation of talent contracts may not bring fans back to the stadium, but it could offer players the ability to manage their cash flow in a whole new way.

At the time of writing, there are still certain barriers that are holding back the growth of security tokens.

- **Lack of investor familiarity:** Getting investors to invest in a new instrument is a difficult task, which has certainly been true with security tokens. For example, at the time of writing, the total value of assets that were issued was still less than US\$2–3 billion.
- **Liquidity:** Whilst it's easy to issue a security token, getting investors to trade them is a different story. For example, the monthly liquidity or volumes of security token trading is still limited and consists of less than US\$10 million per month.
- **Lack of awareness on STO:** Whilst many people know about Bitcoin or cryptocurrencies, a small number know about security tokens (including readers of this book).
- **Lack of standard:** There are numerous STO initiatives taking place globally on various blockchains.

Whilst these barriers are significant, interest remains and a growing number of major players in the capital markets are experimenting with blockchain. NASDAQ's head of Blockchain Product Management said they are “all in” on using blockchain to enable their transactions and to support external marketplaces that are moving into blockchain-based solutions.



13

Non-Fungible Tokens

1 Non-Fungible Tradable Tokens

Non-fungible tradable crypto-assets are tokens that are unique, using the properties of blockchain technology to facilitate more transparent and enforceable scarcity of a digital asset by allowing that scarcity to be easily verified and its ownership transferable.¹ For example, a Bitcoin is equivalent to any other Bitcoin or in the non-digital world, a \$5 bill is equivalent to any other \$5 bill. However, a non-fungible tradable token is unique and can be mathematically proven so by using blockchain technology. A good example is buzz from 2017 by a system of non-fungible tradable tokens called CryptoKitties, built on the Ethereum blockchain, that allows users to buy and “breed” virtual cats, with unique sets of properties. When launched, they became so popular they represented 25% of traffic on the Ethereum network and resulted in network slowdowns.²

In the non-digital world, we have a vast array of goods that are non-fungible. Your house or a piece of art you made is likely to be non-fungible, as it's unique and there are no two of the same kind. The sports memorabilia industry, estimated to be worth over US\$5 billion dollars annually, is a good example with people collecting not only bespoke items, like jerseys worn by certain players, to more widely available but still rare ones, like rookie sports cards.³ Many Magic the Gathering and Pokémon cards are worth thousands of dollars,^{4,5} and there are already vast arrays of digital goods that would be considered non-fungible, including internet domain names with many selling for high prices. For example, the domain “carinsurance.com” sold for

almost US\$50 million and both “insurance.com” and “vacationrentals.com” for almost US\$35 million, and perhaps surprisingly higher than some of the obvious choices you may have thought of like “sex.com” (US\$14 million), “porno.com” (US\$9 million), “shoes.com” (US\$9 million, and “beer.com” (US\$7 million). Staying in the crypto space, the domain “crypto.com” was allegedly bought for US\$15 million dollars from a cryptography professor.⁶ Another example is in the video game industry where buying unique “skins” are proving to be big business, with Epic Games, the company behind the popular game Fortnite, having reportedly made more than US\$2.4 billion in 2018 by selling mostly skins.⁷

In many ways, non-fungible CryptoKitties are no different than other traditional physical or digital card sets such as sports cards, “Magic the Gathering” cards, or “Pokémon” cards. In each case, the cards provide value to their owner, but are also tradable with other card collectors. Unfortunately, in traditional centralised systems, the issuer of the cards may be tempted to debase the cards’ value, for example, by selling many copies of a highly prized card, thereby making it less rare and less valuable, or by unilaterally changing the rules of the game to undermine the value of existing cards and generate demand for new cards now on sale. Digital goods are often more difficult to sell as they cannot easily be transferred from one to another. Non-fungible tokens on the blockchain can solve this problem as they provide certain specific attributes:

- **Tradability:** Allows NFTs to be traded on various marketplaces in the same way that you can sell your baseball card at a card fair or your painting on Craigslist or eBay.
- **Traceability:** Allows you to ensure that the NFT you want to buy is authentic and the ownership chain before.
- **Immutability:** Allows hard coding of certain variables that will ensure its uniqueness. For example, it can be programmed that only 1000 pieces of a certain skin will ever be produced.
- **Interoperability:** Allows NFTs to move easily across platforms so they’re not “stuck” in a particular game or ecosystem and can be moved to someone’s digital wallet or to a marketplace.
- **Liquidity:** Brings more interest and capital to the asset allowing the ecosystem to be healthier.
- **Standardisation:** This is crucial as it allows for the establishment of standards that all NFTs use thus enabling most of the benefits listed above.

Most standards being used at the time of writing are Ethereum-based (ERC-721, ERC-1155/ERC-998), but there are also some standards being developed on other blockchains like EOS and Cosmos.⁸

There is no doubt that NFTs became mainstream with the launch of the cute digital cats, the CryptoKitties, in late 2017, although experiments had taken place previously with coloured coins on the Bitcoin network⁹ and the “CryptoPunks”, a set of 10,000 unique collectible characters, each with their proof of ownership on the Ethereum blockchain.¹⁰ Launched at the ETH Waterloo Hackathon in the fall of 2017, the team behind CryptoKitties sought to solve some of the problems mentioned above by using blockchain to create firm limitations on the issuance of each cat and establishing the provable uniqueness of each kitty using a non-fungible token protocol called ERC-721.¹¹ In the words of the game-maker’s marketing materials, “CryptoKitties is a game centred around breedable, collectible, and oh-so-adorable creatures we call CryptoKitties! Each cat is one-of-a-kind and 100% owned by you; it cannot be replicated, taken away, or destroyed”.¹²

Each kitty has a unique visual appearance determined by its immutable “genes” which are stored in a smart contract on the Ethereum blockchain. Players can “breed” their cats to create new kitties whose physical appearance (phenotype) is determined by their parents’ combined genes (genotype). The founding team noted that they were seeking to create “an exciting, self-sustaining community where users can create new collectibles and trade them”.¹³ Whilst the interest in CryptoKitties eventually waned, their hype brought venture capital funding to the industry, including for the CryptoKitties that raised US\$12 million funded by high profile VCs like Andreessen Horowitz and Union Square Ventures.¹⁴ More importantly, it showed that NFTs have interesting potential as, in theory, such NFTs can be created for any type of digital collectible. Over the past few years, we’ve seen many new innovative developments in this space, and several established brands have entered the space. For example, Formula 1 launched the blockchain-based game F1 DeltaTime, the first Formula 1 NFT car was sold for US\$100,000 dollars,¹⁵ and the U.S.-based Major League Baseball launched its MLB Crypto baseball league.¹⁶

The MLB Crypto Baseball league concept was original as it allowed baseball fans to collect their favourite players across its 30 teams on the blockchain instead of using physical cards. Only 500 digital players were released for every MLB team with 15,000 collectibles in total (a number that could not be increased subsequently). As each team has roughly 40 men on its roster, the collectible would not be distributed in equal quantities with some players

having only one blockchain figure. These rules were set and programmed in an ERC-721 smart contract making it impossible to change later (unlike physical baseball cards which could be increased subsequently) and having them on the blockchain allowed more functionality impossible with physical cards. For example, holders of a certain collectible receive certain points based on the real-life performance of the player; if the player does something exceptional (e.g., hits a grand slam), then the holder of the collectible could receive a one-of-a-kind game collectible giveaway.¹⁷

Another NFT example worth highlighting was Decentraland, which has a finite, traversable, 3D virtual space called LAND, a non-fungible digital asset maintained in an Ethereum smart contract. Land is divided into parcels identified by Cartesian coordinates (x,y), with each 10 m-by-10 m parcel permanently owned by members of the community and purchased using MANA, Decentraland's cryptocurrency token. This gives users full control over the environments and applications they create, which range from anything like static 3D scenes to more interactive applications or games. Each LAND token includes a record of its attributes, its owner, and a reference to a content description file or parcel manifest that describes and encodes the content the owner wishes to serve on her land.¹⁸ Decentraland has evolved substantially with many features including the ability to showcase some of your NFT art (like CryptoKitties) inside a museum district within the Decentraland virtual world.¹⁹ The Sandbox is another metaverse where you can buy an NFT of land, also called LAND for its ecosystem.

Many NFT-based games and experiments have appeared in the market recently. One is a role-playing game called “My Crypto Heroes” with the motto “Your time and passion will become assets”.²⁰ Another that’s quite popular at the time of writing is a digital collectible card game called “Gods Unchained”,²¹ and we’ve seen crypto exchange Binance issue Chinese New Year gifts as NFTs.²² Some more established players have entered the space as well, with Microsoft Azure announcing the launch of its NFT meant to compensate for positive behaviour in Azure’s community, with each token representing a cartoon badge and with a limited supply ranging from just 100 to 10,000 units.²³ Microsoft also announced that it is partnering with a major game developer to develop a NFT card game for a classic gamebook,²⁴ and the Austrian postal service started experimenting by launching a limited number of 150,000 stamps at 6.90 euros that not only functions as a real stamp, but also contains credentials that can be scanned to claim the NFT collectible.²⁵

Where to Buy an NFT?

Buying an NFT is relatively simple. There are numerous marketplaces where you can browse and choose the NFT that you want. In many ways, it's not too dissimilar to buying a regular item on Amazon or eBay. For example, there are numerous NFT platforms like OpenSea or Nifty Gateway that enable users to buy their favourite pieces as well as NFT marketplaces linked to many of the existing large platforms like Crypto.com. Users need to link their crypto wallet (e.g., MetaMask) to the platform for transactions to take place and whilst the process is easy to understand for those comfortable with cryptocurrencies, it still requires some effort for those not yet comfortable using crypto wallets. This will undoubtedly change over the coming months and years as users will be able to buy an NFT as easily as they buy physical goods on e-commerce platforms today.

The pivotal moment for the NFT ecosystem happened in early 2021 when the NFT industry exploded. Weekly NFT trade volumes on January 1, 2021 were less than US\$10 million in total, before climbing to almost US\$200 million only six weeks later, with the number of users growing rapidly as well, skyrocketing from under 25,000 in early January to over 500,000 only a couple of weeks later.²⁶ A few things of note happened in that period: the image of a meme of an animated flying cat with a Pop-Tart body leaving a rainbow trail in its wake was sold for just under US\$600,000 and a painting by the enigmatic Banksy was digitised and transformed into an NFT before being burned down. Even former Twitter CEO Jack Dorsey muscled his way into the action, selling his very first tweet as an NFT for US\$2.5 million at a charity auction.

The catalysing moment, meanwhile, was in March 2021, when a piece of digital art by the artist known as Beeple set a record for digital artwork in a sale at Christie's, with the JPEG auctioned off at a price of US\$69.3 million. Dubbed "Everydays – The First 5000 Days", the piece is a montage-like mosaic of all the images that Beeple has been posting online since 2007.

What is unique in all these cases is that the piece of art is digitally native. Unlike traditional art where the original is on canvas and there are digital copies, here the original is digital and whilst we can make unlimited digital copies or even physical reproductions of that piece, there is one that is the original NFT. The other major development was the incredible growth in popularity of the NBA Top Shot, launched in late 2020 but really gaining mainstream popularity in early 2021. NBA Top Shot has become an incredible success story, emerging as by far the most popular NFT, attracting the highest number of users whilst almost singlehandedly steering NFTs into the

mainstream, all whilst generating US\$230 million in sales. The basic idea of NBA Top Shot is that users can build and compile their own collection of basketball highlights, purchasing a digital pack of 10–15-s random moments from real-world games, and essentially getting a cross between a TV reel and a traditional sports card.

What gives these “moments” value is that Top Shot rests on the same foundation that gives a Bitcoin value, that of scarcity. For instance, Top Shot highlights can range from thousands of digital copies to only one digital copy, and the process behind acquiring a Top Shot pack is like going to a real brick and mortar store to buy a new pair of limited-edition sneakers, with users “lining up” in a digital queue; the “first come, first served” principle reigns supreme. Once a collection sells out, that’s it. Whilst a Top Shot pack could typically go for as low as \$9, these packs frequently and quickly sold out. As an example of just how much hype was building up behind Top Shot, an iconic LeBron James dunk sold for US\$208,000. Although the digital highlights contained within the Top Shot packs are freely available to stream endlessly on YouTube, the number of Top Shot users showed no sign of slowing down, functioning as the latest frontier in the collectibles craze whilst combining crypto, basketball, and market speculation. Ultimately, this is all music to the NBA’s ears, as the Top Shot revolution sparked an even more intense level of passion for the sport whilst allowing the league to capitalise on the hype at a time when many teams were suffering from the loss of in-person fans due to the COVID-19 pandemic.

What Are the Benefits of Artists Using NFT Platforms?

Whilst many groups, from collectors to the general public, stand to benefit from NFTs, one group that may benefit are artists, as NFTs provide a solution to some longstanding challenges they’ve been facing for a long time:

- **Royalties:** Today when an artist sells a piece of art, he has generally no control on to whom it is then resold and does not benefit from any potential increase in price that may take place. NFTs allow artists to automatically receive their royalties as soon as a certain piece is sold
- **Fakes:** There is not surprisingly a huge market of counterfeit art globally. The beauty of an NFT is that authenticity is easy to prove and provable to anyone anywhere, eliminating the need for all the experts who spend their days trying to authenticate pieces of art
- **Independence:** The NFT ecosystem allows any artist to leverage his own community of fans and build a direct relationship with them. Whilst it is likely that galleries and middlemen will still play a role in the NFT

world, especially when it comes to bridging the gap between NFT and old collectors, artists have more flexibility in an NFT ecosystem.

As we've seen, whilst still early days of NFT experimentation and that most applications so far have been for collectibles or gaming, this is an area that has quite a lot of potential and where there is still significant room for innovation. We're really at the beginning of the NFT revolution and over the coming years, many everyday items will be offered as NFTs, from concert tickets and songs to birth certificates and land titles.

Like any other hype, there will be boom and bust cycles for NFTs. One of the problems with NFTs is that unlike Bitcoin or other liquid assets, their value is more difficult to determine, because these assets are non-fungible and each is unique, like the large difference in value that someone determines a piece of art is worth (Table 1).

Table 1 Top NFT collections by market capitalization (January 2022)

1	CryptoPunks
2	Bored Ape Yacht Club
3	Decentraland*
4	Mutant Ape Yacht Club
5	The Sandbox*
6	Cool Cats
7	Superrare
8	Cryptoadz
9	Parallel Alpha
10	Punks Comic

*Decentraland and Sandbox NFT volumes are measured by land purchases

I also think there's a generational issue here as well. When I speak to my students or young people in general, they're often very comfortable with owning digital-only goods with many already owning digital skins or weapons in video games. The concept is often harder to grasp with older people who are used to physical assets, which is something faced in the early days of Bitcoin and cryptocurrencies as well. Whilst some NFT values are certainly inflated, perhaps driven by celebrity interest, one can argue that that's not necessarily a bad thing; the hype is generating interest, and more interest means greater opportunities for people to learn and educate themselves on the space. Ultimately, a stronger understanding of what an NFT is and the variety of possibilities they create, like the endless opportunities for artists and creators mentioned before, will lead to even more mainstream adoption.

Is There Insider Trading in NFTs?

Insiders will often take advantage of a new and booming market, especially when there are opportunities to profit. Many suspect that lots of insider trading occurs in the NFT world, from people artificially inflating prices to questions of potential money laundering and front running. That's precisely what happened in late 2021 with OpenSea, one of the largest NFT platforms, when the crypto Twitter community screenshotted a series of suspicious wallet transactions that raised eyebrows,²⁷ alleging that something foul was afoot at OpenSea.²⁸

OpenSea later admitted that one of their employees had indeed purchased items that they knew were set to display on the marketplace's home page before they had become available to the trading public, with CEO David Finzer publishing a blog post condemning the employee's actions.²⁹ It's surprising that no rules prohibited such behaviour at OpenSea as this is something that any organisation that aims to become world-class and attract institutional buy-in needs to have in front of mind. It will now be interesting to see if any action is taken against OpenSea, as after all, most NFTs are probably not securities, nor are they financial instruments³⁰ (although some offering fractionalisation or revenue share probably are). Since users were paying artificially inflated prices, do the users have a claim against the platform, or against the rogue employee? I'm sure lawyers will have lots of fun (and billable hours) debating this topic. One issue now is whether other employees have taken advantage of insider privileges in the past, and whether similar behaviour exists on other NFT platforms as well. Most crypto exchanges today have compliance policies and procedures that prohibit client front running, for obvious reasons, and we should expect NFT platforms to have similar policies in place.

2 Non-Tradable and Non-Fungible NFTs

The final category in our taxonomy of crypto-assets are non-fungible non-tradeable tokens. You might be wondering why such a token would exist given that the entire point of a blockchain is to facilitate the transfer of assets between users. The answer is that in some cases the immutability of all blockchains provides value, but the ability to transfer a token would render it meaningless. Take for example a token designed to provide proof of reputation. Such a token might aggregate reviews of a small business that could be proven to come from real users of that business, which could help overcome prospective customers' concerns about fake reviews, but obviously would not be credible if a business with a poor reputation could simply purchase a reputation token from a business with a good reputation.

Another potential use case for non-fungible, non-transferable tokens is identity. Blockchain-based tokens could enable a user to more effectively prove their identity attributes—age, country of residence, or that they hold a given certification—with an online environment. In theory, such a system could give users improved control over their personal data and allow them greater discretion in the identity attributes that they choose to share with counterparties.

One example of such a system under development today is Sovrin. Sovrin is a non-profit foundation dedicated to the establishment of a new online identity system, that in the words of the founding team, “bring[s] the trust, personal control, and ease-of-use of analogue IDs – like driver’s licenses and ID cards – to the Internet”. The system is designed to be “self-sovereign” in that “the individual identity holder can access and use their credentials on the Sovrin Network whenever and however they please”.³¹ These non-fungible non-tradable tokens have the potential to fulfil a range of exciting use cases; however, the many projects in this space are currently at a nascent stage and only time will tell which projects (if any) will be successful in scaling and achieving broad-based adoption.



14

Bitcoin and Crypto Mining

In this book, we'll cover how new crypto-assets are created and distributed. There are many methods to do so including mining, forks, yield farming, airdrops, and the suite of token offering options (ICOs, STOs, IEO), but crypto mining is such an important method of creation and distribution of new tokens, especially as that is how Bitcoin operates, that it deserves its own chapter.

1 The Evolution of Bitcoin and Crypto Mining

We've already discussed how mining works in depth when explaining Bitcoin at the beginning of this book. As we've seen, new Bitcoins are added to the network via a process called mining, where every 10 minutes or so, there are 6.25 Bitcoins that are created (since May 2020 as was 12.5 Bitcoin previously). These new Bitcoins are issued to the miner who wins the game of chance called proof-of-work to compensate them for the computing power they spent to win that game of chance.

In theory, anyone can connect to the Bitcoin network, download past blocks, keep track of new transactions, and try to crunch the data to find the golden hash, as this is one of the key benefits of the Bitcoin network.¹ However, mining Bitcoin has now become extremely difficult; simply plugging in your laptop and hoping to find the golden hash is unlikely. The technology used for mining has evolved quickly from CPUs in computers

and graphical processing units (GPU) in graphic cards to application specific integrated circuits (ASIC). To put things in perspective, some of the best ASIC devices that are available on the market at the time of writing have hash rates of over 100 TH/s, allowing you to crunch data and output a hash 100 trillion times a second.²

How Has Bitcoin Mining Evolved Over the Years?

Bitcoin mining has evolved considerably since the early days of crypto. In 2009, Bitcoin's first year, mining was done using the central processing units (CPU) of regular computers. By 2010, graphic processing units (GPU) that handle display functions and are generally referred to as graphic cards quickly took over, as they offered superior efficiency and processing speed. Things changed again in 2011 with the use of Field Programmable Gate Array (FPGA), a particular hardware device with a performance vastly superior to graphic cards and which comes close to the performance of customised hardware chips.

More major changes followed in 2013, when miners switched to using Application-Specific Integrated Circuits (ASIC), which are customised hardware chips specifically optimised for performing a single task, ensuring that all resources are optimised for the task of generating hashes.³ Whilst Bitcoin miners have been using ASIC machines since, their quality has significantly improved in a short period of time, forcing miners to get rid of old machines and replace them with new ones to be competitive. In general, we can expect mining equipment to become obsolete in roughly 1.5 years, causing many environmental concerns that will be discussed shortly.⁴

In the case of the Bitcoin network, the protocol specifies a fixed upper limit of 21 million Bitcoins that can be mined. In theory, when this number is reached in the year 2140, Bitcoin miners will only be rewarded through fees paid by users to have their transaction added to the next block. However, it is important to know that this is a specific protocol design choice of the Bitcoin protocol; other crypto-assets have chosen not to specify a fixed cap for the number of new tokens to be mined and instead only defined the rate at which new tokens will be created by miners. As of the time of writing, most cryptocurrencies, around 65% in market cap based on some estimates, used proof-of-work,⁵ with Bitcoin the best example of an asset that uses proof-of-work. Proof-of-work mining has many advantages:

- **Democratic:** In the sense that anyone can be a miner and try to find the next block.
- **Truly decentralised:** The removal of any one node or miner has no impact on the blockchain network that can continue to operate.

At the same time, there are some serious negative effects as well:

- **Negative environmental impact:** Whilst this was not the case in the early days, the increased processing power required for the mining of some of the large and popular cryptocurrencies has a serious environmental impact.
- **51% risk:** In theory, it would be possible for a group of miners to come together and take control of a blockchain network.

Miners will normally mine a number of cryptocurrencies, with research showing the majority of smaller miners tend to mine two or fewer crypto-assets whilst most larger miners tend to mine six or more (Fig. 1).

What also makes a certain miner mine a particular crypto-asset really varies. According to research by the University of Cambridge, the five most important criteria mentioned by miners include the market cap, the price, the daily reward amount offered by a crypto-asset, reputation, and energy requirements (Table 1).

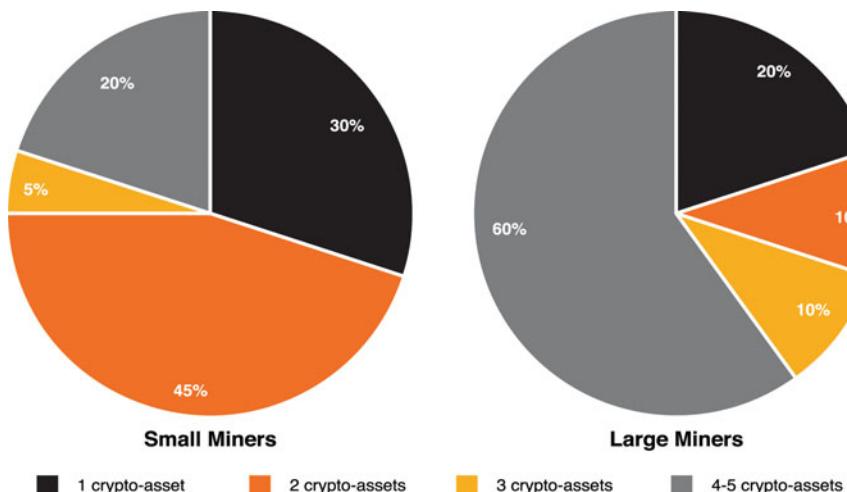


Fig. 1 Number of crypto assets mined (Source “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)

Table 1 The five most important criteria mentioned by mines include market cap, daily reward amount, price of crypto-asset, reputation, and energy requirements

	Large Miners	Small Miners
Market capitalisation	88%	38%
Daily reward amount	88%	52%
Price of crypto-asset	88%	76%
Reputation	75%	29%
Energy requirement	63%	24%
Proof system	63%	29%
Low number of other miners/mining pools	25%	19%
Large number of other miners/mining pools	13%	10%
Ideology/personal affection	13%	19%
Friends/colleagues recommendation	13%	5%

2 What Are Mining Pools?

A mining pool is a structure that “pools” together computational resources provided by connected hashers (often called “pool contributors”) in order to increase the likelihood and frequency of finding a new block, resulting in smoother payouts via the block reward,⁶ which is then shared between the various pool contributors based on pre-agreed formulas. The concept is like buying a bunch of lottery tickets with a group of friends or co-workers, who each contribute to a pot. This increases their chances of winning the lottery (as more tickets are bought collectively), but the payout will be reduced (as it will need to be shared in proportion to everyone’s contribution). The only difference between Bitcoin mining and the lottery is that you probably have higher chances of mining a Bitcoin block than the random chance of winning the jackpot.

There are numerous mining pools in the market. For example, there are more than 50 mining pools for Bitcoin alone, although none control more than 20% of market share (Fig. 2).

The number of contributors varies widely from one pool to another, as does the share of active members. Most pools consider hashers to be active when they contribute hash power at least once a week. According to survey data compiled by the Cambridge Centre for Alternative Finance, the hash power contribution follows a power law distribution: on average, one-third of the pool’s total hashrate is provided by the top 1% of contributors, whereas 10% of active pool members contribute 68%.⁷

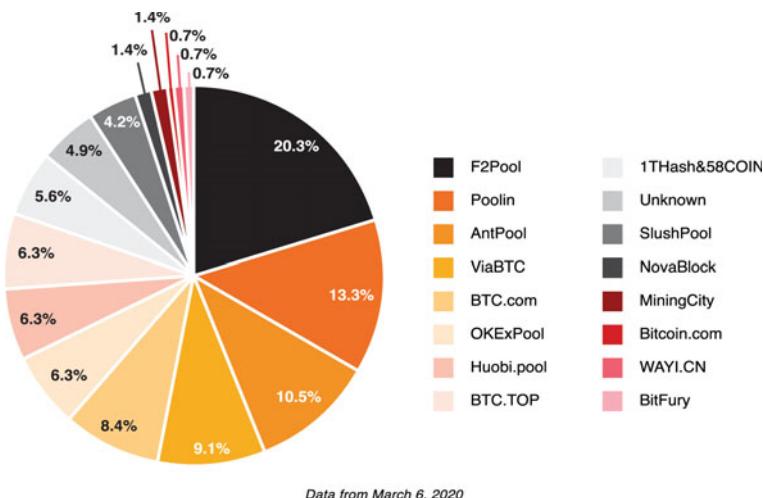


Fig. 2 Mining pool concentration (Source BTC.com)

There are also concerns with regards to the governance and decision-making processes of some pools. According to the same research, changes to pool policy (e.g., decision to mine a new coin) are equally likely to be made unilaterally by a single individual (38% of surveyed pools) or a group of operators (38%); only 26% of pools take a more user-focused approach, allowing users to participate in a vote-by-CPU (or equivalent) agreement, and other mining pools indicate using a combination of all these factors to instigate modifications of the pool policy.⁸ The geographic distribution of mining pools varies significantly from one crypto-asset to another, although Asia, Europe, and North America are generally the dominant regions. Bitcoin mining pools seem to be relatively equally distributed, whereas the Bitcoin Cash pool landscape is dominated by pools in Asia and European pools are dominant in Ethereum and Monero mining (Fig. 3).⁹

3 The Environmental Impact Debate

The environmental impact of crypto mining has been in the news recently, especially as sustainability is becoming a critical aspect of our everyday decisions. Therefore, it's worth looking at this issue and understanding the facts and different perspectives. When experts look at Bitcoin's effect on the environment, many of them focus on three different aspects: the electricity consumption, the carbon footprint, and the electronic waste.¹⁰

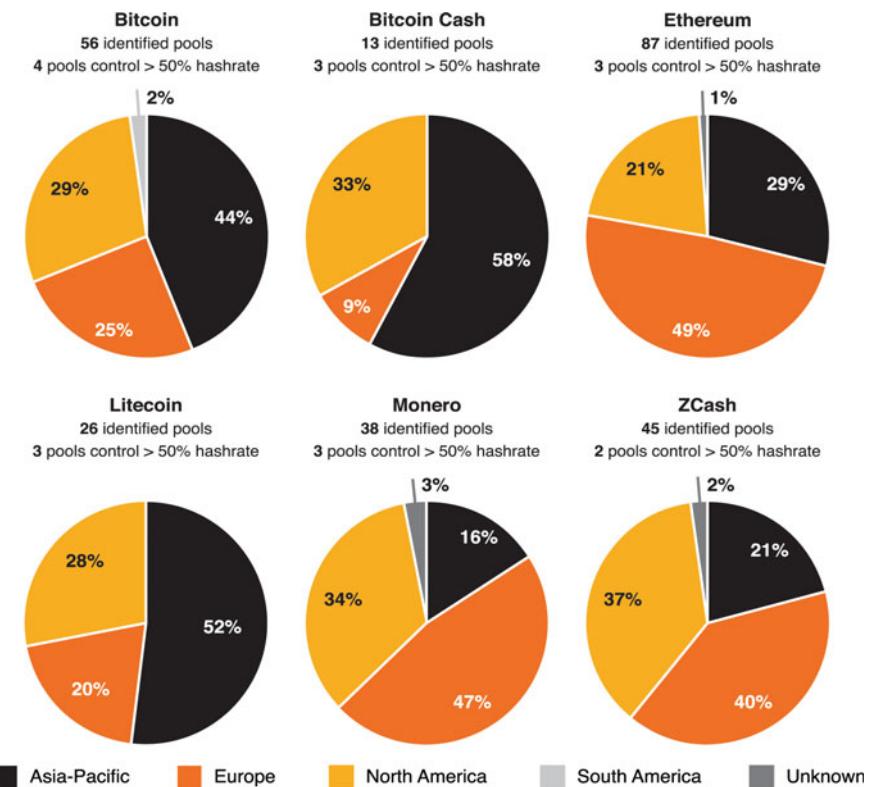


Fig. 3 Mining pools by crypto asset (Source "3rd Global Cryptoasset Benchmarking Study," Cambridge Center for Alternative Finance, 2020)

So, let's spend some time looking at each one of these in detail, starting with electricity consumption. The proof-of-work mining process that Bitcoin and other cryptocurrencies use indeed consumes a lot of electricity. That was not the case in the early days of Bitcoin when users were able to mine Bitcoin on their PC, but Bitcoin mining is an extremely competitive activity nowadays. Whilst the upside is that this reduces the risk of a 51% attack, the downside is that more electricity is being consumed. For example, it's estimated that at the time of writing, the Bitcoin network consumes over 190 TWh per year, meaning the network is consuming a comparable amount of power as the entire nation of Thailand¹¹ (Figs. 4 and 5).

A good indication of the rising amounts of electricity can be found when looking at the hashrate data of the Bitcoin blockchain, which has gone up materially in recent years.¹²

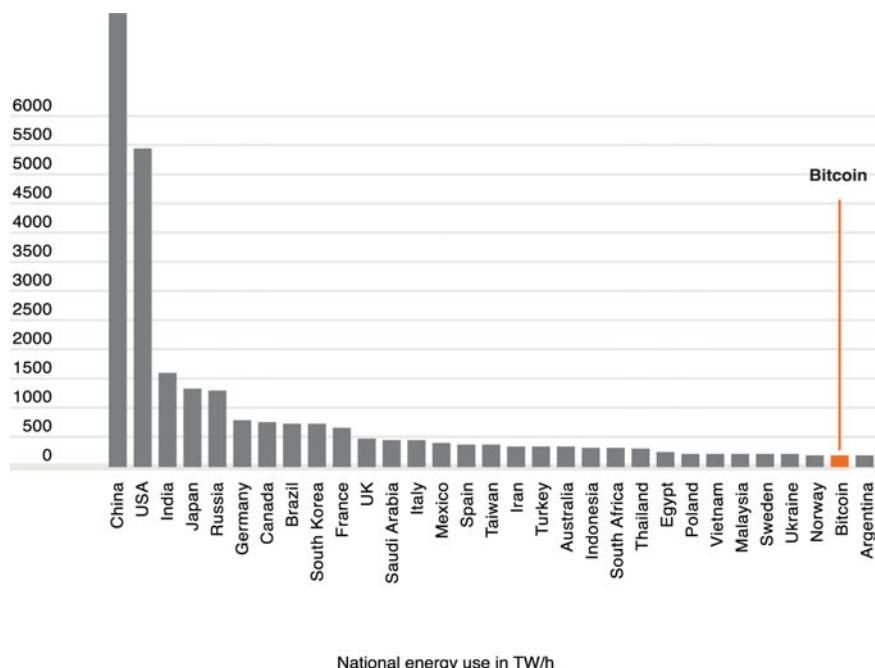


Fig. 4 National energy use compared with the bitcoin network's energy consumption (Source "3rd Global Cryptoasset Benchmarking Study," Cambridge Center for Alternative Finance, 2020)

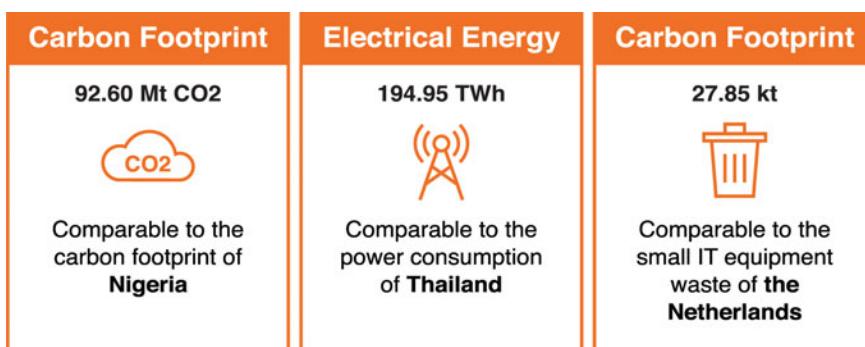


Fig. 5 Total annualized footprints (Carbon/Electricity/Waste) as of January 2022 (Source Digiconomist)

What Is a Hashrate?

Bitcoin's proof-of-work consensus mechanism consists of a game of chance wherein miners try to guess the correct hash, consisting of a 256-digit alphanumeric string that must begin with 18 zeros. For example, a hash of blocks looks something like this:

```
00000000000000000000f359f884320a688b7c9d29b2aa3d77e25b40d0c2d149a  
00000000000000000000e03b2141868558c3bc461b5adeb4728367d6d33bc5da1
```

In order to get to this hash, Bitcoin miners must try their luck. By way of analogy, it is similar to a group of friends throwing a pair of dice. The first one who rolls a double six gets to be the lucky miner. To compensate these miners for their hard work, they're rewarded with Bitcoin. That transaction is called a coinbase transaction, which is the very first transaction of each block. The reward was 12.5 Bitcoin per block, but gets halved every 210,000 blocks and was most recently halved to 6.25 coins per block in May 2020.¹³ The next halving is expected to take place around May 2024.¹⁴

Meanwhile, the hashrate is the total number of times that such tries are being conducted every second across the Bitcoin network. To use our figurative example, it's the number of times that these metaphorical dice are thrown to get that double six. It should not come as a surprise that being the lucky Bitcoin miner is exponentially more difficult than just getting a double six! This number is currently very high and at the time of writing, the hashrate was over 90,000,000 TH/S (90 million tera hash), where 1 TH/S is 1,000,000,000,000 (one trillion) hashes per second.

A high hashrate signifies that there are a lot of miners active in that blockchain and that the blockchain is healthy, but it also means that electricity consumption is high (Fig. 6).

Energy consumption is a direct function of hash power. Unless new, more energy-efficient mining hardware is introduced, total electricity consumption will rise in a somewhat linear fashion with hash power. However, as new mining machines with vastly improved energy efficiency are gradually introduced into the market, shouldn't that lead to a decrease in the total amount of electricity consumed? The short answer is no. Although better machines should improve efficiency, increased margins will incentivise other hashers to expand operations, resulting in a higher hash rate and, ultimately, proof-of-work difficulty. Over time, energy efficiency effect is cancelled out by the increase in hashrate, and eventually total energy consumption levels rise again.¹⁵

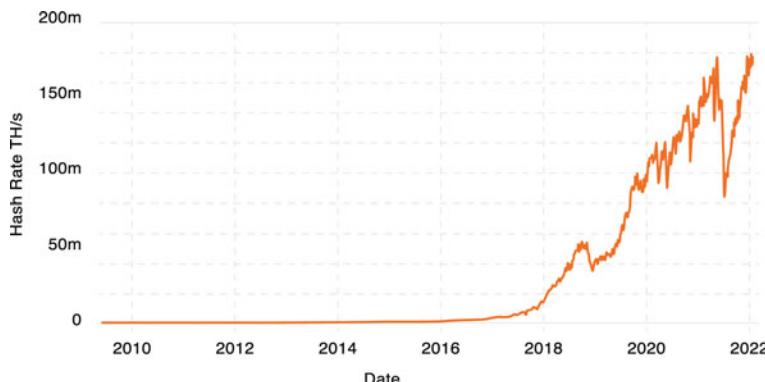


Fig. 6 Total hashrate (TH/s) (as of January 2022) (Source blockchain.com)

The second way to look at the environmental impact is via the total carbon footprint, the total amount of greenhouse gases (including carbon dioxide and methane) generated by our actions. At the time of writing, the Bitcoin network had a carbon footprint of over 90 tons of CO₂ a year, comparable to the carbon footprint of Nigeria.¹⁶ The third way to look at the environmental impact is via the amount of electronic waste generated. At the time of writing, the Bitcoin network alone generates over 27 tones of electronic waste a year, comparable to the electronic waste generated in the Netherlands. When you break it down to a transactional level, a single Bitcoin transaction generates the equivalent of over 275 grams of electronic waste, which is similar to throwing a newer iPhone model into the garbage.¹⁷

There are two main explanations for this surge in electronic waste. First, each crypto-asset uses a particular mining algorithm for its proof-of-work, and each algorithm has its own peculiarities with a particular type of hardware equipment best suited for the task. This means that a machine doing well in Bitcoin mining is not necessarily suited for Ethereum mining, and vice versa (Fig. 7).¹⁸

How to Understand Bitcoin's Difficulty Level

One amazing feature that Satoshi added to the Bitcoin blockchain was a “self-regulatory” mechanism called the “difficulty”. This adjustment is done roughly every two weeks with a target of miners mining a new block on average every 10 minutes. The difficulty level will constantly adapt so when the hashrate increases (i.e., there are more people mining) then the difficulty level will go up to try to compensate for the arrival of more hashing power, making Bitcoin mining harder. On the other hand, when the hashrate

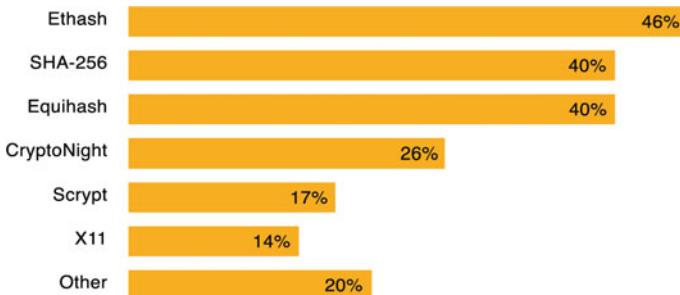


Fig. 7 Mining algorithms and hardware requirements (Source "3rd Global Cryptoset Benchmarking Study," Cambridge Center for Alternative Finance, 2020)

decreases (i.e., there are fewer people mining), then the difficulty level will be lowered to compensate for the drop in hashing power, making Bitcoin mining easier.

In July 2021, the Bitcoin blockchain saw the biggest difficulty drop in its history, plummeting by over 25%. In the days leading to this drop, a new block was being mined on average every 13.8 minutes, significantly higher than the 10 minutes needed. This meant that the difficulty level was too high and that the network needed to drop the difficulty level in order to "make it easier" for miners to mine.

Unsurprisingly, the level of difficulty is often related to the price of Bitcoin, as the higher the price of Bitcoin, the more profitable mining becomes, as the amount of Bitcoin given to the lucky miner every 10 minutes is the same, which is why the hashrate will often increase when the Bitcoin price increases and decreases when the price of Bitcoin decreases. The record drop in difficulty level was mainly due to Bitcoin miners in China shutting down their mining operations and moving overseas. As about 65% of Bitcoin mining happened in China until June 2021,¹⁹ this had a material impact on the total hash power on the Bitcoin network. The total hashrate fell almost 50% between May to June 2021 as Chinese miners started turning off their mining machines.²⁰

The difficulty level adjustments demonstrate once again the genius of Satoshi, with the network adapting itself (without the need of a committee meeting or an executive decision) to an external change in a decentralised way, with one group really benefiting from this difficult level drop: Bitcoin miners, as they have a higher chance of mining a block without the need of additional investment.

The second reason is that technology evolves. Research suggests that crypto mining machines, which are specialised single purpose machines,

become obsolete roughly every 1.5 years,²¹ and as more powerful machines are released, older ones will inevitably become outdated. For example, each manufacturer regularly comes up with their latest models,²² including Bitmain with their Antminer models; MicroBT with their Whatsminers; Canaan with their Avalons; and so on. Unsurprisingly, most mining machines are made in China and Taiwan, although some manufacturing also takes place in South America (e.g., Chile, Paraguay), Western Europe (e.g., France, UK), and in the former Soviet Union (e.g., Russia, Belarus) (Fig. 8).²³

Unlike an older iPhone model or iPad that still functions, using older mining machines is simply not viable for miners when compared to the newer, more powerful models, especially when you take electricity consumption into account. As these machines have no other purpose beyond the single (but powerful) task of mining Bitcoin, they quickly become electronic waste. To give another idea of the scale, at the time of writing, the two biggest miners, Bitmain and Canaan, had sold over 5 million mining machines between them,²⁴ and as only 20% of all electronic waste is recycled,²⁵ you can see how this would be a problem. Each of these factors has led to a growing wave of criticism centred on the environmental impact of crypto mining, but like many things in life, it's worth looking at both sides of the debate and moving away from the eye-catching headlines.

First, whilst Bitcoin and some of the earlier cryptocurrencies use proof-of-work consensus algorithms, many of the second-generation cryptocurrencies

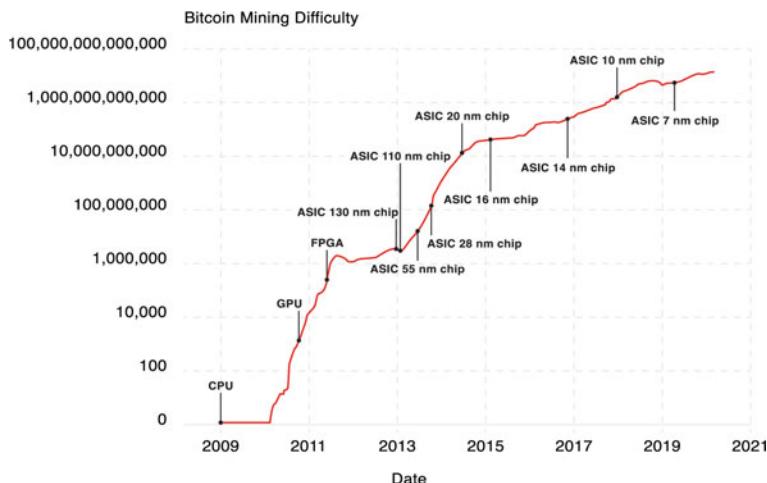


Fig. 8 Bitcoin mining difficulty vs time (Source Michael Bedford Taylor, "The Evolution of Bitcoin Hardware," University of Washington, September 2017; CoinDesk Research)

use other more environmentally friendly consensus mechanisms (e.g., proof-of-stake). Also, whilst Bitcoin mining or sending transactions consumes electricity, the process of holding Bitcoin does not. Second, the comparison between the electricity consumption of one Bitcoin transaction with one Visa credit card transaction is not intellectually honest for a few reasons. For example, the Visa network will always have a lower carbon footprint as it is a centralised network, in contrast to the Bitcoin network, which is completely decentralised.

As we discuss separately in this book, one of the dilemmas confronting any developer in the blockchain community is the “impossible trinity” or the “blockchain trilemma”, the theory that it’s impossible to have security, scalability, and decentralisation at the same time.²⁶ The downside of a decentralised system is that it is not as scalable or fast compared to a centralised system, but on the plus side, a decentralised system means there are no single points of failures or censorship. One way to achieve that is via the use of a proof-of-work mechanism, which consumes a lot of electricity.

Such a comparison with the Visa network also doesn’t consider the energy consumption of the broader traditional financial system or global banking system if we want to put things into perspective.²⁷ Far from looking at the energy consumption of each transaction, we also need to look at the power consumed by the entire financial ecosystem that enables everything to function from the air conditioning of an individual bank branch to the carbon footprint of the IT staff driving to a bank’s headquarters. Some may argue that we should also take into account the carbon footprint of the U.S. military, as a necessity any superpower needs to do to keep the U.S. dollar as a global reserve currency. Therefore, a more appropriate comparison would be between the environmental impact of Bitcoin mining and the environmental impact of the asset that Bitcoin is often held up against, gold. For instance, some argue that gold mining is 50 times costlier than mining Bitcoin and operating the entire Bitcoin network,²⁸ whilst a typical gold wedding band is singlehandedly responsible for 20 tons of waste.²⁹

Others take aim at the goldmining industry, drawing attention to the fact that this activity consumes 475 million gigajoules of electricity: equal to around 131.9 TWh.³⁰ After all, goldmining is heavily dependent upon grid power and fossil fuels, with a World Gold Council (WGC) report highlighting the need for gold sector emissions to fall by 80 percent by 2050 in order to meet guidelines set out in the Paris Climate Agreement.³¹

Third is the fact that whilst crypto mining does consume a lot of electricity, it’s using most of its electricity from renewable sources. Looking at the energy

mix is important because the energy footprint of one MW of energy generated by a coal-fired power station is not equivalent to the footprint of one MW of energy generated by a hydroelectric power station.³² Research shows that more than half of hashing facilities run on an energy mix that contains a share of renewables (Fig. 9).³³

The data shows that most miners use renewable energy as the primary source of their energy mix. Whilst there are exceptions (e.g., Xinjiang Province in China relied almost exclusively on coal before mining stopped in China³⁴), most of the energy mix is generated through renewable sources, with hydroelectric power as the most frequently used energy source.³⁵ Another recent research report estimates the approximate percentage of renewable power generation in the Bitcoin mining energy mix to stand at 73%,³⁶ around four times the global average, and according to the University of Cambridge, existing hydropower today could power the Bitcoin network 32 times over (Fig. 10).³⁷

In mid-2021, the Bitcoin Mining Council (BMC), a group championed by Michael Saylor and Elon Musk geared towards pushing the crypto mining industry to more transparency, announced the findings of its first quarterly survey, which centred around two important metrics: electricity consumption and sustainable power mix.³⁸ After collecting sustainable energy data

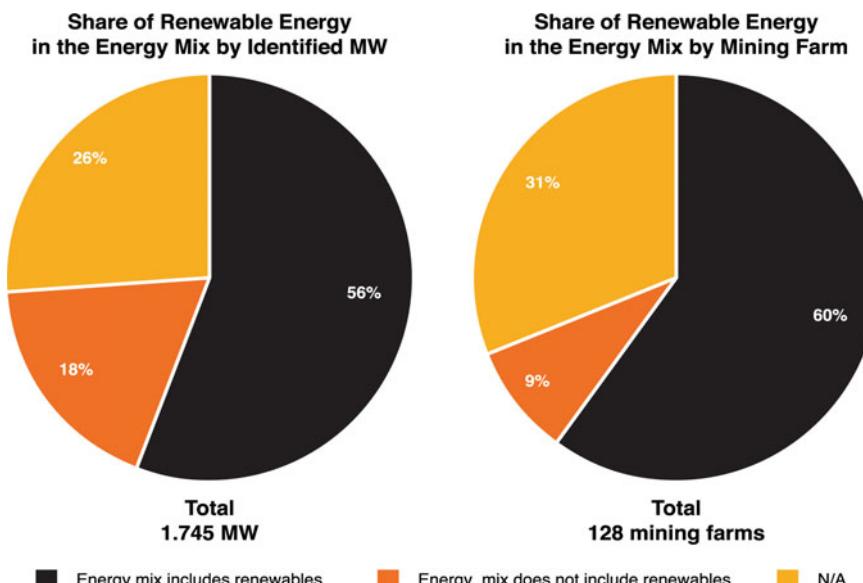


Fig. 9 Share of renewables in Bitcoin mining energy mix (Source "3rd Global Cryptoasset Benchmarking Study," Cambridge Center for Alternative Finance, 2020)

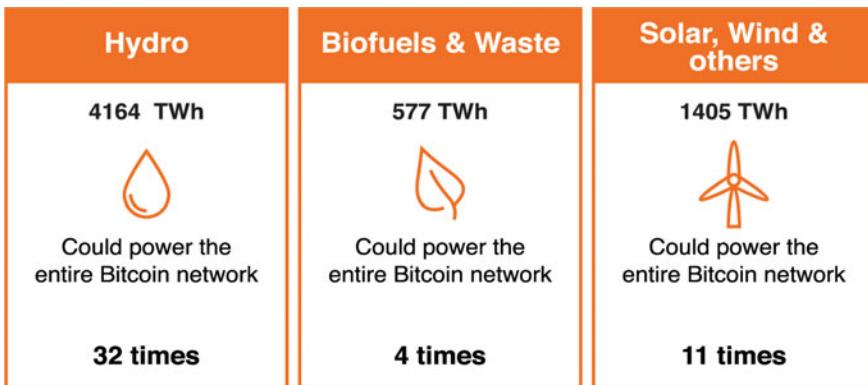


Fig. 10 Total world renewables production (Source "3rd Global Cryptoasset Benchmarking Study," Cambridge Center for Alternative Finance, 2020)

from 32% of the global Bitcoin network, the BMC revealed that the survey participants are now sourcing their electricity from a 67% sustainable energy mix.³⁹ Based on this data, it's estimated that the global mining industry's sustainable electricity mix has grown by approximately 56% over the second quarter of 2021.⁴⁰ We should expect this percentage to continue to grow, especially since mining operations have left China, where a non-negligible percentage of mining was using electricity produced by coal.⁴¹

The fourth aspect we need to consider is the argument that crypto miners are using excess electricity that would otherwise be wasted. Data shows that crypto mining is indeed concentrated in regions where electricity is cheap, with an oversupply of electricity relative to demand. Good examples include China, the United States, Canada, and Iceland, regions where there's an abundance of electricity (often low-cost hydroelectric power) often unused and wasted.

Some argue that Bitcoin mining may act as a global electricity buyer of last resort and could help turn loss making renewables projects profitable and, in time, could act as a driver of new renewables developments in previously uneconomical locations.⁴² Crypto-asset mining may soak up local overcapacities and prevent the waste of otherwise unused renewable energy, power that cannot be easily stored and transmitted over large distances. However, the problem is that the production of electricity in these places often fluctuates. Renewables such as hydro (seasonal variances, dry periods), wind (weather-dependent), and solar (available only for a limited number of hours per day) are intermittent: supply is subject to seasonal changes and conditions and often needs to be supplemented by alternative, non-renewable energy sources during certain periods. Finally, the argument of size also needs to be

considered. For example, whilst many will say that Bitcoin consumes as much electricity as the country of Thailand, it's important to remember that Thailand has a GDP of around US\$500 billion, whereas Bitcoin has a market cap of over \$1 trillion. In any event, this debate is likely not going away anytime soon.

4 Where Does Mining Take Place?

It's not a surprise that crypto mining takes place in regions around the world where there is cheap electricity. Because all other things being equal, the cost of electricity becomes one of the most, if not the most, determinant factor if such mining operations can be run profitably, after the price of Bitcoin. Other conditions miners look for after cheap electricity include good internet connectivity, favourable regulatory conditions, political stability, and cold weather.⁴³

Until early 2021, around 65% of global mining took place in China. Sichuan province was by far the leader, producing around 54% of global hashrate, with the remaining 11% split more or less evenly between Yunnan, Xinjiang, and Inner Mongolia.⁴⁴ Sichuan was a natural location for Bitcoin mining with its ample and cheap electricity due to hydropower.⁴⁵ But all of this changed in Q2 2021. In April 2021, an article appeared in influential peer-reviewed journal Nature Communications, in which seven Chinese academics argued that the carbon emission pattern of the Bitcoin blockchain would become a potential barrier against China's emission reduction targets.

Why Are Chinese Academics Against Bitcoin Mining?

In April 2021, an interesting article about Bitcoin mining appeared in the science journal Nature Communications. The article, written by seven Chinese academics based in China and abroad, argued that the carbon emission pattern of the Bitcoin blockchain would become a potential barrier against China's emission reduction targets.⁴⁶

The article made several observations. Most notably, the authors found that the annualised energy consumption of the Bitcoin industry in China would peak in 2024 at 296.59 Twh.⁴⁷ This figure would vastly exceed the total energy consumption levels of countries like Italy and Saudi Arabia and, if measured as its own country, would rank 12th globally. Meanwhile, the authors found that carbon emitted from Bitcoin mining operations would peak at 130.5 million metric tons per year in 2024, surpassing the total greenhouse gas emissions of countries like the Czech Republic and Qatar.⁴⁸ If we

just focus on China's domestic scene, Bitcoin-related emissions would rank in the top 10 amongst 182 prefecture-level cities and 42 major industrial zones, singlehandedly accounting for over 5.4% of electricity emissions in the country.⁴⁹

The authors were quick to make clear that without meaningful interventions and realistic targets, the energy hungry Bitcoin blockchain operation in China would quickly emerge as an obstacle that could threaten emission reduction efforts and sustainability targets, with the Bitcoin industry's growing carbon footprint impacting China's greenhouse gas reduction efforts.

Under the terms of the Paris Climate Agreement, China agreed to cut 60% of carbon emissions per GDP by 2030 based on 2005 emission levels. The authors also mention that as the use cases and applications of blockchain technology increase, new protocols should be designed and implemented in an environmentally sustainable manner. We'll probably never know whether this high-profile report had any direct impact on the Bitcoin mining crackdown that took place only a couple of weeks later in China, but the timing was indeed very interesting.

In mid-2021, three major financial trade associations issued a statement reminding the public of the risks of cryptocurrency trading, mentioning that virtual currencies are not supported by real value, their prices are easily manipulated, and crypto trading contracts are not protected by Chinese law. But the most important news was a statement from the State Council's Financial Stability and Development Committee, chaired by China's Vice Premier Liu He, which announced, amongst other things, its plans to crack down on Bitcoin mining and trading activities. This had a major impact on the Bitcoin mining industry in China. Whilst the activity was previously tolerated, it was now made clear that it had to stop immediately. Before the China ban, various other regions of the world were also involved in Bitcoin mining, albeit at far smaller levels (Fig. 11).

These areas are generally sparsely populated, well connected from a technology perspective, and hilly or mountainous regions traversed by powerful rivers.⁵⁰

China's anti-mining crackdown could ultimately prove beneficial for Bitcoin's future, as there has been a lot of criticism in the past over China's outsized role in this industry. Whilst the ban in some countries is understandable due to limited resources or capital controls, Norway is probably one of the countries that stands out. Given its unique position as a cold, well-connected, politically stable country with cheap power and enormous untapped hydropower potential, it could arguably be a mining powerhouse.⁵¹

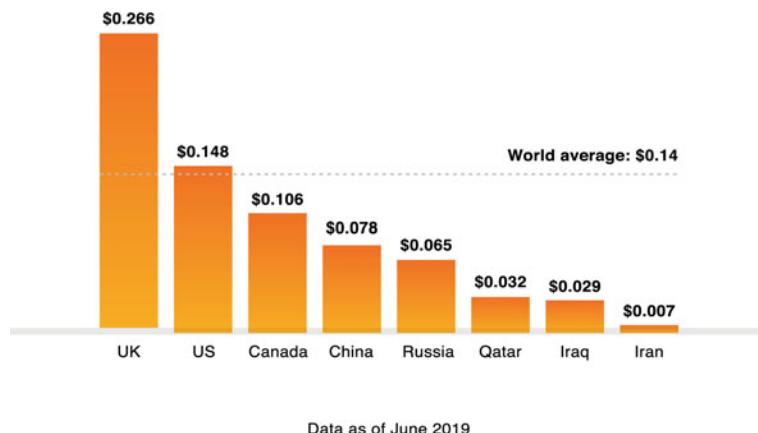


Fig. 11 Comparison between average costs of electricity in major economies (January 2022) (Source Pricing of Electricity by Country," ElectricRate, 2022)

Table 2 The share of global bitcoin mining by country shifted dramatically following China's ban on mining in 2021

August 2020		August 2021	
China	67%	United States	35%
Russia	8%	Kazakhstan	18%
Kazakhstan	5%	Russia	11%
United States	4%	Canada	10%
Canada	2%	China	0%

However, the big winner from the China mining ban was the United States, with data showing that from August 2020 to August 2021, the share of global Bitcoin mining in the United States grew from 4 to 35%, whilst the share of global Bitcoin mining in China evaporated from 67 to 0%. Over the 12-month period from August 2020 to August 2021, the distribution of Bitcoin mining changed drastically (Table 2).

There are several factors contributing to the increasing share of American Bitcoin mining. First, following the China ban, the United States has been welcoming to Chinese miners. The Governor of Texas, for instance, has been active in luring miners to his state following China's crackdown. Second, despite some of its problems, the United States provides strong rule of law and generally predictable policies, important considering the significant CapEx investments that Bitcoin mining requires.⁵² Unlike China, the United States is unlikely to ban Bitcoin with the Federal Reserve Chair confirming that

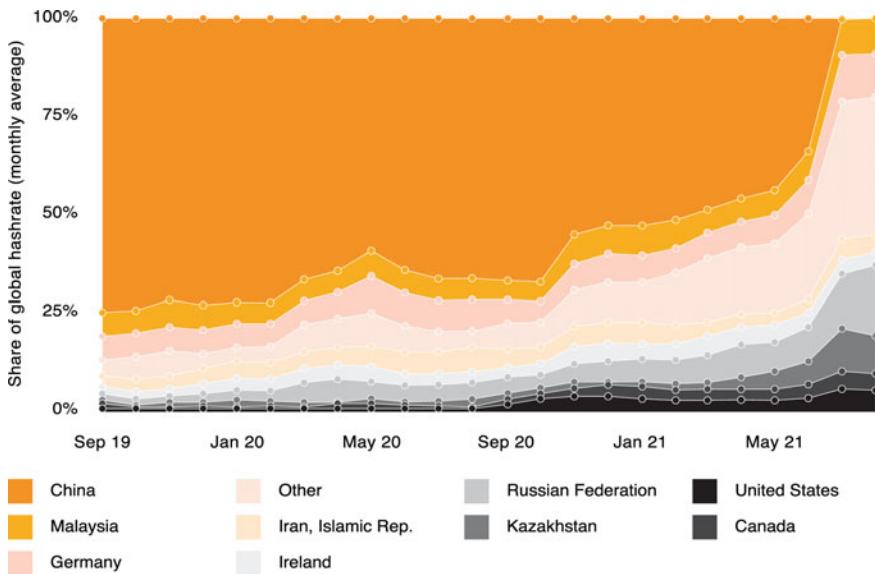


Fig. 12 Evolution of share of bitcoin mining by country (Source "3rd Global Cryptoasset Benchmarking Study," Cambridge Center for Alternative Finance, 2020)

Bitcoin will not be banned in the United States. Third, Bitcoin miners, especially in the United States, are rapidly becoming more energy-efficient, using an increasing percentage of sustainable sources (wind, solar, hydro, geothermal, nuclear) in their energy mix. There is ample renewable energy across the United States and Bitcoin mining may make renewable energy more sustainable, as it can be a buyer of last resort with the increased use of renewables helping to remove concerns around the environmental impact of Bitcoin mining (Fig. 12).

It will be interesting to see how the global distribution of Bitcoin and other crypto mining evolves over the coming years. Time will tell if China's ban was a short-sighted move with minor consequences or a major mistake that will affect its position in building the future of money.



15

Crypto-Asset Creation and Distribution

The enormous diversity of crypto-assets has driven a highly diverse set of approaches to the creation and distribution of new tokens to the community of individuals and organisations interested in holding or using those tokens. In the previous chapter, we covered Bitcoin and crypto mining. Whilst one of the most important methods of new crypto-asset creation and distribution, it's important to focus on the other methods that exist including forks, yield farming, airdrops, and the suite of token offering options (ICO, STO, IEO).

1 Initial Coin Offerings

The tokens in any protocol need to be created but also distributed, and one way to facilitate this distribution is to create a protocol where some or all of the tokens have already been created (sometimes said to have been “minted”) prior to the launch of the protocol itself or a mechanism is in place for how the tokens will be created. These tokens are then sold, or in some cases given away, to individuals interested or involved in the development of the protocol.

The sale of these tokens can be used to fund further development of the protocol and broader ecosystem around the crypto-asset and is often called an initial coin offering (ICO), with more discussed below. The initial number of tokens might be further expanded by mining, or alternatively, the protocol might be designed in such a way that no mining takes place. In these

cases, the total available supply is created at the birth of the currency with a portion released in the market and the remainder generally kept in reserve by the issuing entity. A good example of this is Ripple, a San Francisco-based company that issued 100 billion Ripple tokens (called XRP) of which around 40 billion are in circulation. The rest is controlled by Ripple who can release up to 1 billion XRP a month, and the only way to acquire XRP is via an existing crypto exchange.

Initial coin offerings represent a new approach to financing the development of a service offering by way of the issuance of utility tokens. The first significant ICOs were for Mastercoin in 2013,¹ followed shortly thereafter by Ethereum, which raised US\$15 million; however, significant ICO activity didn't take off until early 2017 with a succession of big ticket ICOs including Filecoin, Tezos, and Block.one, which raised \$257 million, \$230 million, and \$185 million, respectively.² A PwC report estimated that over US\$7 billion was raised in 2017 by over 500 ICOs and around \$20 billion in 2018 by around 1100 ICOs.³ With such eye-popping valuations, it's no surprise that ICOs caught the attention of the financial press and captured the imagination of the average investor. However, amounts raised by ICOs fell drastically as of 2019 and haven't again reached their 2017 and 2018 highs (Fig. 1).

From a technical perspective, the launch of a new token in an ICO need not be complicated, and most existing crypto protocols look to enable innovators to create new crypto-assets that "piggyback" on existing protocols and ecosystems of stakeholders. For example, the majority of ICOs that took place in 2017 used a technical standard on the Ethereum blockchain called ERC20 (Ethereum Request for Comment), providing a suite of open-source standards for the creation of a new token. One way to imagine why such a system would be useful is to think of a mall in the physical world where anyone is welcome to come and open a shop. Everything about that shop is standardised including the dimensions, the positioning of the electricity sockets, the security system, and how customers can pay for goods and services. If you have a business idea, all you need to do is show up and launch it at the mall. And compared to a few years ago, you don't only need to go to the Ethereum mall, but can go to the Solana, Avalanche, Algorand (or any other layer blockchain) mall.

Whilst media commentators frequently compare ICOs with IPOs—the initial public offering of a company's equity on an exchange—they differ in several fundamental ways.⁴ Most importantly, the regulatory treatment of IPOs is tightly defined by regulatory frameworks, with prescribed steps that must be taken and approvals that must be secured before a listing can take place. These rules are well understood by investment banks, exchanges,

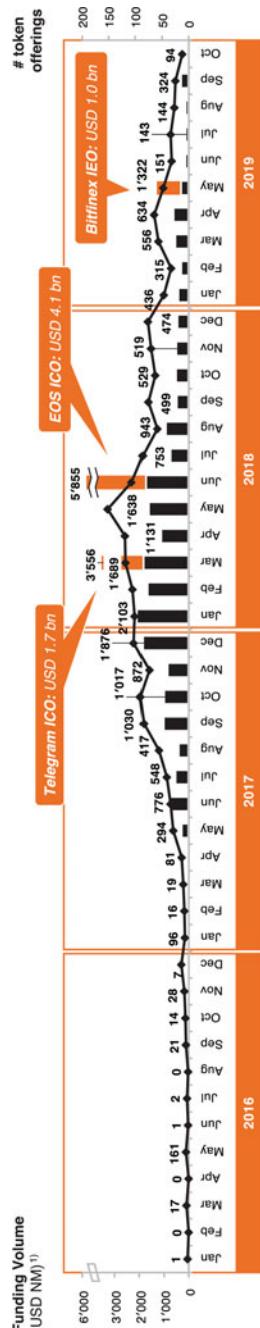


Fig. 1 Key ICOs by funding value and number of token offerings (Source "6th ICO/STO Report," PwC, 2020)

and law firms that guide companies through the IPO process and are tightly enforced by the regulator. By contrast, ICOs, particularly those before 2018, sometimes seemed to be happening in a “Wild West” environment with little clarity in terms of whose regulatory purview that fell under and with many founding teams of new crypto-assets seeking only minimal legal input into their multimillion-dollar token sales.

This regulatory grey zone means that token holders often do not benefit from the same transparency or protections that an investor in an IPO does. Whilst prospective shareholders have well-defined rights and can review highly transparent filings in the lead up to an IPO, there is significant variance in the rights and transparency afforded to prospective token holders in an ICO. Several other significant differences between ICOs and IPOs are listed below (Fig. 2 and Table 1).

Unsurprisingly, regulators have been unwilling to allow this uncertainty to persist indefinitely. As we saw earlier in this book, there have been numerous enforcement actions against companies that have issued tokens, including



An effective way to raise capital for blockchain-based projects



Allows to put together talented team fairly quickly



Removes many of the hurdles present in the equity capital raising process



Receive funding without diluting equity or control



Allows the setup of an ecosystem



Provides optimal visibility in market

Fig. 2 Advantages of a token sale. Whilst frequently compared, the characteristics of an ICO differ significantly from those of an IPO (Source: PricewaterhouseCoopers, “Introduction to Token Sales (ICO) Best Practices” [PwC], accessed January 13, 2019)

Table 1 Key differences between an ICO and an IPO broken down by regulation, token holder/shareholder rights, fundraising strategies, levels of economic exposure, and levels of transparency

ICO	IPO
No specific regulatory framework	Specific and well defined regulatory framework
Generally early stage company	Minimum track record and revenue requirements
Funds generally raised for specific purpose	Funds raised for company's long term development
Limited rights given to token holders	Shareholders have very well defined and regulated rights
Generally no economic exposure to issuing entity	Provides economic exposure to issuing company
Varied levels of transparency	Prescribed and well defined levels of transparency

Block.one and Telegram, but despite these enforcement actions, much of the regulation around ICOs remains unclear and regulatory treatment of these instruments varies widely depending on each jurisdiction. Some jurisdictions such as China⁵ and Korea⁶ have taken a hard-line position of banning ICOs entirely. Other countries like Switzerland, Singapore, Hong Kong, Gibraltar, and Malta have sought to provide various levels of regulatory clarity. Further clarity is expected in the short- and medium-term from regulators around the world, not only in terms of ICOs, but crypto-assets more broadly.

Despite the fluid regulatory environment for the sale of tokens, they represent an interesting new model for the raising of funds to develop a new product or service. Successful ICOs can theoretically enable the rapid “bootstrapping” of a team to develop an idea whilst at the same time taking initial steps towards forming a community of users for the offering. Ideally, they can also democratise aspects of the fundraising process, giving entrepreneurs the ability to raise funds even if they don’t have connectivity to venture capital networks whilst also giving small investors equal access to early-stage investments with potential big impact.

In practice though, there are also serious challenges. Whilst the initial vision of the ICO was of a democratised funding process involving the broader public, the role of established venture capitalists and large funds in the ICO ecosystem has grown significantly, with these players often gaining access to significantly discounted “pre-sales” of tokens.⁷ The lack of regulation to enforce transparency also creates challenges for investors, with a 2017 Wall

Street Journal investigation of 1,450 token sales found 271 projects (which had collectively raised over US\$1 billion) with “red flags that include plagiarised investor documents, promises of guaranteed returns and missing or fake executive teams”.⁸ In some instances, these red flags might be indicative of scams such as PlexCoin whose founders, according to the SEC’s Cyber Unit, promised to give investors a 13-fold return on their investment within one month, but in fact intended to use the funds raised to supplement their own expenses including “home decor projects”.⁹ In other cases, actors including founders, have conspired to actively manipulate their price of tokens in so called “pump and dump” schemes.¹⁰

The excitement surrounding crypto-assets may have allowed some projects with minimal prospect for success to raise significant funds. In some cases, the team might have lacked the necessary technical expertise to deploy their vision, whilst in others, they may have lacked an addressable market of sufficient size or an understanding of the complexity of the market that they were seeking to disrupt. Moreover, unlike start-ups funded by venture capitalists, where funding is doled out in stages to incentivise continued performance by the founding team, ICOs tend to raise all their funding at the beginning of the project’s life cycle, reducing the ability of investors to discipline founding teams that exhibit poor performance (Fig. 3).

Despite some of these many initial hurdles, ICOs clearly represent an interesting new financial instrument that has served as a funding mechanism for many blockchain-based companies. Since the ICO crash of 2018, there have still been new ICOs and token sales, but these tend to be more serious teams with better levels of governance, transparency, and execution capabilities. The reality is that ICOs will always remain as we have a constant flow of new

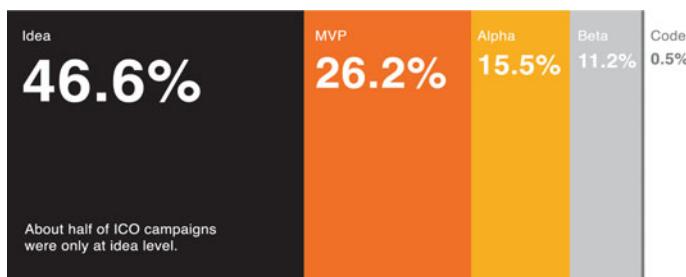


Fig. 3 Distribution of initial coin offerings by stage of product development at the time of the offering. Many ICOs have raised significant funding with little more than an idea (Source Mikhail Mironov and Steven Campbell, “ICO Market Research Q1 2018,” ICORATING, 2018 [23])

protocols that are designed and built, but what matters is that they have proper governance, transparency, and respect various regulatory requirements.

What is a SAFT?

Anyone who has ever considered investing in an early-stage token project has undoubtedly heard about a Simple Agreement for Future Equity (SAFT). But what does a SAFT mean? Simply put, a SAFT is a type of investment contract that helps new crypto ventures and projects raise funds. It's modeled on the SAFE that was pioneered by Y Combinator in late 2013 and has been used by early-stage tech companies ever since as the de facto go-to document for any start-up raising money, from Silicon Valley to Singapore.¹¹ However, unlike a SAFE, which allows an investor to receive equity, a SAFT allows the investor to receive tokens.

The SAFT rose to prominence in the fall of 2017, when the law firm Cooley and Protocol Labs released a paper on the topic.¹² Because of its simplicity (given that it was modeled on the familiar SAFE), the SAFT quickly rose in popularity to the point where it is still used regularly today. How does it work? The SAFT is an investment contract and a SAFT transaction contemplates an initial sale by developers to accredited investors, obligating investors to immediately fund the developers.¹³

The SAFT is a standard document¹⁴ and one of the most important parts is the discount rate.¹⁵ The token project team and the investors simply need to agree on what the discount rate is. Similar to a SAFE, this allows an investor to buy tokens at a discounted rate when the network launches. Ultimately, if a SAFT works as designed, developers get the capital they need to build out their networks and launch tokens. Investors, meanwhile, can take a stake in a promising new venture without wasting time, energy, and money on expensive lawyers.

2 Initial Exchange Offerings

First becoming popular in 2019, an initial exchange offering (IEO) is basically an ICO issued on a crypto exchange. However, the process of subscribing to an ICO can be quite tricky for the average user, as many projects build their own website and investors had to send crypto-assets like ETH to a certain smart contract address, increasing the risk of fraud as background information on some projects was limited. With an IEO, the process may be easier for an investor as the token would be first issued on an exchange

and an investor would simply need to send funds to that exchange wallet, making the process much easier. Any exchange listing a token in an IEO would have done, at least in theory, some level of due diligence on the token, normally to give more comfort to potential investors.

On the other hand, any project wanting to offer its token via an IEO needs to pay listing fees to the exchange, and just because a token is being offered by an exchange does not make it automatically compliant. The U.S. SEC reiterated this point when they issued an investor alert on IEOs in January 2020, reminding the public of the risks with IEOs but that also those tokens may be securities, that the platform may need to register either as a broker dealer or a securities exchange, and that such an exchange may be in violation of federal laws.¹⁶ Many of the large crypto exchanges, from Binance to Bittrex, offer IEOs and whilst they haven't achieved the highs of 2019, when Bitfinex raised over US\$1 billion for its LEO token in May 2019, the process is one that is probably here to stay in the coming years.¹⁷

3 Security Token Offerings

As we saw earlier, security tokens (or investment tokens) are instruments whose primary function is to serve as a financial investment for the holder of the token and thus are considered securities (or in some cases commodities) under most regulatory regimes. These can include both instances where pre-existing physical assets or legal rights (such as a bond or a share of stock) are "tokenised" on a blockchain, and instances where new investment opportunities are created that are native to the crypto-asset ecosystem (including a significant number of ICOs that have security like features).

A security token offering (STO) is the process of offering security tokens to investors. How those security tokens are offered to investors and to what type of investors they are offered is crucial, and in almost all cases, an STO needs to follow existing regulatory frameworks for the issuance of traditional securities. In most jurisdictions, before a security, including a security token, can be sold to the general public, it needs to be registered with regulatory authorities, a process that is typically lengthy, costly, and complex, but is designed to protect small-time investors saving for retirement. Regulators are concerned that average people who lack specialised training in investments and sufficient funds to endure a significant financial loss without experiencing financial hardship, may be persuaded by promises of vast returns to invest in high risk or poorly conceived ventures.

Fortunately, for those wanting to raise capital via the sale of newly created security tokens, “private placement” exceptions exist in most jurisdictions. These allow securities to be sold without the same onerous registration requirements placed on securities issuances to some types of investors and the general public, if certain requirements are met. The most common of such requirements is ensuring that the security is issued only to “accredited investors”, also sometimes called “professional investors”. These are individuals deemed sufficiently sophisticated and wealthy enough to understand and evaluate the risks of their investments and to endure the consequences if the investment fails to meet expectations. Requirements to be considered an accredited investor differ from jurisdiction to jurisdiction, in some cases being determined by income, and in others by liquid net worth, but if the token offering limits marketing only to such individuals it will likely be exempt from registration, or subject to much less onerous requirements.

The important takeaway is that from a legal perspective a security token offering is like a traditional security offering, and whilst there are numerous technological benefits of using security tokens (as explored in detail earlier), from a purely legal perspective, they’re similar.

4 Hard and Soft Forks

The world of crypto-assets is full of colourful disagreements, and disagreements around a particular crypto-asset can manifest themselves by way of forks. The topic of hard and soft forks is one that regularly comes up in crypto conversations and to a certain extent is part of the DNA of how blockchains work. An easy rule of thumb to remember is that a soft fork is when the protocol rules are to become stricter, and a hard fork is when the protocol rules are to become more relaxed.¹⁸ A soft fork is a change of protocol when tighter rules are introduced. For example, if previously all blocks had a block size of 5 MB, then the introduction of a block size limit of 1 MB would be a soft fork. The blocks created in a soft fork can still work with the older version as they are backwards compatible,¹⁹ and because of that, miners need to only update their software, whilst nodes can stay part of the network without updating.²⁰ Segregated Witness (SegWit) is an example of a soft fork that took place on the bitcoin blockchain in the summer of 2017²¹ and the Taproot soft fork is one that took place in November 2021.

A hard fork is a change of protocol where the rules are relaxed so that previously invalid blocks can now become valid. For example, if previously all blocks had a block size of 5 MB, then the introduction of a block size limit of

10 MB would be a hard fork. Since a hard fork makes invalid blocks valid, all network participants, namely miners as well as the nodes (our bookkeepers), must update their systems, or otherwise, they would reject newly valid blocks and be isolated from the network.²² Bitcoin Cash and Ethereum Classic are examples of hard forks that have been successful so far.

Let's look at the Bitcoin Cash fork. Over the years, the Bitcoin community has seen a vigorous set of debates around how the protocol could be improved, with many arguments focused on questions of how transaction processing speed could be increased, a discussion commonly referred to as the "block size debate". In short, a portion of the Bitcoin community favoured increasing the number of transactions in each block on the Bitcoin blockchain to increase transaction processing speed, whilst another larger group favoured keeping the block size and transaction processing unchanged. In August 2017, with the debate at an impasse, one group of miners chose to implement an altered version of the Bitcoin protocol, whilst a larger group chose to maintain the existing system creating a "hard fork".

This hard fork split the Bitcoin blockchain in two, one operating on the original protocol which continued to be called Bitcoin, and a second using larger blocks that became called Bitcoin Cash. Owners of a single unit of Bitcoin at the time of the hard fork were now in possession of two tokens, a unit of Bitcoin and a unit of Bitcoin Cash. In this way, a completely new crypto-asset came into existence as an offshoot of an existing token, was immediately held by a broad group of people, and new units of Bitcoin Cash will continue to be added via the activities of miners.

To try to explain how forks work in practice, let's try to use an imperfect, but hopefully useful analogy, with bookkeepers and auditors used earlier in this book in the Bitcoin chapter. Imagine today, bookkeepers (nodes) have ledgers that have transactions amounting to \$5 a page and that their auditors (miners) can audit up to \$5 of transactions at a time. Now imagine that the auditors decide that they will only audit up to \$1 at a time, so the "audit" rules have become stricter (soft fork). In this case, even if the auditors (miners) audit only \$1 of transactions at a time, these would still fit in the bookkeepers' \$5 per page format. The change in audit rules does not impact the bookkeepers, and this would be the equivalent of a soft fork.

Now imagine that bookkeepers (nodes) have ledgers that have transactions that amount to \$5 a page and that their auditors (miners) can audit up to \$5 of transactions at a time. But one day, the auditors (miners) decide that they want to audit up to \$10 at a time, so the "audit" rules have become more relaxed (hard fork). In this case, if the auditors (miners) audit \$10 of transactions at a time, these will not fit in the old \$5 pages of the bookkeepers

(nodes). They can decide to upgrade their books so that they can keep up to \$10 of transactions per page, or they may decide that they don't agree with this change and that they will only work with auditors that want to stick with the old rules of \$5 of transactions per page. This is a hard fork scenario.

It is important to note that the above hard and soft forks are different from cases where the code of a cryptocurrency is taken, amended, and then launched as a new cryptocurrency. For example, Litecoin is an example of a cryptocurrency based on Bitcoin but with certain amendments (e.g., 84 million coins instead of BTC's 21 million, blocks every 2.5 minutes vs BTC's 10 minutes, Scrypt algorithm vs BTC's SHA-256, etc.). It's not a fork as it is simply launched on a new blockchain as a Day 1 coin.

5 Airdrops

An airdrop (often referred to as a token drop) is the distribution of tokens to the public for free. The criteria for receiving an airdrop vary but generally involve holding a certain token or having been active on a certain protocol. The major difference with an ICO or an IEO is that no monetary consideration is required in exchange of the airdrop; it's given for "free". In many cases, airdrops are used to generate awareness and publicity on the protocol. For example, in November 2020, Uniswap conducted an airdrop in which it distributed millions of UNI governance tokens to wallets that had interacted with the protocol in recent years.²³ In December 2020, 1INCH did a high-profile airdrop by distributing 90 million 1INCH tokens to users who had previously traded on the exchange,²⁴ and even the Ethereum Name Service Platform conducted one in November 2021 to reward users who had previously used the platform.²⁵

Airdrops are likely going to be around for a whilst, as they are an excellent marketing tool to generate awareness on a certain protocol and reward early users whilst allowing the ecosystem to grow by way of a network effect generated by the airdrop. One interesting debate are the tax and regulatory considerations of an airdrop. Should an airdrop follow the same regulations as a token sale like an ICO or an IEO although it is given out for free? What should be the tax consequences of an airdrop and how should they be characterised from an accounting perspective? Whilst there has been some work done on the above, this is an area that we should expect more attention not only from the legal and accounting community but also regulators and tax authorities.

6 Liquidity Mining/Yield Farming

The term “yield farming” became extremely popular in the summer of 2020, during the DeFi boom (to be covered in the next chapter). Yield farming is also often referred to as “liquidity mining”, probably a better description of what it is, which is when a user of a decentralised application is rewarded with a new separate token, in addition to his regular reward, in exchange for a liquidity contribution. In this sense, it’s another way of creating and distributing new tokens.

This was popularised by borrowing and lending platform Compound. Compound announced in early 2020 that it wanted to decentralise its governance and that it would launch its COMP token. Compound would basically be managed by a decentralised community of COMP token holders (or whoever they have delegated their tokens to) who can propose new upgrades to the protocol and vote on them. The distribution happened in June 2020 when COMP tokens began to be distributed to its users. Each day, for a period of four years, 2,880 COMP started being distributed to users of the platforms, both borrowers and lenders, across various assets. As long as someone was interacting with the platform by either borrowing or lending, they would receive some COMP tokens in proportion to that person’s level of activity that day.⁶²⁶

Other protocols, from Balancer⁶²⁷ to Yearn Finance,⁶²⁸ soon followed with the same concept, but yield farming really boomed in popularity when decentralised exchanges started using the model. As we’ll see in the next chapter, some decentralised exchanges will give the user a liquidity token in exchange of the ETH or other asset that they have locked (i.e., transferred) into a certain pool in proportion to how much liquidity they contributed to the pool. Such tokens are entitled to a *pro rata* distribution of the transaction fees during the period that these assets are locked. Yield farming, or liquidity mining, consists of giving, in addition to the liquidity pool token, a new token, somewhat like a bonus to compensate the user for having contributed to that specific liquidity pool. This became popular in the summer of 2020 with the launch of SushiSwap. SushiSwap was a de facto copy of Uniswap, but with some additional community-oriented features.⁶²⁹

SushiSwap proposed not only a yield farming model for its Sushi tokens, but also popularised the concept of liquidity migration. For example, in August 2020, users who provided liquidity to the Uniswap decentralised exchange (and who thus had a Uniswap LP token that gave them exposure to trading fees of that pool) were able to stake those tokens in the Sushi

smart contract that would give them Sushi tokens.⁶³⁰ However, at a predefined block, SushiSwap would move the liquidity of those Uniswap LP tokens from Uniswap to SushiSwap in what became dubbed as vampire mining.⁶³¹ What's important is that yield farming or liquidity mining is another method of token creation in addition to the existing ones like ICOs or IEOs.



16

Decentralised Finance (DeFi)

1 What Is DeFi?

DeFi is short for Decentralised Finance, originally referred to as Open Finance, but with the term DeFi becoming dominant in 2020. DeFi is the ecosystem of financial applications built on top of decentralised ledger technology that enables the delivery of financial services without traditional centralised intermediaries. The DeFi ecosystem is generally open-source, permissionless, and transparent, accessible to everyone and operating without any central authority. Users maintain full control over their assets and interact with the ecosystem through decentralised applications, commonly referred to as dApps.¹

DeFi emerged as one of the hottest spheres in the crypto and blockchain space in 2020, with total value locked (TVL) growing from less than \$1 billion at the beginning of 2020 to around \$15 billion by year's end with and growing tenfold by the end of 2021. Whilst the financial services offerings on a DeFi ecosystem are like what exists in the traditional world, the way they function and operate couldn't be more different. Today, finance as we know it is centralised, with a core set of institutions we all use, handling all your financial activities. When you send a payment to a friend, you need to go through a traditional bank or a payments platform; to get a mortgage, you go to a bank; and when want to invest in stocks, you work through a broker.

That all started to change 10 years ago, when we began to see the rise of decentralised assets like Bitcoin that allow us to send something of value from

one person to another without an intermediary. No bank stands in the middle when you want to send Bitcoin from one person to another, but despite its decentralised nature, anything beyond that still generally takes place today via centralised intermediaries, from centralised crypto exchanges to crypto custodians. This may seem ironic, as we're using the same centralised models used in traditional finance to handle digital assets, but this is where decentralised finance comes in. DeFi allows us to use some of the inherent attributes of blockchain technology to completely reinvent finance to conduct financial transactions without centralised intermediaries.

Unlike centralised entities that have an office and employees, DeFi platforms operate using blockchain smart contracts written in code. If the conditions coded into the contract are met, then the payout or consequences are automatically executed; basically, the contract is fulfilled without any human intervention. Such smart contracts are fully transparent and available to anyone to inspect in order to understand the functionality or to discover bugs. This is very different from traditional banks, which still have many manual processes and human staff to keep their inner workings and operations highly secretive. DeFi not only makes the process faster, cheaper, and more transparent, but also allows such platforms to scale without limitations of human bandwidth. There are inherent scalability challenges depending on which blockchain is used, but these allow for significantly more scalability compared to most systems operated by humans like a bank branch network or a trading desk.

In addition, such platforms are open to anyone. A traditional bank can pick and choose its clients, deciding to work only with those will might be the most profitable or excluding clients from certain countries. In contrast, DeFi platforms are open to anyone with a basic internet connection and access to cryptocurrencies. This is seen by DeFi proponents as another example of how blockchain can help promote financial inclusion and provide access to financial services to anyone, regardless of wealth, status, or place of birth. In addition, DeFi doesn't rely on existing financial infrastructure, so it's not affected by existing legacy systems or vested interests. It doesn't touch fiat currencies, like dollars or euros, and only operates with digital assets, able to leverage the latest blockchain and smart contract technologies and benefit from the speed, security, and transparency of digital assets.

Finally, DeFi smart contracts offer a high level of flexibility, allowing users to use a third-party interface if they don't like the interface of a certain application, as smart contracts have an open API that anyone can build an app for.² What is probably one of the most powerful features of DeFi is its interoperability, or what many call the permissionless composability.

Composability is a design principle that allows various components within a system to be combined, thus allowing any new DeFi application to combine existing DeFi products to form new DeFi products. This is why DeFi is often referred to as financial Legos, as it allows you to combine any number of Lego pieces together to build the creation of your choice.

The analogy with Legos is fitting. When Lego applied for its “toy building brick” patent in October 1961 it introduced the concept of “building bricks or blocks adapted to be connected together by means of projections extending from the faces of the elements and arranged so as to engage protruding portions of an adjacent element when two such elements are assembled ... thus providing for a vast variety of combinations of the bricks for making toy structures of many different kinds and shapes”³ In a way, DeFi allows us to do the same. A good example of composability is that you can take some of the DeFi assets that you have locked in a certain DeFi protocol and use them as collateral for your activities in a separate DeFi application.

2 Can DeFi Be Regulated?

One big question is whether DeFi can be regulated like the rest of the crypto industry increasingly is. Whilst this topic could have been neglected in the past, as DeFi volumes were negligible, the surge of DeFi since mid-2020 has spurred regulators to question how to bring this emerging industry under rein. The SEC has acknowledged that regulating DeFi would be a challenge and the CFTC has also been involved in these discussions. But in practice, there are some challenges trying to regulate DeFi, for example, the basic nature of DeFi platforms making regulation difficult right off the bat. Centralised exchanges or custodians are legally incorporated in a jurisdiction, have a physical office, and have employees on the payroll. Although there are exceptions, many DeFi platforms are not a legal entity on their own and many of their founders remain anonymous, and so whilst regulators can shut down a bank or financial intermediary, it’s very difficult, if not impossible, with DeFi. DeFi platforms operate using blockchain smart contracts written in code using platforms like Ethereum that are open-sourced and decentralised. Third, due to the open source and decentralised nature and the composability of DeFi, anyone can copy a certain application and start a new one immediately. Considering the ease with which users can move funds from one DeFi platform to another (compared to say the headaches of switching from one bank to another), this would be a futile cat and mouse

game for authorities. From a legal perspective, there are practical difficulties to consider. For example, determining liability is a challenge, as software development is protected by the First Amendment in the United States. Whilst arresting the person in charge is easy in a centralised entity, there are several players involved in DeFi platforms, from governance token holders to liquidity providers and holding all these actors liable would certainly be a practical (and legal) challenge.

At the same time, despite all the innovative features of DeFi, there are also clear risks. For example, whilst we can ensure that laundered or terrorist-linked funds cannot enter via centralised exchanges (especially following the enactment of the FATF travel rule in many countries), this is not enforceable on DeFi platforms. This can make DeFi platforms a playground for money launderers and others with illicit funds from hacks or other nefarious activities. For example, the actors behind the KuCoin hack were trying to launder their funds via DeFi platforms, and unlike centralised platforms, ensuring the protection of the public is very difficult. DeFi platforms can obtain independent reviews and audits of their code, but many have been launched without such precautions and with bugs that were later exploited, putting users' funds at risk. For instance, in 2020, the DeFi platform Harvest Finance was victimised by actors who were able to exploit these gaps, and more alarmingly, over half of the total 2020 crypto hacks came from DeFi protocols and exchanges (Fig. 1).

Some solutions have been proposed to address these issues, including a proposed no-action letter or a safe harbour that shields entities from liability if they follow a set of guidelines, a relatively straightforward way to potentially induce DeFi protocols to comply with relevant regulations. Another option

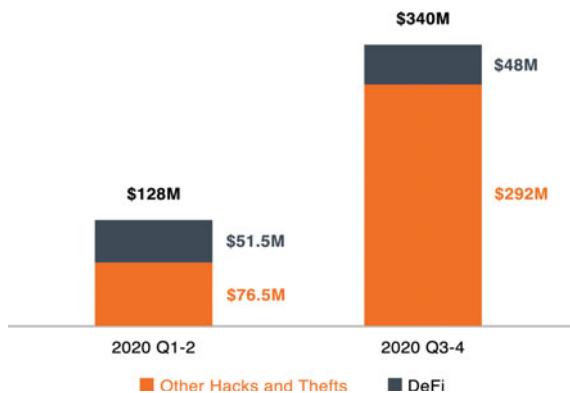


Fig. 1 Total value lost from DeFi Hacks (2020) (Source "2020 Geographic Risk Report: VASP KYC by Jurisdiction," CipherTrace, 2020)

would be to encourage DeFi platforms to self-regulate and agree on certain common standards they'll all respect. This approach is not dissimilar to the steps many leading crypto exchanges and the broader industry took before crypto regulations became commonplace. We've seen early examples of such initiatives, including a recent one to set standards for smart contracts on the Ethereum blockchain, and as DeFi continues to grow, this will be an area to watch.

What Are the Risks of DeFi Interoperability or Composability?

The interoperable or composable nature of DeFi opens a new universe of possibilities when it comes to reimagining the future of financial services. In the same way that Lego blocks allow you to build as much as your imagination allows, you can do the same with DeFi. But there are risks to be aware of. First is the risk at the protocol or blockchain level, where smart contracts operate. For example, if a malicious third party conducted a 51% attack or any other malicious form of attack on a certain blockchain, then it may affect the DeFi ecosystem operating on that blockchain. At the time of writing, almost all DeFi activity was taking place on Ethereum, so the risk of such attacks is low, but this is something to consider for smaller blockchains.

Second is the potential risk to the smart contract of any particular DeFi application. Whilst some of the more high-profile projects undergo smart contract audits, many of the smaller ones don't. This presents a potential risk not only for that application but for any other project that uses that "Lego block" as part of its new DeFi application. Finally, the combination of various DeFi "Lego blocks" potentially increases the overall risk as it grows the attack surface in such a way that is greater than the sum of its parts.⁴ A good analogy would be if you launch an e-commerce business and all your data is stored in a cloud offering, like AWS or Azure. If something happens to that cloud offering, your e-commerce business would be impacted not because you did something wrong, but because of the cloud you were using and the same principle to a certain extent applies to DeFi.

To properly understand the DeFi ecosystem, it's useful to go through the most common applications that we are seeing, and it's important to understand that the DeFi ecosystem is evolving very rapidly. Whilst the information below is accurate at the time of writing, it's possible that certain tweaks were made to the protocols or governance mechanism of some of the DeFi applications discussed below. That said, these practical examples should provide you with a solid foundation to understand DeFI.

3 DeFi Stablecoins

Perhaps not surprisingly, many initial DeFi offerings are like the basic services offered by traditional financial services providers, such as borrowing and lending. The first DeFi offering that really captured mainstream attention was the Maker stablecoin project, launched in December 2017 (and discussed earlier in this book in the chapter about crypto-collateralised stablecoins). It's worth reminding you how Maker and Dai work, as both play an important role in understanding DeFi. I'll go step by step and simplify some notions to ensure that the mechanism is understood.

To start, 1 Dai is worth US\$1. For any traditional fiat-collateralised stablecoin (e.g., USDC, USDT), you can send US\$1 from your bank to the issuer and the issuer will in exchange send you a US\$1 stablecoin (in practice, there are issuance fees and minimum amounts). However, a crypto-collateralised stablecoin like the Dai is backed by ETH. To receive a Dai, you need to send ETH to a collateralised debt position (CDP), which is a smart contract in the Maker ecosystem. Once you've sent your ETH to the CDP, you'll be able to receive Dai. The number of Dai you receive depends on the amount of ETH that you sent and the level of collateralisation required. For example, if the collateralisation level is 150%, then to obtain 100 Dai, I need to send US\$150 worth of ETH, meaning that each Dai is backed by 1.5 ETH. As each Dai is worth US\$1, you can use it for anything you want, from online purchases to trading, or simply swap it for another stablecoin or withdraw your Dai for fiat currency via an exchange. Your collateralised ETH will be held in the CDP until you "return" your 100 Dai, at which point the Dai will be destroyed and you will receive your ETH back.

Of course, there is a cost for borrowing Dai using your ETH as collateral (in the same way that you need to pay interest when you get a mortgage from a bank, with your house as collateral) called the Stability Fee. When you "return" your Dai, you also need to pay this stability fee,⁵ which is relatively straightforward. To begin, if the price of ETH rises, then the Dai becomes more collateralised, and if the price of Dai goes up (i.e., trading for US\$1.02, meaning there is more demand for Dai than people are creating using CDPs), then the stability fee acts as a mechanism to encourage users to create more Dai. For example, if a Dai trades consistently above US\$1, this means that demand is outweighing supply, and market participants are willing to pay a premium to purchase Dai. If this is happening too consistently, it signifies a need to lower the stability fee to incentivise more Dai creation (i.e., becomes "cheaper" to borrow Dai).⁶ If a Dai trades consistently below \$1, this means that supply is outweighing demand, and the market is flooded with too much

Dai. If this happens too consistently, it signifies that the stability fee needs to be raised to slow down Dai creation (e.g., make it “more expensive” to borrow Dai).⁷

This is not dissimilar in theory with how a central bank tinkers with interest rates. The stability fee is determined by a vote of the MKR token holders and varies from close to 0% to almost 20%, depending on some of the factors above.⁸ For example, in the summer of 2021, following a sharp fall in crypto prices, the stability fee fell to less than 5%, as demand for Dai stablecoins was lower.⁹ The obvious risk with the Dai is that the value of the collateralised ETH falls, where in such a case, a user can add more collateral by locking in more ETH (similar to a margin call in traditional finance). If you don’t, and the value of the collateral falls below a certain predetermined threshold, then the CDPs will liquidate your ETH (like a foreclosure in a traditional mortgage). In such a case, a penalty fee also needs to be paid. In the event of a black swan event like a major hacking or security breach, there is a possibility to trigger an emergency shutdown (previously called the global settlement) where Dai holders will be able to redeem their ETH collateral directly.

Whilst the entire system is decentralised, there is still some governance on the platform achieved by the Maker tokens (MKR). Anyone can acquire MKR, which gives certain voting rights on topics like the savings rate or the liquidation ratio, and the value is driven by demand, as the stability fee is paid using MKR tokens. MKR token holders also have the power to “pull the plug” in the event of an emergency shutdown.¹⁰ The downside for MKR token holders is that in the event of an emergency shutdown, if there is not enough collateral to cover all the Dai issued, then additional MKR tokens could be issued and auctioned off to pay the difference (thus negatively impacting via inflation the value of the existing MKR tokens).

Although the Dai is an interesting innovation at the intersection of crypto-assets, traditional lending, and decentralised finance, it still has flaws. For example, due to the underlying volatility of ETH, a lot of collateralisation is required which does not make it very capital efficient. But this situation should improve with time, as volatility in crypto-assets goes down, and in addition, crypto-collateralised stablecoins like Dai are still not easy to use for people who don’t have crypto experience or who may not be familiar with digital wallets or smart contracts. Separately, the entire MakerDAO mechanism is quite complex (as seen above), which makes it difficult for

the average person to use. However, DeFi-based stablecoins (or crypto-collateralised stablecoins) like DAI are experiencing tremendous growth due to the interest in decentralised finance and are a good example of a practical DeFi application.

4 DeFi Borrowing and Lending

Borrowing and lending offerings have been some of the most popular initial DeFi offerings, and at the time of writing, platforms like Compound Finance (with its COMP token) and Aave (with its AAVE token) each have billions of dollars of assets locked. To better understand the purpose they serve, let's use an analogy. Say you have a million dollars' worth of cryptocurrencies, like Ethereum, and you're looking to borrow US\$100,000 for a down payment on a new house. If you go to a traditional bank, you will not be able to borrow money using your crypto-assets as collateral, since your traditional bank does not recognise cryptocurrencies as collateral for a loan. However, a DeFi platform would allow you to deposit \$200,000 worth of cryptocurrency and borrow \$100,000 in U.S. dollar-based stablecoins. You can then sell them on an exchange for U.S. dollars, or simply use those to buy your house.

What these DeFi platforms are doing is like what your bank does when it gives you a mortgage using your house as collateral, or what a private bank does when it lends you cash using your stocks as collateral. Unlike traditional banks, all this happens in a fully automated way, using smart contracts without any human involvement. The collateral and risk management are fully automated, as the smart contracts can start liquidating your crypto-assets if the value of your collateral falls from \$200,000 to \$150,000. This way the platform has efficient risk management around your loan. In practice, many users of such DeFi borrowing platforms do so not to buy a new house, but rather to gain leverage to be able to do even more crypto trading.

The related offering of borrowing is obviously lending. Returning to that theoretical million-dollar pile of Ethereum that you hold, you can use DeFi platforms to lend it out to others who may want to borrow it (i.e., crypto traders) and thus earn interest on your crypto-assets that you lent. Again, this is similar to what your broker does with your stocks (sometimes without customers being aware!) or what an investment bank does with stock borrowing and lending for institutional clients, but once again, this all happens in DeFi without any centralised entity in the middle, and the process is accessible to a much wider base of users than traditional banking. This is why the two main risks with DeFi lending platforms are smart contract risk

(risk of a bug within the protocol code) and liquidation risk (risk on the collateral liquidation process).

A good example is Compound, a lending platform built on Ethereum that lets users instantly lend to or borrow from a pool of assets in a smart contract.¹¹ The interest earned is denominated in the same token that is lent. Interest rates are algorithmically derived and a function of the amount of assets available in each market based on the supply and demand of each asset to reflect market conditions.¹² Compound initially began as a tokenless protocol and upgrades, with changes made unilaterally by the Compound Labs team. The protocol was still non-custodial, but there was a centralised entity that retained administrative privileges. In order to remove themselves from this position, the team introduced COMP, a token used to govern the protocol, with the goal to have Compound fully controlled by COMP holders with no remaining privileges held by Compound Labs.¹³ COMP governance token holders can propose and vote on all protocol changes, including interest rate models and supported collateral types. The COMP token popularised “liquidity mining”, whereby 10 million COMP tokens were created and a predetermined amount (around 40%) of COMP is distributed to all lenders and borrowers every day over a four-year period. Whilst there is no cash flow attached to COMP at the time of writing, many believe that COMP holders will eventually vote for a mechanism to allow some claim on the system’s cash flows.

Another good example is Aave, a decentralised non-custodial liquidity market protocol in which users can participate as depositors or borrowers.¹⁴ The history of Aave is quite interesting, beginning as ETHLend in 2017 after it raised \$16.2 million in an ICO to create a decentralised peer-to-peer lending platform, later rebranding to Aave when it switched to a liquidity pool model. Aave launched the Aave Protocol in 2020, an open-source and non-custodial liquidity protocol that allows users to earn interest on deposits and borrow assets.¹⁵ Similar to Compound with its COMP token, Aave also has its own token called LEND, which later migrated to AAVE in 2020 (at the migration ratio of 100 LEND for 1 AAVE). AAVE is used to vote and decide on the outcome of proposals to improve the protocol, known as the Aave Improvement Proposals (AIP), and can be staked within the protocol (in something known as the Safety Module) to provide security/insurance to the protocol/depositors. In exchange, stakers earn staking rewards and fees from the protocol.¹⁶ There are two interesting differences between Aave and Compound, however. First, Aave allows you to choose between a fixed and floating interest rate, like what traditional banks offer,¹⁷ and second, Aave

enables flash loans that allow users to borrow any available amount of assets without putting up any collateral, so long as the liquidity is returned to the protocol within one block transaction.

5 What Are Flash Loans?

Flash loans are special uncollateralised loans that allow the borrowing of an asset if the borrowed amount and a fee (of 0.09% at the time of writing) is returned before the end of the transaction. There is no real-world analogy to flash loans, so it requires some basic understanding of how the state is managed within blocks in blockchains.¹⁸ Flash loans take advantage of a feature of most blockchains, which is that transactions are only finalised when a new bundle of transactions, known as a block, is accepted by the network. But adding each new block takes time; on Bitcoin, that interval is roughly 10 minutes and on Ethereum, it's around 13 second. An Aave flash loan therefore takes place in that 10–13 second period.

A borrower can request a flash loan from Aave, but must then pay back the loan amount plus the 0.09% fee within the same block, or in other words, within 13 second before the block is mined. If the borrower doesn't do this, the entire transaction is cancelled, so that no funds were ever borrowed. As a result, Aave doesn't take a risk and neither does the borrower. Such flash loans have been frequently used for swapping and/or migrating positions. There are also numerous other use cases, from doing arbitrage between assets (without needing to have the principal amount to execute the arbitrage) to swapping collateral of loan positions (without having to repay the debt of the loan positions).¹⁹

To give a basic example, a trader can write a smart contract to borrow on a flash loan; buy low on one market; sell high on the other market; repay the loan; and pocket the profit. Again, this is all done within the same on-chain transaction via decentralised exchanges. Unfortunately, such flash loans have been used to conduct attacks as well. One example was two attacks on the bZx lending platform in February 2020 which allowed the attacker to drain hundreds of thousands of dollars worth of ETH from the platform.²⁰ These are not cyber-attacks per se in which a hacker is stealing assets, but rather a situation in which the attacker is taking advantage of a bug in the system. Instead of just buying low and selling high, the attacker or attackers used the borrowed funds to manipulate markets that were unusually vulnerable to it.

In the first attack against bZx, through a complex web of transactions, the attacker pumped and then dumped wBTC ("wrapped Bitcoin," an Ethereum

token backed by actual Bitcoin) on Uniswap, a decentralised exchange. The attacker then took profits in Ether; repaid the flash loan; and took another loan on bZx related to the wBTC pumping.²¹ The second attack focused on pricing data. For a DeFi lending market to run properly, lenders must know the value of the collateral, so they need pricing information, often gathered from decentralised crypto exchanges. In bZx's case, the source was the decentralised exchange Kyber. The attacker focused on Synthetix USD (SUSD), a dollar-pegged stablecoin on the Synthetix Network, borrowing 7,500 Ether on bZx then pumping the value of SUSD on Kyber by swapping Ether for SUSD. The purchase of so much SUSD caused the price to jump two and a half times the prevailing market rate of \$1. The attacker then took advantage of bZx's dependency on Kyber for pricing data, putting up the SUSD as collateral for a large sum of Ether on bZx; in fact, 2,000 more Ether than the same amount of SUSD that would have normally purchased on an open market. After paying back the flash loan, the attacker reneged on paying back the under collateralised SUSD/ETH loan just taken out on bZx, resulting in a tidy 2,378 ETH profit.²² Whilst these bugs have since been discovered and patched, the reality is that flash loans can be used against the lending platforms, as illustrated above.

6 DeFi Exchanges

One area seeing tremendous growth is the ecosystem of decentralised exchanges, with some popular exchanges like Uniswap, SushiSwap, Curve, and Balancer seeing tremendous growth. Whilst we'll look at the centralised and decentralised exchange ecosystem later in this book, it's worth explaining how decentralised exchanges work.

To start, when you want to buy or trade a certain cryptocurrency, you'll either go to a centralised or decentralised exchange. The centralised exchange has many benefits, in that it's often regulated, has a company or an individual behind it, has an "office", and can offer other services in addition to basic trading, like custody, and is perfect for beginner and reasonably advanced traders. Decentralised exchanges achieve the same goal of letting you buy or trade digital assets, but they do in a different way as there is no central counterparty. Trades are done peer-to-peer between two users using smart contracts and each user custodies their own assets in their own wallet. These exchanges are normally suited for more advanced traders as individuals new to the crypto world tend to first dip their toe in using a centralised exchange. Whilst most crypto trading has taken place on centralised exchanges, the

trading volumes on decentralised exchanges started rising rapidly in the summer of 2020 (Fig. 2 and 3).

A big development happened with the rise of a decentralised exchange called Uniswap. Whilst its decentralised exchange offering is nothing new, Uniswap popularised an innovative concept called automated market making (AMM). The AMM concept was previously used by other decentralised exchanges like Bancor, but Uniswap is what made it popular in the summer of 2020.

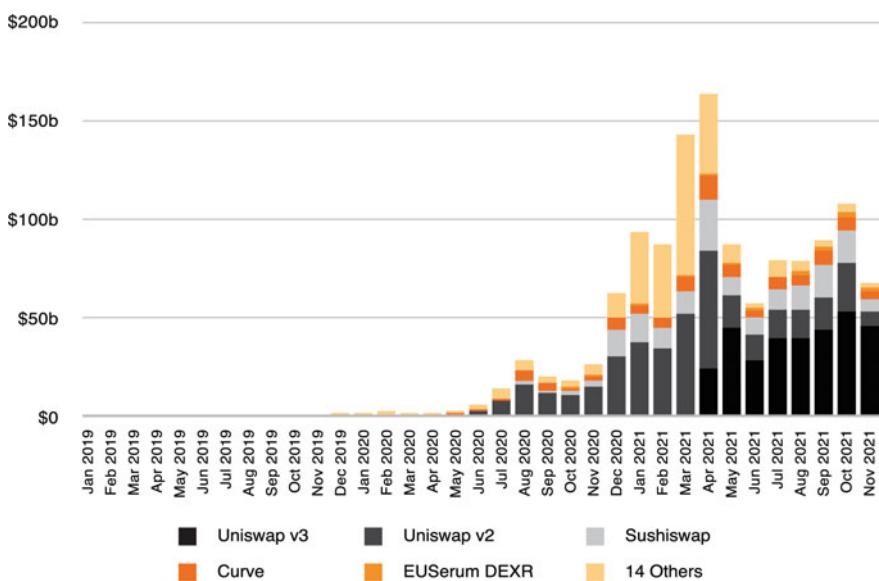


Fig. 2 Trading volumes at key decentralised exchanges (DEXs) (Jan. 2022)

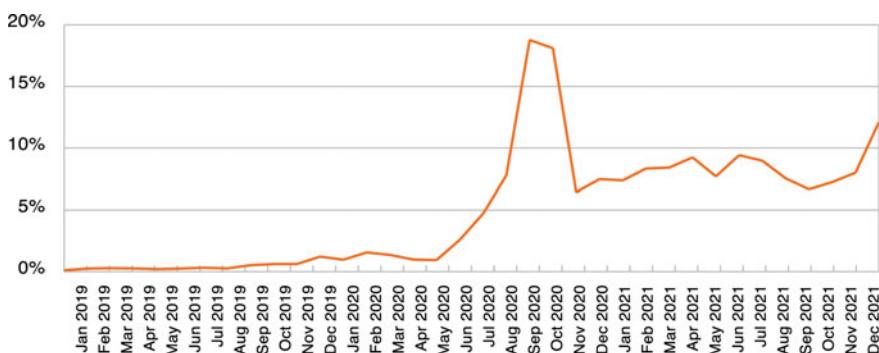


Fig. 3 Decentralised (DEX) spot trading volumes compared to centralised exchange (CEX) spot trading volumes (Jan. 2022)

7 What Are Automated Market Makers (AMM)?

In a traditional centralised exchange, traders can see the liquidity (what is available to trade and at what price) by looking at the order book. Market makers (who are professional firms that provide such liquidity by buying and selling those assets at certain prices) need to actively and continuously manage their orders (although it's done in a fully automated way using sophisticated trading infrastructure and algorithms). Whilst this continues to work quite well in centralised exchanges, it has challenges in a decentralised world as there is no centralised entity to host and maintain the order book and to match buyers and sellers. Also, becoming a market maker is not something that is possible for a small or retail trader due to the costs and trading infrastructure required, thus allowing only large and well-funded entities to participate.

Such a barrier of entry is one of the problems that DeFi wants to solve in making finance more inclusive, accessible, and open. In addition, whilst traditional structures work well for assets that are widely available and traded, they're not as convenient for continuously new assets coming to the market as a new asset needs to convince market makers to make markets in its token and such players will only do so if they believe such a token will see a lot of trading, so it's not ideal for encouraging the development of new tokens in the ecosystem. Based on this reality, Uniswap tried via the launch of Uniswap 1.0 in November 2018 to reimagine crypto trading by leveraging the benefits of smart contracts in a permissionless environment like DeFi where anyone can participate. Unlike traditional centralised exchanges, Uniswap decided not to use an order book or traditional market makers and instead used Liquidity Pools.

Liquidity pools operate in a clever way. For example, each Uniswap liquidity pool is a trading venue for a pair of ERC20 tokens, and anyone can create a liquidity pool for a new pair of tokens. When a pool contract is created, the balances of each token are zero, but anyone can become a liquidity provider and deposit an equal value at the then market rate of both tokens into the pool. It is important that an equal value at the current market rate of both tokens is deposited or else that immediately creates an arbitrage opportunity for a third party.²³ When other liquidity providers add to an existing pool, they must deposit pair tokens proportional to the current market price as well. If they don't, the liquidity they added is at risk of being quickly arbitraged. If they believe the current price is not correct, they may arbitrage it to the level they desire, and add liquidity at that price as they

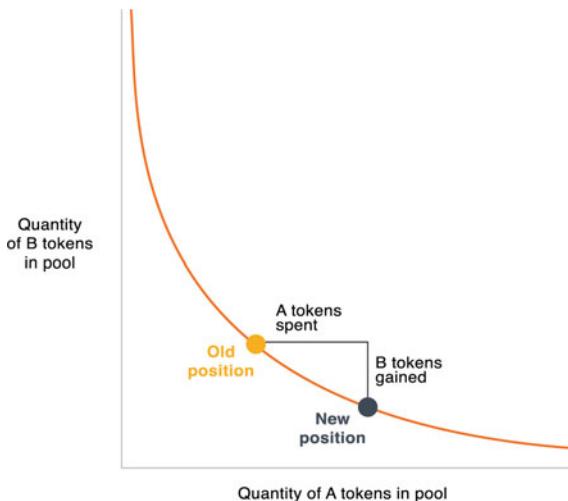


Fig. 4 X-Y-K market makers (Source Vitalik Buterin, "Improving Front Running Resistance of $x*y = k$ Market Makers," Ethereum Research, March 2018)

would in a traditional exchange.²⁴ The mechanism is known as the " $x*y = k$ " formula popularised by Vitalik Buterin, who himself was inspired by previous DeFi projects like Augur and Gnosis (Fig. 4).²⁵

In the " $x*y = k$ " formula, as x multiplied by y must always equal the same value (k), the resulting curve depicts all possible exchange rate values with the red dot on the curve representing the exchange rate. The balance of ETH and ERC20 tokens ultimately reflects the supply and demand of said token, resulting in the exchange rate price.²⁶ Whenever liquidity is deposited into a certain pool, special tokens known as *liquidity tokens* are minted to the provider's address, in proportion to how much liquidity they contributed to the pool. Each pool has its own liquidity token, and these tokens are a representation of a liquidity provider's contribution to that pool. Whenever a trade occurs, a trading fee (of 0.3% at the time of writing) is levied and distributed *pro rata* to all the liquidity providers in the pool at the time of trade. That distribution is the incentive that liquidity providers have for depositing their assets in that pool or what the DeFi world calls "locking" their assets. To receive the underlying liquidity back, plus any fees that were accrued whilst their liquidity was "locked", liquidity providers must burn their liquidity tokens. Liquidity providers can also choose to sell, transfer, or otherwise use their liquidity tokens in any way they see fit.²⁷ The amount of assets that are "locked" in such liquidity pools is measured by the Total Value Locked (TVL).

Ironically, such a decentralised exchange still needs centralised exchanges and market makers to enable price discovery as the decentralised exchange cannot do the price discovery on its own. Traders will simply see the prices of those assets trading on other exchanges and do any arbitrage needed on the decentralised exchange until the price corrects itself. Such a decentralised exchange has many advantages as it allows anyone to create an exchange for any token pair by providing the initial liquidity and it removes the centralised exchanges often known for charging large listing fees, especially in bull markets. However, trading tokens could be cheaper and more convenient on such an exchange, especially for newer or less liquid tokens, and there are also benefits if you want to focus on a specific asset type. The decentralised exchange Curve has been the go-to DeFi exchange when it comes to trading stable coins.²⁸

However, there are disadvantages. For example, decentralised exchanges may not be suitable for large traders if the liquidity pools are still small, and in addition to trading fees, Ethereum gas is needed to conduct transactions as they're on the Ethereum blockchain. In case of high transaction volumes, as was the case in the summer of 2020, gas prices may make small trade not worth it.²⁹ Also, such decentralised structures are not regulated which can be complicated for some large funds or trading firms who prefer or are required to trade with regulated exchanges. The liquidity pool model has many benefits on its own as well. The major benefit is that it allows anyone to be a "market maker" by providing tokens to the platforms and receiving a fee. In addition to generating a yield on crypto-assets that would otherwise remain idle, they can get involved in yield farming.

Like everything else in crypto, these DeFi platforms continue to evolve. For example, following the launch of Uniswap v.2 in May 2020, Uniswap v.3 debuted in May 2021, providing new features including concentrated liquidity, which gives individual liquidity providers granular control over what price ranges their capital is allocated to. It aggregates together individual positions into a single pool, forming one combined curve for users to trade against. Another innovation of Uniswap v3 is multiple fee tiers which allow liquidity providers to be appropriately compensated for taking on varying degrees of risk.³⁰ Despite the launch of Uniswap v3, the Uniswap v2 protocol will remain functional and available for use if the Ethereum network continues to exist. However, in practice, it's likely that an increasing amount of liquidity will migrate to v3 to take advantage of its features.³¹

7.1 What is Total Value Locked (TVL)?

TVL is a term that is widely used across the DeFi space, which is simply the total value of crypto that is locked in DeFi platforms. For example, when looking at decentralised exchanges, the TVL will provide the aggregate value of crypto that is “locked” in the various liquidity pools on the various decentralised exchanges. The term “locked” is technically incorrect, as most of these liquidity pools allow you to withdraw your crypto at any time. There are no lockups that require you to leave your crypto in a specific pool for a certain amount of time.

For this reason, a better term would probably be “total value committed” or “total value deposited”. Regardless of what it’s called, TVL is a good indication to determine the health of the DeFi ecosystem, as one can deduct that the higher the TVL, the healthier the ecosystem. There are numerous websites that track TVL, with one of the most popular being Defipulse.³² However, you also need to be careful and put TVL in context. For instance, most DeFi platforms run on Ethereum, and the collateral needed for DeFi applications is ETH. So even if there is no increase in activity, the TVL may simply increase or decrease based on the price of ETH, and thus, one needs to be careful and look at the data not only in absolute, but relative, terms as well.

7.2 What Is Impermanent Loss When Referring to Decentralised Exchanges?

Impermanent loss (also referred to as divergence loss) happens when you provide liquidity to a liquidity pool, and the price of your deposited assets changes compared to when you deposited them. Pools that contain assets that remain in a relatively small price range will be less exposed to impermanent loss. Stablecoins or different wrapped versions of a coin, for example, will stay in a relatively contained price range thus exposing liquidity providers to a smaller risk of impermanent loss.³³ Traders are still happy to provide liquidity to AMMs and become a liquidity provider as they receive 0.3% of the fees, which can make it profitable despite the risks of impermanent loss.

The best way to explain impermanent loss in practice is to go through an example. Let’s imagine a hypothetical scenario where Alice deposits 1 ETH and 100 DAI in a liquidity pool. As the deposited token pair needs to be of equivalent value, this means that the price of ETH is 100 DAI at the time of deposit, and that the total dollar value of Alice’s deposit is US\$200 at the time of deposit.³⁴ In addition, there’s a total of 10 ETH and 1,000 DAI in the pool, funded by other liquidity providers like Alice. Alice has a 10% share

of the pool, and the total liquidity is \$10,000. Let's imagine that the price of ETH in the market goes up to 400 DAI. Because AMMs are disconnected from external markets, if token prices change on external markets, an AMM doesn't automatically adjust its prices. It requires an arbitrageur to come along and buy the under-priced asset or sell the overpriced asset until prices offered by the AMM match external markets.³⁵

Wanting to take advantage of this price change, arbitrageurs will want to balance the AMM by selling DAI for ETH until both sides of the AMM are balanced again. Whilst the total value of the pool remains constant at \$10,000, the ratio of the assets change. If ETH is now 400 DAI, the ratio between how much ETH and how much DAI is in the pool has changed and there's now 5 ETH and 2,000 DAI in the pool, thanks to the work of arbitrage traders. Alice then decides to withdraw her funds, and as we know from earlier, she's entitled to a 10% share of the pool. As a result, she can withdraw 0.5 ETH and 200 DAI, totalling US\$400. Whilst it may seem that Alice made a profit by receiving \$400 compared to her original \$200, the reality is that she could have made more money by simply holding both assets outside the AMM as her 1 ETH and 100 DAI would now be worth 500 USD. This is an impermanent loss. Of course, if the price were to return to the same value as when Alice added her liquidity (1 ETH equals 100 DAI), this loss would disappear. This loss is only realised when the liquidity provider withdraws their liquidity and is based on the divergence in price between deposit and withdrawal, and so many have argued that the name impermanent loss should be changed to divergence loss,³⁶ though there's already a clear formula that allows traders to understand their risk of impermanent loss (Fig. 5).

To put it another way³⁷:

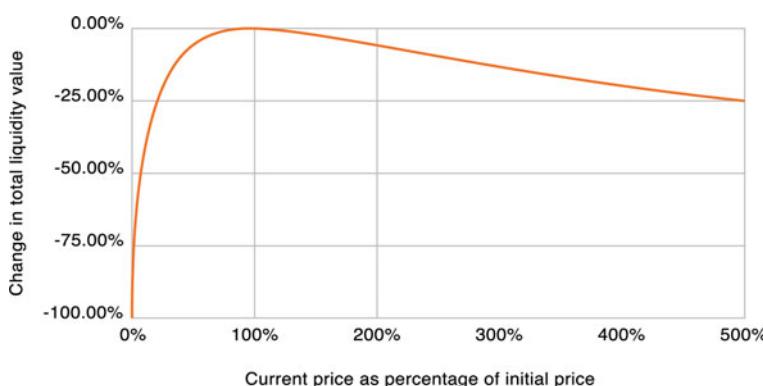


Fig. 5 Impermanent loss (Source "Uniswap: A Good Deal for Liquidity Providers," Pintail, August 30, 2020)

- a $1.25 \times$ price change results in a 0.6% loss relative to holding
- a $1.50 \times$ price change results in a 2.0% loss relative to holding
- a $1.75 \times$ price change results in a 3.8% loss relative to holding
- a $2 \times$ price change results in a 5.7% loss relative to holding
- a $3 \times$ price change results in a 13.4% loss relative to holding
- a $4 \times$ price change results in a 20.0% loss relative to holding
- a $5 \times$ price change results in a 25.5% loss relative to holding

An additional important point is that the loss is in the same direction the price change occurs (i.e., whether the price of the assets go up or go down). Once again, this is a risk that many traders are happy to take by becoming liquidity providers, as they're receiving the trading fees (e.g., 0.3% in the case of Uniswap).

8 DeFi Synthetic Assets

Many DeFi users want to be able to trade real-world assets without leaving the digital assets environment. A good example is the DAI stablecoins that allow users to have USD exposure without holding dollars, but blockchain technology enables us to push this concept even further by enabling users to create and exchange synthetic versions of assets like gold, commodities, or other cryptocurrencies. At the time of writing, the most popular such DeFi application was Synthetix, which is a protocol for issuing and trading synthetic assets on Ethereum. Each synthetic asset (called a Synth) is an ERC20 token which tracks the price of an external asset. For example, each sUSD token (the “s” stands for Synth) tracks the price of 1 US dollar. In principle the system can support any asset with a clear price and provides on-chain exposure to an unlimited range of real-world assets.³⁸

Like other DeFi applications, Synthetix is composed of a smart contract infrastructure and a set of incentives which maintains Synth prices, underpinned by the value of the Synthetix Network Token (SNX). The SNX acts as collateral as staking a proportional value of SNX is required to mint new Synths, and like some decentralised exchange platforms, stakers are rewarded for supporting the system with a *pro rata* share of fees generated by activity in the system.³⁹ The Synthetix platform allows any DeFi trader to get exposure to not only other digital assets, but also commodities (e.g., oil, gold), securities (e.g., FTSE or NIKKEI indexes or Google/Amazon stocks), and foreign currencies (e.g., USD, CHF, GBP, JPY).

The big unknown in such offerings is what will be the regulatory impact of these products? If a centralised entity offered such products in the non-crypto world, it would most certainly need to be regulated, especially if open

to retain investors. These DeFi platforms currently fall in a grey zone which makes regulatory compliance uncertain. Who and how DeFi protocols are to be regulated (if it's even possible) is a topic that will generate much debate in the foreseeable future.

9 DeFi Insurance

What often comes as a surprise to many is that there are also some DeFi insurance offerings that have developed in recent years. In the traditional crypto space, a crypto company buy insurance for certain risks from a broker. Whilst that is still difficult and expensive, it is increasingly becoming possible. However, insuring DeFi risks would be very difficult for a traditional broker as insurance companies have very basic and limited knowledge of crypto, so it was perhaps not surprising to see the DeFi community come up with its own insurance offering.

The best early example of an early DeFi offering was Nexus Mutual which uses blockchain technology to create a mutual (a risk sharing pool) built on the Ethereum public chain. It allows anyone to become a member and buy insurance coverage. It also replaces the idea of a traditional insurance company by being wholly owned by its members. The model encourages engagement as members get economic incentives for participating in three different activities: risk assessment, claims assessment, and governance.⁴⁰ In many regards, it resembles a traditional mutual, and was established as a company limited by guarantee in the UK and it has received approval by the UK Financial Conduct Authority to use the protected word “mutual” in the company name. By becoming a member, each participant in the mutual becomes a part-owner; however, it's solely based on blockchain, and those membership rights are represented by NXM tokens that can only be bought directly from Nexus.⁴¹

The insurance product offered by Nexus was smart contract insurance, which provided protection against hacks in smart contracts and was designed to cover “unintended uses of code” where someone, not necessarily the insurance coverage purchaser, suffered a financial loss on a smart contract, following a hack for example. Members who purchase that smart contract coverage choose a fixed sum, called the cover amount, to be paid out should the claim be approved by the claims assessment process. This is important as it means that the pay-outs wouldn't necessarily be matched to the losses incurred by the smart contract bug or hack but rather the prespecified cover amount. That has several benefits including that the claims assessment is a

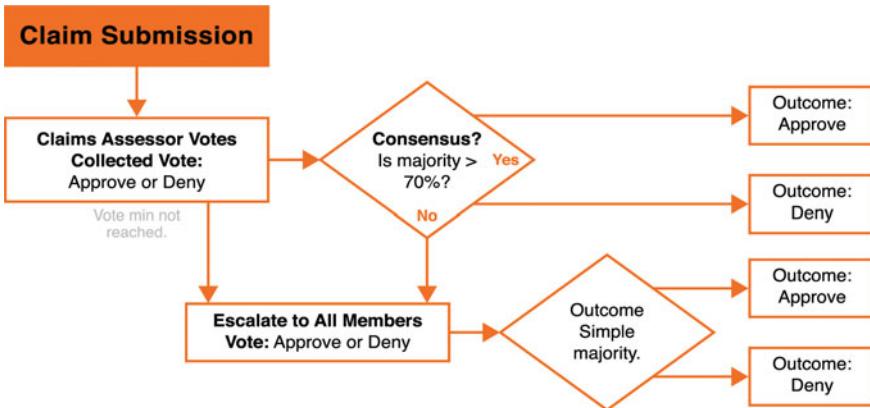


Fig. 6 The DeFi insurance process (Source “Nexus Mutual Gitbook,” Nexus Mutual, 2021)

simple ‘yes’ or ‘no’ rather than requiring an assessment of how much damage has occurred.⁴²

However, in true DeFi ethos, Nexus Mutual doesn’t approve or reject claims (which are visible to all members) according to conditions like a regular insurance company would, instead of providing a platform where members as claims assessors by voting on claims submitted by other members. The member voting process has full discretion on whether to pay a claim or not and their opinion is final (Fig. 6).

What is also interesting in the Nexus Mutual model is the role of risk assessors, who are people with smart contract auditing skills and who can stake NXM tokens against specific smart contracts they think are well-coded and secure. They are economically incentivised by earning rewards, in the form of extra NXM tokens, as insurance coverage is bought on the staked smart contracts. These risk assessors stake tokens and their personal reputation by giving their assessment that a certain smart contract does not have any bugs that would potentially be a risk.⁴³ Whilst it is still the early days in the field of DeFi insurance, this provides us as another example of how DeFi enables us to take a principles-based approach to longstanding products like insurance.

10 Aggregators

DeFi aggregators scan the DeFi universe and find the most optimal decentralised lending, yield enhancement, and trading options, allowing an investor to explore these platforms by allocating capital to DeFi aggregator.

They are like the decentralised asset management firms of the DeFi world, with many aggregator offerings popping up in recent years. For example, Yearn Finance is a suite of decentralised finance (DeFi) products focused on “creating a simple way to generate high risk-adjusted returns for depositors of various assets via best-in-class lending protocols, liquidity pools, and community-made yield farming strategies on Ethereum”.⁴⁴ Yearn’s Vault offering is similar to what a traditional fund manager would do except that all investments take place in a fully decentralised manner. For example, the Yearn Vault platform charges a 2% management fee and a 20% performance fee extracted by minting new shares of the vault.⁴⁵ Instead of fund directors, there’s a YFI token that provides governance capabilities with which token holders can vote.

It will be interesting to see how these DeFi aggregators evolve in the coming years. Like all DeFi offerings, there is an inherent smart contract risk, where investors could lose their funds if there is a bug in the code. It’s also not clear if and how such offerings could be regulated by regulators around the world. The services offered are clearly like what would constitute a regulated activity in most jurisdictions, but things are moving very fast, meaning this is an area to keep an eye on.

11 Benefits and Challenges of DeFi

The world of DeFi moves quickly. To put things in perspective, there was less than US\$1 billion in TVL in January 2020 before growing 50 times over the next 18 months. Some of the biggest benefits of DeFi, like composability, for example, are quite promising, allowing anyone to leverage the work that others have done and seamlessly build on top of it, and ensuring the DeFi ecosystem can benefit from network effects and with a $1 + 1 = 3$ phenomenon. Interestingly, regulators have tried in some countries (e.g., PSD2 in Europe) to create this dynamic by forcing banks to embrace an open banking or open API approach, but this has not been very successful due to traditional financial institutions natural propensity to keep their technology proprietary. DeFi is de facto open banking and it’s genuinely permissionless, meaning that anyone from anywhere, regardless of country of birth or nationality, can conduct financial services if he has basic internet access. Yes, whilst this opens the door to many potential regulatory and legal challenges, it is already quite an interesting experiment. Although DeFi has its own risks (the smart contract risk that can be more amplified due to composability risk is

a good example), it removes the well-known counterparty risks linked with centralised intermediaries.

There are also numerous challenges as well, including regulatory risk. DeFi is still very small (even in crypto terms); only a small percentage of crypto users (let alone the general population) are involved; and the technical complexity makes it unlikely that a financially illiterate or a vulnerable grandmother would get involved in DeFi yield farming and trading on an average Tuesday morning. However, as DeFi interfaces become more user-friendly and TVL levels increase, we shouldn't be surprised to see regulators pay more attention.

The big question is how do you even try to regulate DeFi? Due to its permissionless and decentralised nature, it's difficult to regulate the entity as it has no headquarters (and often no CEO, leadership team, or board of directors). Who you would regulate in the first place is already a challenge, and in addition, even if you were to regulate DeFi Exchange A, as the code is open source, anyone could copy it and launch DeFi Exchange B where users could make the efforts of regulating the first exchange useless. Whilst regulating DeFi platforms is challenging, it's possible for regulators to force centralised exchanges to monitor tokens coming from DeFi platforms and ask for additional transaction monitoring information. Whilst not banning DeFi exchanges, it makes it cumbersome for users and may drive volumes back to centralised exchanges.

Finally, the risks of hacking in DeFi are always going to be present. Whilst DeFi removes the counterparty risk due to the lack of centralised counterparties, the risk that hackers find and exploit a bug in the smart contract will always exist as the US\$600 million hack of Poly Networks in August 2021 showed. Whilst such hacks will encourage more DeFi protocols to get independent smart contract audits, the risk will always exist. Whilst still in early stages, this is an area to follow.

The Composability Risk of DeFi Financial Legos

In September 2020, DeFi lending protocol bZx was attacked, losing \$8 million due to a faulty code (although this amount was later recovered). The hacker was able to exploit a flaw in bZx's smart contracts to duplicate assets and increase their iToken (bZx's token) balance. As DeFi platforms rely on smart contracts and there are no centralised entities (no call center to help you block a transaction), the code behind these smart contracts needs to be extremely sound. This is particularly the case as one of the most powerful and attractive features of decentralised finance is its interoperability, or what many

call the permissionless composability. Composability is a design principle that allows various components within a system to be integrated together, thus allowing any new DeFi application to combine any existing DeFi products to form entirely new DeFi products. This is why DeFi is often referred to as financial Legos, as this model allows you to combine any number of pieces together to build the creation of your choice. Yet whilst this system certainly has plenty of benefits, it only takes a single crack for one of the Lego pieces upon which the others are built for the entire structure to fall to pieces. With the growing wave of excitement and enthusiasm for DeFi, we need the industry to be more active and diligent in addressing this issue moving forward.



17

Crypto Regulations and Compliance

I often say that the world of crypto-assets moves at a “dog year” pace with each year in the crypto world the equivalent of seven years in the traditional financial system. This rapid evolution has posed a serious challenge for regulators seeking to provide proper guidance for this industry, whilst also fulfilling their responsibilities for systemic stability and consumer protection. Regulators know the decentralised nature of crypto-assets means they cannot simply stop the emergence of these asset classes, much in the same way that it would not be feasible to “stop” the internet.

However, their disposition towards, and classification of, various assets and stakeholders in the crypto-asset ecosystem will have a powerful impact on the evolving structure of the industry. They must walk a challenging line: on one hand, they do not wish to stifle innovations that could drive growth and improve the efficiency and accessibility of the financial system, whilst on the other hand they must ensure that the best interests of the public are protected. Most difficult of all, regulators cannot simply sit on the sidelines indefinitely waiting to see how crypto-assets evolve, as some financial incumbents have; they must decide and act.

In more and more jurisdictions, we’re seeing action from regulators, clarifying their disposition towards crypto-assets, and in the years to come, we should expect this trend to continue. Whilst the regulatory landscape is complex and highly varied, we can generally categorise responses into three broad approaches: (i) Positive, (ii) Neutral, and (iii) Negative. In the pages that follow, we’ll briefly explore each of these.

1 Different Approaches to Crypto Regulations

1.1 A Positive Disposition to Crypto-Assets

Some jurisdictions have taken the view that by clearly articulating the requirements for issuing and dealing in crypto-assets, whilst at the same time expressing a welcoming disposition towards these instruments, they can both achieve their regulatory aims and attract new businesses and innovators to their country's broader financial ecosystem.

Switzerland was an early example of a jurisdiction that took early action on a positive stance and benefited tremendously, at least from a marketing perspective. For example, the Financial Market Supervisory Authority (FINMA) adopted an active hands-on approach to crypto-assets and in early 2018, FINMA published its initial coin offering guideline¹ whilst the canton of Zug, often referred to as "the Crypto Valley", announced that residents could pay for government services using cryptocurrencies.² Whilst Switzerland lost some of its lead in the subsequent years, this enabled great PR and many early projects (for example Ethereum) had a strong Switzerland nexus. Many smaller countries or island states also benefited by taking a proactive stance early on. Gibraltar, Malta, the Bahamas, and Bermuda are good examples of an approach where governments and regulators have taken a proactive approach to crypto-assets.³ For example, many crypto companies set up a presence in places like Bermuda and Malta following such developments and crypto exchange FTX moved from Hong Kong to the Bahamas in 2021 after the country proactively introduced crypto regulations.⁴

Some of the established financial centres benefited as well after they moved from a neutral/wait and see approach to a more positive one, with Singapore a great example. Singapore's financial regulator, the Monetary Authority of Singapore, issued a Frequently Asked Questions page on crypto in 2017 during the ICO boom that provides clarity on the distinction between investment and utility tokens.⁵ In 2019, it issued the Payment Services Act looking at regulating crypto exchanges thus attracting many of the crypto industry players.⁶

Dubai in the United Arab Emirates is another jurisdiction that quickly pivoted from a neutral stance to embracing crypto in a very visionary way. It even set-up a crypto focused regulator, the Dubai Virtual Assets Regulatory Authority (VARA), to provide the level of regulatory expertise needed. Another good example is in the United States, which took a neutral stance at first before migrating to a more positive one. However, this has

not been an easy task due to the complex and multi-layered regulatory structure of the country. For example, crypto payment tokens can be considered commodities and are regulated by the country's Commodity Futures Trading Commission (CFTC). However, a security token offering would be regulated by the Securities and Exchange Commission (SEC) and many banking activities would fall under the Office of the Comptroller of the Currency (OCC). Further complicating the issue, both federal and state level regulations may apply to some crypto-assets. For many types of crypto entities, from crypto funds to crypto custodians, the United States remains a good place to set up a business. Whilst the regulatory maze may create headaches, these firms are welcomed and able to operate from New York with its Bitlicense to Miami with its MiamiCoin to various states like Texas, which has looked at attracting Bitcoin miners, and Wyoming that has looked at attracting crypto companies by way of welcoming legislation.

1.2 A Neutral Approach to Crypto-Assets

Some jurisdictions took a neutral (or wait and see) stance to crypto-assets, neither explicitly welcoming nor prohibiting dealing in these instruments, and instead trying to fit them into existing regulatory frameworks or see how they evolve. In many cases, the focus of these jurisdictions has been on ensuring public protection whilst also adopting that wait and see stance as the crypto ecosystem and its technology evolves.

Ironically, whilst many jurisdictions initially fit in this category, many of them have since moved on to provide specific guidance on crypto-assets, but some of the larger jurisdictions are still in this position. A good example is Brazil, where, at the time of writing, despite the nonexistence of crypto-specific laws or regulations issued by the financial authority, cryptocurrency entities can operate based on pre-existing laws and regulations applicable to the financial sector.⁷

1.3 A Negative Approach to Crypto-Assets

A third group of countries has taken a more negative disposition towards the crypto ecosystem, seen particularly in 2017 in response to the growth of ICOs, which several countries including China, India, and Russia viewed as a major risk to the retail public and sought to restrict. Whilst many of these countries gradually started taking a more neutral stance on crypto, some have

continued with their anti-crypto stance despite the broader wave of increased crypto regulatory clarity in 2020–2021.

China provides a particularly strong example of this view. The country undoubtedly has an active and sophisticated blockchain ecosystem, and indeed some would argue it boasts amongst the world's deepest expertise on blockchain technologies. However, this technology may also be viewed as a threat to the Chinese government's tight control of the national economy, particularly currency and capital flows. Moreover, in early 2017, as the ICO craze began to take off in China, people from all backgrounds and age groups began to actively invest in ICOs with over US\$400 million invested in the first half of 2017 alone. This sounded alarm bells for the country's authorities, who in September 2017 announced a ban on all ICOs, which remains in force at the time of writing this book. Whilst China regularly repeated that it did not welcome cryptocurrencies, in September 2021, 10 Chinese government entities, including the People's Bank of China, issued a notice effectively banning all crypto-related activities in the country, only months after the country banned Bitcoin mining.

India is another country that has taken a negative stance on cryptocurrencies with the Reserve Bank of India issuing warnings against cryptocurrencies multiple times in recent years. In many cases, these bans are linked to a broader macro policy. For example, China has strict capital controls, so if transactions in Bitcoin were allowed, then it would make such capital controls pointless as users could simply buy Bitcoin and cash it overseas, basically bypassing the various capital control requirements.

1.4 The Future of Crypto-Asset Regulation

Over the coming years, we should expect many more regulators globally to clarify regulatory and policy frameworks for the crypto ecosystem, and in many cases, this will be driven by global requirements. For example, the Financial Action Task Force has indicated that it would require its member countries to impose AML and licencing requirements on crypto exchanges.⁸ In other cases, it may be a policy decision where the government determines that the crypto-asset ecosystem provides an opportunity for them to take a leadership role in an emerging financial services area, as has been the case for many countries already.

A final area of regulation that should not be overlooked is that of self-regulatory initiatives that emerge from within the crypto-asset ecosystem to address gaps resulting from the inaction or slow action of regulators and shape the future of regulatory policy. There are a growing number of examples of

such initiatives globally, from a best practices document focused on crypto exchanges produced by the Asia Securities Industry and Financial Markets Association (ASIFMA)⁹ and an ICO best practice guide from the FinTech Association of Hong Kong¹⁰ to a voluntary code of conduct proposed by the global industry body Global Digital Finance¹¹ and various policy guides by the World Economic Forum.

We should expect to see such initiatives continue to emerge, particularly in jurisdictions where regulatory disposition remains uncertain and whilst the crypto industry continues to evolve, the industry is trying to tackle the inherent lag between tech development and regulatory clarity.

2 Different Approaches to Crypto Tax

We often talk about the need for regulatory clarity in the crypto industry, but tax clarity is equally important. Taxes and death are inevitable and so it should be no surprise that taxes are finding their way into the crypto-asset ecosystem. Whilst many crypto-related enterprises and individuals are keen to be transparent and declare their crypto holdings, others have tried to remain under the radar, causing tax authorities to begin looking for them. For example, in late 2017, a federal court judge ordered San Francisco-based crypto exchange Coinbase to comply with a summons that required it to identify 14,355 accounts, which have accounted for nearly nine million transactions. This action was taken in response to a discovery by the IRS that only 802 people across the United States had declared Bitcoin-related losses or gains in their 2015 electronic tax filings. This is a practice that U.S. tax authorities have been regularly conducting for many years. For example, in May 2021 the IRS filed a John Doe summons to obtain the details of every American client who has traded over \$20,000 in cryptocurrencies from 2016 to 2020 on crypto exchange Kraken.¹²

Unfortunately, even for those wishing to comply, the details of tax treatment for crypto-assets remain complex and uncertain. Whilst many established accounting and tax advisors are keen to help their crypto clients, the absence of rules and guidance on the topic has been a major hurdle. Whilst some tax authorities have issued guidance, these insights have been limited and at a high level, and if holdings of crypto-assets are to continue to grow, further clarification and guidance from these authorities will be essential. Thankfully, many jurisdictions have understood the importance of providing such clarity. For example, PwC published a report on crypto taxes and jurisdictions around the world¹³ with the data showing that whilst

most jurisdictions surveyed in the report have issued some guidance on the calculation of capital gains and losses for individuals and businesses, almost none have issued guidance on important topics like crypto borrowing and lending, decentralised finance (DeFi), non-fungible tokens (NFT), and staking income. The reality is that tax authorities need to quickly start paying serious attention to this space. PwC publishes an annual ranking of tax authorities on the level of tax clarity they provide, with Liechtenstein topping the rankings, followed closely by Australia, Malta, Switzerland, Germany, and Singapore (Fig. 1).¹⁴

To devise these rankings, PwC identified 20 different components that make up the breadth of comprehensive crypto tax guidance. Whilst no surveyed country has accomplished this feat, the higher the score, the more guidance has been issued on the taxation of crypto-assets. Ultimately, the report shows that tax authorities have significant work ahead of them when it comes to catching up with a rapidly evolving new asset class.¹⁵

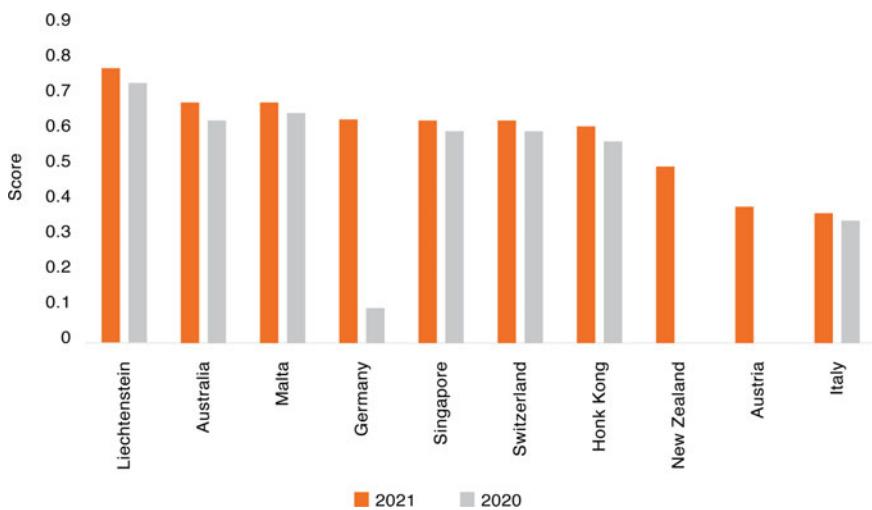


Fig. 1 Crypto tax guidance clarity by jurisdiction. The PwC Crypto Tax Index was developed to help illustrate and compare the level of comprehensiveness of tax guidance between jurisdictions. Covering 19 different areas relevant to the taxation of crypto-assets, the Crypto Tax Index measures whether a particular issue is addressed by the existing guidance of each jurisdiction (Source "Annual Global Crypto Tax Report," PwC, 2021)

3 Crypto and Illicit Activities

As with most areas of the emerging crypto-asset ecosystem, the use of tokens for the purpose of payments lacks regulatory clarity and regulatory treatment of these instruments often varies significantly from jurisdiction to jurisdiction. Despite this, there is a growing consensus amongst regulatory authorities that supports the view of the Financial Action Task Force (an intergovernmental organisation founded in 1989 to combat money laundering) that crypto-asset-based payment service providers should be subject to the same obligations as their non-crypto peers.¹⁶ In most jurisdictions, this would mean that any organisation facilitating the exchange of crypto-assets would be bound to observe a host of AML, KYC, and combating terrorist financing (CTF) regulations.

These regulations are an important step in creating a smoother interface between the crypto industry and traditional financial institutions. Many banks have serious concerns about their ability to effectively enforce AML, KYC, and CTF regulations on businesses in the crypto-asset ecosystem. As a result, many financial institutions will traditionally refuse to provide banking services to crypto entities, on the grounds that they may inadvertently facilitate the violation of AML, KYC, or CTF regulations, placing them at risk of a significant fine.¹⁷ However, given that global money laundering transactions are estimated to total US\$1–2 trillion a year, crypto transactions are at worst a drop in the bucket of total global money laundering.¹⁸ Also, traditional financial institutions are often the worst offenders, with Danske Bank putting aside US\$2.7 billion in 2019 for fines related to facilitating over US\$200 billion in suspicious transactions through their Estonian branch over a nine-year period¹⁹ and HSBC paying over \$2 billion dollars in fines in the past decade alone.²⁰

There are dozens of other examples. FinCEN has found that more than \$2 trillion in suspicious transactions was laundered via banks between 1999 and 2017.²¹ Are criminals also laundering money with Bitcoin? Not in any meaningful amounts yet, according to SWIFT.²² But that doesn't mean that crypto is clean; whilst exchanges have always been a popular off-ramp for illicit cryptocurrency, they've taken in a steadily growing share in recent months. For example, in 2019, Chainalysis traced \$2.8 billion in Bitcoin from criminal entities to exchanges, with just over 50% going to two specific exchanges, Huobi and Binance.²³ That's still a rounding error when you consider that, according to the United Nations, the estimated amount of money laundered globally is between 2 and 5% of global GDP, or up to \$2 trillion in current U.S. dollars.²⁴ However, this should not be an excuse and the crypto

ecosystem should continue to lead by example with ecosystem players continuing to implement strict KYC and AML processes and procedures. The data shows there is less crypto being used in illicit activities than many may expect. For example, in its annual crypto crime report, Chainalysis shows that even though 2020 represented a historic year for Bitcoin and other digital assets when it comes to trading and activity, illicit activity has dropped significantly compared to previous years.²⁵

In 2019, for instance, illicit activity represented slightly over 2% of all cryptocurrency transaction volumes, roughly equivalent to over \$21 billion, but in 2020, the share of illicit cryptocurrency activity fell to just 0.34%, or \$10 billion in transaction volume. That's a drop in the bucket compared to the \$800 billion to \$2 trillion laundered every year through traditional banks.²⁶ However, despite these astonishing numbers from the traditional financial world, the prevailing narrative is that cryptocurrencies are mainly used by criminals. But make no mistake; criminal activity is still going on, despite the inherent features of Bitcoin, including its transparency and traceability. What specific kinds of crime is driving illicit crypto activities? Scams (including Ponzi schemes) comprised most crypto crime in 2020 at 54% of all illicit activity, and such scams are not crypto-specific, but criminals often use the euphoria around cryptocurrencies to commit fraud (Fig. 2).

However, fraud numbers declined in 2020. One reason to explain this significant fall is that 2020 had nothing remotely comparable to 2019's Plus-Token Ponzi scheme, in which a group of individuals bilked investors out

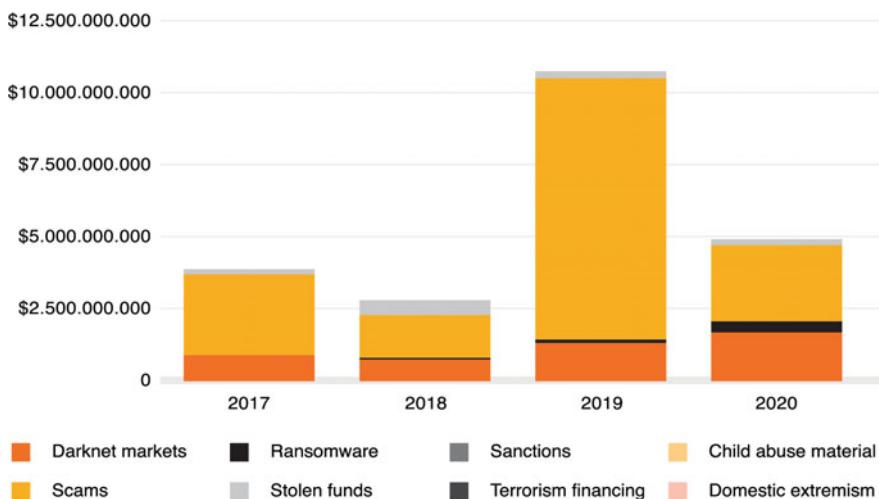


Fig. 2 Total cryptocurrency value received by illicit entities (Source "Chainalysis 2021 Crypto Crime Report," Chainalysis, 2021)

of roughly \$3 billion after promising returns of up to 30% on the PLUS token. But despite this good news, one area of concern moving forward is the role of crypto-related ransomware. After all, ransomware as a share of illicit crypto activity was virtually the one category of crime that rose from 2019 to 2020. For instance, even though ransomware accounted for only 7% of all funds received by criminal addresses in 2020 (roughly \$350 million of cryptocurrency), this still represents a massive 311% increase from 2019.

This can partially be attributed to the fact that COVID-19 forced so many organisations to quickly adopt work-from-home measures, opening themselves up to new vulnerabilities along the way. Regardless of why ransomware is on the rise, these figures should prompt swift action from law enforcement authorities, as ransomware is a uniquely destructive force that accounted for over \$20 billion in economic losses globally in 2020.²⁷ Ultimately, by understanding these year-to-year trends, crypto platforms and law enforcement can work together to make sure these numbers continue to fall.

There are fewer crypto transactions linked to criminal activities than what many believe, and the traceability features of Bitcoin and other blockchains make it difficult in practice for bad actors to launder their crypto without leaving any traces. This is why bad actors looking to avoid sanctions are trying to find new avenues, a topic that blockchain analytics firm Elliptic recently analysed²⁸ including:

- **Privacy Coins:** Elliptic's research indicates that illicit actors, especially dark web markets, are increasingly looking to privacy coins like Monero and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) included Monero, Dash, Verge, and Zcash addresses belonging to sanctioned cybercriminals²⁹ on its Specially Designated Nationals List (SDN).³⁰
- **Privacy Wallets:** Throughout 2020, the use of privacy wallets such as Wasabi Wallet for Bitcoin laundering exploded, shooting up 220% from the previous year with over \$160 million worth of Bitcoin laundered through privacy wallets in 2020 according to Elliptic. Privacy wallets are less vulnerable to law enforcement disruption than centralised mixing services, and criminals are increasingly looking to them to obfuscate funds.
- **Coinswap Services or Mixers:** Mixers are crypto-to-crypto exchange platforms that generally do not collect KYC information and are often located in high-risk money laundering jurisdictions.
- **Decentralised exchanges (DEX):** DEXs and other apps in decentralised finance (DeFi) are de facto permissionless and not regulated, meaning that anyone can access them without the need to go through KYC.

- **Crypto Mining:** Bad actors are also looking at mining their own tokens, with Iran as a good example of the crypto mining route.

Based on data collected from miners by the Cambridge Centre for Alternative Finance³¹ along with statements from Iran's state-controlled electricity company, Elliptic estimates that close to 600 MW of electricity was being used for crypto mining and that about 4.5% of global Bitcoin mining takes place in Iran, with crypto mining on that scale bringing in nearly \$1 billion in annual revenue (Fig. 3).

The important thing to remember with sanctioned countries like Iran and North Korea is that they frequently use third-party countries to hide their traces. For example, Elliptic has found that Iranian sanctions evaders have frequently looked to countries such as Turkey or Lebanon to avoid U.S. scrutiny, and both Iran and North Korea have utilised financial institutions in countries like China, Malaysia, and Singapore to elude both U.S. and international restrictions.

The good news for crypto firms is that there are a lot of red flags that they can watch out for, from identifying IP addresses or basic contact information in blacklisted jurisdictions to keeping a diligent eye out for suspicious activity on P2P trading platforms known to operate in a sanctioned jurisdiction. For example, crypto exchanges should pay attention to users that attempt to engage in indirect transactions, or suspicious transactions separated by more than one hop. Being able to identify the receiving wallet is also key, as in many cases suspicious transactions use clusters of wallet addresses. Sometimes these red flags are as simple as spotting transaction activity with entities known to

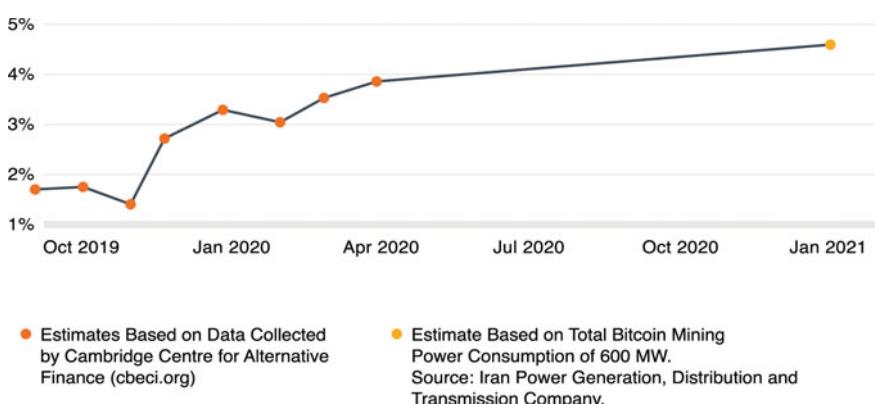


Fig. 3 Iran's share of Global Bitcoin Mining (2021) (Source "Sanctions Compliance in Cryptocurrencies: Using Blockchain Analysis to Navigate the Minefield," Elliptic, 2021)

operate in a country with a history of sanctions evasion activity, and users sending or receiving funds from an exchange that requires no KYC should always raise eyebrows. Ultimately, even though far fewer instances of money laundering or financial foul play occur in crypto markets than in the traditional global banking system,³² these issues are still a reality and addressing and tackling them is key for the future growth of the crypto ecosystem.

4 Crypto Compliance

It's important to understand that compliance is not something unique to the crypto ecosystem, as it has become part of the day-to-day reality of the traditional financial services industry as well. Compliance with AML and CTF requirements are an area of intense focus for the financial services industry and there are concerns that crypto-assets could be used to facilitate new vectors of illicit financial flows for several reasons:

- Crypto-assets may allow greater anonymity than traditional non-cash payment methods.
- The global reach of crypto-assets means that responsibility for AML/CTF compliance and supervision/enforcement may be unclear.
- Components of a crypto-asset system may be in jurisdictions that do not have adequate AML/CTF controls.³³

In the early days of crypto, volumes and users were relatively limited. As the number of Bitcoin and other crypto-asset users has increased along with volumes, this became an increased area of focus by regulators and policy-makers. Specific regulations for crypto exchanges were limited until 2018, and whilst some crypto exchanges were leading by example by self-regulating, the lack of specific guidance on the topic created much confusion and consequently risks for users, especially in the early days of the crypto industry.

The low hanging fruit of compliance is KYC. Some would argue that many crypto exchanges around the world have weak KYC, but is that the case? Once again, the best approach is to look at the data. In the early days of the industry, crypto exchanges had limited or no KYC, but the situation changed gradually as crypto became more mainstream and as regulations started to become clearer. Many of the world's leading crypto exchanges, especially those who are regulated in Tier 1 jurisdictions in North America, Europe, or Asia, have state of the art KYC/AML/CTF measures in place. In many cases these are better than what traditional financial institutions use as these

crypto exchanges had the luxury of not having legacy systems to deal with. However, the level of compliance varies depending on jurisdiction and type of exchange.

For example, Blockchain analytics firm CipherTrace analysed the Know-Your Customer (KYC) processes of over 800 crypto exchanges from over 80 countries around the globe³⁴ and even though many countries included in their analysis had existing anti-money laundering (AML) regulations, these same countries continue to host crypto exchanges, called virtual asset service providers (VASP), with either weak or outright porous KYC. For example, the report found that 56% of VASPs around the globe have weak KYC (Fig. 4).

Like any other analysis, the reality is that often some of the biggest and most high-profile exchanges are regulated and have proper KYC procedures in place, but the data shows that many of the smaller ones don't. Some of these exchanges are in regions where you would expect better regulations, where for example, breaking the issue down regionally, the data shows that Europe has the highest count of VASPs with deficient KYC procedures, with 60% of European VASPs determined to have weak KYC procedures (Fig. 5).

When looking at the weakest KYC countries in the world, CipherTrace analysts discovered that 60% of the top 10 worst KYC countries in the world are in Europe, 20% are in Latin America and the Caribbean, and the remaining 20% are in APAC countries. But the most alarming lack of KYC occurs on decentralised exchanges (DEX), with researchers finding that over 90% of DEXs within a clearly domiciled country had deficient KYC, with 81% having little to no KYC whatsoever. As we've discussed in this book, the topic of DeFi and regulations will be one to watch over the coming years. Whilst the situation is improving with many countries not only clarifying their KYC and AML requirements for VASPs but also enforcing them, we

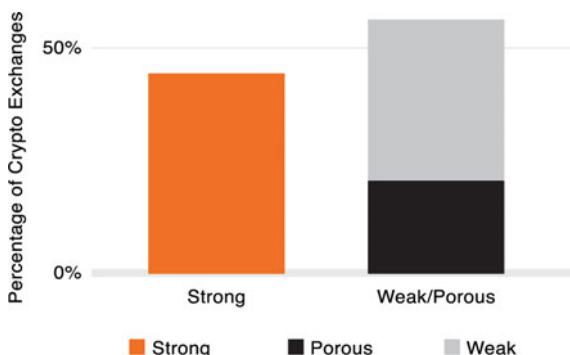


Fig. 4 Percentage of VASPs with weak or porous KYC (Source "2020 Geographic Risk Report: VASP KYC by Jurisdiction," CipherTrace, 2020)

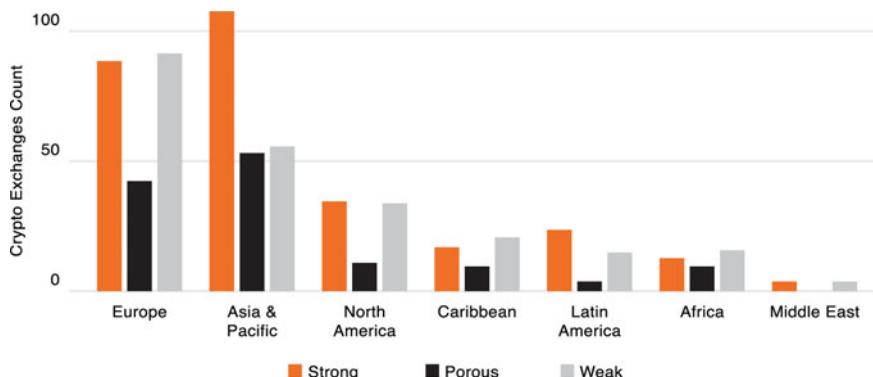


Fig. 5 Percentage of VASPs with weak or porous KYC by region (Source "2020 Geographic Risk Report: VASP KYC by Jurisdiction," CipherTrace, 2020)

should expect the gaps in KYC with crypto exchanges to improve materially over the coming years.

Law enforcement is getting increasingly involved as well. Arrests were made at exchanges like BTC-e that did not conduct KYC and were suspected of money laundering and their sites have been shut down.³⁵ Separately, a report released by the New York Attorney General in September 2018 on crypto exchanges found that many crypto exchanges lacked sufficient internal controls with regards to conflicts of interest, market manipulation, and protection of customer funds.³⁶ These developments always act as a catalyst in ensuring more players start taking topics like crypto compliance seriously. For example, to address these issues, some industry-led initiatives were launched aimed at establishing best practices for crypto exchanges. For example, in 2018, the Asia Securities Industry & Financial Markets Association (ASIFMA), an independent Asia-focused trade association, published a report with best practices that crypto exchanges could adopt. It covered listing and regulatory recommendations, as well as suggestions for KYC/AML and custodial practices,³⁷ a good example of how best practices from the traditional financial services industry could be transferred into the crypto-asset ecosystem.

The good news is that some level of KYC has now become standard practice across fiat-to-crypto exchanges, especially for those that are looking to build a long-term institutional grade business. However, there were still some crypto-to-crypto exchanges (and of course decentralised exchanges) that operate without any formal KYC mechanisms. Although there may not have been any strict regulatory requirements that required crypto-to-crypto exchanges to conduct KYC procedures, many crypto exchanges chose to

voluntarily adopt such practices, due in part to attract large institutional investors as such clients need to be comfortable with the level of compliance of their counterparties. However, many crypto-to-crypto exchanges also knew that there were serious legal risks in not conducting KYC that could result in serious criminal and other violations, thus they recognised the need to implement KYC procedures.

An important catalyst when it comes to the development of compliance in the crypto space has been the Financial Action Task Force (FATF) which started focusing on the issue of KYC and AML for crypto exchanges (which they call VASPs) in the second half of 2018.³⁸ Whilst the FATF had been looking at the KYC/AML risks with virtual currencies as early as 2014, it was in 2018 that the pace accelerated.³⁹ In October 2018, the FATF adopted changes to its recommendations to explicitly clarify that they apply to financial activities involving virtual assets, and added two new definitions, “virtual asset” or “VA” (broadly referring to crypto-assets) and “virtual asset service provider” or “VASP” (broadly referring to crypto exchanges and custodians).⁴⁰ In June 2019, the FATF adopted the Interpretative Note to Recommendation 15, which clarified how the FATF requirements apply in relation to VAs and VASPs or crypto-assets and crypto exchanges/custodians.⁴¹ This became known as the “travel rule” guidance.

The guidance from the FATF addressed the application of a risk-based approach (RBA) to Virtual Asset activities or operations and Virtual Asset Service Providers. The guidance covered a range of topics including the supervision or monitoring of VASPs for AML/CFT purposes, licencing, customer due diligence, recordkeeping, suspicious transaction reporting, sanctions, and other enforcement measures. This type of guidance has far-reaching consequences as it requires all FATF member jurisdictions to impose specified AML/CFT requirements on VASPs as well as traditional financial institutions and designated non-financial businesses and professionals like lawyers and accountants. Through membership in FATF or FATF-style regional bodies, more than 200 countries and territories were affected by the guidance. The FATF gave member countries 12 months to implement these recommendations in their home country, and as these recommendations cover both fiat-to-crypto and crypto-to-crypto exchanges and most centralised custodians, it catalysed a wave of new regulations globally for crypto exchanges, with FATF guidance taken seriously by countries and policymakers around the world. For example, being put on the FATF grey list, let alone the black-list, can cause a lot of practical headaches, from additional compliance checks done by correspondent banks to concerns from foreign investors, which is why FATF guidance matters. What the FATF did was de facto impose the

same requirements that apply to traditional financial institutions to the crypto industry.

The FATF has set-out a clear definition of a virtual asset and a virtual asset service provider. A virtual asset is defined as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets already covered elsewhere in the FATF Recommendations, but this definition includes cryptocurrencies and utility tokens that are traded on crypto exchanges. A virtual asset service provider is defined as any natural or legal person who as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- Exchange between virtual assets and fiat currencies (e.g., fiat-to-crypto exchanges)
- Exchange between one or more forms of virtual assets (e.g., crypto-to-crypto exchanges)
- Transfer of virtual assets and safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets (e.g., crypto custodians)
- Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Notably, the scope of the FATF definition includes both crypto-to-crypto and fiat-to-crypto transactions or financial activities or operations,⁴² and the FATF requires member countries to implement some of the existing FATF recommendations (e.g., Recommendation 10, Recommendation 16) for VASPs and VAs. These include recommendations on the type of due diligence that should be performed⁴³:

- VASPs should design a Customer Due Diligence (CDD) process to help them in assessing the AML/CFT risks associated with covered VA activities and customers.
- CDD must be performed in the context of establishing a business relationship or whilst carrying out occasional transactions for non-customers with a value greater than USD 1,000 or EUR 1,000.
- CDD comprises identifying customer and applying a risk-based approach to verifying customer identity using reliable and independent information, data, or documentation. Where the customer is not a natural person, the customer's beneficial ownership must be determined. The CDD process

also includes understanding purpose and intended nature of business relationship, where relevant, and obtaining further information in higher-risk situations.

- Ongoing due diligence of the customer relationship must be performed and transactions must be scrutinised.

The recommendations also cover what type of information needs to be obtained for transitions. For example, it stipulates that when a Virtual Asset Service Provider conducts a transfer of Virtual Assets on behalf of a customer, it is required to:

- Obtain and hold accurate (i.e., verified for accuracy) originator information, including customer name and wallet address, as well as other data such as physical address, date of birth, or other specified alternatives.
- Obtain and hold beneficiary information, specifically the customer's name and wallet address.
- Transmit the originator and beneficiary information to a receiving Virtual Asset Service Provider (or other obliged entity, such as a financial institution), if any. This requirement, which banks already adhere to, is known as the Travel Rule.

Originator and beneficiary information must be screened to ensure that transactions with designated persons and entities (e.g., those subject to financial sanctions) are identified, reported to competent authorities, and are subject to freezing measures.⁴⁴ These FATF developments catalysed a series of new regulatory requirements for crypto exchanges globally, and by June 2020, the FATF mentioned that 35 out of 54 reporting jurisdictions had already implemented the revised FATF Standards, with 32 of these regulating VASPs and three of these prohibiting the operation of VASPs.⁴⁵

Whilst some more libertarian-inclined advocates for crypto-assets strongly disagreed with identification requirements, arguing that they invalidate the very purpose of crypto-assets, the reality is that facilitating financial crime has negative impacts on society at large and on the popular opinion of crypto-assets. Furthermore, putting in place such measures are likely to help crypto-assets become more mainstream. In the months following the FATF guidance, many jurisdictions tried to use this as an opportunity to promote themselves and carve a niche to attract a certain type of crypto exchange. For example, Hong Kong issued a licencing framework aimed at crypto exchanges targeting institutional clients⁴⁶ and Singapore issued a similar one geared towards crypto exchanges targeting the retail market.⁴⁷ Other jurisdictions

from Bermuda to Gibraltar did the same aimed at providing a clear regulatory framework for crypto exchanges that would be a balance between investor protection and the development of the crypto industry in that market.

The elephant in the room when it came to the FATF guidance was what would happen with decentralised exchanges. As much as regulators would love to regulate these exchanges, the reality is that it is very difficult, and frankly, it would only be a stupid criminal who would spend time trading on centralised exchanges when decentralised exchanges with ample liquidity are available. Moreover, how would these FATF rules apply to the NFT space? As we have seen earlier, billions are now being traded every year in NFTs and we should expect this to be a major area of focus for policymakers globally. For example, billions are laundered every year in the art world,⁴⁸ and there's no reason why similar laundering will not take place with NFTs since due to their non-fungible nature, their value is unique and thus subject to manipulation, much like the traditional art world.

How to Run a Ponzi Scheme with a Crypto Exchange

Whilst many people are working hard on building the future of money, there are still some bad apples operating in the digital currency space. A recent example was the 2019 collapse of Quadriga, in which Canada's largest crypto exchange had to be put under bankruptcy protection after over 76,000 customers were owed \$215 million CAD (US\$160 million) after its 30-year-old CEO, Gerry Cotten, suddenly died whilst on honeymoon in India. Cotten's death, and the ensuing efforts to locate assets, exposed the extent of Quadriga's problems. It was widely believed at the time of his death that the inability to access people's assets was due to lost or inaccessible private keys, but this was not the case and Quadriga would have most likely collapsed even if Cotten had lived as the exchange was a Ponzi scheme.

By the time of his death, the platform owed approximately \$215 million CAD to clients but had almost no assets to cover these liabilities. The Ontario Securities Regulators later released a thorough report on their findings that describes the criminal behaviour that was taking place at Quadriga.⁴⁹ The report reads like a crime novel and some highlights include (some copied verbatim from the report):

- **Shady Founders:** Gerry Cotten co-founded Quadriga with Michael Patryn. According to some media reports, they met in 2003 on a website dedicated to Ponzi schemes called TalkGold.⁵⁰ Patryn had been convicted in 2005 in the United States of conspiracy to transfer identification documents in relation to an online money laundering service under his prior name, Omar Dhanani.

- **Lack of Oversight:** Cotten had sole control of Quadriga and its hundreds of thousands of clients. He ran the business as he saw fit, with no proper system of internal oversight or controls or proper books and records.
- **Fake Assets:** Cotten traded with Quadriga clients using numerous alias accounts, which he credited with fake crypto-assets and fake fiat currency through manual adjustments to Quadriga's internal ledger. With a few keystrokes, Cotten could make any amount of fake money or crypto-assets appear in his alias accounts, and he apparently regularly did so.
- **Fraudulent Trading:** The bulk of the asset shortfall (\$115 million CAD) arose from Cotten's fraudulent trading using alias accounts. Cotten sustained real losses when the price of crypto-assets changed, thereby creating a shortfall in assets to satisfy client withdrawals. Cotten covered this shortfall with other clients' deposits, basically operating a Ponzi scheme.
- **Use of Client Assets:** Cotten regularly moved clients' crypto-assets into accounts he had opened on other crypto-asset trading platforms. He lost \$28 million CAD trading client assets on such external platforms.
- **Lack of Books and Records:** Quadriga did not maintain adequate books and records regarding its operations. From 2016 onwards, Quadriga had no accounting ledger or other accounting records relating to its financial situation or the assets that it controlled.
- **Non-segregation of Assets:** Quadriga did not maintain boundaries between its own assets and those of its clients, pooling all funds together and using client assets for its own purposes. Cotten used client funds to pay operating expenses including contractor fees, IT infrastructure fees, and payment processor fees.
- **No Cold Storage:** Clients were told that Quadriga used "the tried and tested method of storing 99% coins in cold storage" and that "clients' cryptocurrency is held in secure and offline multi-signature wallets". This was untrue and misleading. Quadriga was primarily using a mix of hot wallets and other crypto-asset trading platforms to store client assets, but many of these assets were not being stored at all because Cotten was steadily depleting client assets.
- **Lack of Compliance:** Quadriga transacted millions of dollars of business in cash. One of Quadriga's major clients was a Canadian Bitcoin ATM company. The president of the company would personally deliver suitcases of cash to Cotten to fund his Quadriga account, sometimes using private jets to meet quickly. Ultimately, Quadriga received over \$20 million CAD in cash from this ATM company, which Cotten knew with this origin would not be accepted by any bank in Canada.

- **Sending Cash by Mail:** Cotton used cash to fund around \$14 million CAD of client withdrawal requests by mailing envelopes of cash across the country.
- **Fake Trading:** Quadriga touted its high trading volume on its website, stating that Quadriga was “a true market, with real orders and trades, not an artificial market designed to look appealing”. In 2018, Cotten claimed that neither Quadriga nor any Quadriga affiliate was a counterparty to any trade on the platform. This was, of course, false and Cotten was party to at least 87% of all trades in Bitcoin settled in Canadian dollars on the platform in its first full year (calculated by value), and 35% over the platform’s lifespan.
- **Misappropriation of Client Assets:** Cotten misappropriated millions in client assets to fund his lifestyle. Between May 2016 and January 2018, he transferred approximately \$24 million CAD of client funds to himself and his wife. Cotten bought a Tesla, a Lexus, a luxury yacht, a plane, a share in a private jet, and multiple properties. This Vanity Fair article on his mysterious life is worth a read.⁵¹

It's quite frustrating that such a criminal took advantage of thousands of Canadians, investing their hard-earned money into digital assets, to pull off his Ponzi scheme. The Canadian regulators made it clear that the misconduct uncovered in relation to Quadriga should not cast a cloud on the entire crypto industry. They mentioned that when properly conducted, crypto trading is a legitimate and important component of capital markets and that they remain committed to working with the industry to foster innovation. Unfortunately, bad apples will always exist so it's important to ensure that the industry continues to focus on having adequate regulatory frameworks in place whilst adopting best practices in areas like governance and transparency to minimise the risks of such incidents happening again.



18

Crypto Exchanges

Any asset class, including crypto-assets, needs a marketplace where they can be bought and sold. Equities are traded on exchanges like the New York Stock Exchange or the London Stock Exchange, and the crypto-asset ecosystem has its equivalent service providers in many shapes and sizes but broadly separated into two categories: centralised exchanges and decentralised exchanges.

1 Centralised Crypto-Asset Exchanges

Centralised exchanges operate in a way not dissimilar to the operations of an international stock exchange, matching buyers and sellers of crypto-assets and acting as middleman for all trades without revealing the identity of the buyer or seller. In many cases, they may also serve as the custodian of the assets, a role to be discussed later. A question that often comes up is how many people have accounts at crypto exchanges? A study by the University of Cambridge estimated that a total of up to 101 million unique crypto-asset users across 191 million accounts had an account at a crypto exchange as of the third quarter of 2020, with the total number of user accounts at crypto exchanges increasing tremendously from only five million five years ago.¹ That number increased significantly following the bull market of early 2021, reaching over 200 million with users from around the world entering the crypto ecosystem (Fig. 1).

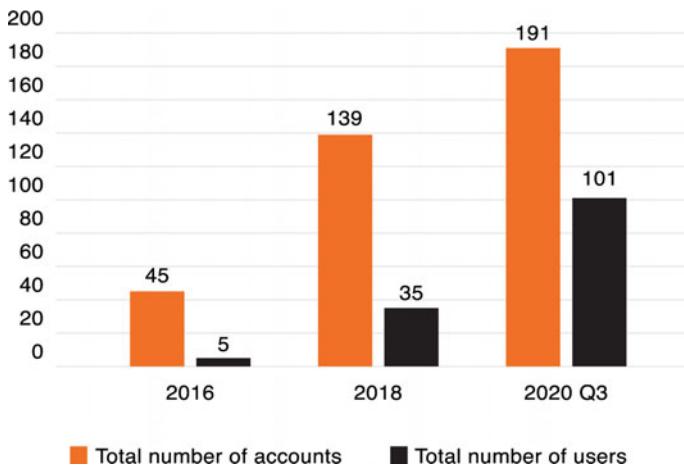


Fig. 1 Total number of crypto users and accounts around the world (2020) (Source “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)

The Cambridge University report also broke down the holders of these accounts by geography and customer type, with clients in most markets retail clients. The clear exception is in North America and Europe, where nearly one third of clients are businesses or institutions (Fig. 2).

This shows that whilst the crypto industry is global in nature, the type of institutional client is still dependent on regional particularities. When looking at centralised crypto exchanges, it’s important to note there are two main types of centralised exchanges: fiat-to-crypto and crypto-to-crypto. There are also crypto derivative exchanges that are generally part of the crypto-to-crypto exchange family.

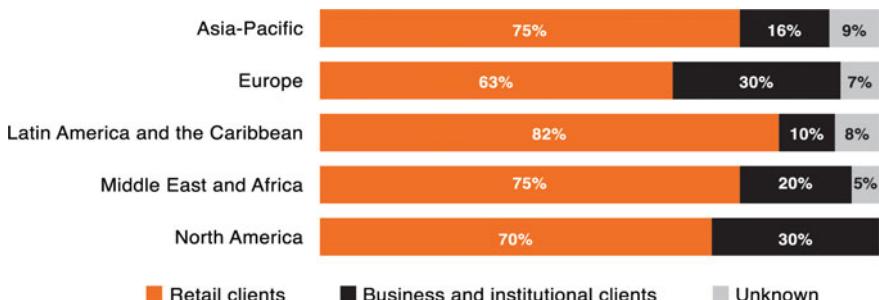


Fig. 2 Crypto customer base breakdown by region (Source “3rd Global Cryptoasset Benchmarking Study,” Cambridge Center for Alternative Finance, 2020)

Coinbase's Secret Message on the Blockchain

Coinbase's spring 2021 public listing was a major milestone in the history of digital assets, yet what may have slipped by under the radar is that Coinbase also published a secret message on the Bitcoin blockchain that references the record level of money printing around the globe. Coinbase revealed that it had asked Bitcoin mining pool F2Pool to embed a secret message that appeared in block 679,189 of the Bitcoin blockchain on the same day as its listing. The secret message refers to a recent title of the New York Times that reads "TNYTimes 10/Mar/2021 House Gives Final Approval to Biden's \$1.9T²", referring to the U.S. Congress greenlighting a \$1.9 trillion stimulus program.

Coinbase noted that their secret message is an homage of sorts to Satoshi Nakamoto, who also embedded a secret message (which refers to the UK bank bailout in the wake of 2008 banking crisis) in the very first Bitcoin block that he mined on January 3, 2009. Both hidden messages make rather oblique references to massive levels of quantitative easing and government spending, which many in the crypto community believe will lead to the continued devaluation of fiat paper money and an increase in the price of Bitcoin. Although Satoshi started the trend, other crypto miners have also used hidden messages to mark notable events in Bitcoin history. For instance, on the final block right before the Bitcoin reward halving in May 2020, a secret message was added to the blockchain that read, "With \$2.3T Injection, Fed's Plan Far Exceeds 2008 Rescue". There are numerous ways to encode messages on the blockchain, from fake Bitcoin transaction recipient addresses to miners inserting them in the blockchain field that provides for 100 bytes of arbitrary data. Messages over the years have varied from marriage proposals³ to Nelson Mandela tributes.⁴ Ultimately, this secret message from Coinbase will remain in the Bitcoin blockchain forever, and sends a strong message about the vision of the future of money that many believe in.

1.1 Fiat-to-Crypto Exchanges

A fiat-to-crypto exchange allows a user to deposit fiat funds in their account (e.g., USD, EUR, JPY) and convert that into the desired crypto-asset. For most individuals, a fiat-to-crypto exchange will be the first on-ramp to the crypto industry. This generally happens after someone hears about Bitcoin from a friend at a party or family dinner or from the news. During a crypto bull market, this can happen very fast; for example, U.S.-based exchange Coinbase opened over 100,000 new accounts over the 2017 Thanksgiving holiday,⁵ and crypto exchange Binance added 250,000 new accounts in just

Table 1 Key differences between centralised and decentralised exchanges broken down by levels of regulatory compliance, user accessibility, liquidity, and fee structures

Centralised Exchanges	Decentralised Exchanges
Regulated (at least majority)	Not regulated
KYC/AML (at least majority)	No KYC/AML required
Subject to traceability regulations (e.g. FATF)	Difficult to regulate
Easier to use, suitable for beginner traders	Suitable for individuals with significant crypto experience, not suitable for beginner traders
Liquidity depending on exchange and asset	Liquidity depending on exchange and asset
Trading fees (paid to exchange directly)	Typically lower fees (paid to liquidity providers)

an hour after it reopened its platform in 2017.⁶ The same phenomenon occurred during the first quarter 2021 bull market, which saw many new retail users enter the crypto ecosystem, with an estimate of 100 million people with an account at a crypto exchange in the third quarter of 2020, jumping to 220 million by the end of the first quarter of 2021 (Table 1).

However, operating a fiat-to-crypto exchange was challenging for many years, mainly due to the difficulties of opening and maintaining a traditional bank account. Until 2020, having a bank account with a “traditional” bank was very challenging, and there were only a handful of banks globally that were publicly comfortable dealing with crypto firms. Whilst some were in niche markets (e.g., Deltec in the Bahamas or Bank Frick in Liechtenstein), the main ones were in the United States (e.g., Signature, Silverlake).

Why Are Banks Worried About Dealing with Crypto Companies?

For many years, traditional banks were reluctant to deal with crypto companies, with a main reason was the fear of losing their correspondent banking relationships. Correspondent banking is an essential component of the global payment system, especially for cross-border transactions. Through correspondent banking relationships, banks can access financial services in different jurisdictions and provide cross-border payment services to their customers.⁷

Without this, banks would be limited to their home jurisdictions which can be quite limited in the current global context.

However, acquiring and maintaining a correspondent banking relationship, especially with the United States, is a lengthy and costly process, but also crucial considering the role of the U.S. dollar in international trade. In most jurisdictions globally, only a handful of large banks in a certain market have such U.S. correspondent banking relationships and the other smaller banks need to rely on them to access the United States (or other global markets). Until 2020, some large U.S. correspondent banks were negative on crypto-assets and would ask their counterparties around the world if they had any clients involved in crypto-assets. For this reason, no bank, especially those in smaller jurisdictions with no or almost no bargaining power, would deal with crypto clients. However, we should expect this reluctance towards crypto to gradually change over the years as many of those correspondent banks have become active in crypto.

Ironically, many fiat-to-crypto exchanges would not accept clients in the United States and would not even have a presence in the United States, but they would still bank with one of the small U.S. banks that accepted crypto clients as these banks were the only ones not worried about losing their correspondent banking relationships as they were already U.S.-based. However, this started to change in 2020 when several developments took place. First, a few large traditional banks started directly accepting crypto clients. A good example was May 2020.^{8,9,10,11}

Second was the increased crypto regulatory clarity that took place globally from 2018 to 2020 and specially in the United States in 2020. For example, in July 2020, the Office of the Comptroller of the Currency (OCC) stated that providing custody and safekeeping services for cryptocurrencies is a modern version of traditional banking services and should be allowed.¹² This generally provided comfort to more conservative banks that were cautious to deal in this space, though we're still quite far from the day when opening a bank account with a traditional bank for a fiat-to-crypto exchange is easy. Having solid banking relationships remains key for any such exchange and the situation is likely to remain the same for the short to medium term.

Fiat-to-crypto exchanges play an important role in the ecosystem as they're often the first point of entry for someone entering the crypto space. The dominant fiat-to-crypto exchanges are also often different from the dominant crypto-to-crypto exchanges. For example, in November 2021, the crypto exchanges with the biggest market share for fiat-to-crypto were Coinbase, FTX, Upbit, Kraken, and Bitfinex, quite different from the top five

crypto-to-crypto exchanges which were Binance, OKEx, Huobi, Gate.io, and Kucoin.¹³

1.2 Crypto-to-Crypto Exchanges

A crypto-to-crypto exchange does not touch handle currencies and only facilitates the exchange of one crypto-asset for another. In order to use the service, a user must send a crypto-asset to the exchange, say Bitcoin or Ether or stablecoins (which she may have gotten from a fiat-to-crypto exchange) and use that crypto-asset to buy other crypto-assets. Most people generally have their first interaction with a fiat-to-crypto exchange first needing to deal with a crypto-to-crypto exchange. However, crypto-to-crypto exchanges play a big role in the crypto ecosystem, especially so in the early days, as these exchanges were often home to a broader range of crypto-assets as they tend to not fall under the same level of regulatory scrutiny as fiat-to-crypto exchanges.

A good example is the crypto-to-crypto exchange Binance, legally incorporated in Malta but operating in over 40 countries with clients from 180 countries. As its main exchange is not regulated in any jurisdiction, it can operate freely and was able to offer over 590 trading pairs in 2019.¹⁴ In contrast, regulated fiat-to-crypto exchanges generally offer a few dozen trading pairs at most. In the early days, many of these crypto-to-crypto exchanges operated under the (perhaps naive) impression that they were not subject to regulations as they operated only in the crypto sphere and did not handle fiat currencies. For example, many crypto-to-crypto exchanges had traditionally less of a focus on KYC and AML compared to fiat-to-crypto exchanges. However, this started changing in 2018. Initially, many exchanges implemented gradual KYC that only applied when users tried to redeem funds. For example, no KYC information was required when you opened an account or when you funded it, but users had to provide identification if they tried to withdraw more than 2 Bitcoin a day. However, these were no requirements for any amount under 2 Bitcoin.

Many exchanges thought this was a good way to give comfort to regulators whilst not affecting the user experience of the onboarding process. The thinking also was that a user will be keener to provide information when she is trying to get her money back rather than at the start when opening an account. However, this approach showed a lack of understanding of basic regulations. Yes, whilst any serious criminal organisation will have a hard time laundering meaningful amounts of money if it will only stay under the 2 BTC limit a day, the reality is that there is often no *de minimis* threshold when it comes to anti-money laundering regulations. In addition, such an

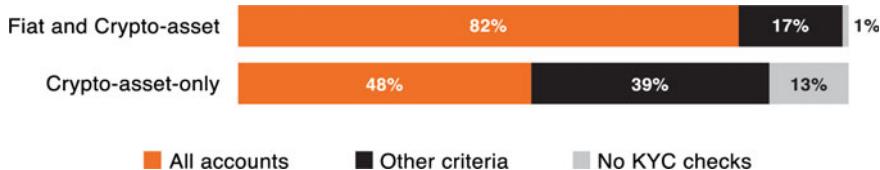


Fig. 3 Share of crypto-crypto exchanges that conduct KYC checks (Source "3rd Global Cryptoasset Benchmarking Study," Cambridge Center for Alternative Finance, 2020)

exchange may be dealing with individuals who are on a sanctioned list or from a sanctioned country, which is automatically an offence in many countries. This is why many crypto-to-crypto exchanges gradually put in place a KYC framework, and according to the latest data available, the percentage of crypto-to-crypto exchanges that do not conduct any KYC fell from 48 to 13% between 2018 and 2020 (Fig. 3).

One of the reasons was clarification from various authorities that such exchanges are not outside the law, even though they're not touching fiat currencies and only deal in crypto. A good example were the accusations from both the U.S. CFTC and the Department of Justice against BitMEX, a large crypto-to-crypto derivatives exchange, due in part to the fact that it did not have KYC in place until 2020.¹⁵ The fact that criminal procedures were taken against BitMEX was a reminder to the entire industry that not taking this seriously can have serious consequences.

1.3 Crypto Derivative Exchanges

Derivatives also exist in the crypto space and as is the case in the traditional financial services industry, volumes in crypto derivatives are quite significant. For example, since January 2021, the monthly volumes of Bitcoin futures alone has been over \$1 trillion a month, many times the volume of spot Bitcoin. Data shows that the ratio between spot Bitcoin and Bitcoin futures is between 0.2 and 0.4,¹⁶ and whilst there are now regulated Bitcoin futures offered by players like the CME, the reality is that the majority of Bitcoin and crypto derivatives takes place in crypto-to-crypto exchanges like Binance, FTX, and BitMEX.

One reason for the liquidity on such platforms as that's where such instruments have been trading for many years, with regulated products like that of the CME being relatively new. The story behind crypto derivatives is quite interesting.

The Invention of the Perpetual Swap

In May 2016, a relatively new crypto exchange called BitMEX announced the launch of a new product called the perpetual swap. This innovative product would end up playing an outsized role in the development of crypto markets. The XBT/USD leveraged swap (XBT is like BTC) product allowed traders to trade on the Bitcoin/USD exchange rate with up to 100× leverage with no expiration. The perpetual swap was an innovative development and a new type of financial derivative, with the logic behind it being that if crypto markets operate 24/7, 365 days a week, then why should crypto derivatives operate in outdated traditional futures products with expiration dates that are tradeable only during business hours? Or to put it differently, in a market that never stops, why should a crypto futures product need to expire?

Whilst the perpetual swap offered many of the traditional benefits of derivatives, like leverage or the ability to trade without the need to hold the underlying asset, its real innovation came from how it dealt with the basis risk. For example, unlike futures contracts where the price can sometimes deviate from the spot underlying price (commonly referred to as basis), perpetual swaps had to be closely pegged to the underlying assets they track. This was addressed by introducing something called a “funding rate mechanism”, which you can think of as either a fee or a rebate for traders to hold their positions. This is where the “perpetual” in “perpetual swap” comes into play.

To ensure that the contract matches the price of Bitcoin, holders either pay or receive funds every eight hours depending on the position they took (long or short) and whether the swap price is higher or lower than the price of Bitcoin. Before long, other exchanges took notice and began their own copycat models with Bybit, OKEx, Binance, FTX, Huobi, and many others following BitMEX’s lead and releasing their own perpetual swap products between 2016 and 2020. The perpetual swap has been a success with over \$3 trillion traded on the BitMEX platform alone, with the crypto derivatives space growing since the first BitMEX 2016 announcement. This is definitely an area to watch as the crypto derivatives space will grow over the coming years as more institutional investors and funds enter the crypto space.

Regulatory Challenges

However, despite its innovative features, there has been a lot of backlash as well. The BitMEX exchange has been involved in numerous regulatory investigations and legal proceedings in recent months, with its founders about

to face trial in the coming months. In addition, many regulators, from the UK to Hong Kong, have explicitly banned retail investors from trading such instruments due to the risks they may present. Many countries have imposed restrictions against crypto derivatives trading for retail investors,¹⁷ with Hong Kong¹⁸ and the UK¹⁹ two such examples.

Many crypto derivatives platforms also ban clients from the United States²⁰ However, verifying compliance with these rules can be challenging without investigating the actual clients of those exchanges, especially since users can easily use VPNs to mask their real location. Research firm Inca Digital published an insightful report in which they argue that derivatives traders operating on the major derivatives platforms and where those traders reside are far more diverse than what is often divulged by the exchange operators.²¹ By using a mix of Twitter identification, geotagging, API geodata, language identification, and multi-language Geographical Named Entity Recognition models, the report tries to paint a portrait of where these traders are from. It's worth looking into each of these techniques separately and how they're employed to verify customer backgrounds.

The first technique is geotagging. For example, from a sample of 2,939 unique Twitter users engaged in derivatives trading on FTX, Huobi Futures, Binance Futures, OKEx, Bybit, Bitfinex, and BitMEX, Inca Digital successfully identified the locations of 2,164 traders around the globe, with 372 from the United States. This is revealing, as most crypto derivatives platforms explicitly ban U.S. customers. The second approach is to look at Twitter API geodata. For example, researchers can use geolocation metadata, which is found in the tweet itself or in the user's bio. This once again demonstrated that many of the clients could be from the United States, but also Indonesia, Turkey, and India, countries that have not always been the most favourable to the crypto industry. A third tool to employ is the language identification technique, which relies on utilising geographically isolated languages to identify where a user lives. The data collected using this method is different from the Twitter API metadata and provides unique information that can be combined with other sources of data to give a glimpse into the specific locations of retail traders. In some cases, a regional dialect of a language is often characteristic of a unique location, which makes geotagging even more precise. This can be observed with Turkish and Japanese, for example. The final technique is Named Entity Recognition (NER), one of the most sophisticated strategies and given how much data this route can provide, it's not terribly surprising that NER requires an extremely extensive collection of speech samples along with geographic tags.

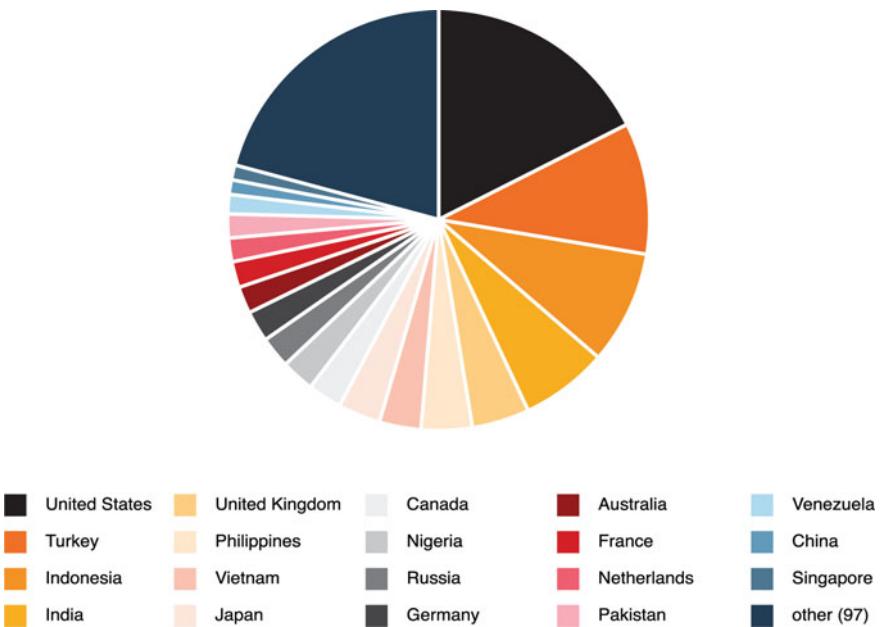


Fig. 4 Share of crypto derivatives trading by country (Source Christina Tkach, Sofia Sedlova, Evgeny Dmitriev and Adam Zarazinski, "Geotagging Crypto Derivatives Traders With NLP," Inca Digital, 2021)

The fascinating thing about NER is that it uses information submitted by Twitter users, everything from references to a local bar or cafe to traffic clogged streets, to accurately predict the true residencies of derivatives traders, revelations that occasionally directly contradict the statements made by those traders over the course of the KYC onboarding process at their trading venue of choice. The real magic happens when you combine all these different methods, with this graph showing the most popular residencies of crypto derivatives users (Fig. 4).

Crypto derivatives have been in the news for some time now and we should expect regulators to take a closer look at these platforms, as many regulators believe that such products are of higher risk than traditional spot exchanges.

2 Decentralised Crypto-Asset Exchanges

As we saw earlier in the decentralised finance chapter, decentralised crypto exchanges operate somewhat differently from their centralised counterparts. Instead of acting as a middleman, trading takes place directly between buyers and sellers. Decentralised exchanges saw tremendous growth starting in the

summer of 2020 as part of the overall surge of interest and awareness in DeFi. Centralised exchanges have many benefits, including that they are increasingly regulated, suited for retail investors with customer support and often offering other services like custody, perfect for beginner traders.

Decentralised exchanges achieve the same goal of letting you buy or trade digital assets but do so in a different way as there is no central counterparty. Trades are done peer-to-peer between two users using smart contracts and each user manages their own assets in individual wallets. These exchanges are normally suited for more advanced traders as individuals new to the crypto world first dip in a toe using centralised exchanges. Decentralised exchanges have numerous advantages in terms of lower fees or being permissionless; however, they are also more complex to use, particularly for the average retail investor.

Whilst most crypto trading has taken place on centralised exchanges, trading volumes on decentralised exchanges began rapidly rising in summer 2020. As of August 2020, on certain days, the daily volume on a decentralised exchange like Uniswap was even higher than that of established centralised exchanges like Coinbase.²² Whilst decentralised exchanges still represent less than 10% of volumes of centralised exchanges, we should not be surprised to see their market share rise over the coming years.

It will be interesting to watch the evolution of decentralised crypto exchanges over the coming years. We should expect traders and the broader crypto ecosystem to be more comfortable with such decentralised exchanges, but the big unknown is whether the rise of decentralised exchanges will increase the crypto trading pie or will it simply chip away from the revenues of centralised exchanges?

What Is the Role of Crypto OTC Brokers?

It's important to mention the role played by OTC brokers in the crypto-asset ecosystem. Each trade that a buyer and seller conduct on an exchange is known to the world (although the identity of the buyer and seller is typically only known to the exchange). This can present a challenge to anyone seeking to conduct a very large transaction, as that large transaction may move markets. For this reason, individuals or institutions seeking to conduct large transactions (often called block trades) will often use an OTC desk. These are brokers that are regularly in touch with large institutional investors and can match a buyer and a seller (in exchange for a fee) or simply buy it from a seller (placing it on their own balance sheet) with the objective of reselling it at a higher price in the near future. In many cases, these brokers are also

able to put together customised products (e.g., crypto derivative, customised basket) tailored to the needs of a certain investor.

3 Cybersecurity and Hacking Considerations

3.1 Inherent Risks with Crypto-Assets

When people think about crypto-assets, one of the things comes to mind are hackers, and they're right. In the traditional financial services world, transactions can be easily blocked or reversed in the event of a hack. Banks and other financial intermediaries have decades of experience and proper cybersecurity protocols and procedures in place. If I hack someone's account and start transferring those funds, the various banks in the process would be able to quickly freeze the relevant accounts and even reverse the transactions (unless they have been "cashed out" from an ATM). Hacks in the crypto space more resemble the mythical bank robberies from the movies where a criminal steps into a bank and leaves with a bag of cash.

As we discussed earlier, once you hold Bitcoin (or hold the private keys to be precise), it's almost impossible for anyone to reverse it or take it from you, with certain specific exceptions. For example, the Ethereum blockchain conducted a hard fork after the 2016 DAO hack, which allowed the ecosystem to "go back in time" as if the hack never happened. Crypto exchanges play the de facto same role as traditional banks by being able to block suspicious transactions. For example, following the 2020 Twitter hack, crypto exchange Coinbase blacklisted the hacker's wallet address and was able to prevent more than 1,000 customers from sending over \$250,000 dollars in Bitcoin.²³

Lastly, the traceability tools that exist now in the crypto space are becoming increasingly good at tracing transactions. The reality is also that the industry (and users) is becoming better at preventing such attacks. So, whilst the number of attacks may increase, the actual amount stolen by hackers is going down. For example, 2018 saw six attacks with almost \$900 million dollars stolen. In 2019, whilst the number of attacks rose to 11, hackers were able to steal less than \$300 million dollars (Fig. 5).



Fig. 5 Notable decentralised exchange hacks (Source "Chainalysis 2021 Crypto Crime Report," Chainalysis, 2021)

3.2 Centralised Crypto Exchange Hacks

The honey pots that hackers have and will continue to target are crypto exchanges, the reason being that many centralised crypto exchanges also act as the custodian of their clients' crypto-assets. Anyone looking to trade crypto-assets must first send assets to a crypto exchange in order to make a trade, and many clients will also leave their crypto-assets with these exchanges out of convenience.

Thus, crypto exchanges are prime targets for hackers, and many early crypto exchanges were not built with cutting-edge cybersecurity in mind they weren't expecting to handle the volumes and growth they've seen in recent years. This is why many exchanges have been hacked in recent years and why we should expect more to be targeted by hackers.²⁴ The 2013 hack of Mt. Gox, which was at one point handling around 70% of global Bitcoin trading, was a significant setback for the global crypto ecosystem with US\$473 million of Bitcoin stolen. There have since been dozens of other similar hacks, from Hong Kong's Bitfinex, which was robbed of US\$72 million worth of Bitcoin in 2016, to Japan's Coincheck,²⁵ robbed of approximately US\$420 million in 2018. However, the good news is that exchanges are becoming much better at securing themselves; most have ramped up security measures by adding additional verification layers for withdrawals and better monitoring of suspicious activities to increasing their use of cold storage and multi-signatory measures (Fig. 6).

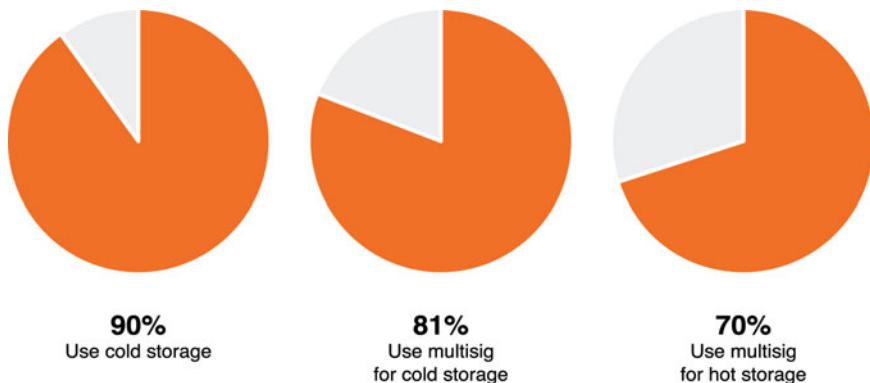


Fig. 6 Share of storage offering throughout the crypto exchange ecosystem (Source "3rd Global Cryptoasset Benchmarking Study," Cambridge Center for Alternative Finance, 2020)

3.3 Decentralised Crypto Exchange Hacks

Not surprisingly, there are also hackers targeting decentralised finance applications and protocols. Whilst there is no centralised counterparty or custodian in DeFi as is the case with centralised crypto platforms, many hackers have tried and will continue to try to exploit bugs in those protocols. A good example involved two attacks on the bZx lending platform in February 2020, which allowed the attacker to drain ETH worth hundreds of thousands of dollars from the platform.²⁶ But by far the biggest was the August 2021 \$600 million hack of Poly Network. The story of this hack is worth sharing as the hacker...ended up returning the funds!

On August 10, 2021, a hacker absconded with \$612 million worth of cryptocurrency from cross-chain DeFi protocol Poly Network, making this the largest theft ever from a DeFi protocol. What's remarkable with this hack is the chain of events from start to finish. On August 9, the hacker transferred privacy coins Monero (XMR) to a Chinese exchange called Hoo.com and then withdrew ETH/BNB/MATIC coins required to pay for the gas fees of the hack transaction.²⁷ The technical details of how the hacker pulled off the hack are beyond the scope of this book, but in short, he exploited a vulnerability between contract calls in the network²⁸ and stole over a dozen types of different crypto-assets, including cryptocurrencies and stablecoins from three different blockchains: Ethereum, Binance Smart Chain, and Polygon.²⁹ In a bizarre twist of events, a user then warned the attacker that his USDT stolen during the hack had been frozen and in exchange for this info, the hacker would tip 13.37 ETH (approx. \$44,000) to the user. It's important to remember that some stablecoins have a feature in place to freeze certain

accounts, and that's exactly what Tether did when it froze \$33 million of USDT taken by the hacker.

After realising that a hack had occurred, Poly Network published the addresses holding the stolen assets and asked miners and exchanges to "blacklist" any tokens coming from those addresses.³⁰ The attacker tried to "launder" the gains by swapping stolen DAI and USDC via the DeFi exchange Curve back to the decentralised stable coin DAI, probably to lessen the chances of being caught.³¹ Wanting to contact the hacker, the Poly Network team posted a message on Twitter addressed to the hacker that urged them to return the stolen funds as quickly as possible.³² Normally in such hacks, the hacker tries to lie low and wait until the dust settles, but that was not the case this time, possibly due to the large scale of the hack and the focus of the global crypto community on the story.³³ Even an attack as carefully planned as this one will still leave traces, and as I've mentioned before, if you're a criminal, trying to launder large amounts of crypto is very difficult, especially after such a public hack.

For example, shortly after the attack, the blockchain security firm SlowMist announced it had identified several pieces of information associated with the hacker, including their mailbox, IP address, and device fingerprints through on-chain and off-chain tracking.³⁴ Perhaps seeing this, the hacker then began communicating with Poly Network by using the transaction input data function on the Ethereum blockchain, sending the message "READY TO RETURN THE FUND!"³⁵ In response, Poly Network wrote a message on Twitter that included three addresses where the hacker could send the funds.³⁶ And as if things couldn't get any wackier, the hacker began a series of Q&As, again using the transaction input feature.³⁷ In these Q&As, the hacker explained his motivation behind the hack and then transferred nearly all the \$611 million in stolen funds, except for the frozen USDT. The Polygon network would start referring to the hacker as a "White Hat" hacker. As a sign of good faith, the Poly Network even offered the hacker a bounty of \$500,000 worth of ETH and offered to hire him as their chief security advisor. Whilst the hacker claims that they always had good intentions, that's difficult to verify. For example, would he have come forward as a White Hat hacker if it was not announced that a lot of his personal information had already been identified?³⁸

Separately, from a practical perspective, the reality is that it would have been almost impossible to launder such a big amount of crypto. The crypto traceability tools these days are advanced, and whilst the hacker could have traded on various DeFi platforms, cashing it out to fiat would be difficult. In addition, chances were high that he would have been identified, so playing the

White Hack card was probably wise. After all, there aren't that many people around the globe that have the crypto + DeFi + programming + cross-chain protocol + hacking expertise on display here who could execute such a heist. The reality is that we should expect DeFi hacks to continue to take place.



19

Crypto Funds

The global asset management industry is estimated to be around \$89 trillion dollars,¹ and serves an important purpose as it allows not only retail investors to put their money to work, but also allows institutional investors to allocate client funds. However, only a tiny fraction of that \$89 trillion even touches crypto-assets. whilst difficult to get an exact amount, it's safe to say that the total crypto-asset management sector in 2020 is less than \$10 billion dollars, whilst the global crypto hedge fund industry was estimated by PWC at around \$2 billion dollars in 2019 and under \$4 billion dollars in 2020.² The sector has probably grown following the bull market of 2021, but it's still a rounding error in the \$3 trillion dollars that the global hedge fund industry is estimated to be.³

What does Warren Buffett think of Bitcoin?

As you might imagine, the Sage of Omaha is not a big fan of Bitcoin. The billionaire CEO and Chairman of Berkshire Hathaway has made this clear numerous times in the past, referring to Bitcoin as “rat poison squared” and arguing that the asset has no value and only attracts “charlatans.” Buffett came roaring right back into the crypto news sphere when he and his Vice Chairman, Charlie Munger, discussed Bitcoin during Berkshire Hathaway’s annual shareholders meeting in May 2021. Munger, who is somehow even more anti-Bitcoin than Buffett, didn’t hold back during the meeting, claiming that Bitcoin is only used by “kidnappers and extortionists” whilst adding, “I

think I should say modestly that the whole damned development is disgusting and contrary to the interests of civilization".⁴ What's interesting about Buffett and Munger's comments that Bitcoin is "contrary to the interests of civilization" is that Berkshire Hathaway has had no issue at all investing heavily in arguably some of the most scandal plagued industries in the world, from fossil fuels to traditional banking. Meanwhile, Buffett and his firm have come under direct criticism over opaque corporate governance, with critics accusing Berkshire Hathaway's board of a lack of independence, with many of the sitting members coincidentally happening to be long-time friends of Buffett. This criticism has become especially pointed in the weeks leading to the annual meeting, with *The Economist* calling for him to step aside and make way for the next generation of leadership at Berkshire Hathaway.⁵ Ironically, this call for Buffett to move on came in an issue with central bank digital currencies featured prominently on the cover.

It's estimated there are hundreds of crypto funds, ranging from those who invest only in tokens to those who offer passive exposure to the crypto ecosystem's largest assets by market capitalisation.⁶ If the interest in crypto-assets by institutional investors continues to grow, we should expect to see an increasing number of crypto funds, that is, funds set up specifically to invest in crypto-assets.

A good example to look at is crypto hedge funds. For example, according to data from PwC at the time of writing, most investors in active crypto hedge funds (90%) are either family offices (48%) or high-net worth individuals (42%). The ticket sizes also tend to be quite small, with the median ticket size US \$0.3 million and average ticket size US \$3.1 million, and with almost two-thirds of crypto hedge funds with average ticket sizes below US \$0.5 million and with a median of 28 investors.⁷ However, it's important to understand that there are various kinds of funds that relate to the crypto industry and that can often be confusing. Whilst they're all "crypto funds", the way they operate is different depending on the type of fund.

How are Crypto-Assets Valued?

The highly varied nature of crypto-assets creates challenges for their valuation, with the unique characteristics of each token informing the appropriate valuation technique. An entire book could be written on the methodologies and challenges of valuing crypto-assets, but we present here a generalised high-level framework:

- Cryptocurrencies are typically priced by the traditional metrics of supply and demand used in the valuation of currencies. For example, given there are only a limited number of Bitcoin in circulation and if there is more demand, then the price of a Bitcoin should increase.
- Security tokens can be valued using traditional financial techniques. The specific technique will differ depending on the underlying asset or financial instrument represented by the token. For example, the appropriate valuation technique or a piece of real estate would differ from that of a bar of gold or a share of equity.
- Utility tokens are probably the most complicated to price today as there are no established frameworks. There are several individuals who have started to develop frameworks to value the economics of utility tokens⁵⁸⁴, a mix of traditional valuation methods that try to integrate the network effects of platforms and the particularities of blockchain technology. If the popularity of consumer tokens accelerates, the valuation methodologies for these assets is likely to evolve significantly.

1 Active Crypto Funds

Active crypto funds are funds that are set up with the goal to invest in crypto-assets and are actively managed, meaning there are individuals who make decisions on what crypto-asset to buy, sell, or invest in. This is compared to a passive fund where the portfolio composition is predetermined (e.g., index) which we will explore later.

There are four broad categories of active crypto funds⁸:

- **Discretionary Long Only:** Funds which are long only and whose investors have a longer investment horizon. These funds tend to invest in early-stage token/coin projects, and also buy and hold more liquid cryptocurrencies. These funds tend to have the longest lock-up periods for investors and are often referred to as “long only crypto hedge funds”.
- **Discretionary Long/Short:** Funds which cover a broad range of strategies including long/short, relative value, event driven, technical analysis, and some strategies which are crypto specific, such as mining. Discretionary funds often have hybrid strategies which can include investing in early-stage projects, and are often referred to as “crypto hedge funds”.
- **Quantitative:** Funds taking a quantitative approach to the market in either a directional or a market neutral manner. Indicative strategies include market-making, arbitrage, and low latency trading. Liquidity is key for

these strategies and restricts these funds to trading only more liquid cryptocurrencies, and are often referred to as “crypto quant funds”.

- **Multi-strategy:** Funds adopting a combination of the above strategies. For instance, within the limitations set in the prospectus of a particular fund, traders may manage discretionary long/short and quantitative subaccounts.

In PwC, Elwood, and AIMA’s most recent Annual Global Crypto Hedge Fund Report, several trends indicate that the crypto hedge fund industry is developing quite rapidly.⁹ The report found that the total AuM (Assets under Management) of crypto hedge funds around the world increased from US\$2 billion to nearly US\$3.8 billion between 2020–2021, and the percentage of crypto hedge funds with over US\$20 million in AuM saw a year-over-year increase from 35 to 46%. Moreover, the average AuM saw nearly a US \$30 million increase to US \$42.8 million, whilst median AuM rose from under US \$4 million to US \$15 million (Table 1).

It should also be noted that crypto hedge funds had some very impressive returns in 2020 (the most recently surveyed year.) When it comes to investor type, most investors in the crypto hedge fund space are either high-net worth individuals (54%) or family offices (30%) (Fig. 1).

The report also shows that the most used crypto strategy is quantitative (37% of funds), followed by discretionary long/short (28%), discretionary long only (20%), and multi-strategy (11%) (Fig. 2).

Not surprisingly, most crypto hedge funds are trading Bitcoin/BTC (92%) and Ethereum/ETH (67%), but it’s interesting to see many funds are trading some of the newer protocols or DeFi tokens, like Chainlink/LINK (30%), Polkadot/DOT (28%), or Aave/AAVE (27%) (Fig. 3).

Whilst half of crypto hedge funds surveyed trade derivatives (56%), short-selling has fallen dramatically, plummeting from 48% in 2019 to 28% in 2020, probably driven by the overall bullish sentiment by most crypto hedge funds. Crypto hedge funds are also quite active in a broader range of activities like staking (42%), lending (33%), and borrowing (24%) (Fig. 4).

Table 1 Average and median AuM of crypto hedge funds

	Average	Median
2020 year-end AuM (US\$m)	42.8	15.0
2019 year-end AuM (US\$m)	12.8	3.8
AuM level at launch (US\$m)	11.3	1.0



Fig. 1 Most common investors in crypto hedge funds (Source "3rd Annual Global Crypto Hedge Fund Report," PwC, 2021)

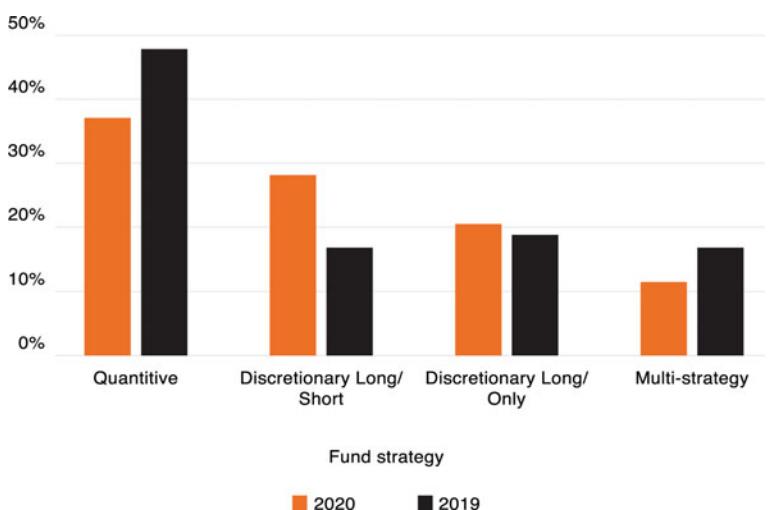


Fig. 2 Most commonly adopted strategies of crypto hedge funds (Source "3rd Annual Global Crypto Hedge Fund Report," PwC, 2021)

What Fees do Active Crypto Hedge Funds Charge?

Like any new niche asset class that requires a specialised skill set, crypto funds can charge higher fees. For example, the data indicates that the median active crypto fund has management and performance fees of 2% and 20% respectively and an average of 2.3% and 21.1%, higher than a typical traditional/non-crypto hedge fund would be able to charge today. It's likely that these fees will go down over the coming years as there are

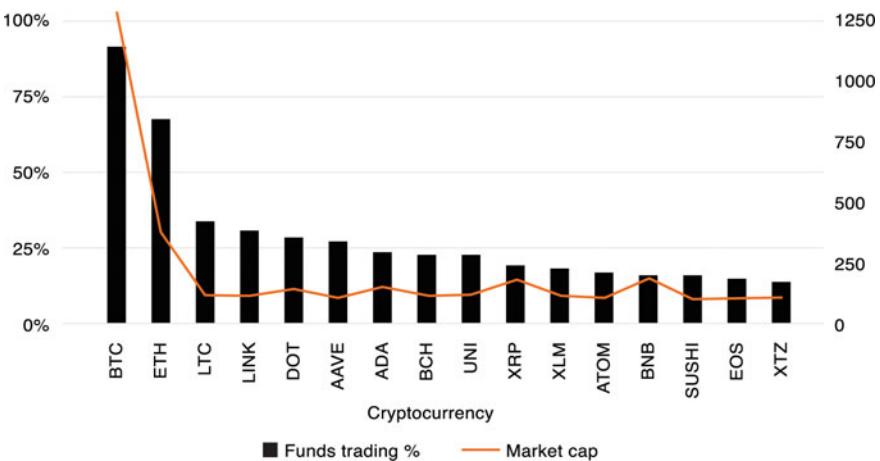


Fig. 3 Cryptocurrencies most commonly traded by crypto hedge funds by market cap (Source "3rd Annual Global Crypto Hedge Fund Report," PwC, 2021)

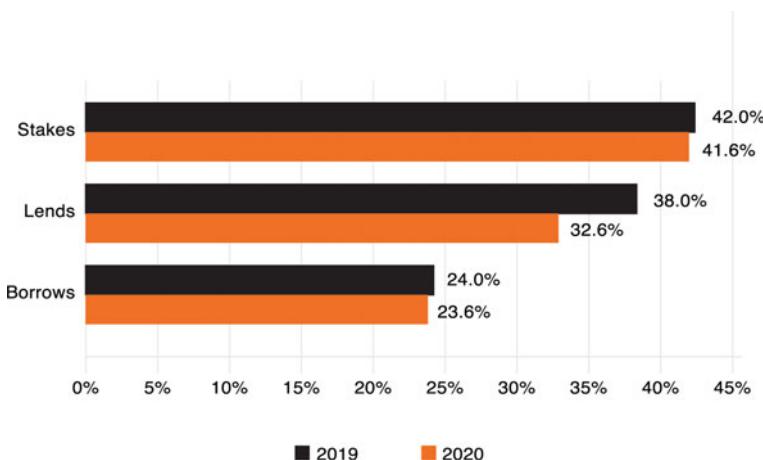


Fig. 4 Percentage of crypto hedge funds involved in staking, lending, and borrowing (Source "3rd Annual Global Crypto Hedge Fund Report," PwC, 2021)

more institutional-grade funds available for investors, competition increases, and investors are becoming more comfortable with the asset class. The same phenomenon happened with traditional hedge funds over the past 20–30 years.

There is nothing unique about the setup of such funds. The setup of a crypto fund is identical in many regards to that of a traditional hedge fund or

venture capital fund with the only difference being that the assets it invests in are crypto-assets. For example, these funds tend to be domiciled in the same jurisdictions as traditional hedge funds, with the top three being the Cayman Islands (34%), the United States (mainly the state of Delaware, 33%), and Gibraltar (9%). The fund managers managing these funds are also often based in the same financial centres. For example, most crypto hedge fund managers are based in the United States (43%), followed by the United Kingdom (19%) (Table 2).

Are Crypto Funds Becoming More Institutionalised?

Similar to the rest of the industry, crypto funds are becoming increasingly institutionalised. And this institutionalisation is happening very fast as many of these funds are adopting the best practices implemented by the traditional funds industry over the past 20 years. For example, the PwC-Elwood annual crypto hedge fund report showed that 86% of such active crypto funds were using an independent fund administrator in 2019, something that was not the case prior to the 2008 financial crisis and in particular the Bernard Madoff fraud.

The same phenomenon applies when it comes to governance. For example, the percentage of active crypto funds using an independent custodian increased from 52 to 81% from 2018 to 2019, and in addition, the percentage with at least one independent director on their board increased from 25 to 43%. This means that many of these crypto funds have simply started at a higher level of institutionalisation compared to their traditional peers at the same stage of their evolution. This is positive as it will make it easier for such funds to receive capital from institutional investors.

Over the coming years, it would not be surprising to see the number and diversity of these funds expand significantly. Not only could some of the established names in the fund management industry potentially launch their

Table 2 Top crypto hedge fund domiciles and top crypto hedge manager locations

Top Crypto Hedge Fund Domiciles	Top Crypto Hedge Manager Location
Cayman Islands	34%
United States	33%
Gibraltar	9%
British Virgin Islands	8%
Luxembourg	3%
Liechtenstein, Netherlands, Singapore, Isle of Man and Australia	< 5%
	United States United Kingdom Hong Kong Cayman Islands Switzerland Spain, Gibraltar, Singapore, Isle of Man, Malta, Canada and Australia
	43% 19% 11% 8% 7% < 5%

own crypto funds, but some of the existing large crypto players may continue to expand their offerings with the goal of capturing that small percentage of a diversified portfolio that investors may want to allocate to crypto-assets.

2 Passive Crypto Funds

A passive crypto fund is a fund that employs a passive strategy like tracking an index. There are no active decisions made nor discretion given to a human; the fund simply needs to buy the assets of that index at the specified weighting. If a certain index goes up, then the fund should go up proportionally. As the crypto industry is still in its (relatively) early days, many passive funds have actually built their own index or have clearly set out in their prospectus what is the composition of the index they use. It's also important to know that there are also single asset funds and in recent years have been the most popular. For example, Grayscale is a firm that has several such products.¹⁰ Its Grayscale Bitcoin Trust product has already several billion dollars in AUM at the time of writing. Such products allow investors to buy a traditional product that gives them exposure to this new asset class (Fig. 5).

There are many reasons why someone would want to buy into a passive crypto product rather than one that is actively managed. For example, some investors may simply want exposure to the asset class without the need of an active manager making investment decisions. One interesting distinction with the traditional world of finance is that passive funds are not necessarily substantially cheaper than actively managed ones. For example, the Grayscale products have management fees between 2–3%, far from the S&P ETFs that traditional investors have gotten used to that charge minimal fees and in some cases, no fees at all.¹¹ However, many passive funds offered via private placement (and with minimum investment thresholds of often \$50,000 or \$100,000 depending on the jurisdiction) have fees that are lower but rarely lower than 1%. Interestingly, a substantial amount of the inflows into such passive products have been from institutional investors like traditional hedge funds, with almost 80% of the inflows coming into Grayscale products from institutional investors (Fig. 6).

The passive crypto investment world is one that should grow significantly over the coming years. The big game changer here will probably be the approval of one of the various Bitcoin ETFs. The first Bitcoin ETF application was submitted in 2013 by the Winklevoss twins¹² and there have been some Bitcoin ETF or ETF-like products available on exchanges in Bermuda, Gibraltar, and Toronto.¹³ The major development that the industry has been



Fig. 5 Grayscale's cumulative quarterly inflows (2020) (Source "Grayscale Q3 2020 Digital Asset Investment Report," Grayscale Investments, 2020)

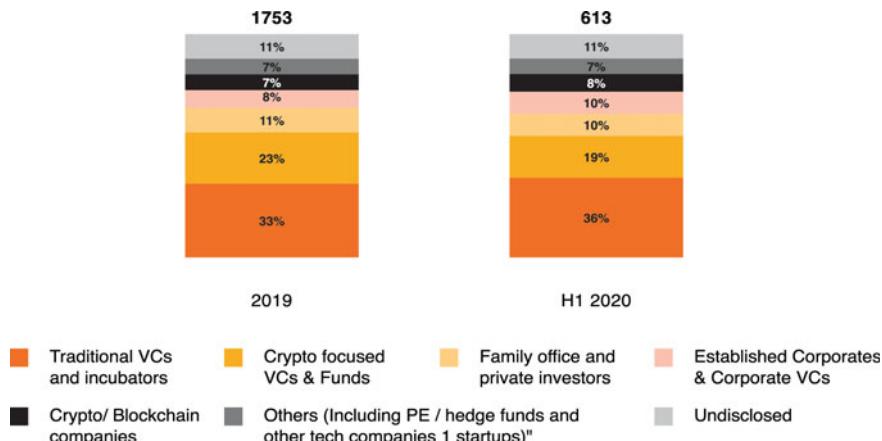


Fig. 6 Venture capital crypto funds (Source "3rd Annual Global Crypto Hedge Fund Report," PwC, 2021)

waiting for is the approval of such a product in the United States, which being the biggest capital market in the world, could have a meaningful impact on the price of Bitcoin and other digital assets.

3 Crypto ETFs

October 2021 featured another historic milestone for Bitcoin and the crypto ecosystem with the listing of the first Bitcoin ETF in the U.S. ProShares Bitcoin Strategy ETF, under the ticker BITO, launched on the New York Stock Exchange on October 19 and surpassed \$1 billion in assets after two days, making this one of the most successful launches of all time, sending the price of Bitcoin to a new all-time high along the way. This was followed by the Valkyrie Bitcoin Strategy ETF going live shortly after the ProShares launch under the ticker BTF on NASDAQ. This was exactly the moment the crypto ecosystem had been waiting on for some time.

But are these the first Bitcoin ETFs? In the United States, yes, but globally, no; there have been Bitcoin ETFs in Canada, for example, and many other ETNs/ETPs in Europe and elsewhere. Also, it's important to remember that neither the ProShares nor the Valkyrie ETFs will hold physical Bitcoin. In this case, the U.S. SEC was not as bold as their Canadian counterparts, where the ETFs that have launched actually hold physical Bitcoin. Rather, U.S.-listed Bitcoin ETFs will hold cash-settled Bitcoin futures listed on the CME, meaning there is no physical Bitcoin delivery at the expiry of those underlying futures contracts. But is this still a very important development? Absolutely. First of all, the launch of the ProShares and Valkyrie ETFs allows a broader swathe of American investors to gain exposure to Bitcoin via an instrument that is common and on a regulated exchange, like the NYSE and NASDAQ. Many investment advisers traditionally had restrictions in investing in Bitcoin and crypto for their clients for various reasons, including:

- Spot Bitcoin being outside the investment instruments they're allowed to trade
- Crypto trading taking place on unregulated exchanges
- Crypto could not be included as part of a 401(k)
- Tax considerations were somewhat ambiguous.

All of these issues disappear with these new Bitcoin ETFs. However, there are also downsides to keep in mind, fees for instance. The ProShares ETF has an expense ratio of around 0.95%, and there are a lot of embedded costs in

running a futures ETF, like the cost of rolling over the futures at expiry, and so holding spot Bitcoin directly may be the preferred option for many investors. However, there's a segment of the market for whom a Bitcoin ETF will be appealing. In the meanwhile, now that the first ETFs are up and running in the United States^S, there are several areas I'm paying close attention to, notably:

- **Inflows:** The ProShares Bitcoin ETF had a very strong start, but will these inflows and trading volumes continue?
- **Competitors:** Many other firms have applied for Bitcoin ETFs, so it will be interesting to see what interest they generate when they launch.
- **Impact on Bitcoin price:** These Bitcoin ETFs buy cash-settled futures, but that still has an impact on the spot price due to normal arbitrage and price discovery.
- **Global Impact:** Now that the SEC has approved their first Bitcoin ETFs, will other global regulators and exchanges accelerate their approvals?
- **Physical Bitcoin ETFs:** A bit of a longer-term question, but it will still be interesting to see what happens to these futures ETFs when physical Bitcoin ETFs are approved.

The future of money is accelerating before our very eyes!

4 Venture Capital Crypto Funds

A venture capital crypto fund is a traditional venture capital fund that invests in crypto companies. These funds normally invest capital in exchange for equity in crypto companies although they sometimes get tokens depending on the nature of the company. Many of these funds invest in seed or series A rounds although some invest in later stage projects, and many of these funds are crypto-specific funds solely focused on the industry. Blockchain Capital, Fenbushi Capital, and Pantera are examples of such firms.¹⁴ Others are part of bigger crypto-focused organisations and tend to be their investment arm, with Coinbase Ventures or ConsenSys Ventures good examples of such firms.¹⁵

Other firms are part of bigger VC firms that have set up a fund focused exclusively on the crypto industry. A16z Crypto, which is part of the broader Andreessen Horowitz group, one of the most famous VCs in Silicon Valley is a good example.¹⁶ In the summer of 2021, Andreessen Horowitz announced a new US\$2.2 billion fund to invest in crypto companies.¹⁷ Both traditional

venture capital and crypto-focused VC firms still play a big role in the global crypto fundraising world, and according to a PwC report, around 56% of equity fundraising deals were done by such firms.

5 Tokenised Funds

Whilst all the types of funds we've discussed above invest in crypto-assets, there's nothing particularly interesting about them. The way they are setup and how they operate is like non-crypto funds, and apart from the fact that they invest in crypto-assets, there's nothing inherently special about them. Tokenised funds, funds whose structure is blockchain-based, are very different and therefore much more innovative, and the shares offered to investors are tokenised and traceable via the blockchain.

This has many benefits. First off, it can provide liquidity. Today when investors invest in a fund, say a private equity fund or a hedge fund, those shares are quite illiquid. If an investor in a private equity fund wants to sell his shares, the process is long and tenuous often requiring approval of the fund directors, but also resulting in selling those shares at a discount in the secondary market as there is little liquidity and price transparency. Moreover, the process of doing that transfer is archaic as it is paper-based and requires the involvement of lawyers and other intermediaries. A tokenised fund can change this as the shareholders or investors in the fund are clearly visible to fund directors, and a transfer and change of ownership can be easily made using blockchain technology. However, where tokenised funds can have a big impact is when it comes to the payment of dividends or distributions. Today, very few hedge funds, venture capital funds, or private equity funds pay dividends. When an exit happens for a private equity or venture capital fund, the funds are distributed in an archaic manner. A tokenised fund could automatically make such payments using stablecoins to whomever is the owner of those tokenised shares. This makes the process faster and safer, and the same applies if a corporate action is needed like a vote of the shareholders.

A tokenised fund can invest in any type of assets and does not need to be related to crypto-assets. However, it's important to cover it here as it is based on blockchain technology and has created confusion for many people. It's important to understand that we're still in the early days of the tokenisation revolution. Private funds will undoubtedly all be tokenised one day, and the question is not if, but when. How soon that will come is unknown, but it's an area to keep an eye on if you're focused on the asset management industry.



20

Crypto Ecosystem Enablers

1 Traditional Financial Institutions

For years, observers have speculated about how and when incumbent financial institutions might make their entry into the crypto-asset ecosystem. After all, whilst they may lack the technical agility and fiery rhetoric of early entrants to the space, their entry could offer a level of institutional credibility that has been elusive and at the same time open the door to a wave of institutional capital. Given this demand for institutional grade service providers, many traditional financial institutions have been slowly entering the space since 2017 and even more so in 2021.

The drivers behind this are numerous. One major catalyst is demand from their existing clients like hedge funds or family offices. For example, one of the main reasons private banks started offering crypto products is due to the demand from their existing high-net worth individual (HNWI) clients and that enabling crypto products allows for new revenues in a range of products or activities, from structured products to market making. Unlike in the early years of crypto, and as we have seen earlier in this book, there is now increasingly regulatory clarity on the topic of crypto-assets. Whilst each traditional financial institution is different and has its own unique strategy, we can group the various strategies used by financial institutions into five broad categories.

The first option is to simply become a service provider. It consists of providing services that the crypto ecosystem needs or that financial institutions looking at entering the crypto ecosystem need. Some are quite basic, like J.P. Morgan providing banking services to firms like Coinbase or Gemini.¹ It

often consists of expanding existing offerings to service the crypto ecosystem, with the efforts of global custodian Northern Trust to offer crypto custody a good example.² In such cases, the traditional financial institution does not necessarily need to build or launch new products or solutions, but rather simply adapts its client acceptance or risk management procedures to enable accepting such clients. Whilst this may sound easy, it has also its own set of complications. Many traditional financial institutions were initially reluctant to deal with crypto companies often due to their lack of knowledge of the industry and often the misconception that the crypto industry was mainly linked to money laundering and other nefarious actors.

The second strategy is to simply invest in crypto companies as pure external equity investors. This allows them to get exposure to the asset class without much risk, except the capital invested and perhaps some reputational risk. Good early examples were the investments that Standard Chartered made into Ripple in 2016 or that Goldman Sachs made in 2018 into crypto exchange Circle and crypto custodian BitGo.³ Numerous other examples followed over the last years, from BNY Mellon investing in crypto custodian Fireblocks to HSBC investing in Consensys.⁴

The third strategy is to partner with crypto firms, the approach used by Nomura who has partnered with a French crypto custody and security company called Ledger to launch a crypto custody offering called Komainu.⁵ Nomura has a large base of traditional institutional clients and, to a certain extent, their trust. Ledger may not have those attributes, at least in the early days, but it has the crypto expertise when it comes to custody and so a partnership where each side brings a unique angle made sense. In many cases the partnership is combined with an investment, with a good example Julius Baer and its partnership with SEBA Crypto AG.⁶

A fourth option is to launch some initiatives in-house with the goal to experiment and innovate within the confines of the institution. Standard Chartered launched SC Ventures, an innovation unit within the bank that was active in building crypto solutions including its own crypto custody solution called Zodia.⁷ Another good example is J.P. Morgan and the efforts it's making with the J.P. Morgan Coin.⁸ Whilst this option provides bank leadership with the most comfort, it has numerous challenges because large financial institutions are not naturally designed to be agile or innovative, which may be one reason why J.P. Morgan ended up switching to the approach below.

The fifth option is to set up a new entity focused solely on crypto-assets, which Fidelity did by setting up a new entity called Fidelity Digital Assets⁹ and which J.P. Morgan did in the fall of 2020 with the launch of Onyx, a

Table 1 Different approaches available to financial institutions looking at entering the crypto ecosystem

Different Approaches Available to Financial Institution Looking at Entering the Crypto Ecosystem				
Becoming a Simple Service Provider to Crypto Firms	Investing in Crypto Companies as an External Investor	Partnering with Crypto Companies	Launching In-House Initiatives	Launch New Entity Focused on Crypto

separate blockchain-focused entity.¹⁰ Such an approach has many benefits, in that it allows for the broader group to capitalise a new entity and give it the liberty and freedom to innovate and move faster. It also allows for this new entity to get involved in activities that would be difficult considering the labyrinth of approvals needed in the “mother ship”, and such a standalone structure may be easier from a hiring perspective as it could potentially enable the hiring of talent that would not be possible in the rigid structures of a traditional bank (Table 1).

2 Crypto-Focused Banks

Even though many large banks are entering the crypto space, the single most difficult thing for any crypto company remains the ongoing struggle of opening a traditional bank account. After all, traditional banks have become notorious for shutting down accounts of crypto companies and sometimes even those of their founders. Excuses range from pure ignorance and disinterest to specific compliance and AML concerns with the fear of losing U.S. correspondent banking relationships often cited as one of the main reasons.

The irony is that whilst many banks around the world push back on potential crypto clients for fear of losing their U.S. correspondent banking relationships, these same correspondent banks are often increasingly involved in crypto. However, several banks around the world have moved in the opposite direction and have been embracing crypto. From Deltec in the Bahamas to Bank Frick in Lichtenstein, some banks have made crypto their comparative advantage and have become dominant players in their ecosystems. For example, Deltec is one of the banks that reportedly holds the cash assets of the Tether stablecoin. But some U.S. banks have also grabbed this opportunity, especially as they don't need to worry about correspondent banking relationships as they are based in the United States. Two of the most public

and successful examples have been Signature Bank, based in New York, and Silvergate, based in California.

These two organisations have been very welcoming towards the crypto industry and in many regards are now more advanced in their crypto offerings than many of their peers. If you've ever sent funds to a global crypto exchange or invested in a crypto fund, chances are your funds went through one of these two banks. For example, Signature Bank reportedly has over 740 crypto clients, with more than US\$10 billion from crypto client deposits,¹¹ meaning that 16% of its \$80 billion in deposits comes from the crypto industry. Signature also became the first FDIC-insured bank to launch their own blockchain-based digital payments platform. Known as Signet, the platform allows the bank's clients to make payments in real time using U.S. dollars, any time of any day. This is a drastic difference from traditional financial institutions, which operate only during a set number of hours on weekdays. Signature also announced their integration with stablecoin issuer Circle and revealed it will also soon offer Bitcoin-backed cash loans.

Meanwhile, Silvergate is the California cousin to Signature and with deposits of \$6.4 billion from 1,100 crypto clients, the bank has emerged as a dominant player in this space. Somewhat like Signature's Signet, Silvergate operates the Silvergate Exchange Network, or SEN. Essentially, SEN allows the bank's digital currency clients and institutional investors to send U.S. dollars from one Silvergate account to another, any time of day, any day of the week,¹² and Silvergate allows clients to obtain cash loans backed by Bitcoin. The role played by Signature and Silvergate is an important element in the global crypto ecosystem. Whilst many of the other banks backed off, often not even spending time to try to understand the basics of crypto or blockchains, various teams at these banks have made intellectual efforts to understand crypto, build an offering tailored for the industry, and dominate this niche. It could even be argued that many of the crypto exchanges and crypto funds operating in the market today would not be able to function if these two banks did not exist. Similarly, if anything happens to these two banks, the crypto exchange ecosystem, at a minimum its fiat-to-crypto leg, would be impacted, as they're too big to fail for the crypto ecosystem.

3 Crypto Borrowing and Lending Platforms

As the crypto ecosystem continues to mature, we've begun to see the emergence of more and more yield enhancement and lending products around

the industry, but what exactly are these yield products? There are essentially two types of yield products: those offered by centralised entities (e.g., BlockFi, Ledn, Celsius, Nexo) and those offered by decentralised platforms (e.g., Aave, Compound). The mechanism is quite simple: a user who has crypto (e.g., Bitcoin, ETH, USDC) can lend that crypto to the platform and in exchange will receive some interest. The platform will then lend that crypto to either institutional investors or retail traders for a higher rate and pocket the difference (Fig. 1 and Table 2).

Whilst the same offering exists on DeFi platforms, the average retail crypto trader is likely to use a centralised platform as they tend to be more user-friendly, offer customer support, and do not require technical skills.

However, trading using such centralised exchanges contains certain risks, with the most obvious counterparty risk. For example, whilst these platforms will always over-collateralise their loans (e.g., a client can only borrow

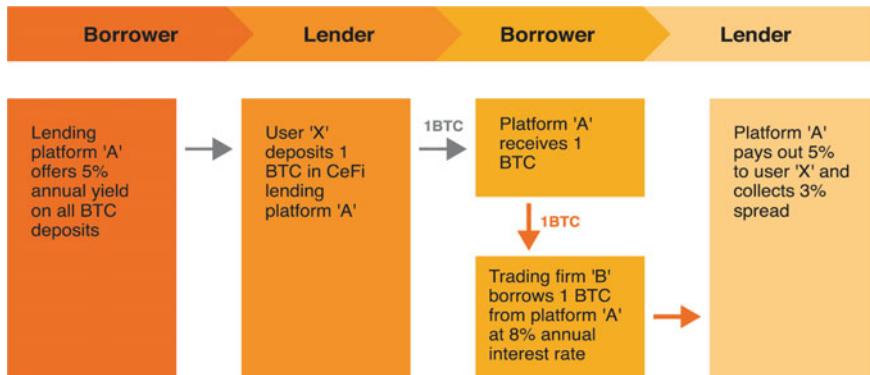


Fig. 1 Borrowing and lending in centralised finance (Source "Deconstructing CeFi," Kraken Intelligence, July 2021)

Table 2 Comparison between centralised and decentralised finance broken down by custody, security, main service, customer support, and accessibility

	CeFi	DeFi
Custody	Managed by an entity	Managed by the user
Security	Managed by an entity	Managed by the user
Main services	Lending/borrowing, trading, and payments (fiat on/off-ramps)	Lending/borrowing, trading, and payments (crypto on/off-ramps)
Customer support	Centralized client support	No centralized client support
Accessibility	Verification needed (KYC, AML)	Permissionless, available to all

\$5,000 for \$10,000 worth of crypto), the risk remains that crypto markets will rapidly fall, and clients will not be able to meet margin calls, or the exchange will not be able to liquidate the collateral in time. Although such platforms were able to easily sustain some of the large market swings in crypto in recent months and years, the theoretical risk remains. Also, unlike leaving your money in a bank, for instance, there is no FDIC-like insurance for such products in the event the platform goes bust.

The second risk to be aware of is hacking or cyber risk. In a DeFi platform, you as the user hold the private keys and, thus custody of your assets, whereas in a centralised lending platform, you transfer your crypto to the platform. This leaves open the inherent risk of a hack, as a bad actor can swoop in and hack that platform or the custodian that holds the funds for that platform. The third consideration comes down to traditional fraud risk. For example, a platform may not be able to give back your funds due to fraudulent activity or negligent risk management, with the bankruptcy of lending platform Cred a good example. However, the reality is that people are generally happy to lend out their crypto to earn a yield on it, and although yields for crypto lending have come down recently, they remain appealing, especially when compared to traditional financial instruments. As many crypto investors are holding Bitcoin and other crypto-assets for the long term, such yield enhancement products allow them to generate returns on their assets whilst they “hodl” them.

Whilst the above relates to centralised lending platforms, it’s important to understand that the same offerings exist in the DeFi space as well, with platforms from Aave to Compound offering similar products but in decentralised fashion. Whilst DeFi has many benefits, from being permissionless to eliminating counterparty risk, some inherent risks remain, like smart contract risk. Whilst there are lots of people reviewing smart contracts, the risk remains and whilst DeFi platforms are used actively by crypto aficionados, they are more difficult to use by the regular retail public, at least currently.

At the end of the day, these developments are worth paying attention to, especially as more and more stories emerge from the crypto ecosystem surrounding these different yield-earning platforms. Just like in the traditional financial world, a healthy and liquid borrowing and lending market is essential for the continued maturation and advancement of the broader crypto industry. More liquidity, after all, would provide crypto funds with the access to assets needed to perform certain trades, like shorting. A healthier debt market would also allow crypto-asset holders to generate yields with their assets by lending out funds before receiving them back with interest.

Platforms like BlockFi, Celsius, and Nexo are already taking this approach, as are others in the DeFi world like Compound.

Regardless, the risks need to be carefully monitored. First, the level of debt in crypto markets is growing fast and is at an all-time high, being driven not only by market rallies in crypto markets with trading activity from crypto hedge funds and traders, but also from the growth of yield farming and the explosion of interest in DeFi. The eye-popping levels of debt on the books could give rise to systemic industry risk down the road, if for instance, in the event of a market crash, lenders could begin making margin calls, and counterparties unable to meet these margin calls may have their positions closed. After the 2008 financial crisis, the traditional financial world learned the hard way about the catastrophic snowball-effect of massive levels of debt. Whilst there are no immediate risks (especially when markets are going up and the crypto ecosystem is far from having the same level of risk we saw in 2018), it would be wise for the crypto ecosystem to begin recognising these potential risks and why crypto firms need to ensure they have the right risk management and counterparty risk measures in place, with experienced individuals in charge, to be able to deal with such a situation if it arises.

4 Institutional Investors

Institutional investors like sovereign wealth funds and pension funds collectively control trillions of dollars around the world, a sum that makes the total crypto-asset market capitalisation seem trivial in comparison. The flow of even a fraction of these funds into crypto-assets would obviously have a massive impact on the value of crypto-assets and the interest in new crypto-asset projects.

Whilst institutional investment to date has been limited when compared to the capital that can be deployed by these players, it would not be the first time that these organisations have expanded the remit of their investments as they have become more educated on an emerging asset class. For example, over the past 25 years, the success of alternative funds has given many institutional investors an appetite for exposure to absolute return strategies, short selling, and illiquid instruments such as distressed debt. Whilst many of these players have either not wanted to make such investments directly, or lacked the in-house expertise to do so, they were able to access these instruments via investments in specialised hedge and private equity funds. If large institutional investors choose to seek exposure to crypto-assets, they're likely to use a similar strategy via crypto funds. If interest in crypto-assets by institutional

investors continues to grow, we should expect to see an increasing number of crypto funds, as discussed in length in this book. Family offices, including some of the largest in the world, are amongst the most aggressive institutional investors in crypto-assets. These organisations have been able to take advantage of their ability to make decisions faster (as there are rarely more than a handful of decision-makers) and the freedom offered by having only proprietary capital (i.e., they have no capital from external investors).

Whilst many may have expected hedge funds to be early adopters and active in the crypto space, they have been initially careful in doing so without raising new funds, fearing that their existing investors may not be comfortable with allocations to this new asset class. Further, the continued lack of traditional players providing services like institutional grade custodianship, fund administration, trading systems, and auditing had been a concern, at least until 2020. Starting in 2020, we have seen increased activity from hedge funds with a number of catalysts taking place. First, following the financial crisis caused by the COVID-19 epidemic, central banks around the world started record amounts of quantitative easing, causing a number of hedge funds to look at assets that can provide a hedge to inflation. A good example was the legendary hedge fund billionaire Paul Tudor Jones, who announced in May 2020 that he was holding 1–2% of his \$22 billion funds in Bitcoin.¹³

Another catalyst was the presence of numerous instruments that such funds could use to get Bitcoin exposure, with the Chicago Mercantile Exchange (CME) launching cash-settled Bitcoin Futures in January 2020¹⁴ making it easy for traditional financial firms like hedge funds as they already are used to trading derivatives on that exchange. Many large hedge funds, like the \$160 billion plus Renaissance Technologies, amended their legal documents to be able to trade such instruments.¹⁵ At the same time, many large crypto service providers started getting regulatory approval or getting third-party certifications that many of these institutional investors would seek. For example, the prospectus or offering memorandum of many institutional investors only allow such funds to trade with regulated counterparties. As regulations around crypto are becoming clearer and most organisations are becoming regulated, this allows institutional investors to start trading with such regulated counterparties, from OTC desks to exchanges. Another example is that many institutional investors can only trade with counterparties that have obtained certain third-party certifications, like SOC, ISAE, or ISO.

What are SOC, ISAE, and ISO certifications?

Many crypto exchanges, crypto custodians, and crypto service providers are in the process or have already obtained control reports, most commonly Systems and Organisation Controls (SOC) or International Standard on Assurance Engagements (ISAE) reports. These reports are often completed by the large accounting or consulting firms (e.g., the Big 4) in response to many of these firms having to demonstrate to their clients and auditors that they have robust frameworks of internal governance and controls. These control reports are different from financial audits that most companies need to obtain annually and are intended more for the shareholders of the company.

There are two major categories of controls reports.

- **SOC 1:** This is a review of controls on financial reporting. The distribution of this report is restricted and is intended mainly for the customers of the business and their auditors. The level of assurance provided is one of reasonable assurance only. There is also a ISAE 3402 report that is in practice similar to SOC 1.
- **SOC 2:** This is a review of operational controls. The distribution of the report is also restricted and intended for the customers of the business and auditors, but also counterparties and regulators. The level of assurance provided is also one of reasonable assurance only. There are also small variants of the SOC 2, for example, the SOC 2 + also covers additional items like cybersecurity for example or the SOC 3 is like a SOC 2, but its distribution is unrestricted.

There is a third form of controls report, called the ISAE 3000, a customised review based on specific needs or to suit the reporting needs of the entity. It's also important to understand that the two types of controls report above (SOC 1 and SOC 2), can be issued under either a Type 1 or Type 2 opinion.

- **Type 1:** Provides an opinion on whether the organisation's systems or controls are suitable at a point in time
- **Type 2:** Provides an opinion on whether the organisation's systems and controls are suitable over a period of time.

Another type of report sometimes discussed is International Organisation for Standardisation (ISO) certifications. Whilst ISO certifications are a good first step in providing comfort, they're not as stringent compared to SOC or ISAE reports. For example, ISO reports do not contain an opinion of the auditors and no statement from management as is the case with SOC or ISAE reports, so ISO reports do not give the same reliance that auditors and other sophisticated investors would expect. However, a crypto firm is better to have an ISO report than not have one at all. Whilst the number of crypto platforms that

have such certifications is still small at the time of writing, we should expect this to change over the coming years.

We should expect the level of interest from institutional investors to increase over the coming years, but at the same time, we need to be realistic and understand that this may take some time. Institutional investors are often conservative by nature, and whilst most institutional investors have exposure to alternative funds, like hedge funds or private equity funds, this took place over two or three decades. In 2021, Fidelity published a summary of its annual survey on digital assets, which focuses on the growing number of institutional investors entering the crypto space.¹⁶ When it comes to this topic, the survey was full of interesting takeaways. First and foremost, more than 90% of surveyed institutions interested in digital assets expect to have a greater allocation of funds tied into crypto over the next five years, and over half of the surveyed institutions mentioned they currently invest in digital assets. Zooming in on regional trends, the report showed that digital asset adoption grew in the United States from 22% in 2019 to 33% in 2021, whilst adoption in Europe has seen a similar jump, growing from 45 to 56%. Broader adoption in Asia, meanwhile, considerably dwarfs both markets when it comes to digital asset exposure, sitting at an impressive 71%. Ultimately, there is no doubt that institutional interest is here to stay and that this trend is just beginning. It will be interesting to see what impact this will have on both the future of the broader crypto ecosystem as well as the traditional financial world.

How to Determine Bitcoin's Value?

One question on every crypto investor's mind is what the price of Bitcoin will look like, say, 2 months (let alone 2 years) down the road. Not surprisingly, many have come up with different models on how to value the crypto-asset. One of the most common methods has been the stock to flow (S2F)

Table 3 Stock-to-flow metrics for key precious metals

	Stock (tn)	Flow (tn)	SF supply growth	Price \$/Oz	Market Value
Gold	185,000	3,000	62	1.6%	\$ 1300
Silver	550,000	25,000	22	4.5%	\$ 16
Palladium	244	215	1.1	88.1%	\$ 1400
Platinum	86	229	0.4	266.7%	\$ 800

model, which is an indicator used in commodities for decades and has now been popularised by authors like Saifedean Ammous through his book “The Bitcoin Standard”¹⁷ and by bloggers like PlanB.¹⁸ It’s easy to understand why stock to flow has gained popularity, as it is relatively simple to grasp and has proven surprisingly accurate to date. The model can be simplified by the following equation:

$$SF = \text{stock}/\text{flow}$$

Stock is the size of the existing stockpiles or reserves and flow is the yearly production. When applied to Bitcoin, it tracks well the price well and the beauty of the S2F formula lies in its simplicity. All one needs to do is divide the current supply, or stock, of the commodity (or digital asset) by its flow, or annual production. When the crypto blogger PlanB unveiled the Bitcoin S2F model, the author included a chart that compared Bitcoin’s value with that of precious metals and commodities that shared the common theme of scarcity (Table 3).

If we refer to the chart above, the third column (SF) refers to the number of years it would take to double the existing supply of an asset if current production levels remained the same. It would take 62 years to mine the existing levels of gold out of the ground, making the supply we have right now relatively scarce. By way of comparison, it would take 22 years for silver, 1.1 for palladium, and 0.4 for platinum. The higher the number in the SF column, the scarcer the asset. When this chart was first released on PlanB, Bitcoin’s SF was 25, with 17.5 million coins in stock and 700,000 coins in production per year. That made Bitcoin scarcer than silver but not quite as scarce as gold. But since the chart was released, Bitcoin’s S2F has become significantly higher. Its total stock has increased to 18.6 million units and, because of the halving that took place in 2020, the issuance schedule fell to 328,500, raising Bitcoin’s SF from 25 to 56.6.

But how do these figures compare to gold? According to the World Gold Council, there were 197,576 tonnes of above-ground stock of gold in 2019.¹⁹ If we divide that by 3,000, we arrive at a new SF for gold of 65.85. So, whilst gold’s SF has gone up, Bitcoin is rapidly making up ground, which again has to do with the halving, not to mention the fact that gold production is expected to hit a record in 2022. In fact, one of the biggest reasons why Bitcoin advocates believe in the SF model is because the production schedule is predictable.

The stock to flow model can be used for a variety of different assets. For example, seashells have been used in various regions around the world throughout time as money, given that they can be hard to find, whilst cigarettes have been used as a form of currency in prisons because they are

difficult to procure and produce. As this model has become more popular, more and more crypto hedge funds have taken to using the formula to try to predict the price of Bitcoin. A different approach also gaining in popularity is to look at Bitcoin's usage rate. For instance, crypto hedge fund Pantera has argued that for every million new users, the price of Bitcoin will rise by \$200.²⁰ Based on this model, once 1 billion people begin using Bitcoin, the value would shoot up to \$200,000.²¹ By extrapolating on this model, if the price continues to rise \$200 for every million new users, and if the 3.5 billion people around the world who own a smartphone start using Bitcoin, then Bitcoin would hit \$700,000. Of course, there is no certain, failproof way to predict the price of Bitcoin as there are many black swan events that could happen, from a government ban to the rise of a new asset that investors prefer. Nevertheless, it's important to know that there are different approaches that investors have been using to try to predict the price of Bitcoin and we should expect many new models to see the light of day in the future.

5 Crypto-Asset Custodians and Wallets

Once someone has purchased a crypto-asset, she will require a facility to safely store that asset. In the case of crypto-assets, this generally refers to the storage of the private keys, the string of digits that allow its holder to prove that he is the owner or that crypto-asset. The immutability of transactions conducted on the blockchain means that if the holder of an asset loses control of her private keys, there will be no way to repudiate or reverse the loss of those assets. This is different from traditional equity markets. The average investor is not particularly worried that the shares in her retirement savings account will be stolen. By contrast, investors in crypto-assets must be cognisant about the vulnerability of their investments to hacking and must determine if they wish to hand over these assets to a third-party custodian or store them themselves in what is called self-custody. Before discussing the different type of custodians, it's worth understanding the methods of custody, which can be generally separated into two types: hot and cold wallets,²² with the basic details of each type covered in the Table 4.

Table 4 Key differences between hot and cold crypto wallets along with advantages and disadvantages of each model

Type of Wallet	Characteristics
Hot Wallets/Hot Storage	<ul style="list-style-type: none"> Connected to the internet Can be accessed through the internet or is on a platform that has internet access Pros: Faster to move assets in and out as connected to the internet. Useful for conducting transactions on a frequent basis. Cons: Higher risk of hack due to existing internet connection.
Cold Wallet/Cold Storage	<ul style="list-style-type: none"> Not connected to the internet Not accessible unless gaining physically access to the wallet Pros: Significantly lower risk of hack as not connected to the internet. Cons: Requires more time to conduct a transaction as requires reconnecting to the internet

It is important to understand that the concept of hot and cold wallets applies to both self-custody and third-party custody as it relates to how it is done rather by whom.

What is Warm Custody?

As the crypto custody ecosystem evolves, we should expect new variants that try to find the right balance between security and convenience. Where this balance is will be a constant debate between cybersecurity aficionados. Warm custody is, as its name implies, a mix of features from both hot and cold custody. Whilst what can be interpreted as warm varies a lot, it generally refers to custody where the private keys are partitioned off the internet and housed in a secure storage module called a hardware security module (HSM), that is itself connected to the internet and is able to conduct certain tasks that would normally be done by humans in a cold storage context (e.g., signing transactions, storing keys).

5.1 Third-Party Crypto Custodians

Investors in crypto-assets can hand their crypto to a third-party custodian for safekeeping with two broad types of third-party custodians: crypto exchanges and independent custodians. Many centralised exchanges (e.g., Binance, Kraken, Coinbase) provide custodianship services for their clients, offering customers a high level of convenience, reducing frictions around the purchase and sale of those assets. However, several high-profile incidents have highlighted the risk of hacking faced by centralised exchanges as they are prime targets for hackers. Whilst many of today's exchanges have learned from these events and instituted improved security measures, as well as in some cases some levels of insurance, significant risks remain.

Independent custodians, in contrast, simply provide custody for clients. There are numerous such players in the market (e.g., BitGo, Anchorage, Coinbase Custody, HEX Trust), but unlike crypto exchanges that provide trading to their clients as their main business with custody being ancillary, crypto custodians are solely focused on custody. In addition, they also often offer white label services for exchanges. So, whilst a client may think that the exchange is providing custody for their assets, it's in practice taking place behind the scenes with a third-party custodian.

Why are Institutional Investors so Focused on Custody?

Crypto custody presents a challenge for large institutional investors, such as family offices and hedge funds, who have shown increased interest in investing in crypto-assets. These institutions are subject to strict fiduciary requirements and regulatory oversight. If not bound by regulations, many such investors, like hedge funds, have requirements in their investment management agreements that not only they are not allowed to hold client assets, but also that their assets need to be held with an independent third-party custodian. This is why the development of an institutional grade custody ecosystem is so important for the entry of institutional players.

Thankfully there have been major milestones in recent years with many traditional institutional players entering the space from Fidelity to Northern Trust. Over the coming years, we should expect this crypto custody ecosystem to be significantly larger and more developed than what it is today.

5.2 Self-Custody

Those who are not comfortable with entrusting their crypto-assets to a third party may choose to instead transfer them to a personal “wallet”. A crypto-asset wallet enables an individual to manage the secure storage of her private keys and is comparable to storing money into a personal vault rather than at a bank. Many crypto OGs (i.e., those who have been in the crypto space since its early days) believe in the mantra of “not your keys, not your coins”. By this they mean that they should be able to self-custody their assets and not let it under the ownership of any third party, even if this means that they need to do a bit more work.

There are numerous self-custody solutions in the market (e.g., Ledger, Trezor). These look like fancy versions of a USB stick that allow its user to store its crypto private keys. Others are online decentralised platforms that allow the user to hold assets (e.g., Metamask, MyEtherWallet). Users of self-custody are happy to sacrifice the convenience of a third-party custodian in exchange for the peace of mind and independence that they own their keys. However, this comes at a certain risk as, in the same way that someone who loses his wallet full of banknotes may never find it, if that person loses the self-custody device, she has lost all her assets. The convenience of many of these self-custody solutions has greatly improved in recent years and we should expect further improvement in the coming years, giving users a real choice in the event they want to self-custody.

6 Large Tech Firms

When it comes to crypto offerings to the retail market, it also is worth keeping an eye on the large tech players. The first signs of this have been messaging apps, with Japanese tech giant Rakuten launching its own crypto token²³ and acquiring a crypto exchange.²⁴ Japanese messaging app Line has also launched its own crypto token²⁵ and the 200 million user messaging app Telegram conducted a private placement for its own utility token that raised over US\$1.5 billion, but was forced to cancel the project due to regulatory issues with the U.S. SEC.²⁶ The most publicly known example is probably Facebook/Meta with its announcement in June 2019 of Libra and its amended version a couple of months later. We covered Libra (now renamed Diem) extensively earlier in this book, and it would not be surprising to see other large tech firms launch their own crypto payment tokens. Ironically, in

my last book, *The Future of Finance*, written in 2017–2018, months before the Libra announcement in June 2019, I wrote the following:

For example, Facebook today has more than two billion users. The social media network is widely available throughout the world and most would agree that, despite the recent scandals over their treatment of customer data, a large portion of users trust Facebook. So, what if Facebook launched its own payment token? Such a token could be exchanged between users, as well as spent within the network's own ecosystem, for example to pay for advertising.²⁷

This was not due to some supernatural foresight but rather basic common sense. Facebook is of course not the only large multinational with the required brand recognition, global reach, and vibrant ecosystem who could decide to launch a crypto payment token. Take Amazon. The credit card and bank fees that a firm like Amazon and merchants using Amazon's platform must pay is not negligible. Now imagine the potential cost savings if everyone in that online marketplace could use a hypothetical Amazon Coin. The coin could be used to make all manner of payments and some individuals might even be willing to use such coins in transactions that have nothing to do with Amazon or its online marketplace. A survey conducted by LendEDU concluded that over half of 1,000 online shoppers would be willing to try an Amazon-created cryptocurrency.²⁸

We should expect the large tech platforms to get increasingly involved in crypto over the coming years. Twitter enabled users to tip others leveraging the Bitcoin lightning network in 2021.²⁹ There is no reason that other social media should not follow, with the rebranding of Facebook to Meta in 2021 another example of things to come.

7 Service Providers

With any industry, there will be an ecosystem of service providers developing to support them. We are already beginning to see a growing number of law firms and consulting firms with dedicated crypto-asset offerings as well as research firms focused on providing high-quality insights and analysis about emerging blockchain projects. The Big 4 accounting firms are a great example with many of them having dedicated crypto teams and regularly publishing reports on the topic. For example, I launched the PwC global crypto team out of Hong Kong in early 2017, and that team has grown from an experiment to a team of hundreds in over 24 countries. There are now similar teams in most of the large consulting firms as well as law firms. In time, we're likely to

see the emergence of rating agencies dedicated to tracking the probability of failure for a given token, and specialised auditors dedicated to evaluating the details of smart contract or attesting to the reserves of a stablecoin.

Whilst many of these actors may not use blockchain in their daily activities, their ability to provide specialised services will be critical to both those entrepreneurs seeking to build out crypto-asset projects with broad-based adoption, as well as to the prospective users of and investors in these projects. There are also many industry associations and advocacy groups that have set up in recent years, which might include trade or advocacy organisations, such as the Chamber of Digital Commerce or the Global Business Blockchain Council and dozens of similar regional organisations.

8 Crypto Media Ecosystem

The crypto media ecosystem has also evolved considerably in line with the gradual mass adoption and acceptance of digital assets. Today there are numerous media publications including CoinDesk, The Block, Decrypt, Cointelegraph, and many others that specialise in delivering crypto-related news to the public. In addition, since 2017, most large financial publications from Bloomberg to CNBC regularly cover crypto developments, with their level of coverage varying depending on general interest in the asset class. In 2020, some of these journalists came together to create The Association of Crypto Journalists and Researchers to provide education, mentorship, and training to ensure crypto journalists aspire to the highest ethical and journalistic standards.³⁰ We should expect the crypto journalism space to also evolve and mature over the coming years in line with the broader crypto ecosystem.



21

Future Trends to Watch

The crypto industry moves fast and there are several macro trends that will have an overarching impact on the rest of the crypto ecosystem. For example, in my most recent book in 2019, *The Future of Finance*, we ended by explaining that topics like decentralised finance would grow rapidly and have a big impact, and they did. The same may happen with some of the developments set out here, from Web 3.0 to the metaverse. Over the coming years, this topic will become part of the mainstream not only in the crypto industry, but the broader financial services industry. If one day we have a second edition of this book, these might be part of the main body of the book and not listed as something in the “future”.

1 Web 3.0

With the rise of NFTs and DeFi, the topic of Web 3.0 comes up more frequently and it's a topic that will generate a lot of debate in the coming years. In order to properly understand Web 3.0, it's important to discuss what Web 1.0 and Web 2.0 are first (Fig. 1).

Web 1.0's vision of the internet was a forum where everyone could meet and collaborate, and the rise of online service platforms like AOL, Yahoo!, and other portals became the gateway to this new environment, luring individuals, businesses, and governments. Although the content was mostly static, it was already a great milestone and the launch of Netscape's web browser

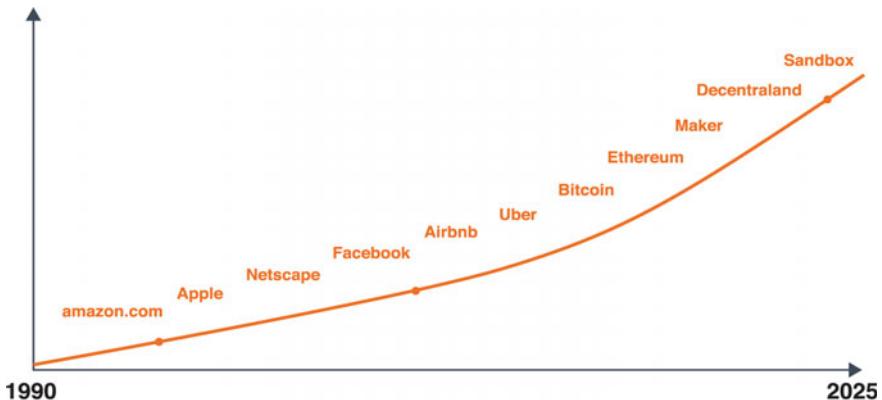


Fig. 1 The progression of Web 1.0 to Web 3.0

in 1994 only hastened this revolution. Then came Web 2.0. Whereas Web 1.0 was defined more by content consumption, new social media platforms like Facebook, Twitter, and YouTube gave rise to an online environment that empowered consumers to begin creating their own material, completely transforming the media, advertising, and retail industries. Web 2.0 was dynamic, allowing users to interact with content with software accessing data via APIs, thus enabling entire suites of new products, from podcasts to live-streaming. However, the danger of Web 2.0 is that it relies on a model in which user data is not owned by the individual, but rather third-party companies that also control access to these platforms, like Google, Facebook, and Amazon. In addition, Web 2.0 has become inseparable from targeted advertising and the monetisation of users and their data.

Web 3.0, meanwhile, is the natural evolution of its forerunners and is made possible by the rise of new technologies like AI, big data, and blockchain. Furthermore, the concept of this latest iteration of the Web proposes a return to Tim Berners-Lee's original vision of the internet, a place in which "no permission is needed from a central authority to post anything ... there is no central controlling node, and so no single point of failure ... and no kill switch".¹

Web 3.0 has certain unique characteristics²:

- **Open:** Built using open-source software by an accessible community of developers, with full transparency
- **Trustless:** Participants can interact either publicly or privately without the need of a trusted third-party intermediary
- **Permissionless:** Anyone can participate; no permission from any centralised governing body is needed

The rise of new technologies, from smart contracts to artificial intelligence, ultimately paves the way for further decentralisation of our data, creating a secure and transparent ecosystem that stands sharply at odds with Web 2.0. Part of the vision of Web 3.0 is that decentralised platforms and apps could disrupt and eventually displace the centralised tech giants, giving individuals control over their own data, whilst also making the web more resilient overall. Web 3.0 should ultimately result in a more democratised online environment that puts control back in the hands of individuals. This has been described as true sovereignty or asserting control over not only who owns your data, but who profits from one's time and personal information. Web 3.0's decentralised environment would make it easier for users to navigate an internet where they own their data and can be compensated if they choose to sell it, phasing out a status quo where the only ones profiting from user data is Big Tech.

It will be interesting to see whether the large tech firms of Web 2.0 will be able to adapt and how fast the transition from Web 2.0 to 3.0 will be. Web 3.0 will give rise to many new business models and ecosystems that we can barely imagine now, but one thing is certain and that crypto-assets will be the “money” that people will use in decentralised ecosystems. From the basics like buying and selling goods in a Web 3.0 ecosystem to being compensated for activity that one does on such platforms. The rise of Web 3.0 is an exciting area to follow in the future.

2 The Metaverse

The term “metaverse” leapt to the forefront of everyone’s mind with Facebook announcing the decision to rebrand their corporate name to Meta in 2021. But what exactly is the Metaverse? In contrast to the normal internet that we all know and use, the metaverse is a 3D immersive environment where users can interact with others via avatars. The first person to write about the

metaverse was Neal Stephenson in his 1992 novel “Snow Crash”, although the concept had been discussed in many other sci-fi books.

For an early example of the metaverse, look no further than the online virtual reality game Second Life. Launched in 2003, Second Life is an open world environment that allows users to live a literal “second life” through their avatars, from playing music and taking a trip to the store to even gambling. At its peak, it’s estimated that Second Life was reaching one million users per day. Facebook/Meta CEO Mark Zuckerberg has described the concept as a “virtual environment” that users can enter and immerse themselves in, rather than just staring at content on a screen. Think of it as a limitless world of interlinked virtual communities where individuals can meet, hang out, and engage in all sorts of virtual activities, all using emerging technology like VR headsets, augmented reality glasses, smartphone apps, and other devices.

The important thing to note here as the metaverse gains more mainstream traction is that it has also become tightly linked with all sorts of developments in both the Web 3.0 movement and the broader crypto ecosystem, particularly when it comes to NFTs and DeFi. Take the Sandbox, for instance, a blockchain-based metaverse built on Ethereum that allows players to create their own items, mint them as NFTs, and monetise their creations by selling them in a virtual NFT marketplace. The Sandbox and other metaverses like Decentraland also use in-game currencies and assets (MANA in Decentraland; SAND and LAND in the Sandbox) that power every aspect of these virtual worlds. Users can even buy and monetise virtual real estate in the Sandbox.

Over the coming years, we should expect every Fortune 500 company to have a metaverse presence and strategy. Twenty years ago, every business had to develop an e-commerce or online strategy and businesses will soon need to think about their metaverse strategy. Like Web 3.0, crypto-assets will not only be the “money” used in decentralised metaverse ecosystems, but the asset themselves, from the virtual land NFTs to the in-game NFT skins. The metaverse will also bring millions of new people to crypto, especially via the various gaming ecosystems, which is why metaverse developments are an area to watch in the future.

3 Quantum Computing

Quantum computing is another topic that we should expect to see in the spotlight in the coming years. Quantum computing seeks to deliver new computational capabilities by harnessing the complex and often counter-intuitive world of subatomic particles through a branch of physics called

“quantum mechanics”.³ These subatomic particles don’t behave in the same way as physical objects in our daily activities, which have well-defined positions and characteristics. Instead, subatomic particles exhibit a property called “superposition” where they can effectively exist in multiple places at the same time, a property that’s important for computing. Traditional computers, from the most basic calculator to the most powerful supercomputer, all perform calculations using something called “binary code” where all data is encoded as a series of ones or zeros called bits. A quantum computer also uses ones and zeros, but through “superposition”, a quantum bit, or qubit, can be a one and zero at the same time.⁴ This phenomenon of superposition of being a one and zero at the same time allows devices to perform certain tasks much faster than their bit-based counterparts. To put qubits into superposition, researchers manipulate them using precision lasers or microwave beams, and a quantum computer with several qubits in superposition can crunch a vast number of potential outcomes simultaneously.⁵

Another foundational term in quantum theory is entanglement. Researchers can generate pairs of qubits that are “entangled”, which means the two members of a pair exist in a single quantum state. Changing the state of even one of the qubits will instantaneously change the state of the other one in a predictable way, and this happens even if they are separated by long distances. Nobody really knows quite how or why entanglement works, and it even baffled Albert Einstein, who famously described it as “spooky action at a distance”. But it’s key to the power of quantum computers. In a conventional computer, doubling the number of bits doubles its processing power, but thanks to entanglement, adding extra qubits to a quantum machine produces an exponential increase in its number-crunching ability.⁶ Superposition and entanglement are what give quantum computers the ability to process so much more information so much faster than regular computers. However, the quantum state is extremely fragile. The slightest vibration or change in temperature can cause these qubits to tumble out of superposition, which is why researchers do their best to protect qubits from the outside world in extremely cold refrigerators and vacuum chambers. This interaction of qubits with their environment in ways that cause their quantum behaviour to decay and ultimately disappear is called decoherence.⁷

Scientists have only been able to keep qubits in a quantum state for fractions of a second, often too short a period to run an entire algorithm.⁸ Quantum computational power is determined by how many qubits a machine can simultaneously leverage. Starting with a humble two qubits achieved in the first experiments in the late 1990s, the most powerful quantum computer today, operated by Google, can use up to 53 qubits.⁹

However, researchers in China announced that they had developed a quantum computer in December 2020 that was 10 billion times faster than that of Google.¹⁰ If that doesn't make any sense, don't worry. Physicist Richard Feynman, who won a Nobel prize for his contributions to the field, once quipped that "nobody understands quantum mechanics".¹¹ What matters is that a quantum computer would enable us to quickly solve problems that are extremely difficult for conventional computing systems. Today's data encryption techniques, including those used for Bitcoin and most cryptocurrencies, largely rely on asymmetric cryptography or on a branch of mathematics called "one-way functions" that are easy to compute if you already have the answer (e.g., the private key), but where reverse engineering that key through guesswork might take many years for a conventional computer, a powerful quantum computer could theoretically break through the encryption that secures our most valuable data in seconds.

In 1994, the mathematician Peter Shor published a quantum algorithm that can break the security assumption of asymmetric cryptography¹² and any malicious actor with a quantum computer could use Shor's algorithm to guess the private keys of a wallet or address and appropriate the digital assets. The relevant question for us now is can quantum computers be a risk for Bitcoin and other cryptocurrencies, and the answer depends on how your Bitcoin is stored. In short, if your Bitcoin is in an address that you have already used, it could be at risk, but if it's in a new address, the risk is limited because the Bitcoin blockchain uses an algorithm called Elliptic Curve Digital Signature Algorithm (ECDSA) to generate a public key using a private key. Experts believe that ECDSA could be potentially broken by quantum computers using a modified version of Shor's algorithm.¹³ However, the other algorithm used in Bitcoin, SHA-256, is seen by many experts as being quantum-safe, which means that there is no efficient known algorithm, classical or quantum, which can invert it. Whilst there is a known quantum algorithm, Grover's algorithm, which performs "quantum search" over a black-box function, SHA-256 has proven to be secure against it.¹⁴

To explain the above in simple terms, let's focus on simple person-to-person Bitcoin payments. These can be divided into two categories, each affected differently by a quantum computer. In the first type, a public key directly serves as the Bitcoin address of the recipient and a transaction to such an address is called "pay to public key" (P2PK). This was the most common address type used in the early days of Bitcoin and many of the original coins mined by Satoshi Nakamoto are still stored in such addresses.¹⁵ Since all transactions in Bitcoin are public, anyone can obtain the public key from any P2PK address and a quantum computer running Shor's algorithm could

then be used to derive the private key from this address, allowing a malicious actor with a quantum computer to take control of the coins stored at that address.

In the second type of transaction, the address of the recipient is composed of a hash of the public key, and as a hash is a one-way cryptographic function, the public key is not directly revealed by the address. The first and most popular implementation of this is called “pay to public key hash” (P2PKH). The public key cannot be retrieved from such an address and is only revealed when the owner (or the one with the private key) initiates a transaction, meaning that as long as funds have never been transferred from a P2PKH address, the public key is not known, and the private key cannot be derived using a quantum computer as quantum computers are unlikely to break a SHA 256 algorithm. However, if any funds of any amount have been transferred from a specific P2PKH address, the public key is revealed and a quantum computer running Shor’s algorithm could be used to derive the private key from this address.¹⁶

In practice, usage of P2PK addresses declined significantly since the introduction of P2PKH in 2010 and as of 2012, P2PKH has become dominant. In addition, most wallets today are programmed not to use the same address more than once which reduces the risk with P2PKH.¹⁷ A real risk of a quantum attack remains for all Bitcoins in P2PK addresses and reused P2PKH addresses, and many have tried to quantify this risk, including a team of researchers from Deloitte who analysed the Bitcoin blockchain to quantify this risk.¹⁸ They found that the number of Bitcoin in P2PK addresses has stayed practically constant over the years at around 2 million Bitcoin, and these coins can be assumed to have been generated through mining and never moved from their original address.¹⁹

Following the introduction of P2PKH in 2010, most Bitcoin has been stored in such addresses. The team also found that the number of Bitcoin stored in reused P2PKH increased from 2010 to 2014, and since then has been decreasing slowly to reach a current amount of 2.5 million Bitcoin, which suggests that people are generally following the best practice of not using P2PK address as well as not reusing P2PKH addresses.²⁰ However, this means that there are still around 4.5 million Bitcoin potentially vulnerable to a quantum attack or about 25% of the total amount of Bitcoin that will ever exist.²¹

What can be done to mitigate this risk? In theory, if everyone transfers their Bitcoin to a new P2PKH Bitcoin address, then they will not be vulnerable to a quantum attack. The reality is that this will be impossible as many of the early Bitcoin “owners” have probably lost their private keys, and about

2 million Bitcoin are basically sitting ducks waiting for the first person to use quantum computers to guess their private keys. Whilst some have proposed solutions (e.g., providing a time ultimatum to move them to a new address or else miners will refuse transactions from such addresses), such a solution is unlikely to work for practical and ideological reasons.²² The reality is that for the moment, we're far from quantum computers being an immediate risk to the Bitcoin network and many experts believe that over 1500 qubits would be required to break the Bitcoin blockchain and they would all need to be entangled, so many experts believe we still have some time.²³ Most specialists think that this feat would require a universal quantum computer (one capable of performing a wide variety of calculations), which is at least more than a decade away according to researchers in the field. Yet other researchers suggest that this could happen sooner, using emerging quantum computational devices that have more limited capabilities.²⁴

The good news is that there are solutions. To start, the one-way cryptographic functions used to secure Bitcoin, like ECDSA, can be upgraded to a quantum-resistant one. Many believe that this is like the Y2K bug as there is a clear path as to how we can fix the issue, and which can be implemented when the time is right. These alternative encryption functions should be equally difficult to reverse using conventional or quantum computers, and although not completely secure, these could be run on existing hardware and although they could also be deciphered eventually, it would buy us a reasonable amount of time.²⁵ Second, quantum cryptography can be used to replace classical digital signatures and to encrypt all peer-to-peer communications in the blockchain network, which would be a good solution as it would ensure that nobody with a quantum computer could decipher the private key based on a public key, but the reality is that we are still far from this.²⁶

Finally, and with an even longer time horizon, we could try to build a quantum internet connecting quantum computers across a quantum communications network. Using quantum technology for communicating as well as for the computational processing of blockchain data would further enhance security and enable blockchains to become faster and more efficient, bypassing some computationally intensive steps of current verification and consensus processes, and thus more efficient and more secure. However, the quantum internet is several decades away,²⁷ and whilst quantum computers could pose a theoretical risk to today's blockchains, this is not an immediate problem and one for which there are solutions. However, we should expect this debate to pop up regularly over the coming years as we continue to make progress in the field of quantum computing and so it's important that the crypto ecosystem is aware of the risks and the potential solutions.

4 Zero-Knowledge Roll-Ups

The debate around Ethereum's scalability intensified in 2021 as it explored an upgrade to ETH 2.0, and the topic of Zero-Knowledge Rollups (or ZK-Rollups for the aficionados) began to pop up more frequently and we should expect this to be a topic of discussion over the coming years. But what exactly are ZK-Rollups? Essentially, rollups and the different forms they can take revolve around competing visions on how to scale a blockchain ecosystem.²⁸ As explained by Vitalik²⁹:

First, you can make the blockchain itself have a higher transaction capacity. The main challenge with this technique is that blockchains with “bigger blocks” are inherently more difficult to verify and likely to become more centralized. To avoid such risks, developers can either increase the efficiency of client software or, more sustainably, use techniques such as sharding³⁰ to allow the work of building and verifying the chain to be split up across many nodes; the effort known as “eth2” is currently building this upgrade to Ethereum.³¹ Second, you can change the way that you use the blockchain. Instead of putting all activity on the blockchain directly, users perform the bulk of their activity off-chain in a “layer 2” protocol. There is a smart contract on-chain, which only has two tasks: processing deposits and withdrawals and verifying proofs that everything happening off-chain is following the rules.

The three major types of layer 2 scaling are rollups, state channels, and Plasma. In short, the main difference to remember is that Plasma and channels are “full” layer 2 schemes, in that each tries to move both data *and* computation off-chain.³² But in sharp contrast, rollups move computation (and state storage) off-chain whilst keeping some data per transaction on-chain. The important thing to remember when it comes to this topic is that rollups execute transactions outside of the Ethereum main (layer 1) chain whilst posting transaction data on that layer 1 chain,³³ and because transaction data is kept on layer 1, the rollups themselves can be secured on the chain, incorporating various security features of layer 1 technology whilst executing transactions off-chain. To simplify things, rollups contain three unique properties³⁴:

- Execute transactions outside of layer 1
- Provide proof of transaction data on layer 1
- Roll up smart contracts in layer 1 that enforce transaction executions on layer 2 via the layer 1 transaction data.

Another important thing to keep in mind is that rollups require operators to stake a bond in the smart rollup contract. This provides an incentive to operators to flawlessly verify and execute transactions, which is ultimately beneficial when it comes to lowering fees for users on the network, not to mention increasing transaction speeds and opening up to even more participants. To take things even further, there are two primary rollups, each with its own predefined security model.³⁵ Zero-Knowledge Rollups,³⁶ or ZK-Rollups for short, gather and “roll up” hundreds of different transfers off-chain before generating a cryptographic proof, which is known as a succinct non-interactive argument of knowledge (SNARK) which functions as a validity proof on layer 1.³⁷ The ZK-Rollup smart contract contains the state of every layer 2 transaction,³⁸ and the only way to update the smart contract is with the SNARK validity proof, meaning that ZK-Rollups need one single validity proof instead of voluminous amounts of transaction data to function. As one can probably guess, validating a block via a ZK-Rollup is much quicker and cheaper than other options, given that less data is needed.

But on the other side of the coin, we have what are known as Optimistic Rollups, which sit in parallel to the main Ethereum chain on layer 2. Optimistic Rollups have many attractive features, particularly when it comes to scalability, as they don’t do any computation by default. Rather, after each transaction, these rollups essentially “notarise” new transactions by proposing a new state to the main net. Given that Optimistic Rollups don’t compute the transaction, there needs to be a mechanism in place to ensure that transactions are legitimate and not linked to any cases of fraud. Enter the fraud proofs. If someone notices any fraudulent or suspicious transactions, the rollup will automatically execute a fraud proof and run the transaction’s computation using the available state data.³⁹ Unfortunately, the downside is that Optimistic Rollups may result in longer wait times for transaction confirmation than a ZK-Rollup, as transactions can be challenged for verification issues.⁴⁰ The key thing to remember about the differences between the two is that ZK-Rollups submit a validity proof to the chain⁴¹ whilst Optimistic Rollups assume that transactions are valid, submitting a fraud proof in the event of a challenge.⁴² The topic of ZK-Rollups is going to be important to monitor over the coming years as the topic of scalability comes to the forefront. Each blockchain and ecosystem will propose different approaches and solutions and we should expect to see debates on what approaches are best or most appropriate.

5 Decentralised Autonomous Organisations (DAO)

As its name implies, a Decentralised Autonomous Organisation (DAO) is decentralised (i.e., its decision-making is made by its members and there is no centralised executive team or board) and autonomous (i.e., the organisation runs itself regardless of individual internal or external actions). A DAO is governed by a set of rules in the form of a smart contract and lives on the blockchain, with rules that are clear and transparent for everyone to see. Think of these DAOs like an internet-native business that's collectively owned and managed by its members.⁴³ There's no CEO who can authorise spending based on their own whims and no chance of a dodgy CFO manipulating the books, since everything is in the open and the rules around spending are baked into the DAO via its code (Table 1).

As mentioned, the decision-making process within a DAO is different from that of a traditional company or organisation, although the intent is the same. For instance, a traditional company will have articles of association or a shareholders' agreement, but these documents are typically kept confidential, whilst the rules of a DAO are open to the public, visible for everyone to see. Whilst a traditional company has a board of directors elected by shareholders and entrusted to make decisions, a DAO is set up in a fashion that resembles a system in which shareholders can vote directly for any necessary changes. In the event of a dispute between a traditional company's shareholders and its board of directors, the parties will wind up going to court over a resolution. However, in a DAO, every decision is automatically executed; there are no grey areas open to interpretation. Once a vote passes, the outcome is seamlessly executed, due to the smart contract backbone of the DAO model,

Table 1 Differences between DAOs and traditional organisations broken down by structure, governance, and levels of transparency

DAO	Traditional Organisation
Flat and fully democratised.	Hierarchical with a CEO or a leadership team.
Members can vote for any change.	Most changes can be done by decision of the board although some may need approval by shareholders.
Following a vote, outcome is implemented automatically by leveraging smart contract functionalities.	In cases that shareholding voting needs to take place, it needs to be manually counted or handled by a centralised entity.
DAO activities are public and fully transparent for anyone to see.	Most of the activity is private or limited to its shareholders.

which defines the rules of the organisation and maintains the group's treasury. Once the contract is live on the blockchain, no one can change the rules except by a vote. If anyone tries to do something outside the bounds of the code, it will fail, and since the rules of the treasury are also defined by smart contract code, no one can spend any money without group consent. This means that DAOs don't need a central authority,⁴⁴ and the group makes collective decisions and grants authority to distribute payments once the requisite number of votes pass. Most DAOs that exist today operate on a token membership model,⁴⁵ and in order to vote, a user needs to hold tokens which are available for anyone to buy.

One of the first public examples of a DAO was known as The DAO, which launched in June 2016 following a crowdfunding haul of US\$150 million. Unfortunately, The DAO was almost immediately hacked and drained of US\$50 million in cryptocurrency. Fortunately, the hack was reversed shortly afterwards, and the funds recovered via a hard fork of the Ethereum blockchain, which ironically gave rise to Ethereum Classic. Another milestone took place in April 2021 after the U.S. state of Wyoming allowed DAOs to obtain legal company status.⁴⁶ This was an innovative step, as it allowed DAOs to operate in a decentralised manner whilst holding legal status. For example, the Wyoming legislation requires that a DAO specify its structure by having "DAO" or "DAO LLC" in its registered name⁴⁷ (in the same way that a normal company limited by shares would have Limited or Ltd.). The law also requires that the DAO's articles of organisation be clearly indicated, though in this case, the articles of organisation can be written in code.⁴⁸

The most notable DAO-related event occurred in November 2021 when a DAO was created to buy a copy of the U.S. Constitution. Formed entirely over Discord, an 8,000-person collective of crypto aficionados used crowdfunding for over \$40 million worth of ETH in less than a week to bid on a rare copy of the Constitution up for auction at Sotheby's, one of only thirteen in existence. In exchange for ETH donations, supporters received PEOPLE, an ERC-20 token that would grant holders of the token governance powers in the DAO. However, the \$43.17 million bid submitted by the group, known as ConstitutionDAO, fell just short (ironically to the Citadel hedge fund founder Ken Griffin). Despite the outcome, ConstitutionDAO fueled a flood of new interest for DAOs, with everyone from the New York Times to the Wall Street Journal racing to explain how these vehicles work and as the auction crept closer, Google searches for the term hit an all-time peak.

Whilst DAOs pave the way for a radically different approach to corporate organisation and governance, there are several considerations to be aware of

moving forward. Most importantly, it's tough to change the rules of a smart contract once it has been deployed on the blockchain, making it difficult for a DAO to change course once an input has been set, thus removing the group's flexibility, and in addition, requiring consensus from all could lead to fragmented, unresponsive decision-making. Ultimately, DAOs are yet another exhilarating new feature of the decentralised, crypto-driven Web 3.0 movement, an entirely new structure for autonomous decision-making and self-governance and as we move towards Web 3.0, we should expect to see the concept of a DAO become more mainstream.



Correction to: The Book of Crypto

Correction to:

H. Arslanian, *The Book of Crypto*,

<https://doi.org/10.1007/978-3-030-97951-5>

This book was inadvertently published with the following errors, which have now been corrected. The book has been updated with the changes.

Abbreviations:

p. = page

l. = line

→ = should be replaced by

Corrections:

P.5 – Omit “For the people....served as commodity money.” (as its repeated twice)

P. 46 – Omit last line of 1.1 “Its’s important to mention....known until 1976. (as its repeated twice)

P.54 – “knownas” → known as..

P. 97 – Omit “last week’s” in the box

The updated version of these chapters can be found at

https://doi.org/10.1007/978-3-030-97951-5_1

https://doi.org/10.1007/978-3-030-97951-5_2

https://doi.org/10.1007/978-3-030-97951-5_3

https://doi.org/10.1007/978-3-030-97951-5_6

https://doi.org/10.1007/978-3-030-97951-5_8

P138 – Omit the “pt” in “ptPseudo-anaonymous.”

P. 142 – “Fig. 3” → Fig. 3 Security/Scalability/Decentralisation.

P. 172 – Figure 1 should be at the bottom of that page.

Conclusion

My goal through this book was to provide you all with a solid foundation on the world of crypto-assets and empower you with knowledge for whatever goal you have in mind, from joining a new crypto company to exploring crypto as an investment. I hope that the book made you reflect, gave you new ideas, and even made you think of new opportunities based on your own unique perspective and expertise. The future of money is here and is marked by both excitement and uncertainty. Unlocking the full potential of financial innovation will require all stakeholders to work together. You have a role to play in this new reality and hopefully, this book gave you the foundational knowledge to do so.

If you enjoyed this book, feel free to put a review on whatever platform you bought it from. It really helps us authors bring more visibility to the book. If you'd like to connect, feel free to contact me on my website (www.henriarslanian.com), LinkedIn (<https://www.linkedin.com/in/henriarslanian/>) or Twitter (<https://twitter.com/HenriArslanian>). I'd love to hear your feedback and discuss the future of money in more depth.

It was a pleasure sharing my knowledge and expertise via this book and I truly hope that you found it interesting and insightful. Welcome to the future of money!

Henri Arslanian

Notes

Frontmatter

1. Book is available on official website of the publisher Palgrave <https://www.palgrave.com/gp/book/9783030145323> or Amazon <https://www.amazon.com/Future-Finance-FinTech-Financial-Services/dp/3030145328>.

Chapter 1

1. If interested in the history of money, there are dozens of interesting and insightful books worth reading. I would recommend either James DiBianco's "From Cowries to Crypto" or Jack Weatherford's "The History of Money", both of which I quote extensively in this book.
2. <https://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm>, accessed January 1, 2022.
3. <https://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm>.
4. Glyn Davies, "A History of Money", 4th edition, p. 17.
5. <https://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm>.
6. Davies, p. 12.
7. Davies, p. 12.
8. Davies, p. 13.
9. Davies, p. 15.
10. Davies, p. 17.

11. Weatherford, p. 23.
12. Davies, p. 21.
13. Davies, p. 21.
14. <https://www.theguardian.com/world/2019/mar/13/venezuela-hyperinflation-bolivar-banknotes-dollars> and <https://www.thenewhumanitarian.org/news/2013/01/10/ringing-changes-end-bartering-zimbabwe> and <https://www.jstor.org/stable/27733572>, accessed January 1, 2022.
15. Weatherford, p. 21.
16. Weatherford, p. 21.
17. Weatherford, p. 21.
18. Weatherford, p. 21.
19. Davies, p. 44.
20. Weatherford, p. 22.
21. Weatherford, p. 23.
22. The History of Money, Jack Weatherford, p. 19.
23. Davies, p. 37.
24. <https://www.cambridge.org/us/academic/subjects/history/regional-history-after-1500/shell-money-slave-trade>, accessed January 1, 2022.
25. Davies, p. 38.
26. <https://en.wiktionary.org/wiki/%E8%B2%9D#Translingual>, accessed January 1, 2022.
27. Weatherford, p. 24.
28. Weatherford, p. 24.
29. Weatherford, p. 24.
30. <https://www.bankofcanadamuseum.ca/2017/06/yap-stone-returns/>, accessed January 1, 2022.
31. <https://indiancountrytoday.com/archive/from-beads-to-bounty-how-wampum-became-americas-first-currencyand-lost-its-power>, accessed January 1, 2022.
32. Davies, p. 41.
33. <https://indiancountrytoday.com/archive/from-beads-to-bounty-how-wampum-became-americas-first-currencyand-lost-its-power>.
34. <https://indiancountrytoday.com/archive/from-beads-to-bounty-how-wampum-became-americas-first-currencyand-lost-its-power>, accessed January 1, 2022.
35. <https://indiancountrytoday.com/archive/from-beads-to-bounty-how-wampum-became-americas-first-currencyand-lost-its-power>.
36. James DiBiasio, From Cowries to Crypto, p. 10.
37. DiBiasio, p. 11.
38. Weatherford, p. 26.

39. Weatherford, p. 26.
40. Weatherford, p. 27.
41. Davis, p. 58.
42. Davis, p. 58.
43. Davis, p. 58.
44. Davis, p. 58.
45. Davis, p. 58.
46. DiBiasio, p. 18.
47. Davis, p. 186.
48. Davis, p. 59.
49. DiBiasio, p. 18.
50. DiBiasio, p. 18.
51. DiBiasio, p. 20.
52. Weatherford, p. 30.
53. DiBiasio, p. 21.
54. Weatherford, p. 32.
55. DiBiasio, p. 21.
56. Weatherford, p. 33.
57. DiBiasio, p. 21.
58. Weatherford, p. 43.
59. DiBiasio, p. 26.
60. Davies, p. 73.
61. DiBiasio, p. 28.
62. DiBiasio, p. 29.
63. DiBiasio, p. 29.
64. DiBiasio, p. 34.
65. Davies, p. 84.
66. DiBiasio, p. 34.
67. DiBiasio, p. 35.
68. DiBiasio, p. 36.
69. Weatherford, p. 48.
70. DiBiasio, p. 36.
71. Davis, p. 101.
72. Davis, p. 112.
73. DiBiasio, p. 39.
74. Davis, p. 112.
75. Weatherford, p. 61.
76. DiBiasio, p. 44.
77. DiBiasio, p. 46.
78. DiBiasio, p. 48.

79. DiBiasio, p. 50.
80. DiBiasio, p. 50.
81. DiBiasio, p. 47.
82. Davis, p. 159.
83. Davis, p. 160.
84. Davis, p. 160.
85. Davis, p. 161.
86. Weatherford, p. 65.
87. Weatherford, p. 66.
88. Weatherford p. 66.
89. DiBiasio, p. 72.
90. Weatherford, p. 71.
91. Weatherford, p. 72.
92. Weatherford, p. 74.
93. Weatherford, p. 75.
94. Weatherford, p. 79.
95. Weatherford, p. 85.
96. Weatherford, p. 85.
97. Weatherford, p. 85.
98. Weatherford, p. 86.
99. Weatherford, p. 86.
100. Weatherford, p. 87.
101. Weatherford, p. 87.
102. Weatherford, p. 87.
103. Weatherford, p. 88.
104. DiBiasio, p. 54.
105. DiBiasio, p. 56.
106. DiBiasio, p. 56.
107. DiBiasio, p. 58.
108. DiBiasio, p. 62.
109. DiBiasio, p. 62.
110. Weatherford, p. 95.
111. DiBiasio, p. 66.
112. DiBiasio, p. 69.
113. Weatherford, p. 99.
114. Weatherford, p. 108.
115. Weatherford, p. 101.
116. DiBiasio, p. 85.
117. DiBiasio, p. 86.
118. DiBiasio, p. 87.

119. DiBiasio, p. 93.
120. <https://www.bankofengland.co.uk/about/history>, accessed January 1, 2022.
121. DiBiasio, p. 94.
122. <https://www.bankofengland.co.uk/about/history>, accessed January 1, 2022.
123. https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/p/Pound_sterling.htm, accessed January 1, 2022.
124. Weatherford, p. 158.
125. Weatherford, p. 117.
126. Weatherford, p. 117.
127. Weatherford, p. 118.
128. Weatherford, p. 132.
129. <https://www.uscurrency.gov/history>, accessed January 1, 2022.
130. Weatherford, p. 137.
131. <https://www.uscurrency.gov/history>.
132. DiBiasio, p. 101.
133. <https://www.uscurrency.gov/history>.
134. DiBiasio, p. 111.
135. <https://www.history.com/news/where-did-the-dollar-sign-come-from>, accessed January 1, 2022.
136. Weatherford, p. 118.
137. <https://projects.exeter.ac.uk/RDavies/arian/dollar.html>, accessed January 1, 2022.
138. <https://projects.exeter.ac.uk/RDavies/arian/dollar.html>.
139. <https://www.history.com/news/where-did-the-dollar-sign-come-from>, accessed January 1, 2022.
140. Weatherford, p. 180.
141. <https://www.uscurrency.gov/history>, accessed January 1, 2022.
142. <https://www.federalreservehistory.org/essays/bretton-woods-created>, accessed January 1, 2022.
143. The 730 delegates at Bretton Woods agreed to establish two new institutions. The International Monetary Fund (IMF) would monitor exchange rates and lend reserve currencies to nations with balance-of-payments deficits. The International Bank for Reconstruction and Development, now known as the World Bank Group, was responsible for providing financial assistance for reconstruction after World War II and the economic development of less developed countries.
144. DiBiasio, p. 113.

145. <https://www.federalreservehistory.org/essays/gold-convertibility-ends>, accessed January 1, 2022.
146. DiBiasio, p. 114.
147. <https://www.federalreservehistory.org/essays/gold-convertibility-ends>.
148. DiBiasio, p. 128.
149. <https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html>, accessed January 1, 2022.
150. “Bitcoin History: The Complete History of Bitcoin [Timeline]”, accessed January 13, 2019, <http://www.historyofbitcoin.org/>.
151. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, May 2009, <https://bitcoin.org/bitcoin.pdf>, accessed January 1, 2022.
152. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, May 2009, <https://bitcoin.org/bitcoin.pdf>.
153. For simplicity’s sake, we refer to Satoshi Nakamoto as he/him in gender pronouns, although no one has ever been able to conclusively prove who this mysterious figure is.
154. “Bitcoin Forum,” Bitcointalk.org, accessed January 13, 2019, <https://bitcointalk.org/>.
155. Satoshi Nakamoto,” Wikipedia, January 12, 2019, https://en.wikipedia.org/w/index.php?title=Satoshi_Nakamoto&oldid=878012844.
156. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” May 2009, <https://bitcoin.org/bitcoin.pdf>.
157. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” May 2009, <https://bitcoin.org/bitcoin.pdf>.
158. For any reader interested in learning more in detail about the mechanics of how the Bitcoin blockchain works, I recommend “The Basics of Bitcoins and Blockchains” by my friend Antony Lewis, who explains in detail how the Bitcoin blockchain works. For programmers keen to learn more about the code, I recommend “Master Bitcoin: Programming the Open Blockchain” by Andreas Antonopoulos. There are obviously many books out there, but I think these are good starting points.

Chapter 2

1. “Cryptography”, Wikipedia, January 11, 2019, <https://en.wikipedia.org/w/index.php?title=Cryptography&oldid=877811989>.
2. “Encryption”, Wikipedia, January 12, 2019, <https://en.wikipedia.org/w/index.php?title=Encryption&oldid=878014939>.

3. Chris Burniske and Jack Tatar, “Crypto-Assets: The Innovative Investor’s Guide to Bitcoin and Beyond”, McGraw Hill Professional, 2017.
4. Chris Burniske and Jack Tatar, “Crypto-Assets: The Innovative Investor’s Guide to Bitcoin and Beyond”, McGraw Hill Professional, 2017.
5. “Cryptography”, Wikipedia, January 11, 2019, <https://en.wikipedia.org/w/index.php?title=Cryptography&oldid=877811989>.
6. “Cryptography”, Wikipedia, January 11, 2019, <https://en.wikipedia.org/w/index.php?title=Cryptography&oldid=877811989>.
7. “RSA (Cryptosystem)”, Wikipedia, January 6, 2019, [https://en.wikipedia.org/w/index.php?title=RSA_\(cryptosystem\)&oldid=877066365](https://en.wikipedia.org/w/index.php?title=RSA_(cryptosystem)&oldid=877066365).
8. Antony Lewis, “The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology That Powers Them”, Mango Media, 2018.
9. Jameson Lopp, “Bitcoin and the Rise of the Cypherpunks”, CoinDesk (blog), April 9, 2016, <https://www.coindesk.com/the-rise-of-the-cypherpunks>.
10. David Chaum, “Security without Identification: Transaction Systems to Make Big Brother Obsolete”, *Communications of the ACM* 28, no. 10 (October 1, 1985): 1030–1044, <https://doi.org/10.1145/4372.4373>.
11. Jimmy Aki, “ECash Founder David Chaum Makes Bold Promises with Elixir Blockchain”, *Bitcoin Magazine*, accessed January 13, 2019, <https://bitcoinmagazine.com/articles/ecash-founder-david-chaum-makes-bold-promises-elixir-blockchain/>.
12. <https://cointelegraph.com/top-people-in-crypto-and-blockchain/david-chaum#:~:text=David%20Chaum's%202019%3A&text=In%20August%20Chaum%20revealed%20a,of%20its%20sister%20project%20Elixir>, accessed January 1, 2022.
13. <https://www.youtube.com/watch?v=Y7wltsTCROY>, accessed January 1, 2022.
14. Robert Manne, “The Cypherpunk Revolutionary: Julian Assange | The Monthly”, *The Monthly*, March 2011, <https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary>.
15. Eric Hughes, “A Cypherpunk’s Manifesto”, Activism.net, March 1993, <https://www.activism.net/cypherpunk/manifesto.html>.
16. Adam Back, “[ANNOUNCE] Hash Cash Postage Implementation”, Hashcash.org, March 28, 1997, <http://www.hashcash.org/papers/announce.txt>.

17. Wei Dai, “BMoney”, November 6, 2018, <http://www.weidai.com/>.
18. Wei Dai, “Wei Dai’s Home Page”, November 6, 2018, <http://www.weidai.com/>.
19. William Suberg, “John Oliver Compares Bitcoin with Bitconnect, Ridicules Tapscott’s ‘Dumb’ McNugget Metaphor”, Cointelegraph, March 12, 2018, <https://cointelegraph.com/news/john-oliver-com-pares-bitcoin-with-bitconnect-ridicules-tapscotts-dumb-mcnugget-metaphor>.
20. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, May 2009, <https://bitcoin.org/bitcoin.pdf>.
21. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, May 2009, <https://bitcoin.org/bitcoin.pdf>.
22. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, May 2009, <https://bitcoin.org/bitcoin.pdf>.
23. Chris Burniske and Jack Tatar, “Crypto-Assets: The Innovative Investor’s Guide to Bitcoin and Beyond”, McGraw Hill Professional, 2017, p. 212.
24. <https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>, accessed January 1, 2022.
25. Chris Burniske and Jack Tatar, “Crypto-Assets: The Innovative Investor’s Guide to Bitcoin and Beyond”, McGraw Hill Professional, 2017, p. 212.
26. “Bitcoin Block Reward Halving Countdown”, accessed January 13, 2019, <https://www.bitcoinblockhalf.com/>.
27. <https://www.bitcoinblockhalf.com/>.
28. Chris Burniske and Jack Tatar, “Crypto-Assets: The Innovative Investor’s Guide to Bitcoin and Beyond”, McGraw Hill Professional, 2017, p. 214.
29. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, May 2009, <https://bitcoin.org/bitcoin.pdf>.
30. Chris Burniske and Jack Tatar, “Crypto-Assets: The Innovative Investor’s Guide to Bitcoin and Beyond”, McGraw Hill Professional, 2017, p. 212.
31. <https://www.techradar.com/news/best-mining-rig>, accessed January 1, 2022.
32. “Laszlo Hanyecz”, Bitcoin Wiki, accessed January 13, 2019, https://en.bitcoin.it/wiki/Laszlo_Hanyecz.
33. <https://bitcointalk.org/index.php?topic=137.msg1141#msg1141>, accessed January 1, 2022.

34. Kitco News, “2013: Year Of The Bitcoin”, Forbes, December 10, 2013, <https://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/#2f0b622e303c>.
35. Kitco News, “2013: Year of The Bitcoin”, Forbes, December 10, 2013, <https://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/#2f0b622e303c>.
36. “Confirmed Transactions Per Day”, Blockchain.com, accessed January 13, 2019, <https://www.blockchain.com/charts/n-transactions>.
37. Jake Frankenfield, “Silk Road”, Investopedia, October 26, 2016, <https://www.investopedia.com/terms/s/silk-road.asp>.
38. <http://www.deepwebthemovie.com/#land>, accessed January 1, 2022.
39. <https://time.com/3673321/silk-road-dread-pirate-roberts/>, accessed January 1, 2022.
40. <https://freeross.org/>, accessed January 1, 2022.
41. Andy Greenberg, “Your Sloppy Bitcoin Drug Deals Will Haunt You for Years”, Wired, January 26, 2018, <https://www.wired.com/story/bitcoin-drug-deals-silk-road-blockchain/>.
42. <https://decrypt.co/41127/how-chainalysis-helps-catch-cryptocurrency-criminals>, accessed January 1, 2022.
43. <https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-lchainalyargest-darknet-child>, accessed January 1, 2022.
44. Andy Greenberg, “Your Sloppy Bitcoin Drug Deals Will Haunt You for Years”, Wired, January 26, 2018, <https://www.wired.com/story/bitcoin-drug-deals-silk-road-blockchain/>.
45. Robert McMillan Metz Cade, “The Rise and Fall of the World’s Largest Bitcoin Exchange”, Wired, November 6, 2013, <https://www.wired.com/2013/11/mtgox/>.
46. Andrew Norry, “The History of the Mt Gox Hack: Bitcoin’s Biggest Heist”, Blockonomi, November 19, 2018, <https://blockonomi.com/mt-gox-hack/>.
47. Garrick Hileman, “State of Bitcoin and Blockchain 2016: Blockchain Hits Critical Mass”, CoinDesk, January 28, 2016, <https://www.coindesk.com/state-of-bitcoin-blockchain-2016>.
48. Evelyn Cheng, “Bitcoin Tops \$8,700 to Record High as Coinbase Adds 100,000 Users”, CNBC, November 26, 2017, <https://www.cnbc.com/2017/11/25/bitcoin-tops-8700-to-record-high-as-coinsbase-adds-100000-users.html>.
49. Gedalyah Reback, “Binance Claims 240,000 New Users in One Hour after Relaunching Service”, Cointelligence, January 11, 2018, <https://>

- www.coindiligence.com/content/binance-claims-240000-new-users-in-one-hour-after-relaunching-service/.
50. Sean Williams, “5 Brand-Name Businesses That Currently Accept Bitcoin—The Motley Fool”, The Motley Fool, July 6, 2017, <https://www.fool.com/investing/2017/07/06/5-brand-name-businesses-that-currently-accept-bitc.aspx>.
 51. PricewaterhouseCoopers, “PwC Accepts Payment in Bitcoin for Its Advisory Services”, PwC, November 30, 2017, <https://www.pwchka.com/en/press-room/press-releases/pr-301117.html>.
 52. Kate Rooney, “Nouriel Roubini: Bitcoin Is ‘Mother of All Scams’”, CNBC, October 11, 2018, <https://www.cnbc.com/2018/10/11/roubini-bitcoin-is-mother-of-all-scams.html>.
 53. <https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo44>, accessed January 1, 2022.
 54. <https://news.gallup.com/poll/266807/percentage-americans-owns-stock.aspx>, accessed January 1, 2022.
 55. <https://www.finder.com/how-many-people-own-cryptocurrency?ref=hackernoon.com>, accessed January 1, 2022.
 56. <https://www.ledger.com/nomura-ledger-global-advisors-building-komainu-secure-digital-asset-custody/>, accessed January 1, 2022.
 57. <https://www.jpmorgan.com/global/news/digital-coin-payments>, accessed January 1, 2022.
 58. <https://www.reuters.com/article/us-julius-baer-seba-crypto/julius-baer-gets-into-crypto-banking-with-seba-partnership-idUSKCN1QF1H8>, accessed January 1, 2022.
 59. <https://libra.org/en-US/>, accessed January 1, 2022.
 60. <https://www.coindesk.com/chinas-central-bank-likely-to-pilot-digital-currency-in-cities-of-shenzhen-and-suzhou-report>, accessed January 1, 2022.
 61. <https://bitslog.com/2019/04/16/the-return-of-the-deniers-and-the-revenge-of-patoshii/>, accessed January 1, 2022.
 62. <https://blog.bitmex.com/satoshis-1-million-bitcoin/>, accessed January 1, 2022.
 63. <https://blog.bitmex.com/satoshis-1-million-bitcoin/>.
 64. <https://www.forbes.com/sites/billybambridge/2020/11/19/leaked-citybank-report-reveals-bitcoin-could-rocket-to-300000-price-by-end-of-2021/>, accessed January 1, 2022.
 65. https://www.dbresearch.com/servlet/reweb2.ReWEB?rwsite=RPS_EN-PROD&rwoj=ReDisplay.Start.class&document=PROD0000000000513730, accessed January 1, 2022.

66. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/09/2020-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf>, accessed January 1, 2022.
67. <https://markets.businessinsider.com/news/currencies/paypal-cash-app-buying-newly-mined-bitcoin-2020-11>, accessed January 1, 2022.
68. <https://markets.businessinsider.com/news/currencies/paypal-cash-app-buying-newly-mined-bitcoin-2020-11>.
69. <https://decrypt.co/50783/wells-fargo-bitcoin-cryptocurrencies-no-fad>, accessed January 1, 2022.
70. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/>, accessed January 1, 2022.
71. https://crypto.com/images/202107_DataReport_OnChain_Market_Sizing.pdf, accessed January 1, 2022.
72. <https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/>, accessed January 1, 2022.
73. <https://link.springer.com/article/10.1134/S1019331619060145>, accessed January 1, 2022.
74. <https://www.gemini.com/state-of-us-crypto>, accessed January 1, 2022.
75. <https://www.bankofcanada.ca/wp-content/uploads/2020/08/sdp2020-8.pdf>, accessed January 1, 2022.
76. <https://www.fca.org.uk/publications/research/research-note-crypto-asset-consumer-research-2021>, accessed January 1, 2022.
77. <https://www.worldbank.org/en/country/elsalvador/overview#1>, accessed January 1, 2022.
78. <https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=SV>, accessed January 1, 2022.
79. <https://www.govinfo.gov/content/pkg/STATUTE-79/pdf/STATUTE-79-Pg254.pdf#page=1>, accessed January 1, 2022.
80. <https://pastebin.com/syrmj3ET>, accessed January 1, 2022.
81. <https://bitcoin.org/bitcoin.pdf>, accessed January 1, 2022.
82. https://www.pcworld.com/article/499375/could_wikileaks_scandal_lead_to_new_virtual_currency.html, accessed January 1, 2022.
83. <https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280>, accessed January 1, 2022.
84. History.com Editors, “Ford Motor Company Unveils the Model T”, History, November 13, 2009, <https://www.history.com/this-day-in-history/ford-motor-company-unveils-the-model-t>.
85. <https://www.bloomberg.com/news/videos/2021-01-22/bitcoin-based-on-faith-has-nil-value-grantham-says-video>, accessed January 1, 2022.

86. <https://markets.businessinsider.com/news/currencies/bitcoin-value-negative-environmental-impact-nouriel-roubini-cryptocurrencies-2021-2>, accessed January 1, 2022.
87. Manny Trillo, “Visa Transactions Hit Peak on Dec. 23”, Visa’s Blog – Visa Viewpoints (blog), January 12, 2011, <https://www.visa.com/blog/archives/us/2011/01/12/visa-transactions-hit-peak-on-dec-23/index.html>.
88. <https://digiconomist.net/bitcoin-energy-consumption>, accessed January 1, 2022.
89. <https://lightning.network/lightning-network-paper.pdf>, accessed January 1, 2022.
90. <https://static1.squarespace.com/static/60377b34e7791c1277aaae97/t/615cb9aeaab8c63e1a732771/1633466815710/The+State+of+Lightning.pdf>, accessed January 1, 2022.
91. <https://static1.squarespace.com/static/60377b34e7791c1277aaae97/t/615cb9aeaab8c63e1a732771/1633466815710/The+State+of+Lightning.pdf>.
92. <https://static1.squarespace.com/static/60377b34e7791c1277aaae97/t/615cb9aeaab8c63e1a732771/1633466815710/The+State+of+Lightning.pdf>.
93. <https://static1.squarespace.com/static/60377b34e7791c1277aaae97/t/615cb9aeaab8c63e1a732771/1633466815710/The+State+of+Lightning.pdf>.
94. <https://medium.com/liquality/hash-time-locked-contracts-htlcs-explained-e88aa99cc824>, accessed January 1, 2022.
95. <https://lightning.network/lightning-network-summary.pdf>, accessed January 1, 2022.
96. <https://www.pwc.ch/en/insights/digital/crypto-custody-risks-and-controls-from-an-auditors-perspective.html>, accessed January 1, 2022.
97. <https://blogs.worldbank.org/peoplemove/lightning-disruption-remitance-costs-silver-lining-entrepreneurship-during-crisis>, accessed January 1, 2022.
98. Colin Harper, “Making Sense of Proof of Work vs. Proof of Stake”, CoinCentral, January 24, 2018, <https://coincentral.com/making-sense-of-proof-of-work-vs-proof-of-stake/>.
99. Colin Harper, “Making Sense of Proof of Work vs. Proof of Stake”, CoinCentral, January 24, 2018, <https://coincentral.com/making-sense-of-proof-of-work-vs-proof-of-stake/>.
100. <https://www.binance.vision/blockchain/proof-of-stake-explained>, accessed January 1, 2022.

101. Shaan Ray, “The Difference Between Traditional and Delegated Proof of Stake”, Hacker Noon, April 23, 2018, <https://hackernoon.com/the-difference-between-traditional-and-delegated-proof-of-stake-36a3e3f25f7d>. (It’s important to note that in few cases, new currency units can be created by inflating the coin supply and can be used to reward forgers.)
102. Shaan Ray, “The Difference Between Traditional and Delegated Proof of Stake”, Hacker Noon, April 23, 2018, <https://hackernoon.com/the-difference-between-traditional-and-delegated-proof-of-stake-36a3e3f25f7d>. (It’s important to note that in few cases, new currency units can be created by inflating the coin supply and can be used to reward forgers.)
103. <https://docs.ethhub.io/ethereum-basics/monetary-policy/>, accessed January 1, 2022.

Chapter 3

1. Alyssa Hertig, “What Is Ethereum?—CoinDesk Guides”, CoinDesk (blog), accessed January 13, 2019, <https://www.coindesk.com/information/what-is-ethereum>.
2. <https://docs.ethhub.io/ethereum-basics/history-and-forks/>, accessed January 1, 2022.
3. <https://docs.ethhub.io/ethereum-basics/history-and-forks/>.
4. <https://docs.ethhub.io/ethereum-basics/history-and-forks/>.
5. <https://docs.ethhub.io/ethereum-basics/history-and-forks/>.
6. <https://docs.ethhub.io/ethereum-basics/monetary-policy/>, accessed January 1, 2022.
7. <https://etherscan.io/chart/blocktime>, accessed January 1, 2022.
8. <https://ethereum.org/en/eth2/>, accessed January 1, 2022.
9. Alyssa Hertig, “How Do Ethereum Smart Contracts Work?”, CoinDesk (blog), accessed January 13, 2019, <https://www.coindesk.com/information/ethereum-smart-contracts-work>.
10. Alyssa Hertig, “What Is a Decentralized Application?”, CoinDesk (blog), accessed January 13, 2019, <https://www.coindesk.com/information/what-is-a-decentralized-application-dapp>.
11. Jake Frankenfield, “Smart Contracts”, Investopedia, April 18, 2017, <https://www.investopedia.com/terms/s/smart-contracts.asp>.
12. “ERC-20”, Wikipedia, December 19, 2018, <https://en.wikipedia.org/w/index.php?title=ERC-20&oldid=874510987>.
13. <https://media.consensys.net/a-short-history-of-ethereum-a8fdc5b4362c>.

14. <https://docs.ethhub.io/using-ethereum/mining/#uncle-blocks>, accessed January 1, 2022.
15. <https://ethereum.org/en/whitepaper/>, accessed January 1, 2022.
16. <https://ethereum.org/en/whitepaper/>.
17. <https://ethereum.org/en/whitepaper/>.
18. <https://docs.ethhub.io/ethereum-basics/what-is-ether/>, accessed January 1, 2022.
19. <https://ethereum.org/en/developers/docs/gas/>, accessed January 1, 2022.
20. <https://docs.ethhub.io/using-ethereum/transactions/#summary>, accessed January 1, 2022.
21. <https://media.consensys.net/solidity-is-twice-as-popular-as-the-next-blockchain-coding-language-9330af9aeaa3>, accessed January 1, 2022.
22. <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md>, accessed January 1, 2022.
23. <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md>.
24. <https://www.theblockcrypto.com/data/on-chain-metrics/ethereum>.
25. <https://www.theblockcrypto.com/data/on-chain-metrics/ethereum>, accessed January 1, 2022.
26. <https://www.theblockcrypto.com/data/on-chain-metrics/ethereum>.

Chapter 4

1. <https://blockchain-comparison.com/blockchain-protocols/>, accessed January 1, 2022.
2. <https://ethereum.org/en/developers/docs/scaling/>, accessed January 1, 2022.
3. <https://www.gemini.com/cryptopedia/blockchain-layer-2-network-layer-1-network#section-layer-2-scaling-solutions>, accessed January 1, 2022.
4. <https://www.avax.network/>, accessed January 1, 2022.
5. <https://www.avax.network/>.
6. <https://www.avax.network/>.
7. <https://research.binance.com/en/projects/bnb>, accessed January 1, 2022.
8. <https://research.binance.com/en/projects/bnb>.
9. <https://www.binance.com/en/blog/ecosystem/introducing-bnb-autoburn-a-new-protocol-for-the-quarterly-bnb-burn-421499824684903205>, accessed January 1, 2022.
10. <https://research.binance.com/en/projects/bnb>, accessed January 1, 2022.
11. <https://www.bitcoincash.org/roadmap/>, accessed January 1, 2022.
12. <https://www.bitcoincash.org/roadmap/>.
13. <https://bitcoinsv.com/en>, accessed January 1, 2022.

14. <https://bitcoinsv.com/en/why-bsv>, accessed January 1, 2022.
15. <https://www.coindesk.com/crypto-genius-or-fake-the-craig-wright-saga-explained>, accessed January 1, 2022.
16. <https://iohk.io/en/research/library/>, accessed January 1, 2022.
17. <https://cointelegraph.com/blockchain-for-beginners/a-beginners-guide-to-the-cardano-network-and-the-ada-ecosystem>, accessed January 1, 2022.
18. <https://cardano.org/>, accessed January 1, 2022.
19. <https://cardano.org/>.
20. <https://roadmap.cardano.org/en/>, accessed January 1, 2022.
21. <https://www.gemini.com/cryptopedia/what-is-chainlink-and-how-does-it-work>, accessed January 1, 2022.
22. <https://chain.link/use-cases>, accessed January 1, 2022.
23. <https://www.gemini.com/cryptopedia/what-is-chainlink-and-how-does-it-work>.
24. <https://www.dash.org/faq/>, accessed January 1, 2022.
25. <https://multicoин.capital/2018/03/02/delegated-proof-stake-features-tradeoffs/#edd-free-download-modal>, accessed January 1, 2022.
26. <https://medium.com/loom-network/understanding-blockchain-fundamentals-part-3-delegated-proof-of-stake-b385a6b92ef>, accessed January 1, 2022.
27. <https://medium.com/loom-network/understanding-blockchain-fundamentals-part-3-delegated-proof-of-stake-b385a6b92ef>.
28. <https://steemit.com/dpos/@dantheчman/dpos-consensus-algorithm-this-missing-white-paper>, accessed January 1, 2022.
29. <https://www.coindesk.com/google-cloud-eos-block-producer-candidate>, accessed January 1, 2022.
30. <https://steemit.com/dpos/@dantheчman/dpos-consensus-algorithm-this-missing-white-paper>.
31. <https://eosnetworkmonitor.io/>, accessed January 1, 2022.
32. <https://www.coindesk.com/everyones-worst-fears-about-eos-are-proving-true>, accessed January 1, 2022.
33. <https://www.coindesk.com/on-eos-blockchain-vote-buying-is-business-as-usual>, accessed January 1, 2022.
34. <https://coinmarketcap.com/currencies/eos/>, accessed January 1, 2022.
35. <https://hedera.com/>, accessed January 1, 2022.
36. <https://hedera.com/>.
37. <https://help.hedera.com/hc/en-us/articles/360000674097>, accessed January 1, 2022.

38. <https://messari.io/asset/hedera-hashgraph/profile>, accessed January 1, 2022.
39. <https://www.iota.org/get-started/what-is-iota>, accessed January 1, 2022.
40. <https://cryptalker.com/iota-miota/>, accessed January 1, 2022.
41. <https://litecoin.org/>, accessed January 1, 2022.
42. <https://en.cryptonomist.ch/2019/06/15/mining-algorithms-proof-of-work/>, accessed January 1, 2022.
43. <https://www.litecoinpool.org/pools>, accessed January 1, 2022.
44. "Monero FAQ", The Monero Project, accessed January 13, 2019, <https://getmonero.org/get-started/faq/index.html>.
45. <https://www.getmonero.org/get-started/faq/#anchor-different>, accessed January 1, 2022.
46. <https://www.monerooutreach.org/quick-facts.html>, accessed January 1, 2022.
47. <https://polkadot.network/PolkaDotPaper.pdf>, accessed January 1, 2022.
48. <https://polkadot.network/technology/>, accessed January 1, 2022.
49. <https://wiki.polkadot.network/docs/learn-comparisons-ethereum-2>, accessed January 1, 2022.
50. <https://polkadot.network/technology/>, accessed January 1, 2022.
51. <https://polkadot.network/technology/>.
52. <https://wiki.polkadot.network/docs/learn-DOT>, accessed January 1, 2022.
53. <https://polygon.technology/lightpaper-polygon.pdf>, accessed January 1, 2022.
54. <https://ripple.com/xrp/>, accessed January 1, 2022.
55. <https://xrpl.org/xrp.html>, accessed January 1, 2022.
56. <https://xrpl.org/>, accessed January 1, 2022.
57. <https://xrpl.org/intro-to-consensus.html>, accessed January 1, 2022.
58. <https://xrpl.org/intro-to-consensus.html>.
59. <https://xrpl.org/overview.html>, accessed January 1, 2022.
60. <https://xrpl.org/intro-to-consensus.html>.
61. <https://xrpl.org/intro-to-consensus.html>.
62. <https://xrpl.org/xrp.html>.
63. https://woofpaper.org/SHIBAINU_Ecosystem_WOOF_Paper.pdf, accessed January 1, 2022.
64. https://woofpaper.org/SHIBAINU_Ecosystem_WOOF_Paper.pdf.
65. <https://docs.solana.com/introduction>, accessed January 1, 2022.
66. <https://docs.solana.com/introduction>.
67. <https://docs.solana.com/introduction>.
68. <https://docs.solana.com/history>, accessed January 1, 2022.

69. <https://solana.com/solana-whitepaper.pdf>, accessed January 1, 2022.
70. <https://medium.com/solana-labs/proof-of-history-a-clock-for-blockchain-cf47a61a9274>, accessed January 1, 2022.
71. <https://docs.solana.com/history>.
72. <https://explorer.solana.com/supply>, accessed January 1, 2022.
73. https://docs.solana.com/inflation/inflation_schedule, accessed January 1, 2022.
74. <https://docs.solana.com/introduction>.
75. <https://docs.solana.com/cluster/synchronization#:~:text=Solana%20takes%20a%20very%20different,before%20the%20proof%20was%20generated>, accessed January 1, 2022.
76. https://docs.solana.com/transaction_fees, accessed January 1, 2022.
77. <https://docs.solana.com/cluster/synchronization>, accessed January 1, 2022.
78. <https://docs.solana.com/cluster/synchronization>.
79. <https://docs.solana.com/cluster/synchronization>.
80. <https://www.stellar.org/learn/anchor-basics>, accessed January 1, 2022.
81. <https://www.stellar.org/lumens>, accessed January 1, 2022.
82. <https://www.stellar.org/foundation?locale=en>, accessed January 1, 2022.
83. <https://wiki.tezos.com/learn/whitepaper>, accessed January 1, 2022.
84. <https://tezos.com/learn/what-is-tezos/>, accessed January 1, 2022.
85. <https://tezos.com/learn/bake/>, accessed January 1, 2022.
86. <https://wiki.tezos.com/learn/whitepaper#economy> and <https://messari.io/asset/tezos/profile/supply-schedule>, accessed January 1, 2022.
87. <https://coinmarketcap.com/currencies/tezos/>, accessed January 1, 2022.
88. <https://tron.network/faq?lng=en>, accessed January 1, 2022.
89. <https://coinmarketcap.com/currencies/tron/>, accessed January 1, 2022.
90. <https://tron.network/faq?lng=en>.
91. https://www.vechain.org/whitepaper/#bit_hcihs, accessed January 1, 2022.
92. https://www.vechain.org/whitepaper/#bit_hcihs.
93. <https://z.cash/technology/>, accessed January 1, 2022.
94. <https://z.cash/technology/>.
95. <https://www.amazon.com/Future-Finance-FinTech-Financial-Services/dp/3030145328>, accessed January 1, 2022.
96. <https://z.cash/technology/>.
97. <https://messari.io/asset/zcash/profile>, accessed January 1, 2022.

Chapter 5

1. Chris Burniske and Jack Tatar, “Crypto-assets: The Innovative Investor’s Guide to Bitcoin and Beyond”, McGraw Hill Professional, 2017.
2. Richbodo, “Usage of the Word ‘Blockchain’”, *Richbodo* (blog), September 20, 2017, <https://medium.com/@richbodo/common-use-of-the-word-blockchain-5b916cecef29>.
3. Chris Burniske and Jack Tatar, “*Crypto-assets: The Innovative Investor’s Guide to Bitcoin and Beyond*”, McGraw Hill Professional, 2017.
4. Edward Robinson and Matthew Leising, “Blythe Masters Tells Banks the Blockchain Changes Everything—Bloomberg”, Bloomberg News, accessed January 13, 2019, <https://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything>.
5. “The Trust Machine—The Promise of the Blockchain,” The Economist, accessed January 13, 2019, <https://www.economist.com/leaders/2015/10/31/the-trust-machine>.
6. Chris Burniske and Jack Tatar, “*Crypto-assets: The Innovative Investor’s Guide to Bitcoin and Beyond*”, McGraw Hill Professional, 2017.
7. <https://www.merriam-webster.com/words-at-play/new-words-in-the-dictionary-march-2018>, accessed January 1, 2022.
8. <https://www.coindesk.com/one-network-many-chains-the-case-for-blockchain-interoperability>, accessed January 1, 2022.
9. Michael J. Casey and Paul Vigna, “In Blockchain We Trust”, MIT Technology Review, April 9, 2018, <https://www.technologyreview.com/s/610781/in-blockchain-we-trust/>.
10. “What is the Difference between DLT and Blockchain? | BBVA”, BBVA, accessed January 13, 2019, <https://www.bbva.com/en/difference-dlt-blockchain/>.
11. Max Thake, “What’s the Difference between Blockchain and DLT?”, *Nakamo.To* (blog), February 8, 2018, <https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd>.
12. Max Thake, “What’s the Difference between Blockchain and DLT?”, *Nakamo.To* (blog), February 8, 2018, <https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd>.
13. Praveen Jayachandran, “The Difference between Public and Private Blockchain”, Blockchain Pulse: IBM Blockchain Blog, May 31, 2017, <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/>.
14. Chris Burniske and Jack Tatar, “*Crypto-assets: The Innovative Investor’s Guide to Bitcoin and Beyond*”, McGraw Hill Professional, 2017.

15. <https://b3i.tech/who-we-are.html>, accessed January 1, 2022.
16. <https://www.bbva.com/en/large-spanish-companies-form-alastria-consortium-develop-blockchain-ecosystem-spain/>, accessed January 1, 2022.
17. <https://bsnbase.io/g/main/index>, accessed January 1, 2022.
18. Jesus Leal Trujillo, Steve Fromhart, and Val Srinivas, “The Evolution of Blockchain Technology”, Deloitte Insights, November 6, 2017, <https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html>.
19. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf>, p. 30, accessed January 1, 2022.
20. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf>, p. 46, accessed January 1, 2022.
21. https://www.accenture.com/t20170120T074124Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf, accessed January 1, 2022.
22. “AXA Goes Blockchain with Fizzy | AXA”, AXA, September 13, 2017, https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy%23xto%3DCS3-9-%5BShared_Article%5D-%5Baxa_goes_blockchain_with_fizzy%5D.
23. Dentons Rodyk, “Establishing a Chain of Title—Leveraging Blockchain for the Real Estate Industry”, November 20, 2017, <https://dentons.rodyk.com/en/insights/alerts/2017/november/21/establishing-a-chain-of-title-leveraging-blockchain-for-the-real-estate-industry>.
24. Molly Jane Zuckerman, “Swedish Government Land Registry Soon To Conduct First Blockchain Property Transaction”, Cointelegraph, March 7, 2018, <https://cointelegraph.com/news/swedish-government-land-registry-soon-to-conduct-first-blockchain-property-transaction>.
25. Alexandru Oprunenco and Chami Akmeemana, “Using Blockchain to Make Land Registry More Reliable in India”, United Nations Development Programme, May 1, 2018, <http://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html>.
26. <https://www.straitstimes.com/asia/east-asia/let-it-go-japan-pm-declares-war-on-ink-stamp-hanko>, accessed January 1, 2022.
27. <https://www.bloomberg.com/news/articles/2020-05-20/need-for-digital-signatures-gives-japan-firm-a-22-fold-return?sref=EsSwv0DV>, accessed January 1, 2022.

Chapter 6

1. This is the same approach that I took in my previous book as well. I believe there is merit in continuing with the same approach for consistency purposes. <https://www.amazon.com/Future-Finance-FinTech-Financial-Services/dp/3030145328>, accessed January 1, 2022.
2. <https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.pdf>, accessed January 1, 2022.
3. The only exception here is if Bitcoin is coming from a tainted wallet or has been used in nefarious activities, but let's suppose that's not the case here.
4. <https://news.bitcoin.com/industry-execs-freshly-minted-virgin-bitcoins/>, accessed January 1, 2022.
5. Ricky Cove, "Breaking down Bitcoin and Cryptocurrencies: Key Characteristics", Market Realist, November 21, 2017, <https://marketrealist.com/2017/11/breaking-down-bitcoin-and-cryptocurrencies-key-characteristics>.
6. <https://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm>, accessed January 1, 2022.
7. <https://www.merriam-webster.com/dictionary/cryptocurrency>, accessed January 1, 2022.
8. <https://coinsharesgroup.com/assets/resources/Research/bitcoin-mining-network-december-2019.pdf>, accessed January 1, 2022.
9. <https://ftalphaville.ft.com/2019/09/11/1568182095000/Don-t-bet-on-decentralised-exchanges-becoming-the-new-crypto-frontier--/>, accessed January 1, 2022.
10. <https://neo-ngd.github.io/reference/How-To-Become-NEO-Consensus-Node.html#current-consensus-nodes>, accessed January 1, 2022.
11. <https://www.forbes.com/sites/billybambridge/2019/12/20/xrp-disappears-after-ripples-surprise-boost/#2ec2f1722568>, accessed January 1, 2022.
12. <https://www.nber.org/papers/w26214.pdf>, accessed January 1, 2022.
13. <https://www.getmonero.org/resources/moneropedia/ringCT.html#:~:text=RingCT%2C%20short%20for%20Ring%20Confidential,all%20transactions%20on%20the%20network>, accessed January 1, 2022.
14. <https://localmonero.co/knowledge/monero-stealth-addresses?language=en>, accessed January 1, 2022.
15. <https://www.perkinscoie.com/images/content/2/3/v7/237411/Perkins-Coie-LLP-White-Paper-AML-Regulation-of-Privacy-enabling.pdf>, accessed January 1, 2022.

16. <https://ciphertrace.com/ciphertrace-files-two-monero-cryptocurrency-tracing-patents/>, accessed January 1, 2022.

Chapter 7

1. <https://www.blockchain.com/ru/static/pdf/StablecoinsReportFinal.pdf>, accessed January 1, 2022.
2. <https://www.economist.com/leaders/2019/04/13/the-cost-of-cross-border-payments-needs-to-drop>, accessed January 1, 2022.
3. <https://www.economist.com/leaders/2019/04/13/the-cost-of-cross-border-payments-needs-to-drop>.
4. <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2019/09/stablecoins-a-global-overview-of-regulatory-requirements-in-asia-pacific-europe-the-uae-and-the-us.pdf>, accessed January 1, 2022.
5. <https://www.pwc.com/us/en/industries/financial-services/library/pdf/pwc-loopring-stablecoin-paper.pdf>, accessed January 1, 2022.
6. <https://www.pwc.com/us/en/industries/financial-services/library/pdf/pwc-loopring-stablecoin-paper.pdf>.
7. <https://tether.to/fees/>, accessed January 1, 2022.
8. <https://blockchain.capital/the-business-of-stablecoins/#:-text=It%20turns%20out%20that%20stablecoin,upside%20is%20driven%20by%20seigniorage.&text=Stablecoin%20issuers%2C%20on%20the%20ther,issuance%20mechanics%20and%20network%20growth>, accessed January 1, 2022.
9. <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2019/09/stablecoins-a-global-overview-of-regulatory-requirements-in-asia-pacific-europe-the-uae-and-the-us.pdf>, accessed January 1, 2022.
10. <https://support.usdc.circle.com/hc/en-us/articles/360015278132-What-is-CENTRE-and-how-is-it-related-to-Circle-USDC->, accessed January 1, 2022.
11. <https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2.html>, accessed January 1, 2022.
12. <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>, p. 47, accessed January 1, 2022.
13. Matt Robinson and Tom Schoenberg, "Bitcoin-Rigging Criminal Probe Focused on Tie to Tether", *Bloomberg News*, November 20, 2018, <https://www.bloomberg.com/news/articles/2018-11-20/bitcoin-rigging-criminal-probe-is-said-to-focus-on-tie-to-tether>.
14. <https://tether.to/wp-content/uploads/2018/06/FSS1JUN18-Account-Snapshot-Statement-final-15JUN18.pdf>, accessed January 1, 2022.

15. <https://wallet.tether.to/transparency>, accessed January 1, 2022.
16. <https://tether.to/>, accessed January 1, 2022.
17. <https://ag.ny.gov/press-release/2019/attorney-general-james-announces-court-order-against-crypto-currency-company>, accessed January 1, 2022.
18. <https://www.jdsupra.com/legalnews/the-new-york-attorney-general-s-office-9385268/#:-:text=In%20late%20February%2C%20the%20New,%24850%20million%20in%20customer%20funds>, accessed January 1, 2022.
19. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066, accessed January 1, 2022.
20. <https://www.wsj.com/articles/large-bitcoin-player-manipulated-price-sharply-higher-study-says-11572863400>, accessed January 1, 2022.
21. <https://www.coindesk.com/markets/2021/05/13/tethers-first-reserve-breakdown-shows-token-49-backed-by-unspecified-commercial-paper/>, accessed January 1, 2022.
22. <https://www.pwc.com/us/en/industries/financial-services/library/pdf/pwc-loopring-stablecoin-paper.pdf>, accessed January 1, 2022.
23. <https://community-development.makerdao.com/makerdao-scd-faqs/scd-faqs/stability-fee>, accessed January 1, 2022.
24. <https://community-development.makerdao.com/makerdao-scd-faqs/scd-faqs/stability-fee>.
25. <https://community-development.makerdao.com/makerdao-scd-faqs/scd-faqs/stability-fee>.
26. <https://mkr.tools/governance/stability-fee>, accessed January 1, 2022.
27. <https://cointelegraph.com/news/makerdao-slashes-stability-fees-as-stable-coin-demand-wanes>, accessed January 1, 2022.
28. <https://makerdao.com/en/whitepaper/#risk-parameters>, accessed January 1, 2022.
29. <https://www.pwc.com/us/en/industries/financial-services/library/pdf/pwc-loopring-stablecoin-paper.pdf>, accessed January 1, 2022.
30. http://basis.io/basis_whitepaper_en.pdf, accessed January 1, 2022.
31. <http://basis.io/>.
32. http://basis.io/basis_whitepaper_en.pdf, p. 11.
33. <http://basis.io/>.
34. <https://www.coindesk.com/1b-fei-stablecoins-rocky-start-is-a-wake-up-call-for-defi-investors>, accessed January 1, 2022.
35. <https://docs.terra.money/Concepts/Protocol.html>, accessed January 1, 2022.

36. https://assets.website-files.com/611153e7af981472d8da199c/618b02d13e938ae1f8ad1e45_Terra_White_paper.pdf, accessed January 1, 2022.
37. <https://docs.terra.money/Concepts/Protocol.html#the-market-module-and-arbitrage>, accessed January 1, 2022.
38. <https://docs.terra.money/Concepts/Protocol.html#the-market-module-and-arbitrage>.
39. Facebook changed its name to Meta in November 2021 and Libra was changed to Diem. I will use Facebook and Meta interchangeably and will refer to Libra or Diem depending on the period we are referring to.
40. https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf, accessed January 1, 2022.
41. <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/#:~:text=How%20many%20users%20does%20Facebook,the%20biggest%20social%20network%20worldwide>, accessed January 1, 2022.
42. <https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR>, accessed January 1, 2022.
43. <https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR>.
44. <https://www.econstor.eu/bitstream/10419/204501/1/167792165X.pdf>, accessed January 1, 2022.
45. <https://trends.google.com/trends/explore?date=today%205-y&geo=HK&q=libra>, accessed January 1, 2022.
46. <https://www.diem.com/en-us/white-paper/>, accessed January 1, 2022.
47. <https://www.diem.com/en-us/white-paper/>.
48. <https://www.finma.ch/en/news/2020/04/20200416-mm-libra/>, accessed January 1, 2022.
49. <https://www.diem.com/en-us/white-paper/#cover-letter>, accessed January 1, 2022.
50. <https://www.diem.com/en-us/updates/ceo-announcement/>, accessed January 1, 2022.
51. <https://www.diem.com/en-us/updates/diem-association/>, accessed January 1, 2022.
52. <https://about.fb.com/news/2020/05/welcome-to-novi/>, accessed January 1, 2022.
53. <https://www.cnbc.com/2021/05/12/facebook-backed-diem-is-moving-from-switzerland-to-the-us.html>, accessed January 1, 2022.
54. <https://www.ft.com/content/e237df96-7cc1-44e5-a92f-96170d34a9bb>.

Chapter 8

1. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, p. 8, accessed January 1, 2022.
2. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, p. 8.
3. <https://www.money.co.uk/guides/colour-of-currency.htm>, accessed January 1, 2022.
4. <https://www.money.co.uk/guides/colour-of-currency.htm>.
5. <https://www.money.co.uk/guides/colour-of-currency.htm>.
6. <https://www.money.co.uk/guides/colour-of-currency.htm>.
7. <https://documents1.worldbank.org/curated/en/311991468037132740/pdf/WPS5356.pdf>, accessed January 1, 2022.
8. <https://www.unodc.org/unodc/en/money-laundering/overview.html#:~:text=The%20estimated%20amount%20of%20money,goes%20through%20the%20laundering%20cycle.>
9. <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering>, accessed January 1, 2022.
10. <https://www.bis.org/about/bisih/topics/cbdc.htm>, accessed January 1, 2022.
11. <https://www.hkma.gov.hk/eng/key-functions/money/hong-kong-currency/money-past-and-present/history-of-note-issuing-banks-in-hong-kong/>, accessed January 1, 2022.
12. <https://www.hkma.gov.hk/eng/key-functions/money/hong-kong-currency/notes/>, accessed January 1, 2022.
13. <https://www.hkma.gov.hk/eng/key-functions/money/hong-kong-currency/notes/>.
14. <https://www.amcm.gov.mo/en/currency/currency-in-circulation-in-macao>, accessed January 1, 2022.
15. <https://www.bankofengland.co.uk/banknotes/scottish-and-northern-ireland-banknotes>, accessed January 1, 2022.
16. JP Koning, “Fedcoin: A Central Bank-Issued Cryptocurrency”, R3, November 15, 2016, <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/58c7f80c2e69cf24220d335e/1489500174018/R3+Report+-+Fedcoin.pdf>.
17. Aleksander Berentsen and Fabian Schar, “The Case for Central Bank Electronic Money and the Non-Case for Central Bank Cryptocurrencies”, Federal Reserve Bank of St. Louis Second Quarter 2018, Vol. 100, No. 2 (February 28, 2018), <https://doi.org/10.20955/r.2018.97-106>.

18. Morten Linnemann Bech and Rodney Garratt, "Central Bank Cryptocurrencies", BIS Quarterly Review, September 17, 2017, https://www.bis.org/publ/qtrpdf/r_qt1709f.htm, p. 64.
19. Morten Linnemann Bech and Rodney Garratt, "Central Bank Cryptocurrencies", BIS Quarterly Review, September 17, 2017, https://www.bis.org/publ/qtrpdf/r_qt1709f.htm, p. 64.
20. <https://www.bankofcanada.ca/wp-content/uploads/2020/08/sdp2020-8.pdf>, accessed January 1, 2022.
21. <https://www.bankofcanada.ca/wp-content/uploads/2020/08/sdp2020-8.pdf>.
22. https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro-539fa8cd8d.en.pdf, accessed January 1, 2022.
23. <https://pages.consensys.net/central-banks-and-the-future-of-digital-money>, accessed January 1, 2022.

Chapter 9

1. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, p. 8, accessed January 1, 2022.
2. <https://www.bis.org/cpmi/publ/d22.pdf>, accessed January 1, 2022.
3. https://en.wikipedia.org/wiki/Real-time_gross_settlement, accessed January 1, 2022.
4. <https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf>, p. 16, accessed January 1, 2022.
5. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, accessed January 1, 2022.
6. <https://www.adb.org/sites/default/files/publication/539801/adbi-central-bank-digital-currency-and-fintech-asia.pdf>, p. 38, accessed January 1, 2022.
7. "Fintech Experiments and Projects", Bank of Canada, accessed January 13, 2019, <https://www.bankofcanada.ca/research/digital-currencies-and-fintech/fintech-experiments-and-projects/>.
8. "Project Ubin", Singapore Financial Centre | Monetary Authority of Singapore, accessed January 13, 2019, <http://www.mas.gov.sg/singapore-financial-centre/smart-financial-centre/project-ubin.aspx>.
9. <https://www.adb.org/sites/default/files/publication/539801/adbi-central-bank-digital-currency-and-fintech-asia.pdf>, p. 39, accessed January 1, 2022.

10. https://essay.utwente.nl/78027/1/Ginneken_MA_BMS.pdf, p. 14, accessed January 1, 2022.
11. https://essay.utwente.nl/78027/1/Ginneken_MA_BMS.pdf, p. 14, accessed January 1, 2022.
12. https://essay.utwente.nl/78027/1/Ginneken_MA_BMS.pdf, p. 14.
13. In addition, such a wholesale CBDC could reduce settlement and counterparty risks and enable delivery-versus-payment (DvP) or payment-versus-payment (PvP) in cross-border interbank securities transactions and funds transfers. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, accessed January 1, 2022.
14. https://www.boj.or.jp/en/announcements/release_2019/data/rel190604a1.pdf, p. 4, accessed January 1, 2022.
15. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopica_l190604_1.en.pdf, accessed January 1, 2022.
16. https://www.boj.or.jp/en/announcements/release_2019/data/rel190604a1.pdf, p. 5.
17. https://www.boj.or.jp/en/announcements/release_2019/data/rel190604a1.pdf, p. 5.
18. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopica_l190604_1.en.pdf.
19. https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Report_on_Project_Inthanon-LionRock.pdf, p. 7, accessed January 1, 2022.
20. https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Report_on_Project_Inthanon-LionRock.pdf, p. 24.
21. https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Report_on_Project_Inthanon-LionRock.pdf, p. 24.
22. https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Report_on_Project_Inthanon-LionRock.pdf, p. 24.
23. https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Report_on_Project_Inthanon-LionRock.pdf, p. 24.
24. https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Report_on_Project_Inthanon-LionRock.pdf, p. 24.
25. https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Report_on_Project_Inthanon-LionRock.pdf, p. 21.
26. <http://www.sama.gov.sa/en-US/News/Pages/news29012019.aspx>, accessed January 1, 2022.
27. <https://www.bis.org/press/p210610a.htm>, accessed January 1, 2022.
28. <https://ripple.com/riplenet/>, accessed January 1, 2022.

29. https://ripple.com/files/ripplenet_brochure.pdf, accessed January 1, 2022.
30. https://www.boj.or.jp/en/announcements/release_2019/data/rel190604a1.pdf, accessed January 1, 2022.
31. <https://opennodes.com/2021-04-22-02-40-28-multi-cbdcs-designing-a-digital-currency-stack-for-governability>, accessed January 1, 2022.
32. <https://opennodes.com/2021-04-22-02-40-28-multi-cbdcs-designing-a-digital-currency-stack-for-governability>.
33. <https://opennodes.com/2021-04-22-02-40-28-multi-cbdcs-designing-a-digital-currency-stack-for-governability>.
34. <https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin>, accessed January 1, 2022.
35. <https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm>, accessed January 1, 2022.
36. <https://opennodes.com/2021-04-22-02-40-28-multi-cbdcs-designing-a-digital-currency-stack-for-governability>.
37. https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm, accessed January 1, 2022.
38. <https://www.bis.org/about/bisih/about.htm>, accessed January 1, 2022.
39. https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Inthanon-LionRock_to_mBridge_Building_a_multi_CBDC_platform_for_international_payments.pdf, p. 34, accessed January 1, 2022.
40. https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Inthanon-LionRock_to_mBridge_Building_a_multi_CBDC_platform_for_international_payments.pdf.

Chapter 10

1. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, accessed January 1, 2022.
2. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351-c8c18bbd60.en.pdf>, p. 6, accessed January 1, 2022.
3. S. Mohammad Davoodalhosseini, “Central Bank Digital Currency and Monetary Policy”, Funds Management and Banking Department, Bank of Canada, July 2018, <https://www.bankofcanada.ca/wp-content/uploads/2018/07/swp2018-36.pdf>, p. 9.
4. https://en.wikipedia.org/wiki/Zero_lower_bound, accessed January 1, 2022.

5. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351-c8c18bbd60.en.pdf>, p. 6, accessed January 1, 2022.
6. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351-c8c18bbd60.en.pdf>, p. 6.
7. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351-c8c18bbd60.en.pdf>, p. 9, accessed January 1, 2022.
8. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351-c8c18bbd60.en.pdf>, p. 13.
9. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, p. 9, accessed January 1, 2022.
10. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, p. 9.
11. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351-c8c18bbd60.en.pdf>, p. 4, accessed January 1, 2022.
12. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, p. 9.
13. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>, p. 16, accessed January 1, 2022.
14. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>.
15. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>, p. 10.
16. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>, pp. 13–15, accessed January 1, 2022.
17. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>, p. 16, accessed January 1, 2022.
18. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>, p. 7.
19. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>, p. 23, accessed January 1, 2022.
20. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>, p. 35.
21. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, p. 9, accessed January 1, 2022.

22. https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf, p. 24, accessed January 1, 2022.
23. <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf>, p. 43, accessed January 1, 2022.
24. <https://sov.foundation/law.pdf>, accessed January 1, 2022.
25. <https://docsend.com/view/nvi59vw>, accessed January 1, 2022.
26. <https://docsend.com/view/nvi59vw>.
27. <https://docsend.com/view/nvi59vw>.
28. <https://docsend.com/view/nvi59vw>.
29. <https://docsend.com/view/nvi59vw>.
30. <https://docsend.com/view/nvi59vw>.
31. <https://www.centralbanking.com/fintech/cbdc/7840006/imf-warns-marshall-islands-on-digital-projects#:~:text=The%20Marshall%20Islands%20does%20not,rests%20with%20the%20finance%20ministry>, accessed January 1, 2022.
32. <https://docsend.com/view/nvi59vw>.
33. <https://www.imf.org/en/News/Articles/2021/03/22/pr2173-marshall-islands-imf-staff-completes-2021-article-iv-mission>, accessed January 1, 2022.
34. <https://www.reuters.com/business/el-salvador-keep-dollar-legal-tender-seeks-world-bank-help-with-bitcoin-2021-06-16/>, accessed January 1, 2022.
35. <https://www.bis.org/publ/arpdf/ar2021e3.pdf>, p. 78, accessed January 1, 2022.
36. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, accessed January 1, 2022.
37. <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>, accessed January 1, 2022.
38. <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>, p. 1.
39. <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>, p. 12.
40. <https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/stored-value-facilities-and-retail-payment-systems/regulatory-regime-for-stored-value-facilities/>, accessed January 1, 2022.
41. <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>, p. 12, accessed January 1, 2022.
42. https://en.wikipedia.org/wiki/Chicago_plan, accessed January 1, 2022.

43. <https://www.tnbusa.com/about/>, accessed January 1, 2022.
44. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, p. 18, accessed January 1, 2022.
45. <https://www.bis.org/publ/othp33.pdf>, accessed January 1, 2022.
46. http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf, p. 18, accessed January 1, 2022.
47. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf>, accessed January 1, 2022.
48. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf>.
49. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf>, accessed January 1, 2022.
50. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-krona-pilot-phase-1.pdf>, p. 7, accessed January 1, 2022.
51. “D”, representing digital, is prefixed to “XCD”, the international currency code for the EC dollar.
52. <https://www.eccb-centralbank.org/p/security>, accessed January 1, 2022.
53. <https://www.bis.org/publ/arpdf/ar2021e3.pdf>, p. 78, accessed January 1, 2022.
54. <https://www.bis.org/publ/arpdf/ar2021e3.pdf>, p. 79.
55. <https://www.bis.org/publ/arpdf/ar2021e3.pdf>, p. 79.
56. <https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf>, accessed January 1, 2022.
57. <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf>, accessed January 1, 2022.
58. <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf>, p. 25, accessed January 1, 2022.
59. <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf>, p. 26.
60. <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf>, p. 44, accessed January 1, 2022.
61. https://bakong.nbc.org.kh/download/NBC_BAKONG_White_Paper.pdf, accessed January 1, 2022.
62. <https://soramitsu.co.jp/bakong-press-release>, accessed January 1, 2022.
63. https://bakong.nbc.org.kh/download/NBC_BAKONG_White_Paper.pdf, p. 21, accessed January 1, 2022.

64. https://bakong.nbc.org.kh/download/NBC_BAKONG_White_Paper.pdf, p. 23.
65. <https://www.sanddollar.bs/>, accessed January 1, 2022.
66. <https://www.sanddollar.bs/>.
67. <https://www.sanddollar.bs/keyplayers>, accessed January 1, 2022.
68. <https://www.sanddollar.bs/individual>, accessed January 1, 2022.
69. <https://www.bis.org/publ/arpdf/ar2021e3.pdf>, p. 79, accessed January 1, 2022.
70. <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>, accessed January 1, 2022.

Chapter 11

1. “Global Digital Finance Code of Conduct: Taxonomy for Cryptographic Assets”, Global Digital Finance, October 2018, https://www.gdf.io/wp-content/uploads/2018/10/0003_GDF_Taxonomy-for-Cryptographic-Assets_Web-151018.pdf.
2. “Statement on Initial Coin Offerings”, Securities & Futures Commission of Hong Kong, September 5, 2017, <https://www.sfc.hk/web/EN/news-and-announcements/policy-statements-and-announcements/statement-on-initial-coin-offerings.html>.
3. June Lin, “Is a Country Club Membership a Security?”, Primerus, <http://www.primerus.com/business-law-news/is-a-country-club-membership-a-security.htm>, accessed January 13, 2019.
4. <https://www.sec.gov/news/press-release/2019-202>, accessed January 1, 2022.
5. <https://www.cnbc.com/2018/05/31/a-blockchain-start-up-just-raised-4-billion-without-a-live-product.html>, accessed January 1, 2022.
6. <https://www.sec.gov/news/press-release/2019-202>.
7. <https://www.coindesk.com/telegram-doubles-amount-raised-in-ico-to-1-7-billion>, accessed January 1, 2022.
8. <https://www.sec.gov/news/press-release/2019-212>.
9. <https://www.sec.gov/news/press-release/2020-146>, accessed January 1, 2022.
10. <https://telegra.ph/What-Was-TON-And-Why-It-Is-Over-05-12>, accessed January 1, 2022.
11. <https://variant.fund/writing/the-ownership-economy-crypto-and-consumer-software>, accessed January 1, 2022.
12. <https://blockonomi.com/dj-rac-launches-rac-token-ethereum/>, accessed January 1, 2022.

Chapter 12

1. Kate Rooney, “SEC Chairman Clayton Says Agency Won’t Change Definition of a Security”, *CNBC*, June 6, 2018, <https://www.cnbc.com/2018/06/06/sec-chairman-clayton-says-agency-wont-change-definition-of-a-security.html>.
2. <https://www.ledgerinsights.com/blockchain-fintech-figure-raises-100-million/>, accessed January 1, 2022.
3. https://www.bis.org/about/bisih/topics/green_finance/green_bonds.htm, accessed January 1, 2022.
4. “Global Digital Finance Code of Conduct: Taxonomy for Cryptographic Assets”, Global Digital Finance, October 2018, https://www.gdf.io/wp-content/uploads/2018/10/0003_GDF_Taxonomy-for-Cryptographic-Assets_Web-151018.pdf.
5. Helen Zhao, “Own Shares of Brooklyn Building with Tokens Blockchain Real Estate”, March 19, 2018, <https://www.cnbc.com/2018/03/19/own-shares-of-brooklyn-building-with-tokens-blockchain-real-estate.html>.
6. “The Aspen Digital Security Token”, Indiegogo Token Sales, accessed January 13, 2019, <https://blockchain.indiegogo.com/projects/aspen/>.
7. <https://www.coindesk.com/nba-player-spencer-dinwiddies-token-sale-hits-10-of-13-5m-goal>, accessed January 1, 2022.
8. Molly Jane Zuckerman, “Andy Warhol Painting to Be Sold via Blockchain in ‘World’s First’ Crypto Art Auction”, Cointelegraph, June 7, 2018, <https://cointelegraph.com/news/andy-warhol-painting-to-be-sold-via-blockchain-in-world-s-first-crypto-art-auction>.

Chapter 13

1. Phil Glazer, “An Overview of Non-Fungible Tokens”, Hacker Noon, April 1, 2018, <https://hackernoon.com/an-overview-of-non-fungible-tokens-5f140c32a70a>.
2. “CryptoKitties Cripple Ethereum Blockchain”, December 5, 2017, sec. Technology, <https://www.bbc.com/news/technology-42237162>.
3. <https://www.forbes.com/sites/davidseideman/2018/09/19/tech-entrepreneur-determines-first-true-estimate-of-sports-memorabilia-market-5-4-billion/#77c9a9a552e8>, accessed January 1, 2022.
4. <https://www.thegamer.com/pokemon-cards-worth-car-nothing-any-more/>, accessed January 1, 2022.
5. <https://www.thegamer.com/rare-magic-gathering-cards-worth/>, accessed January 1, 2022.

6. <https://techstartups.com/2018/07/06/highly-sought-domain-name-crypto-com-sold-millions-dollars/>, accessed January 1, 2022.
7. <https://www.theverge.com/2019/1/16/18184302/fortnite-revenue-battle-pass-earnings-2018>, accessed January 1, 2022.
8. <https://opensea.io/blog/guides/non-fungible-tokens/>, accessed January 1, 2022.
9. <https://www.coindesk.com/colored-coins-paint-sophisticated-future-for-bitcoin>, accessed January 1, 2022.
10. <https://www.larvalabs.com/cryptopunks>, accessed January 1, 2022.
11. “ERC-721”, accessed January 13, 2019, <http://erc721.org/>.
12. CryptoKitties, “CryptoKitties | Collect and Breed Digital Cats!”, CryptoKitties, accessed January 13, 2019, <https://www.cryptokitties.co>.
13. “CryptoKitties: Collectible and Breedable Cats Empowered by Blockchain Technology”, White Paper (CryptoKitties, n.d.).
14. <https://techcrunch.com/2018/03/20/cryptokitties-raises-12m-from-and-reessen-horowitz-and-union-square-ventures/>, accessed January 1, 2022.
15. <https://www.fldeletatime.com/>, accessed January 1, 2022.
16. <https://mlbcryptobaseball.com/about>, accessed January 1, 2022.
17. <https://fortune.com/2018/08/13/mlb-crypto-baseball-blockchain/>, accessed January 1, 2022.
18. “Decentraland,” accessed January 13, 2019, <https://decentraland.org/>.
19. <https://decentraland.org/blog/tutorials/placing-nft-art-into-a-scene/>, accessed January 1, 2022.
20. <https://www.mycryptoheroes.net/>, accessed January 1, 2022.
21. <https://www.godsunchained.com/>, accessed January 1, 2022.
22. <https://www.binance.vision/blockchain/a-guide-to-crypto-collectibles-and-non-fungible-tokens-nfts>, accessed January 1, 2022.
23. <https://www.microsoft.com/skills/azureheroes>, accessed January 1, 2022.
24. https://www.prweb.com/releases/classic_game_book_series_to_be_revised_to_blockchain/prweb16755121.htm, accessed January 1, 2022.
25. https://www.ots.at/presseaussendung/OTS_20190611_OTS0146/crypto-stamp-oesterreichische-post-praesentiert-die-erste-blockchain-briefmarke-der-welt-bild, accessed January 1, 2022.
26. <https://www.linkedin.com/pulse/future-money-3-new-ideas-you-need-know-week-issue-34-arslanian/>, accessed January 1, 2022.
27. https://twitter.com/RiceFarmerNFT/status/1437956083058978826?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1437956088998072325%7Ctwgr%5E%7Ctwcon%5Es2_&ref_url=https%3A%2F%2Fwww.bbc.com%2Fnews%2Ftechnology-58585342, accessed January 1, 2022.

28. <https://twitter.com/0xZuwu/status/1437921263394115584>, accessed January 1, 2022.
29. <https://opensea.io/blog/announcements/employee-information-use-at-opensea/>, accessed January 1, 2022.
30. <https://www.eublockchainforum.eu/sites/default/files/2021-07/NFT%20%E2%80%93%20Legal%20Token%20Classification.pdf>, accessed January 1, 2022.
31. “Home,” Sovrin, accessed January 13, 2019, <https://sovrin.org/>.

Chapter 14

1. Chris Burniske and Jack Tatar, “Crypto-assets: The Innovative Investor’s Guide to Bitcoin and Beyond” (McGraw Hill Professional, 2017), p. 212.
2. <https://www.buybitcoinworldwide.com/mining/hardware/>, accessed January 1, 2022.
3. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf, p. 73, accessed January 1, 2022.
4. <https://digiconomist.net/bitcoin-electronic-waste-monitor/>, accessed January 1, 2022.
5. <https://cryptoslate.com/cryptos/proof-of-work/>, accessed January 1, 2022.
6. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf, p. 86.
7. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf, p. 86.
8. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf, p. 87.
9. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf, p. 87.
10. <https://digiconomist.net/bitcoin-energy-consumption/>, accessed January 1, 2022.
11. <https://digiconomist.net/bitcoin-energy-consumption>.
12. <https://www.blockchain.com/charts/hash-rate?timespan=all>, accessed January 1, 2022.

13. <https://www.bitcoinblockhalf.com/>, accessed January 1, 2022.
14. <https://www.bitcoinblockhalf.com/>.
15. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf>, accessed January 1, 2022.
16. <https://digiconomist.net/bitcoin-energy-consumption/>, accessed January 1, 2022.
17. <https://digiconomist.net/bitcoin-energy-consumption/>.
18. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf>.
19. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/>, accessed January 1, 2022.
20. <https://www.theblockcrypto.com/post/109315/bitcoin-hasrate-declines-50-percent-china-mining-crackdown>, accessed January 1, 2022.
21. <https://digiconomist.net/bitcoin-electronic-waste-monitor/>, accessed January 1, 2022.
22. <https://coinshares.com/assets/resources/Research/bitcoin-mining-network-december-2019.pdf>, accessed January 1, 2022.
23. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf>, accessed January 1, 2022.
24. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf>.
25. <https://digiconomist.net/bitcoin-electronic-waste-monitor/>, accessed January 1, 2022.
26. https://www.nber.org/system/files/working_papers/w26214/w26214.pdf, accessed January 1, 2022.
27. <https://ponderwall.com/index.php/2018/08/25/stop-worrying-much-energy-bitcoin-uses/>, accessed January 1, 2022.
28. <https://simon.medium.com/bitcoin-and-pollution-the-definitive-answer-a010b0826f2a>, accessed January 1, 2022.
29. https://earthworks.org/publications/how_the_20_tons_of_mine_waste_per_gold_ring_figure_was_calculated/, accessed January 1, 2022.
30. <https://www.forbes.com/sites/lawrencewintermeyer/2021/03/10/bitcoins-energy-consumption-is-a-highly-charged-debate--whos-right/?sh=7545cdf37e78>, accessed January 1, 2022.
31. <https://www.gold.org/news-and-events/press-releases/gold-and-climate-change-the-energy-transition-press-release>, accessed January 1, 2022.
32. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf>, accessed January 1, 2022.

33. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf>.
34. <https://www.bloomberg.com/news/articles/2021-05-26/china-s-crypto-mining-crackdown-followed-deadly-coal-accidents>, accessed January 1, 2022.
35. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf>, accessed January 1, 2022.
36. <https://coinshares.com/assets/resources/Research/bitcoin-mining-net-work-december-2019.pdf>, accessed January 1, 2022.
37. <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf>.
38. https://www.hope.com/content/dam/hope-assets/collateral/Mining-Council-Press-Release-Q2_07-01-2021.pdf, accessed January 1, 2022.
39. https://www.hope.com/content/dam/hope-assets/collateral/Mining-Council-Press-Release-Q2_07-01-2021.pdf.
40. https://www.hope.com/content/dam/hope-assets/collateral/Mining-Council-Press-Release-Q2_07-01-2021.pdf.
41. <https://www.bloomberg.com/news/articles/2021-05-26/china-s-crypto-mining-crackdown-followed-deadly-coal-accidents>, accessed January 1, 2022.
42. <https://coinshares.com/assets/resources/Research/bitcoin-mining-net-work-december-2019.pdf>, accessed January 1, 2022.
43. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf, p. 77, accessed January 1, 2022.
44. <https://coinshares.com/assets/resources/Research/bitcoin-mining-net-work-december-2019.pdf>.
45. <https://www.coindesk.com/sichuan-should-work-to-remain-attractive-to-crypto-mining-policy-advisor>, accessed January 1, 2022.
46. <https://www.nature.com/articles/s41467-021-22256-3.pdf>, accessed January 1, 2022.
47. <https://www.nature.com/articles/s41467-021-22256-3.pdf>.
48. <https://www.nature.com/articles/s41467-021-22256-3.pdf>.
49. <https://www.nature.com/articles/s41467-021-22256-3.pdf>.
50. <https://coinshares.com/assets/resources/Research/bitcoin-mining-net-work-december-2019.pdf>, accessed January 1, 2022.
51. <https://coinshares.com/assets/resources/Research/bitcoin-mining-net-work-december-2019.pdf>, p. 4.
52. <https://bsic.it/why-to-buy-when-you-can-mine-an-analysis-of-bitcoins-pricing-models/>, accessed January 1, 2022.

Chapter 15

1. Laura Shin, “Here’s the Man Who Created ICOs and This Is the New Token He’s Backing”, *Forbes*, September 21, 2017, <https://www.forbes.com/sites/laurashin/2017/09/21/heres-the-man-who-created-icos-and-this-is-the-new-token-hes-backing/#6b4878d81183>.
2. Kate Rooney, “A Blockchain Start-up Just Raised \$4 Billion, Without a Live Product”, CNBC, May 31, 2018, <https://www.cnbc.com/2018/05/31/a-blockchain-start-up-just-raised-4-billion-without-a-live-product.html>. (Block.one would then go on to raise around US\$4 billion.)
3. https://www.pwc.ch/en/publications/2020/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf, accessed January 1, 2022.
4. PricewaterhouseCoopers, “Introduction to Token Sales (ICO) Best Practices”, accessed January 13, 2019, <https://www.pwch.kom/en/industries/financial-services/publications/introduction-to-token-sales-ico-best-practices.html>.
5. “China Bans Initial Coin Offerings”, BBC News, September 5, 2017, sec. Business, <https://www.bbc.com/news/business-41157249>.
6. Reuters, “South Korea Bans All New Cryptocurrency Sales”, CNBC, September 29, 2017, <https://www.cnbc.com/2017/09/28/south-korea-bans-all-new-cryptocurrency-sales.html>.
7. Brady Dale, “Even Investors with Access Want ICO Presale Reform”, CoinDesk (blog), November 19, 2017, <https://www.coindesk.com/ico-presales-boost-vc-3iq-multicoin>.
8. Shane Shifflett and Coulter Jones, “Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud”, Wall Street Journal, May 17, 2018, sec. Markets, <https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115>.
9. Matt Levine, “SEC Halts a Silly Initial Coin Offering,” Bloomberg Opinion, December 5, 2017, <https://www.bloomberg.com/opinion/articles/2017-12-05/sec-halts-a-silly-initial-coin-offering>.
10. Eugene Kim, “SEC Warns on ICO Scams, ‘Pump and Dump’ Schemes,” CNBC, August 28, 2017, <https://www.cnbc.com/2017/08/28/sec-warns-on-ico-scams-pump-and-dump-schemes.html>.
11. <https://www.ycombinator.com/documents/>, accessed January 1, 2022.
12. <https://www.cooley.com/-/media/cooley/pdf/reprints/saft-project-whitepaper.ashx>, accessed January 1, 2022.
13. <https://www.cooley.com/-/media/cooley/pdf/reprints/saft-project-whitepaper.ashx>.
14. <https://www.cooley.com/-/media/cooley/pdf/reprints/saft-project-whitepaper.ashx>.

15. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/emeia-financial-services/ey-the-valuation-of-crypto-assets.pdf, accessed January 1, 2022.
16. https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_initialexchangeofferings, accessed January 1, 2022.
17. https://www.pwc.com/ee/et/publications/pub/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf, accessed January 1, 2022.
18. Antony Lewis, “The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology That Powers Them”, Mango Media, 2018, p. 289.
19. John Light, “The Differences Between a Hard Fork, a Soft Fork, and a Chain Split, and What They Mean for The...”, Medium (blog), September 25, 2017, <https://medium.com/@lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9>.
20. Jackie Liu, “Blockchain Research: What the Fork? What Happens When the (Block)chain Splits?”, Blockchain Research Technical University of Munich, July 31, 2017, https://www.blockchain.tum.de/en/news-single-view/?tx_ttnews%5Btt_news%5D=9&cHash=6d77c31a3e4a8161867ee f483b96cdb4.
21. Noelle Acheson, “What Is SegWit?”, CoinDesk (blog), accessed January 13, 2019, <https://www.coindesk.com/information/what-is-segwit>.
22. Jackie Liu, “Blockchain Research: What the Fork? What Happens When the (Block)chain Splits?”, Blockchain Research Technical University of Munich, July 31, 2017, https://www.blockchain.tum.de/en/news-single-view/?tx_ttnews%5Btt_news%5D=9&cHash=6d77c31a3e4a8161867ee f483b96cdb4.
23. <https://www.coindesk.com/business/2020/11/03/uniswaps-retroactive-airdrop-vote-put-free-money-on-the-campaign-trail/>, accessed January 1, 2022.
24. <https://cointelegraph.com/news/defi-trader-scores-over-20-million-in-1inch-token-christmas-airdrop>, accessed January 1, 2022.
25. <https://www.one37pm.com/nft/finance/ens-airdrop-is-here-why-its-important-how-to-claim>, accessed January 1, 2022.
26. <https://compound.finance/governance/comp>.
27. <https://balancer.fi/whitepaper.pdf>.
28. <https://www.defipulse.com/projects/yearn.finance>.
29. <https://medium.com/sushiswap-org/the-sushiswap-project-8716c429ce1>.

30. <https://medium.com/sushiswap-org/the-sushiswap-project-8716c429cee1>.
31. <https://www.coindesk.com/tech/2020/09/01/uniswap-rises-to-top-of-defi-charts-thanks-to-rival-looking-to-unseat-it/>.

Chapter 16

1. <https://academy.binance.com/blockchain/the-complete-beginners-guide-to-decentralized-finance-defi>, accessed January 1, 2022.
2. <https://blog.coinbase.com/a-beginners-guide-to-decentralized-finance-defi-574c68ff43c4>, accessed January 1, 2022.
3. <https://www.mentalfloss.com/article/66150/original-lego-patent>, accessed January 1, 2022.
4. <https://blog.chain.link/defis-permissionless-composability-is-superchar ging-innovation/#:-:text=DeFi%20composability%20allows%20deve lopers%20to,use%20cases%20and%20financial%20products>.
5. <https://community-development.makerdao.com/makerdao-scd-faqs/scd-faqs/stability-fee>, accessed January 1, 2022.
6. <https://community-development.makerdao.com/makerdao-scd-faqs/scd-faqs/stability-fee>.
7. <https://community-development.makerdao.com/makerdao-scd-faqs/scd-faqs/stability-fee>.
8. <https://mkr.tools/governance/stabilityfee>, accessed January 1, 2022.
9. <https://cointelegraph.com/news/makerdao-slashes-stability-fees-as-stable-coin-demand-wanes>, accessed January 1, 2022.
10. <https://makerdao.com/en/whitepaper/#risk-parameters>, accessed January 1, 2022.
11. <https://compound.finance/>, accessed January 1, 2022.
12. <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf>, p.13, accessed January 1, 2022.
13. <https://messari.io/asset/compound/profile>, accessed January 1, 2022.
14. <https://docs.aave.com/faq/>, accessed January 1, 2022.
15. <https://messari.io/asset/aave/profile>, accessed January 1, 2022.
16. <https://docs.aave.com/faq/>, accessed January 1, 2022.
17. <https://medium.com/aave/aave-borrowing-rates-upgraded-f6c8b27973a7>, accessed January 1, 2022.
18. <https://docs.aave.com/developers/guides/flash-loans>.
19. <https://docs.aave.com/developers/guides/flash-loans>.
20. <https://www.coindesk.com/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack>, accessed January 1, 2022.

21. <https://www.coindesk.com/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack>.
22. <https://www.coindesk.com/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack>.
23. <https://uniswap.org/docs/v2/core-concepts/pools>, accessed January 1, 2022.
24. <https://uniswap.org/docs/v2/core-concepts/pools>.
25. <https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281>, accessed January 1, 2022.
26. <https://medium.com/block-journal/uniswap-understanding-the-decentralised-ethereum-exchange-5ee5d7878996>, accessed January 1, 2022.
27. <https://uniswap.org/docs/v2/core-concepts/pools>.
28. <https://decrypt.co/20881/stablecoins-from-heaven-trading-on-curve>, accessed January 1, 2022.
29. <https://cointelegraph.com/news/using-a-defi-protocol-now-costs-more-than-50-as-ethereum-fees-skyrocket>, accessed January 1, 2022.
30. <https://uniswap.org/blog/uniswap-v3/>, accessed January 1, 2022.
31. <https://uniswap.org/blog/launch-uniswap-v3/>, accessed January 1, 2022.
32. <https://defipulse.com/>, accessed January 1, 2022.
33. <https://academy.binance.com/en/articles/impermanent-loss-explained>, accessed January 1, 2022.
34. <https://academy.binance.com/en/articles/impermanent-loss-explained>.
35. <https://blog.bancor.network/beginners-guide-to-getting-rekt-by-impermanent-loss-7c9510cb2f22>, accessed January 1, 2022.
36. <https://pintail.medium.com/uniswap-a-good-deal-for-liquidity-providers-104c0b6816f2>, accessed January 1, 2022.
37. <https://pintail.medium.com/uniswap-a-good-deal-for-liquidity-providers-104c0b6816f2>, accessed January 1, 2022.
38. <https://docs.synthetix.io/synopsis/>, accessed January 1, 2022.
39. <https://docs.synthetix.io/synopsis/>.
40. <https://nexusmutual.gitbook.io/docs/faq>, accessed January 1, 2022.
41. <https://nexusmutual.gitbook.io/docs/faq>.
42. <https://nexusmutual.gitbook.io/docs/faq>.
43. <https://nexusmutual.gitbook.io/docs/use-cases#risk-assessment>, accessed January 1, 2022.
44. <https://yearn.finance/dashboard>, accessed January 1, 2022.
45. <https://docs.yearn.finance/yearn-finance/yvaults/overview>, accessed January 1, 2022.

Chapter 17

1. FINMA, “FINMA Publishes ICO Guidelines”, Swiss Financial Market Supervisory Authority FINMA, February 16, 2018, <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>.
2. Michael del Castillo, “For Blockchain Startups, Switzerland’s ‘Crypto Valley’ Is No New York”, CoinDesk (blog), October 31, 2016, <https://www.coindesk.com/blockchain-innovation-switzerland-crypto-valley-new-york>.
3. Paddy Baker, “Gibraltar Stock Exchange Confirms Move into Security Tokens”, Crypto Briefing (blog), July 11, 2018, <https://cryptobriefing.com/gibraltar-stock-exchange-security-tokens/>; Viren Vaghela and Andrea Tan, “How Malta Became a Hub of the Cryptocurrency World”, Bloomberg News, April 23, 2018, <https://www.bloomberg.com/news/articles/2018-04-23/how-malta-became-a-hub-of-the-cryptocurrency-world-quicktake>.
4. [https://www.coindesk.com/business/2021/09/24/ftx-moves-headquarters-from-hong-kong-to-bahamas-report/](https://www.coindesk.com/business/2021/09/24/ftx-moves-headquarters-from-hong-kong-to-bahamas-report).
5. “A Guide to Digital Token Offerings”, Monetary Authority of Singapore, November 14, 2017, <http://www.mas.gov.sg/-/media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20%2014%20Nov%202017.pdf>.
6. <https://www.mas.gov.sg/regulation/acts/payment-services-act>, accessed January 1, 2022.
7. https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf, p. 18, accessed January 1, 2022.
8. “Regulation of Virtual Assets”, Financial Action Task Force (FATF), October 19, 2018, <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html>.
9. Manesh Samtani, “ASIFMA Publishes Best Practices Guide for Crypto Exchanges”, Regulation Asia (blog), June 21, 2018, <https://www.regulationasia.com/asifma-publishes-best-practices-guide-for-crypto-exchanges/>.
10. “Fintech Association of Hong Kong”, Fintech Association of Hong Kong, accessed January 16, 2019, <https://ftahk.org/>.
11. “Home”, Global Digital Finance (GDF), accessed January 16, 2019, <https://www.gdf.io/>.

12. <https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used-1>, accessed January 1, 2022.
13. <https://www.pwchk.com/en/research-and-insights/fintech/pwc-annual-global-crypto-tax-report-2020.pdf>, accessed January 1, 2022.
14. <https://www.pwc.com/gx/en/insights/pwc-annual-global-crypto-tax-report-2021.pdf>, accessed January 1, 2022.
15. <https://www.pwchk.com/en/research-and-insights/fintech/pwc-annual-global-crypto-tax-report-2020.pdf>, accessed January 1, 2022.
16. Barbara Stettner, “Cryptocurrency AML Risk Considerations—Allen & Overy”, Allen & Overy, accessed January 13, 2019, <http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Cryptocurrency-AML-risk-considerations.aspx>.
17. Barbara Stettner, “Cryptocurrency AML Risk Considerations—Allen & Overy”, Allen & Overy, accessed January 13, 2019, <http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Cryptocurrency-AML-risk-considerations.aspx>.
18. “UNODC Estimates That Criminals May Have Laundered US\$ 1.6 Trillion in 2009”, UNODC, October 25, 2011, <https://www.unodc.org/unodc/en/press/releases/2011/October/unodc-estimates-that-criminals-may-have-laundered-usdollar-1.6-trillion-in-2009.html>.
19. Frances Schwartzkopff, “Danske Bank Puts €2.4bn aside for Money-Laundering Case”, Independent. ie, accessed January 24, 2019, <https://www.independent.ie/business/world/danske-bank-puts-2-4bn-aside-for-moneylaundering-case-37592181.html> and Juliette Garside, “Is Money-Laundering Scandal at Danske Bank the Largest in History?” *The Guardian*, September 21, 2018, sec. Business, <https://www.theguardian.com/business/2018/sep/21/is-money-laundering-scandal-at-danske-bank-the-largest-in-history>.
20. <https://www.reuters.com/business/hsbc-fined-85-mln-uk-anti-money-laundering-failings-2021-12-17/>, accessed January 1, 2022.
21. <https://www.icij.org/investigations/fincen-files/>, accessed January 1, 2022.
22. https://www.swift.com/sites/default/files/files/swift_bae_report_Follow-The%20Money.pdf, accessed January 1, 2022.
23. <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf>, accessed January 1, 2022.
24. <https://www.unodc.org/unodc/en/money-laundering/overview.html>, accessed January 1, 2022.
25. <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>.

26. <https://www.unodc.org/unodc/en/money-laundering/overview.html>.
27. <https://securityboulevard.com/2021/08/ransomware-the-20-billion-cybersecurity-problem/>, accessed January 1, 2022.
28. https://www.elliptic.co/hubfs/downloads/Elliptic_Sanctions-Compliance-In_Crypto.pdf, accessed January 1, 2022.
29. <https://www.ibanet.org/article/BDF997FB-EB79-498A-88F5-C6CEACF7DDD9>, accessed January 1, 2022.
30. <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>, accessed January 1, 2022.
31. https://ccaf.io/cbeci/mining_map, accessed January 1, 2022.
32. <https://www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks>, accessed January 1, 2022.
33. “ASIFMA Best Practices for Digital Asset Exchanges”, Asia Securities Industry and Financial Markets Association (ASIFMA), June 2018, p. 19.
34. <https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/>, accessed January 1, 2022.
35. Justin Scheck and Bradley Hope, “The Man Who Solved Bitcoin’s Most Notorious Heist,” Wall Street Journal, August 10, 2018, sec. Markets, <https://www.wsj.com/articles/the-man-who-solved-bitcoins-most-notorious-heist-1533917805>.
36. Barbara D. Underwood, “Virtual Markets Integrity Initiative”, Office of the New York State Attorney General, September 18, 2018.
37. “ASIFMA Best Practices for Digital Asset Exchanges”, Asia Securities Industry and Financial Markets Association (ASIFMA), June 2018.
38. “Regulation of Virtual Assets”, Financial Action Task Force (FATF), October 19, 2018, <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html>.
39. <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, accessed January 1, 2022.
40. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>, accessed January 1, 2022.
41. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>.
42. <https://www.pwccn.com/en/financial-services/publications/the-new-fatf-rules-for-crypto-exchanges-and-custodians.pdf>, accessed January 1, 2022.

43. <https://www.pwccn.com/en/financial-services/publications/the-new-fatf-rules-for-crypto-exchanges-and-custodians.pdf>.
44. <https://www.pwccn.com/en/financial-services/publications/the-new-fatf-rules-for-crypto-exchanges-and-custodians.pdf>.
45. <http://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf>.
46. <https://apps.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=19PR105>, accessed January 1, 2022.
47. <https://www.mas.gov.sg/regulation/acts/payment-services-act>, accessed January 1, 2022.
48. <https://www.cnn.com/2020/07/29/business/art-money-laundering-sanctions-senate/index.html>, accessed January 1, 2022.
49. <https://www.osc.gov.on.ca/quadrigacxreport/web/files/QuadrigaCX-A-Review-by-Staff-of-the-Ontario-Securities-Commission.pdf>, accessed January 1, 2022.
50. <https://www.vanityfair.com/news/2019/11/the-strange-tale-of-quadriga-gerald-cotten>, accessed January 1, 2022.
51. <https://www.vanityfair.com/news/2019/11/the-strange-tale-of-quadriga-gerald-cotten>.

Chapter 18

1. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/>, accessed January 1, 2022.
2. <https://www.nytimes.com/live/2021/03/10/us/joe-biden-news>, accessed January 1, 2022.
3. <https://cointelegraph.com/news/couple-gets-married-on-ethereum-blockchain-for-587-in-transaction-fees>, accessed January 1, 2022.
4. <http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html#:~:text=Nelson%20Mandela%20tribute,stored%20in%20the%20Bitcoin%20system>, accessed January 1, 2022.
5. Evelyn Cheng, “Bitcoin Tops \$8,700 to Record High as Coinbase Adds 100,000 Users”, CNBC, November 26, 2017, <https://www.cnbc.com/2017/11/25/bitcoin-tops-8700-to-record-high-as-coinbase-adds-100000-users.html>.
6. Gedalyah Reback, “Binance Claims 240,000 New Users in One Hour after Relaunching Service”, Cointelligence, January 11, 2018, <https://www.cointelligence.com/content/binance-claims-240000-new-users-in-one-hour-after-relaunching-service/>.

7. <https://www.bis.org/cpmi/publ/d147.pdf>, p. 6, accessed January 1, 2022.
8. <https://www.bloomberg.com/news/articles/2020-05-12/jpmorgan-is-now-banking-for-bitcoin-exchanges-coinbase-gemini>, accessed January 1, 2022.
9. <https://www.bloomberg.com/news/articles/2021-04-26/jpmorgan-is-preparing-to-offer-a-bitcoin-fund-to-wealthy-clients>, accessed January 1, 2022.
10. <https://www.bloomberg.com/news/articles/2021-06-24/citigroup-joins-rivals-helping-wealthy-clients-access-crypto>, accessed January 1, 2022.
11. <https://www.bnymellon.com/us/en/about-us/newsroom/press-release/bny-mellon-forms-new-digital-assets-unit-to-build-industrypercent27s-first-multi-asset-digital-platform-130169.html>, accessed January 1, 2022.
12. <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-98.html>, accessed January 1, 2022.
13. <https://www.theblockcrypto.com/data/crypto-markets/spot>, accessed January 1, 2022.
14. <https://www.binance.com/en/blog/418708327988203520/Binance-2019-Year-in-Review>, accessed January 1, 2022.
15. <https://www.reuters.com/article/usa-crime-bitmex-idUSKBN26N08O>, accessed January 1, 2022.
16. <https://www.theblockcrypto.com/data/crypto-markets/spot>, accessed January 1, 2022.
17. <https://www.fca.org.uk/news/press-releases/fca-bans-sale-crypto-derivatives-retail-consumers>, accessed January 1, 2022.
18. <https://markets.businessinsider.com/news/currencies/hong-kong-crypto-exchanges-million-professional-investors-bintcoin-2021-5>, accessed January 1, 2022.
19. <https://www.coindesk.com/markets/2021/01/06/uks-ban-on-crypto-derivatives-goes-into-effect-today/>, accessed January 1, 2022.
20. <https://www.wsj.com/articles/u-s-crypto-traders-e evade-offshore-exchange-bans-11627637401>, accessed January 1, 2022.
21. <https://inca.digital/intelligence/geotagging-crypto-traders/>, accessed January 1, 2022.
22. <https://cointelegraph.com/news/defi-explosion-uniswap-surpasses-coinbase-pro-in-daily-volume>, accessed January 1, 2022.
23. <https://www.bbc.com/news/technology-53485170>, accessed January 1, 2022.

24. "5 High Profile Cryptocurrency Hacks - (Updated)", Blockgeeks, accessed January 13, 2019, <https://blockgeeks.com/guides/cryptocurrency-hacks/>.
25. Nikhilesh De, "Numbers or Not, Coincheck Isn't Mt. Gox", CoinDesk (blog), January 26, 2018, <https://www.coindesk.com/numbers-not-coincheck-isnt-another-mt-gox>.
26. <https://www.coindesk.com/tech/2020/02/19/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack/>, accessed January 1, 2022.
27. <https://slowmist.medium.com/slowmist-tracking-possible-identification-clues-related-to-poly-network-attackers-b330d4d710f>, accessed January 1, 2022.
28. <https://twitter.com/PolyNetwork2/status/1425130017546149891?s=20>, accessed January 1, 2022.
29. <https://blog.chainalysis.com/reports/poly-network-hack-august-2021/>, accessed January 1, 2022.
30. <https://twitter.com/PolyNetwork2/status/1425073990012268556>, accessed January 1, 2022.
31. <https://blog.chainalysis.com/reports/poly-network-hack-august-2021/>, accessed January 1, 2022.
32. <https://twitter.com/PolyNetwork2/status/1425123153009803267>, accessed January 1, 2022.
33. <https://www.elliptic.co/blog/the-poly-network-hack-600-million-in-crypto-stolen-and-returned-in-24-hours>, accessed January 1, 2022.
34. <https://slowmist.medium.com/slowmist-tracking-possible-identification-clues-related-to-poly-network-attackers-b330d4d710f>, accessed January 1, 2022.
35. <https://www.elliptic.co/blog/the-poly-network-hack-600-million-in-crypto-stolen-and-returned-in-24-hours>, accessed January 1, 2022.
36. <https://twitter.com/PolyNetwork2/status/1425321860539949056>, accessed January 1, 2022.
37. <https://www.elliptic.co/blog/the-poly-network-hack-600-million-in-crypto-stolen-and-returned-in-24-hours>, accessed January 1, 2022.
38. <https://slowmist.medium.com/slowmist-tracking-possible-identification-clues-related-to-poly-network-attackers-b330d4d710f>, accessed January 1, 2022.

Chapter 19

1. <https://www.bcg.com/publications/2020/global-asset-management-protect-adapt-innovate>, accessed January 1, 2022.
2. <https://www.pwc.com/gx/en/financial-services/pdf/pwc-elwood-annual-crypto-hedge-fund-report-may-2020.pdf> and [https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-\(may-2021\).pdf](https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-(may-2021).pdf), accessed January 1, 2022.
3. <https://www.bloomberg.com/news/articles/2020-04-24/hedge-fund-assets-dip-below-3-trillion-to-least-in-six-years#:~:text=The%20March%20withdrawals%20wiped%20out,oversee%20an%20estimated%20%242.95%20trillion>, accessed January 1, 2022.
4. <https://buffett.cnbc.com/video/2021/05/03/munger-of-course-i-hate-the-bitcoin-success.html>, accessed January 1, 2022.
5. <https://www.economist.com/leaders/2021/05/08/warren-buffett-should-step-aside-for-his-chosen-successor>, accessed January 1, 2022.
6. Josiah Wilmoth, “Major Milestone: There Are Now More than 300 Cryptocurrency Funds”, CCN, July 27, 2018, <https://www.ccn.com/major-milestone-there-are-now-more-than-300-cryptocurrency-funds/>.
7. <https://www.pwc.com/gx/en/financial-services/pdf/pwc-elwood-annual-crypto-hedge-fund-report-may-2020.pdf>, accessed January 1, 2022.
8. <https://www.pwc.com/gx/en/financial-services/pdf/pwc-elwood-annual-crypto-hedge-fund-report-may-2020.pdf>, p. 7, accessed January 1, 2022.
9. [https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-\(may-2021\).pdf](https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-(may-2021).pdf), accessed January 1, 2022.
10. <https://grayscale.co/>, accessed January 1, 2022.
11. https://www.bloomberg.com/news/articles/2018-08-09/fidelity-bets-on-zero-fee-index-funds?utm_source=google&utm_medium=cpc&utm_campaign=dsa&utm_term=&gclid=Cj0KCQjwxNT8BRD9ARIsAJ8S5xZtD534H4SwB3w0wfwZMgyjJAp2_m9_sKf4GVhu3nyg5DMbgFFs1wQaAoMbEALw_wcB, accessed January 1, 2022.
12. <https://www.coindesk.com/the-journey-of-the-winklevoss-bitcoin-etf>, accessed January 1, 2022.
13. <https://decrypt.co/resources/bitcoin-etf-explained-guide-learn-easy>, accessed January 1, 2022.
14. <https://cointelegraph.com/explained/venture-capital-financing-in-crypto-explained>, accessed January 1, 2022.
15. <https://cointelegraph.com/explained/venture-capital-financing-in-crypto-explained>.

16. <https://a16z.com/crypto/#vertical-landing-investment-thesis>, accessed January 1, 2022.
17. <https://a16z.com/2021/06/24/crypto-fund-iii/>, accessed January 1, 2022.

Chapter 20

1. <https://www.coindesk.com/coinbase-gemini-first-crypto-exchange-customers-jpmorgan-bank-report>, accessed January 1, 2022.
2. <https://www.bloomberg.com/news/articles/2018-07-31/northern-trust-looks-to-join-burgeoning-crypto-custody-business>, accessed January 1, 2022.
3. <https://www.sc.com/en/media/press-release/standard-chartered-completes-strategic-investment-in-ripple/> and <https://www.bloomberg.com/news/articles/2018-10-18/goldman-wades-deeper-in-crypto-betting-on-bitgo-with-novogratz>, accessed January 1, 2022.
4. <https://www.reuters.com/article/us-fireblocks-funding/bny-mellon-invests-in-cryptocurrency-storage-firm-fireblocks-idUSKBN2BA1F6> and <https://www.finextra.com/newsarticle/39238/hsbc-joins-200m-funding--round-for-consensys>, accessed January 1, 2022.
5. <https://www.reuters.com/article/us-crypto-currencies-nomura-idUSKBN23O2AS>, accessed January 1, 2022.
6. <https://www.juliusbaer.com/%E9%A6%99%E6%B8%AF%E7%89%89%E5%88%A5%E8%A1%8C%E6%94%BF%E5%8D%80/%E7%B9%81/news/julius-baer-enters-partnership-for-digital-asset-services-with-seba-crypto-ag/>, accessed January 1, 2022.
7. <https://www.coindesk.com/standard-chartered-to-launch-institutional-crypto-custody-solution> and <https://www.sc.com/en/media/press-release/weve-partnered-with-northern-trust-to-launch-zodia-a-cryptocurrency-custodian-for-institutional-investors/>, accessed January 1, 2022.
8. <https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments>, accessed January 1, 2022.
9. <https://www.fidelitydigitalassets.com/overview>, accessed January 1, 2022.
10. <https://www.cnbc.com/2020/10/27/jpmorgan-creates-new-unit-for-blockchain-projects-as-it-says-the-technology-is-close-to-making-money.html>, accessed January 1, 2022.
11. <https://investor.signatureny.com/pme/press-releases/news-details/2021/Signature-Bank-Reports-2021-First-Quarter-Results/default.aspx>, accessed January 1, 2022.

12. [https://www.coindesk.com/hedge-fund-pioneer-paul-tudor-jones-says-he-holds-1-2-of-assets-in-bitcoin](https://www.silvergate.com/solutions/digital-currency/sen?__cf_chl_captcha_tk__=11f68fb24bb1e35e8a3a3db5ab211faeff10b3-1620390012-0-Af-atr9A5GH3AaLeIAq8quDbjceOfdABCyKncwGJyWfze_Qk2HJHLw_OiWfs58k54ZdABEW9T_rDZo_9mUaUvIgWTD9_KQNIYATWaWnIndXFxknbmkt9drl2i-_1UgCg0ouTm9WP3C-Tr_LePYKOH3CG7eMg1-tWGAi0RQEhFe4Plg-QajxmWp4QhAiLCaDN7ETbdiB_MwqqYxKvR943pxj5p_XmnVMIY9QYCmX9apRFp2PdVf8fGHPvyP7jMeIV6HyumtoowXNCkf4DptbZ3iLjtQKHYSn4_R0bAVMDsZDFl5L1GyO-2slrOOoWDWVrgi7TlvaQuDIqitwxTD51oiVe-VpjT7wFB-nA1FLW6Zy_zzETJCPwfym76kS5Sp2sUcRpB8li-4mPcaH3rPIPlh_idtVzqE1_kg-xPvKXF518Lr8oD6XfozCtjK9hOyp7J5mjq77hYOuXeoW12AioTWbSF2WbPvwkGMpLT5TvdBpWqI8D30MDvxHo65KvcaOWtXnnVzYu-SogQJB2k9a2EIBGKtG9wBK1tNLEsmhKzUh3LawMK12wH8uLjqVOdIU_GTLf_DyCUWRAYfypItLIob9dLYXfuGIXGE_zi3BMYaHsqB8t2E9rZnoR9DmF7RhICajklPquapmIWUPf3aq2c9rBLTm-GLy40AuRLQ1LZ1UzhxA-GsEXwCYggUgEEpjmcMZKuovdeM7ehTfinE, accessed January 1, 2022.13. <a href=), accessed January 1, 2022.
14. https://www.cmegroup.com/media-room/press-releases/2019/11/12/cme_group_announcesjan132020launchforbitcoionoptions.html#:~:text=13%2C%202020%20Launch%20for%20Bitcoin%20Options,,Tue%20Nov%202012&text=CHICAGO%2C%20Nov.,available%20for%20trading%20starting%20Jan, accessed January 1, 2022.
15. <https://www.coindesk.com/166b-asset-manager-renaissance-eyes-bitcoin-futures-for-flagship-fund>, accessed January 1, 2022.
16. The survey was conducted between December 2, 2020 and April 2, 2021, with a total of 1,100 interviews completed via a mix of online surveys and 1:1 phone sessions.
17. <https://www.wiley.com/en-us/The+Bitcoin+Standard%3A+The+Decentralized+Alternative+to+Central+Banking-p-9781119473862>, accessed January 1, 2022.
18. <https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25>, accessed January 1, 2022.
19. <https://www.gold.org/about-gold/gold-supply/gold-mining/how-much-gold>, accessed January 1, 2022.
20. <https://panteracapital.com/blockchain-letter/five-orders-of-magnitude/>, accessed January 1, 2022.
21. <https://panteracapital.com/blockchain-letter/five-orders-of-magnitude/>

22. Stellabelle, "Cold Wallet Vs. Hot Wallet: What's The Difference?", Medium (blog), April 9, 2017, <https://medium.com/@stellabelle/cold-wallet-vs-hot-wallet-whats-the-difference-a00d872aa6b1>.
23. Annaliese Milano, "E-Commerce Giant Rakuten Is Launching Its Own Crypto", CoinDesk (blog), February 27, 2018, <https://www.coindesk.com/e-commerce-giant-rakuten-launching-cryptocurrency>.
24. Wolfie Zhao, "Rakuten Is About to Buy a Bitcoin Exchange for \$2.4 Million", CoinDesk (blog), August 31, 2018, <https://www.coindesk.com/rakuten-seeks-to-acquire-bitcoin-exchange-in-2-4-million-deal>.
25. Wolfie Zhao, "Messaging Giant LINE Is Launching Its Own Cryptocurrency", CoinDesk (blog), August 31, 2018, <https://www.coindesk.com/messaging-giant-line-is-launching-its-own-cryptocurrency>.
26. <https://www.coindesk.com/telegram-abandons-ton-blockchain-project-after-court-fight-with-sec>, accessed January 1, 2022.
27. <https://www.amazon.com/Future-Finance-FinTech-Financial-Services/dp/3030145328>, accessed January 1, 2022.
28. Mike Brown, "Should Amazon Get Into Virtual Currency & Other Products?", LendEDU (blog), February 27, 2018, <https://lendedu.com/blog/amazon-virtual-currency-banking-insurance/>.
29. https://blog.twitter.com/en_us/topics/product/2021/bringing-tips-to-everyone, accessed January 1, 2022.
30. <https://talkingbiznews.com/they-talk-biz-news/crypto-journalists-form-organization/>, accessed January 1, 2022.

Chapter 21

1. <https://webfoundation.org/about/vision/history-of-the-web/>, accessed January 1, 2022.
2. <https://medium.com/fabric-ventures/what-is-web-3-0-why-it-matters-934eb07f3d2b>, accessed January 1, 2022.
3. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.
4. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.
5. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.
6. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.
7. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.

8. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.
9. <https://www.nature.com/articles/d41586-019-03213-z>.
10. <https://www.bloomberg.com/news/articles/2020-12-04/chinese-scientists-claim-breakthrough-in-quantum-computing-race>.
11. <https://link.springer.com/article/10.1007/BF02650179>.
12. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.
13. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.
14. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.
15. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.
16. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.
17. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.
18. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.
19. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.
20. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.
21. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.
22. https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html?id=nl:2em:3cc:4dcom_share:5awa:6dcom:innovatie.
23. https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html?id=nl:2em:3cc:4dcom_share:5awa:6dcom:innovatie.
24. <https://consensys.net/blog/developers/how-will-quantum-supremacy-affect-blockchain/>.
25. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.
26. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.
27. <https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html>.

28. <https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-rollups/>.
29. <https://vitalik.ca/general/2021/01/05/rollup.html>, accessed January 1, 2022.
30. <https://eth.wiki/sharding/Sharding-FAQs>, accessed January 1, 2022.
31. <https://ethereum.org/en/eth2/>, accessed January 1, 2022.
32. <https://ethereum.org/en/developers/docs/scaling/>, accessed January 1, 2022.
33. <https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/>, accessed January 1, 2022.
34. <https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/>.
35. <https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/>.
36. <https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/>.
37. <https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/>, accessed January 1, 2022.
38. <https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/>.
39. <https://ethereum.org/en/glossary/#fraud-proof>, accessed January 1, 2022.
40. <https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/>.
41. <https://ethereum.org/en/glossary/#validity-proof>, accessed January 1, 2022.
42. <https://ethereum.org/en/glossary/#fraud-proof>.
43. <https://ethereum.org/en/dao/>, accessed January 1, 2022.
44. <https://ethereum.org/en/dao/>, accessed January 1, 2022.
45. <https://ethereum.org/en/dao/>.
46. <https://www.jdsupra.com/legalnews/decentralized-autonomous-organizations-5960480/>, accessed January 1, 2022.
47. <https://www.wyoleg.gov/Legislation/2021/SF0038>, accessed January 1, 2022.
48. <https://www.wyoleg.gov/Legislation/2021/SF0038>.

Index

A

airdrops 287
Algorand (ALGO) 100, 102, 122, 142, 155, 233, 278
Amazon 378
American International Group (AIG) 38
American Revolutionary War 31, 80
anti-money laundering (AML)
 requirements 144, 207, 226, 230, 318, 321, 325–9, 340, 365
Avakian, Stephanie 236
Avalanche (AVAX) 100, 102, 142, 233, 278

B

Bahamas 227–9, 316
Bank of England 29–30, 35, 77, 177, 225
Bank of Japan 189, 197
Bank of Thailand 189, 191, 200, 245
barter economy 2–4, 18

gift exchange 3
history of 1–4
hyperinflation and 4
potlach custom 3
sanctions and 4
in Soviet era 4
Binance Coin (BNB) 102–3
Bitcoin
 challenges to 81–3
 Chinese academics and 273
 as company treasury 79–81
 crypto mining 259–73
 crypto mining locations 273–6
 declared “dead” 81
 determining value of 372–5
 difficulty level 267–8
 environmental impact debate 269–73
 evolution of crypto mining 256–61
 growth of 58–70
 as legal tender 75–8
 Lightning Network 83–5
 logo 59–60
 mining pools 262–3

public address 42, 178
retail adoption of 70–5
role of cryptography in 49–51
role of decentralisation in 51
role of immutability in 53
role of proof-of-work in 54–8
self-regulatory mechanism 56,
 267
Taproot “soft fork” upgrade 53,
 285
see also Bitcoin whitepaper;
 Satoshi Nakamoto
Bitcoin Cash (BCH) 53, 103,
 109–10, 263, 285–6
Bitcoin Mining Council (BMC) 271
Bitcoin Pizza Day 59
Bitcoin SV (BSV) 104
Bitcointalk 39, 58–60, 78
Bitcoin whitepaper 38–43, 49–58
 blockchain 122
 cryptography 49–51
 decentralisation 51–5
 electronic coin defined 49
 proof-of-work 54–8
blockchain 121–32
 Bitcoin whitepaper and 122
 challenges to 125–6
 characteristics of 121
 consensus-driven 123
 decentralised and transparent 122
 decentralised ledger technology
 compared with 123
 immutable 123
 layer 1 blockchains 99–101, 115,
 389–90
 layer 2 blockchains 82, 99–101,
 111, 115, 389–90
 origins of the term 122
 private and public blockchains
 123
 use cases of 128–32
 see also cryptocurrencies and
 tokens, individual
blockchain consortiums 126

blockchain innovation theatre 127–8
blockchain trilemma 141, 142, 270
Block.one 107, 236, 244, 278–81
Brady, Tom 69
Bretton Woods 36–8, 165
Buake, Nayib 75, 76, 83
Bündchen, Gisele 69
Buterin, Vitalik 40, 91, 113, 304

C

Cambodia 226
Canada
 Bank of Canada 8, 74, 180, 187,
 204
 Bitcoin ETFs 360
 financial literacy 74
 fur trade 6, 28
 Indian Act of 1876 3
 potlach ban 3
 public opinion on central bank
 digital currency (CBDC) 180
 Quadriga scandal 331–3
Canadian Bank Note Company 176
Cardano (ADA) 104–5
CBDC. *See* central bank digital
 currencies
Ceaușescu, Nicolae 4
central bank digital currencies
 (CBDCs) 171–84
 benefits for central banks 174–6
 definition of 171–4
 history and catalysts for 177–84
 monetary policy and 204
 as “risk-free” asset 207
 see also retail central bank digital
 currencies; wholesale central
 bank digital currencies
Central Bank of The Bahamas 227
CENTRE Consortium 154
Chainalysis 72, 79, 321
Chainlink (LINK) 105, 354
Chaum, David 47–8

- Chicago Mercantile Exchange (CME) 38, 68, 341, 360, 370
- China
- Bitcoin mining 268, 271–6
 - coinage in 12–3
 - digital currency electronic payment (DCEP) 66
 - e-CNY (digital currency) 228–32
 - paper money in 25–7
 - People's Bank of China 66, 201, 228, 318
- Chivo digital wallet (El Salvador) 83
- chops (seals and stamps) 131
- CipherTrace 61, 147, 326–7
- Circle 153–4, 364, 366
- civilisations, development of 10–11
- coinage
- in China 12–3
 - invention of 12–5
 - in Lydia 13–5
 - seigniorage 14
- Coinbase 63, 79, 154, 319, 337–8, 339, 345–6, 361, 363, 376
- compliance. *See* regulations and compliance
- countering the financing of terrorism (CFT) requirements 207, 223, 230, 328, 329
- COVID-19 pandemic 64–7, 80, 132, 176, 179, 208, 222, 239, 247, 254, 323, 370
- crypto asset creation and distribution 277–89
- airdrops 287
 - hard and soft forks 285–7
 - initial coin offerings (ICOs) 277–83
 - initial exchange offerings 283–4
 - liquidity mining/yield farming 288–9
 - security token offerings 284–5
- cryptocurrencies 133–47
- centralised cryptocurrencies 141
 - decentralised cryptocurrencies 140–41
 - definition of 139–40
 - fungible and non-fungible tokens 135–7
 - payment tokens 137–9
 - privacy coins 142–7
- cryptocurrencies and tokens, individual
- Algorand (ALGO) 100, 101–2, 122, 142, 155, 233, 278
 - Avalanche (AVAX) 100, 102, 233, 278
 - Binance Coin (BNB) 102–3
 - Bitcoin Cash (BCH) 53, 103, 109–10, 263, 285–6
 - Bitcoin SV (BSV) 104
 - Cardano (ADA) 104–5
 - Chainlink (LINK) 105, 354
 - Dash (DASH) 105, 142
 - Dogecoin (DOGE) 70, 106–7, 113
 - EOS 107, 123, 141, 142
 - Hedera Hashgraph (HBAR) 108–9
 - IOTA 109
 - Litecoin (LTC) 106, 109, 124, 287
 - Monero (XMR) 110, 138, 142, 143, 147, 263, 323, 348
 - Polkadot (DOT) 110–11, 354
 - Polygon (MATIC) 111, 348, 349
 - Ripple (XRP) 111–3, 117, 141, 194, 278, 364
 - Shiba Inu (SHIB) 71, 106, 113
 - Solana (SOL) 69, 114–6, 122, 233, 278
 - Stellar (XLM) 116
 - Tezos (XTZ) 116–7, 246, 278
 - Tron (TRX) 117, 155
 - Vechain (VET) 118
 - ZCash (ZEC) 118
- crypto ecosystem enablers 363–79

- borrowing and lending platforms 366–70
crypto-asset custodians and wallets 374
crypto-focused banks 365–9
institutional investors 368–74
large tech firms 377–9
media ecosystem 379
self-custody 377
service providers 378–9
third-party crypto custodians 376
traditional financial institutions 363–6
crypto exchanges 335–50
centralised exchanges 335–8
centralised hacks 347–9
Coinbase public listing 337–8
crypto-to-crypto exchanges 340–41
cybersecurity and hacking 346–50
DeFi hacks 349–50
derivative exchanges 341–5
fiat-to-crypto exchanges 337–40
OTC brokers 345
crypto funds 351–62
cryptography
asymmetric/public key cryptography 46–7, 386
Avalanche (AVAX) and 102
blockchain and 122, 138
early cryptocurrencies 47–9
early encryption techniques 45–6
etymology of 45
Libra and 164
payment tokens 137
Project Stella and 197
role of in Bitcoin 49–51, 61
see also hash
crypto mining 259–76
difficulty level 267–8
environmental impact debate 263–73
evolution of 259–61
hashrate 262–8, 273
locations 273–6
mining pools 262–3
crypto spring 66
crypto traceability firms and tools 349
Chainalysis 72, 79, 321
CipherTrace 61, 147, 326–7
Elliptic 61, 323, 324
Crypto Wars 144
crypto winter 64, 66
currencies. *See* cryptocurrencies; cryptocurrencies and tokens, individual
Curry, Steph 69
“Cypherpunk Manifesto, A” (Hughes) 48
Cypherpunk movement 48
- D**
- Dalio, Ray 67
Dash (DASH) 105–6, 142
Decentralised Autonomous Organisation (DAO) 392–3
decentralised finance (DeFi) 291–312
aggregators 310–11
automated market makers (AMM) 303–5
benefits and challenges of 311–2
borrowing and lending 298–300
composability risk of 312–3
Curve exchange 301, 305, 349
DeFi exchange (DEX) 301–2, 323, 326
definition of 291
flash loans 300–1
hacks 294, 297, 309, 312, 348–50, 368–70
history and growth of 291–3
impermanent loss 306–8
insurance 309–10
Nexus Mutual model 309–10
Poly Network 312, 348–50

- regulation of 293–5
 risks of interoperability or
 composability 295
 stablecoins 296–8
 synthetic assets 308–9
 total value locked (TVL) 306
- DeFi. *See* decentralised finance
 deregulation 38
- Diffie, Whitfield 46
- Digicash 47
- digital signature 39, 41, 49, 52, 388
- Dinwiddie, Spencer 69, 246–8
- Dogecoin (DOGE) 70, 106–7, 113
- dollar sign 33–4
- double-spend problem 39, 40–2, 49,
 51, 117, 231
- Druckenmiller, Stanley 67, 161
- E**
- Eastern Caribbean Central Bank 220
- Elliptic 61, 323
- Elliptic Curve Digital Signature
 Algorithm (ECDSA) 47, 386,
 388
- El Salvador 70, 75–7, 83, 216
- EOS 107, 123, 141, 142
- Ether (ETH) 88, 91, 94–6
- Ethereum 91–8
 Buterin, Vitalik 40, 91, 113, 304
 differences from Bitcoin 92–4
 “gas” concept 94–6
 GHOST protocol 93–4
 history of 91–2
 London Fork 95–7
 scalability issues 101
 smart contracts and 92–3
 uncle blocks 93–4
 upgrades 93
- Ethereum 2.0 97–8
 Beacon Chain 97
 end of proof-of-work 98
 proof-of-stake 88–9, 92, 93, 97,
 98
- shard chains 97
 sharding 97
 three phases of 97–8
- European Central Bank 189
- ExtraNonce 67
- F**
- Facebook 40, 381–4. *See also* Libra
 faith 19–23
 Buddhism 19
 Christianity 20–2
 Crusades 21
 Hospitallers and Templars 21–3
 Islam 19–20
- Faster Payments Services (FPS) 186
- Federal Deposit Insurance
 Corporation (FDIC) 153, 366,
 368
- Federal Reserve Act (1913) 35–6
- Ferguson, Niall 67
- Fidelity Digital Asset Services 65
- financial crisis of 2008 38, 165, 357,
 369
- financial futures contracts 38
- financial literacy 74
- FinTech 62, 126–8, 217, 225, 245,
 319
- FinTech Capsule 48
- Ford, Gerald 35–6
- Franklin, Benjamin 31
- French Revolution 80
- future trends 392–3
- Decentralised Autonomous
 Organisation (DAO) 392–3
- metaverse 383–4
- quantum computing 384–8
- Web 3.0 381–3
- Zero-Knowledge Rollups
 (ZK-Rollups) 389–90
- G**
- Germany

butter standard 4
 gold standard 34
 hyperinflation 4, 80
 Nazi Germany's Enigma machine 46
 Giancarlo, J. Christopher "Crypto Dad" 63–4
 golden hash 54–8, 259
 gold standard 34–8
 Gold Standard Act 35
 Google 109, 144, 382, 385
 Grantham, Jeremy 82
 Great Depression 35–7, 38, 179
 Greece 15–7
 Griffin, John M. 156
 Griffin, Ken 392

H

Hamilton, Alexander 32
 Hanyecz, Laszlo 58
 hard forks 82, 103, 286, 346, 392
 hash 49–51, 53–8, 67, 94, 112, 115–6
 defined 50
 golden hash 55–8, 259
 SHA-256 (Secure Hash Algorithm) 50, 54, 106, 287, 386
 Hashed Timelock Contracts (HTLC) 85, 190–91
 hashers (pool contributors) 262, 266
 hashrate 262–8, 273
 Hedera Hashgraph (HBAR) 108–9
 Hellman, Martin 46
 Hong Kong 316, 330, 342–5
 Armenian Community of Hong Kong and China 62
 BIS Innovation Hub 245
 Bitfinex 156–7, 284, 339, 343, 347
 chops used in 131
 FinTech Association of Hong Kong 319

issuance of bank notes 176
 legal treatment of securities 234
 Meitu 79
 Stores Value Facility (SVF) 217
 Hong Kong Monetary Authority 189, 191, 200, 245
 Howey Test 234–7
 Hughes, Eric 48
 hyperinflation 4, 27, 73, 80

I

impossible trinity 142, 270
 India 7, 20, 27, 28, 113, 130, 131, 172, 317, 318
 initial coin offerings (ICOs) 277–83
 initial exchange offerings 283–4
 Instagram 166, 239
 International Monetary Fund (IMF) 37, 64, 76, 165, 167, 168, 215–6, 223
 International Standard on Assurance Engagements (ISAE) 371–2
 IOTA 109

J

Japan 36–8, 76, 77, 132, 165, 343, 347, 377
 Jevons, William Stanley 3
 JPM Coin 66

K

know-your-customer (KYC)
 requirements 207, 216, 226–8, 230, 321–8, 340–2, 344

L

Lagarde, Christine 64
 layer 1 blockchains 99–101, 115, 389–90
 layer 2 blockchains 82, 99–101, 111, 115, 389–90

legal tender 75–8
 Lehman Brothers 38
 Lerner, Sergio Demian 67
Libra 163–70
 announcement and impact 40,
 66, 163, 171, 179, 377–9
 CBDCs and 169, 179
 compared with IMF Special
 Drawing Rights 165
 goals of 163
 Libra 1.0 164–6
 Libra 2.0 166–70
 rebranding to Diem 163, 170,
 377
 Libra Association 165–70
 Libra Reserve 164–6, 167–70
 Lightning Network (Bitcoin) 53,
 83–85, 378
 liquidity mining/yield farming
 288–9
 Litecoin (LTC) 106, 109–10, 124,
 287
 Lydia 13–7

M

MakerDAO 158–60, 296–8
 Marcus, David 40
 Marshall Islands, Republic of the
 213–6
 Masters, Blythe 122
 mathematics, history of 24–5
 medium of exchange 1–3, 7, 91,
 137, 139, 164
 Meta. *See* Facebook
 metaverse 384
 millennial generation 64
 mining. *See* crypto mining
 Monero (XMR) 110, 138, 142, 143,
 147, 263, 323, 348
 money, characteristics of 2, 139
 money, history of
 age of discoveries 27–8

American colonies and paper
 banknotes 31–3
 animal skins and furs 6
 Bank of England 29–30
 barter economy compared with
 1–4
 Bitcoin whitepaper 38–43
 cacao beans 6
 cattle 5
 China and rise of paper money
 25–7
 cowrie shells 6–7
 Dutch innovations 28–9
 faith and 19–22
 financial crisis 38
 human beings 5
 impact on development of
 civilisations 10–11
 invention of coinage 12–5
 Italian bankers and the
 Renaissance 23–5
 leaving the gold standard 34–8
 primitive forms of 4–10
 stones 7–9
 transformative impact 15–9
 wampum beads 8–10
 Mt. Gox scandal 60, 61, 347–9
 Murphy, Frank 235

N

Nakamoto, Satoshi. *See* Satoshi
 Nakamoto
 Netherlands 28, 267
 Nixon, Richard 36–8
 non-fungible, non-tradable tokens
 257
 non-fungible tokens (NFT)
 artists/celebrities and 239–40,
 242, 253–5
 athletes and 69, 247, 255
 attributes of 250–1
 Beeple digital artwork 137, 253
 Bored Ape Yacht Club 69, 137

- CryptoKitties 137, 249, 250–2
 CryptoPunks 137, 251
 Decentraland 252
 definition of 139
 Ethereum ecosystem and 101
 Financial Action Task Force and 331
 first Formula One NFT car 251
 fungible versus non-fungible tokens 135–7
 growth of 69, 240, 253–6
 insider trading and 256
 metaverse and 384
 NBA Top Shot 253
 NFT-based games and experiments 252
 social tokens 239–40
 tradable and non-tradable tokens 137
 tradable tokens 257
 where to buy NFTs 253
- O**
 Organisation for Standardisation (ISO) 111–2, 195, 370, 371
- P**
 Patoshi Pattern 67
 PayPal 70
 People's Bank of China 66, 201, 228, 318
 philosophers, Greek 16
 Pierce, Hester 238, 245
 Polkadot (DOT) 110–11, 354
 Polygon (MATIC) 111, 348, 349
 Ponzi scheme 331–3
 Portugal 27–8
 privacy coins 138, 142–7, 323, 348
 private key 42, 46–7, 49–51, 138, 139, 331, 346, 368, 374, 375, 377, 385–8
 proof-of-stake
- Algorand (ALGO) and 102
 DASH and 105–6
 definition of 88–9
 delegated proof-of-stake 107–8
 EOS and 107, 141
 Ethereum 2.0 and 88–9, 92, 93, 97
 Polkadot (DOT) and 110–11
 proof-of-work compared with 88–9
 Terra protocol and 162
 Tezos (XTZ) and 116
 Tron (TRX) and 117
 XRP Ledger Consensus Protocol compared with 112
 proof-of-work
 advantages of 260
 Bitcoin and 39, 42, 54–8, 259–60
 Bitcoin Cash and 103
 Bitcoin SV and 104
 DASH and 106
 definition of 54
 Dogecoin and 106
 end of 98
 environmental impact of 82, 98, 263, 269
 Ethereum 2.0 and 88, 92, 93, 97
 hashrate and 266
 Litecoin and 110
 proof-of-stake compared with 88–9
 as undemocratic 89
 XRP Ledger Consensus Protocol compared with 112
 ZCash and 118
 public key 41, 46–7, 49, 62, 138, 139, 388
- Q**
 Quadriga 331–3
 quantitative easing (QE) 7, 18, 34, 64, 67, 70, 76, 80, 218, 370–2

quantum computing 384–8

R

regulations and compliance 315–33
 approaches to regulations 316–9
 approaches to taxation 319–20
 crypto compliance 325–31
 future of crypto-asset regulation 318–9
 illicit activities 321–5
 negative approach to crypto-assets 317–8
 neutral approach to crypto-assets 317
 positive approach to crypto-assets 316–7
 Quadriga Ponzi scheme 331–3
 Renaissance 23–5
 Renaissance Technologies 67, 370
 retail central bank digital currencies 203–32
 account-based 210–11
 benefits of 203–4
 decentralised approach 213–6
 definition of 203
 direct approach 216
 disadvantages of 206
 e-CNY (China) 229–32
 e-krona (Sweden) 209
 forms of 211–32
 platform approach 223–9
 Project Bakong (Cambodia) 226
 Sand Dollar (Bahamas) 227–9
 sovereign (Republic of the Marshall Islands) 213–6
 synthetic approach 216–8
 token-based issuance 206–10
 two-tier/intermediated approach 218–23
 U.S. digital dollar proposal 222
 Riksbank (Swedish Central Bank) 208–11, 220–5

Ripple (XRP) 111–3, 117, 141, 194, 278, 364

Romania 4

Rome 17–9

Roosevelt, Franklin Delano 35–6

Roubini, Nouriel 64, 82

Russia 71–3, 317

S

Satoshi Nakamoto
 Bitcoin difficulty level
 (self-regulatory mechanism) 267–8
 Bitcoin Satoshi Vision 103
 Bitcoin whitepaper 38–42, 49–60, 122
 Coinbase's secret message as homage to 337
 final message on the blockchain 78
 identity of 39–40
 as miner 140
 Patoshi Pattern 67
 Securities and Exchange Commission (SEC) 234–9, 244, 282, 284, 293, 317, 360, 361, 377
 security tokens 241–8
 Aspen Digital Security Token 246
 barriers to growth of 248
 pro athletes and 247
 real estate 245–7
 tokenisation 241–3
 tokenisation of new investment instruments 243–5
 tokenisation of pre-existing investment instruments 245–8
 security token offerings 284–5
 seigniorage 14, 152
 Shams, Amin 156
 Shiba Inu (SHIB) 71, 106, 113
 signal bit 53
 Silk Road 19, 60, 136

Simple Agreement for Future Equity (SAFT) 283
 Singapore 187, 197, 199, 316, 320, 324, 330
 social tokens 239–40
 soft forks 53, 82, 285–7
 Solana (SOL) 69, 114–6, 122, 233, 278
 Spain 27–8
 stablecoins
 benefits of 149–52
 classification challenges 154
 crypto-collateralised stablecoins 157–60
 Dai 158–60, 296–8
 definition of 149
 fiat-collateralised stablecoins 152–3
 Gemini Dollar (GUSD) 153
 Libra (Facebook) 163–70
 Libra coins 165–70
 non-collateralised stablecoins 160–3
 non-regulated fiat stablecoins 155–7
 Paxos Standard (PAX) 153
 regulated fiat stablecoins 153–4
 Terra protocol 162
 Tether 150, 153, 155–7, 349, 365
 USD Coin (USDC) 153, 154, 157, 162, 296, 348, 349
 used by banks for payment activities 154
 use incentives 152
 Stellar (XLM) 116
 store of value 1, 2, 5, 60, 82, 106, 137, 139
 Sweden 208–11, 220–5
 Systems and Organisation Controls (SOC) 371–2

T

Tapscott, Don 49

Telegram 236–8, 244, 281, 377
 Tesla 70, 79, 81
 Tezos (XTZ) 116–7, 246, 278
 tokenisation 241–3
 of new investment instruments 243–5
 of pre-existing investment instruments 245–8
 see also security tokens
 tokens. *See* cryptocurrencies and tokens, individual; non-fungible, non-tradable tokens; non-fungible tokens (NFT); security tokens; social tokens; utility tokens
 Tor 60
 Tron (TRX) 117, 155
 Trump, Donald 166
 Turing, Alan 46

U

Ulbricht, Ross 60
 United Arab Emirates Central Bank 193, 201
 unit of account 1, 2, 139, 165
 U.S. Commodity Futures Trading Commission (CFTC) 63–4, 239, 293, 316–7, 341
 utility tokens 233–40
 definition of 233–4
 safe harbour provision 238
 tokens as securities 234–9

V

Vechain (VET) 118

W

Web 3.0 381–3
 WhatsApp 164, 166
 wholesale central bank digital currencies 185–201

- compatible CBDC systems 195
cross border corridor model 188–94
cross border multi-CBDC model 195–7
interlinked CBDC systems 197–8
multi-CBDC (mCBDC) 195, 198–201
national model 185–7
Project Stella 187, 189–92, 197
real-time gross settlement (RTGS) systems 185–90
- single mCBDC multi-currency system 198–201
World War I 36
World War II 4, 36, 46
Wright, Craig 40, 104

Z

- ZCash (ZEC) 118–9
Zero-Knowledge Rollups (ZK-Rollups) 389–90
Zuckerberg, Mark 40, 384