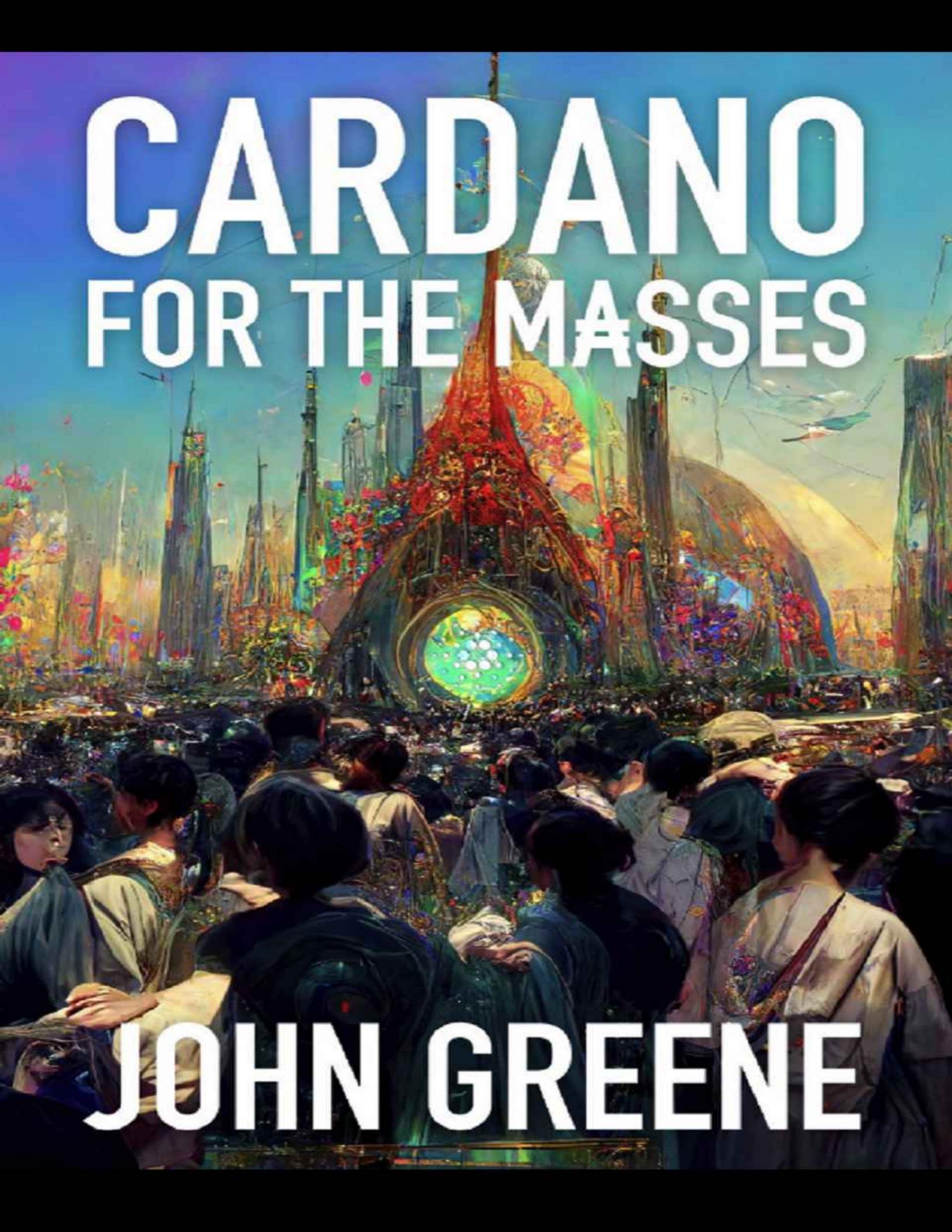


CARDANO FOR THE MASSES



JOHN GREENE

CARDANO FOR THE MASSES

*A financial operating system for people who
don't have one*

John Greene BSc, MSc, CISSP, C|EH

kindle | direct
publishing

Cardano for the Masses: A financial operating system for people who don't have one
By John Greene

Copyright © 2022, Published by Kindle Direct Publishing

Notice of Rights:

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without prior written permission, except in the case of brief quotations embedded in articles or reviews.

Notice of Liability:

The author has made every effort to ensure the information in this book is accurate. However, information contained in this book is sold without warranty, either express or implied. The author will not be held liable for any damages to be caused either directly or indirectly by contents of this book. The advice contained in this book may not suit your situation. You should consult with a professional where appropriate. Readers should be aware that websites listed in this book may have changed or disappeared between when this book was written and when it was read.

Cover Designer:

Billy Romero

Proofreaders:

Diarmuid Buckley
Kevin Pendred
Oussama Benmahmoud

About the Author

John Greene has a background in cloud infrastructure and security with an MSc in Digital Currencies from the University of Nicosia. This is his ‘difficult second book’ after *AWSeasy* in 2015 (outdated now). He lives in Dublin and enjoys Cardano for the mind, mountain running for the body, and playing the bodhrán for the soul.

Contact:

twitter.com/CardanoBook,
john@cardanobook.com

Preface

Chapter 1: In the beginning

Origins of blockchain and cryptocurrencies

Charles Hoskinson's early days in crypto

Cardano is born

Cardano Timeline

Chapter 2: What is Cardano?

Foundational concepts

Why is Cardano different?

Why choose Cardano?

Cardano roadmap

How does Cardano work?

Cardano design decisions

Behind the names

Chapter 3: Proof of Stake

What is proof of stake?

'The green blockchain'

Philosophy of POS

Stake Pool Personas

Setting up and running your own stake pool

Cardano network

How to Research Stake Pools

Stake Pool Performance

Ranking Stake Pools

Types of Addresses in Cardano

Pledging

Delegation

Pledging and rewards

Pledging and Delegation Options

Types of Keys in Cardano

Cardano RTView

Cardano tracking tools

Chapter 4: Consensus (Shelley)

The Scalability Challenge

What is a Consensus Protocol?

Ouroboros

The different implementations of Ouroboros

How the Consensus Layer Works

Hard Forking Business

Path to Full Decentralization

d (=0) Day and beyond

The 3 different sides of full Decentralization

Ouroboros lays the foundation for the Basho Era

Chain v transaction confirmation

P2P (peer-to-peer)

Cardano Entropy (Randomness)

Fees on Cardano

Chapter 5: Smart Contracts (Goguen)

Extended UTXO – the basis for Cardano's DeFi strategy

The DeFi Revolution

DeFi vs RealFi

'Neither smart nor a contract'

Metadata on Cardano

[Token Locking on Cardano](#)
[Native Tokens](#)
[Multi-Asset Support \(MAS\)](#)
[Creating native tokens on Cardano](#)
[The lifecycle of native tokens on Cardano](#)
[Min-ada-value requirement](#)
[Native Token FAQ](#)
[Multi-assets on Exchanges](#)
[The Different Devnets](#)
[Smart Contracts Rollout](#)
[Predictable Transaction Validation](#)
[The concurrency non-issue](#)
[Deploying DApps on Cardano](#)
[Babel Fees](#)
[Stablefees](#)
[Djed algorithmic stablecoin](#)
[How EUTXO copes with impermanent loss](#)
[ERC20 Converter](#)
[Certified DApps on Cardano](#)
[Oracles on Cardano](#)
[UTXO alliance](#)
[It takes time](#)
[*Chapter 6: Plutus*](#)
[What is Plutus?](#)
[The Ledger Model](#)
[Typical Plutus Use Cases](#)
[Plutus Tools](#)

[Writing Plutus transactions](#)

[Datums and Redeemers](#)

[Plutus Scripts](#)

[Collateral mechanism](#)

[Learning Plutus](#)

[Plutus Pioneer Programs & educational partnerships](#)

[Cardano Stack Exchange](#)

[Plutus FAQ](#)

[What the Vasil Hard Fork meant for Plutus](#)

[Chapter 7: Marlowe](#)

[What is Marlowe?](#)

[Marlowe Language Structure](#)

[Marlowe Playground](#)

[Using Blockly with Marlowe](#)

[Using the Editor for Haskell or JavaScript](#)

[Marlowe Run](#)

[Actus Smart Contracts](#)

[Marlowe for P2P Finance](#)

[Marlowe Playground evolves](#)

[Marlowe FAQs](#)

[Chapter 8: Voltaire](#)

[Money is social](#)

[Cardano Improvement Proposals \(CIPs\)](#)

[What is Project Catalyst?](#)

[Catalyst's first fund](#)

[Initial Funds](#)

[Fund4, the first million-dollar fund](#)

Catalyst Circle

The Cardano cFund

Catalyst Natives

Catalyst Fund8

dReps

Fund9

Chapter 9: Basho (Scalability)

Scaling in 2022

Block size increases

Parameter Adjustments

Pipelining

On-disk storage

Plutus script enhancements

Node enhancements

Sidechains

Hydra

Off-chain computing

Mithril

Tiered Pricing as the network scales

February 2022 release

Input Endorsers

Appendix: Cardano Architecture

Cardano Node

Cardano cli (command line interface)

Cardano wallet

Cardano DB Sync

Carp – dcSpark's replacement for db-sync

[GraphQL API Server](#)

[Rosetta API](#)

[Adrestia](#)

[REST API Components](#)

[Stake Pool Metadata Aggregation Server \(SMASH\)](#)

[Glossary](#)

Preface

I discovered Cardano while researching a college project in 2018. Ever since I asked a question of Cardano co-founder Charles Hoskinson in one of his AMAs^[1] I had intended to write a book of some sort. I tried different ideas, gave up, and returned several times. On hearing that the much-anticipated *Mastering Cardano* book would be delayed, I felt there might be a space for a 'can opener' in the meantime.

Writing about cryptocurrencies is challenging. Most of the best-selling crypto books have 'Flesch reading ease scores' in the 50s. I wanted this book to be more inclusive.

With so much jargon in the blockchain space, I decided to arm the reader with explainers throughout. However, I didn't want to obstruct the flow either. As Kindle automatically converts footnotes to a popup format, explainers are accessible by clicking on superscripts in the text. The explainers also form a glossary at the end of the book.

I added excerpts from Charles Hoskinson's various updates to interweave his perspective throughout the book. I felt they add context to many technology decisions while painting a vision for the overall project and industry.

I made every effort to be accurate, however, Cardano is evolving rapidly. There has probably been a change, or update of some sort, as you read this. I intend to update the book regularly, improving readability with each edition.

For e-readers, graphics are best viewed in 'landscape' mode.

Intended audience

This book is mainly for Cardano newcomers. It does not go deep into

the weeds of the technical research papers,^[2] or explore concepts in great detail. The goal is to give a broad overview of Cardano. Each chapter can be read on its own, however, it's best to read from start to finish if you are new to Cardano. OGs^[3] can browse and read sections independently.

Chapter 1 is a high-level overview of blockchain and how Cardano started. Chapter 2 goes through foundational concepts and Chapter 3 addresses proof of stake and Cardano's differentiators. The remaining chapters walk through different aspects of the Cardano roadmap (roadmap.cardano.org). The appendix gives a high-level overview of Cardano's architecture.

IOG and IOHK

Input Output was founded in Hong Kong, hence the abbreviation IOHK. However, the company has since moved its base to Wyoming, US and is rebranding itself as Input Output Global (IOG). At some stage, the website will probably migrate from iohk.io to iohg.io.

Acknowledgments

It's best to come clean at the outset and admit I'm not Satoshi Nakamoto, nor did I invent the *Ouroboros* consensus protocol or think up Babel fees.

This book was inspired by the brilliant minds at IOG/IOHK and the Cardano ecosystem. For some of the technical concepts and features still in research, I did not stray far from the documentation. I have tried to reference all sources.

Chapter 1: In the beginning

*'The best prophet of the future
is the past'*

- Lord Byron

Origins of blockchain and cryptocurrencies

Anyone who doubts the adage ‘the truth is stranger than fiction’ should look at the history of money.^[4] From the round stones on Yap island, to the Irish ‘paying through the nose’ to the Danes, to the peace and prosperity of the Belle Époque era, to the adoption and abandonment of the gold standard...cryptocurrencies, and the blockchains^[5] they run on, are just the latest twist in a long and colorful story.

To understand a third-generation blockchain such as Cardano, we must first review its predecessors. The first generation is Bitcoin,^[6] whose goal was to create decentralized money. Could there be a scarce, tradable token that lived on some sort of decentralized blockchain maintained by people all around the world?

This wasn’t a new pursuit. Bitcoin happened to be the breakthrough, but it was built on previous attempts. The idea of Bitcoin started in the 1980s, with a lot of ideas coming from the ‘cypherpunk’ movement.^[7] Ecash preceded DigiCash with pioneering work from Hal Finney and David Chaum. During the 1990s and into the early 2000s, Nick Szabo proposed the ‘bitgold’ system. There were other contributing factors like the technological advances of the Arm chip powering smaller devices, making processing possible.

In 2008, Bitcoin was just a pipe dream in the form of a white paper.^[8] Satoshi Nakamoto is the pseudonym for whomever it was who wrote this paper. The Bitcoin founder has remained anonymous, even after their email account was compromised and emails publicly shared. Since the beginning, Bitcoin has been shrouded in mystery. It is an experiment born out of discontent with the way things are, and idealism for how things should be. On January 3, 2009, Satoshi Nakamoto mined the first block – the genesis block^[9] – for Bitcoin. These 100,000 lines of mediocre C++ code^[10] attracted a lot of brilliant minds.

From early supporters such as Hal Finney to Martti Malmi, many others flocked over the years as Bitcoin grew from a few crypto anarchists on a mailing list, to a global movement. All this despite no marketing budget, with a logo provided by a forum user with the name Bitboy.^[11] Bitcoin has since proven its resilience. It has been declared dead countless times and endured many crashes. It has lost many of its early contributors. Developers such as Mike Hearn and Gavin Andresen fell out and left. Satoshi Nakamoto, the pseudonymous founder, vanished. Despite these obstacles and setbacks, the dream has persisted.

Within a few years, Bitcoin accrued thousands of users who could send and receive value without a trusted third party, or intermediary. The price of a bitcoin token went from less than a penny to \$1 in 2011, to \$1,000 in 2013, \$17,000 in 2018 and a peak of \$67,000 in 2021. Amid this, there were the crashes, such as the ‘crypto winter’ of 2017, when the bitcoin price fell from about \$20,000 to \$6,000 within weeks. There was a similar crash in early 2022, with two-thirds of the price again being lost.

The idealism of Bitcoin is about creating better money, or ‘sound money^[12] in a digital age’ as described by the economist Saifedean Ammous in *The Bitcoin Standard*. Bitcoin appeared after the 2008 financial meltdown, the worst global financial crisis since the Great Depression. Many people were starting to go back to first principles, questioning whether central banks could be trusted to create ‘sound money’? Can other people create better money? Does the world really need banks to act as middlemen? Can’t I just be my own bank? Questions like these, along with a mistrust of institutions, were the seeds from which Bitcoin grew.

What are the properties of sound money?

Money is usually defined as having three primary properties:

- 1) Unit of account
- 2) Medium of exchange
- 3) Store of value.

Money being a **unit of account** means we have the ability to measure prices in a consistent way. We should be able to compare goods and services in dollars, euros or sterling. Without it, it might be like prison where you compare and trade cigarettes for bread, books, baseball cards, or whatever is lying around. It would obviously be chaotic, making price discovery^[13] next to impossible.

Medium of exchange, means the token should be widely accepted. For a proposed money to function, it should be able to be exchanged for goods and services and act as an intermediary instrument. Being a valid means of exchange avoids the limitations of the barter system, where what one wants must be exactly matched with what the other has to offer.

Finally a **store of value** is the property, whereby when you get money, it doesn't fade, doesn't evaporate into thin air, spoil or rot. Many goods have some of the properties of money. For example, if you were in prison, bananas or tinned food may be a viable means of exchange. But, in general, food can't be used as a store of value because it perishes. For money to be a store of value, it must be durable in value over time. It should be physically durable also. Even if you forget to empty your pockets before washing your clothes, euro notes and coins are usually usable afterwards. There are plenty of coins still around from Roman times and earlier.

There are many other properties. Like is it transportable? Gold is often said to be a poor means of exchange because it's difficult to haul over long distances. Would a large store of gold in a basement be valuable to someone fleeing war? **Transportability** of money may supersede all other properties in such a scenario.

Fungibility was a term familiar only to commodity traders until the 2021 craze for NFTs (non-fungible tokens).^[14] It's a measure of *sameness*, of whether two things are identical, or whether each is unique. If fungible, then there is no practical difference between two things. For business to flow smoothly, there must be consistency in

that a dollar is a dollar, is a dollar. This could be in digital form in a credit card payment, a loan, or a physical note handed over. This is what you would expect with two units of the same currency. However, if you buy an expensive painting from a gallery, you want it to be non-fungible, a unique object.

Divisibility is another important property. You can try, but a coffee shop is unlikely to accept seashells as payment. So it is convenient to replicate a ‘cash in, cash out’ system. Digital currencies facilitate divisibility in a mathematical sense very well by design. However, some are more intuitive in practice. For example, paying a \$10 equivalent for this book in different cryptocurrencies (July 2022) would work out as follows:

0.00043 Bitcoin (BTC)
0.0063 Ethereum (ETH)
20.01035705 Cardano (ADA)

Some real currencies are losing divisibility and there have been proposals to get rid of the penny, which is a fundamental unit of account. Rounding was introduced for cash transactions in Ireland in 2015, which means that the total amount of a bill will be rounded up or down to the nearest five cents.

How you might go about defining the different types of inflation and what exactly is ‘sound money’ is worthy of a book of its own. Bitcoin takes a stance on how to provide the properties required for a form of money. It is scarce, with just 21m bitcoins in existence. One bitcoin is divisible into 100,000,000 satoshis. Bitcoin is digital, so regards itself as durable. Bitcoin is portable as a monetary asset. In April 2020, a crypto exchange transferred coins worth \$1.1bn in a single transaction in a matter of minutes at a cost of 68 cents.^[15] Bitcoins are fungible, but not perfectly so, because anyone can trace transfers between wallets on the blockchain.

At a high level, Bitcoin attains the above properties through decentralization.^[16] There is no set definition of what exactly

decentralization is. This has been a bone of contention for some time, especially when it comes to proposing legislation. Charles Hoskinson wants to see a ‘decentralization index’ to bring clarity.^[17] This index is being developed by the University of Edinburgh.^[18] At a high level, decentralization is about removing, or ‘killing’ the middleman.

The haves and the have-nots

If we were to meet for a coffee in a developed country, the apparatus and mechanisms are in place to make payment seamless. Although paying with a credit card is effortless and instant as a consumer experience, there is a lot of ‘centralized’ activity behind the scenes. You, the card holder, got your credit card from an issuer. This issuer is typically a bank, or some financial institution, issuing credit cards on behalf of the big networks (Visa and Mastercard). The coffee shop is the merchant in this case. Then there is a fourth party involved, the acquirer. This is usually a bank, such as JP Morgan Chase or HSBC, where the coffee shop (merchant) has its account.

This entire authorization process, from the time you tap your card for payment takes a few seconds. It doesn’t matter if your bank is in Ireland and the merchant’s bank is in Japan, the data flows quickly in real time. The full authorization and value transfer between banks can take several business days behind the scenes. The settlement process is heavily regulated, expensive and not inclusive.

Banks would not offer these services if it were not profitable for them. As a consequence, there are three billion people ‘unbanked’, mostly in the developing world, where such infrastructure doesn’t exist. For these people, there are no banks, there are no accompanying services such as credit or insurance.

Any form of money is only as good as the trust people have in it. Trust is variable and affected by economic events large and small. People must have faith that the money they use is worth something, that it holds the properties and characteristics they expect.

So this is what Bitcoin set out to achieve. It was, and is, a very ambitious and idealistic goal to offer an online form of money that was not reliant on a central authority issuing it. People had to have faith in it as a viable form of money. There is no Federal Reserve or central bank involved. Nobody is in charge, but everyone is in charge. Bitcoin achieves this through cryptography (explained in later chapters) to preserve ‘inclusive accountability’, the notion that everyone can ‘check each other’s homework’.^[19] Everyone can see and review the record to ensure transaction(s) are valid and nobody is telling fibs.

Another driving force behind Bitcoin was discontent and exasperation. People lost faith in institutions and their mechanisms. The genesis block of Bitcoin had embedded within it a reference to a headline from *The Times* newspaper of January 3, 2009, ‘Chancellor on the brink of second bailout for banks’, implying frustration with events of the time. The 2008 financial meltdown was just the latest in a line of institutional failings.

Most, if not all fiat currencies^[20] eventually lose their value and/or collapse. Power corrupts. There are so many political and moral temptations to debase the currency for short-term benefits, at the expense of long-term gains. You don’t have to look far back in history for examples. The Weimar Republic in Germany, Venezuela, Argentina and Zimbabwe have all suffered from hyperinflation.^[21] The effects of the 2008 financial crisis are still rippling and have been compounded by the costs of keeping people in jobs during the Covid-19 pandemic, with trillions of US dollars printed out of nowhere.

What is blockchain?

Bitcoin runs on a blockchain. However, cryptocurrency is just one application of blockchain. If creating and trading digital tokens, they reside on a ledger somewhere. This ledger is often compared to a database. Some crypto skeptics claim, ‘It’s just a database! What is

the point?' Blockchain has the potential to remove the need for a central authority in many scenarios. That is a pretty compelling selling point. You can think of blockchain as a 'trust broker' where separate parties, who don't trust each other, need to work together. Blockchain is also commonly referred to as a distributed ledger technology (DLT).^[22]

So it's a special kind of database; it stores a record of events and all sorts of metadata (data about data) related to transactions. Normally an intermediary such as Revolut, or Bank of Ireland, would verify and hold all your banking history on behalf of Visa or Mastercard. What if you don't trust them anymore? Or if you don't want to pay transaction processing fees? This is the core innovation of Bitcoin, to provide an alternative system with a blockchain that acts as a 'trust broker'. So, succinctly, a blockchain is simply a ledger and it stores transactions and associated data so anyone can verify claims.

Blockchains achieve this using cryptographic methods and a consensus protocol.^[23] Think of it as using mathematics and computer science to create a type of database in the cloud. Once a record is written, it's immutable, it's a fact that cannot be altered. So once there is a decentralized trust broker that eliminates the need for a centralized authority, it can be used for many other things. If the human element can be removed by creating decentralized money, the obvious next question was 'can the same mechanisms be used for decentralized authentication? ...for decentralized voting, and so on?'

Voting can be recorded on a blockchain and be immutable, transparent, tamper-resistant, inexpensive and convenient (vote with a mobile app). Is democracy safe when such a high percentage of an electorate don't believe in the outcome of an election? Should a country's leader be able to decide unilaterally to invade another country without a public vote? Without passing a high majority threshold?

Property rights are currently managed by some form of central registry. So if you have a title, or deeds to a house, a central actor has to maintain that database. What happens if that actor can manipulate or edit that database? What happens if there is a change of government? Like when Isis took over Syria, or the turmoil in Ukraine. If the central actor(s) can just decide to update the history, then it becomes very difficult, after peace returns, to decide who actually owns what and where. Millions of people throughout the world live on disputed land. A blockchain could provide a more just system, without the presence of a central authority.

Along with Banking, **Publishing** is one of the oldest industries around. Although e-readers and online book shops disrupted the model to some extent, most companies operate in a centralized manner. You are typically buying a license to view an eBook, without ever owning the product. BookToken (booktoken.io) is an innovative new platform that aims to disrupt the publishing space by bringing books ('decentralized encrypted assets') to the blockchain. Under this model, the buyer owns the digital asset, can resell the book after reading it, and 'read to earn' rewards to buy other books or engage with the platform in other ways, such as AMAs (ask-me-anything) with the author. There are all sorts of implications for readers, authors and publishers outlined in BookToken's whitepaper.^[24]

Supply chains are another ideal use for blockchains. During the Covid-19 pandemic, supply chains for personal protective equipment and vaccines were critical for millions of people. These goods were handled by many companies, and people were making life-and-death decisions based upon the stability of these supply chains and the reliability of the information in them. With blockchain technology, you don't have to trust a central authority or third parties to make sure that the records were accurate.

Identity itself is a critical personal asset that is essential for many services to function inclusively for all. Traditionally you would need a passport or driver's license for know-your-customer (KYC) checks or just get a credit score to be eligible for a loan. Many people's identity

has become linked with personally identifiable information (PII) in online profiles held by Facebook, Google and other centralized behemoths.

Today, your identity is at the mercy of third parties. Statements and claims are then made about that identity, again by credit agencies and government services. You, the subject, don't actually own your own identity online. You're not in control, and your identity – usually in the form of many identities online – is typically managed by middlemen and third parties who have the potential to manipulate the records against your best interest. Decentralized identity made possible by decentralized IDs (DIDs)^[25] and DID documents,^[26] resolves many of these issues and provides greater privacy to the user.

Decentralized finance (DeFi) is about blockchain disrupting traditional banking services. DeFi is enabled by decentralized ID and DID documents. Banking customers in the developed world are not in dire need of DeFi. In the developing world, where you might pay up to 80% interest on a microfinance loan, it's easy to see why DeFi is starting to be accepted. That's an important potential aspect of blockchain and cryptocurrencies – bringing three billion 'unbanked' people into the economy, liquefying trillions of dollars of illiquid wealth.

The above examples only scratch the surface. There are many other platforms that we use daily that can be improved with decentralized alternatives. So the point of these systems is to find a way to build them in a way where they work for the small guy in Africa, as much as they do the affluent banker sitting in a Manhattan office.

Charles Hoskinson's early days in crypto

Charles Hoskinson is a Colorado-based technology entrepreneur and mathematician. He studied analytic number theory before he

discovered cryptography. He was a supporter of the Ron Paul campaign for the US presidency campaign in 2008 and often speaks glowingly of how Paul inspired him.^[27] Hoskinson was involved with Bitcoin from the early days:^[28]

So the 2008 financial crisis happened and then I just kept seeing political failure after political failure. I said, there's got to be a different way and then when Bitcoin came out, it was a marriage of a lot of things I loved. I love open-source^[29] software and I love cryptography and the real hard science stuff, but then at the same time, there's kind of this political undercurrent of anarcho-capitalism and libertarian ethics and these things that lived in the Bitcoin space and there was a completely different monetary policy. I said, 'wow that's really cool, it'll never work ... but it's really cool', because it was one of those 'chicken and the egg' type of ecosystems where you say, 'Well, for it to work, a lot of people have to take it seriously, but people only take it seriously if it works. How do you get that critical mass?' Everybody said, 'Oh, deflationary money can't work ... We tried that in the 19th century, and it was a miserable failure so, yeah, don't even think about it.' All the economists said Bitcoin would die.

I was a speculator. I bought a lot of Bitcoin and I was a miner. I had an AMD CrossFire set-up, and I was on Slush Pool^[30] ... 1.2 giga hashes of mining power, which was quite a lot back in those days and I made a lot of Bitcoin, but I didn't take the space too seriously. Then right around 2013, I noticed an inflection point; it was after the Cypriot crisis^[31] where the government said, 'Okay, it's alright for us to just start taking money out of other people's bank accounts to pay for things.' Whoa! That's probably going to happen here if we're not so careful, and lo and behold bitcoin went from \$4 to, I think \$263. It was just a crazy surge and so, I said this will probably be a big thing. I need to get on the ship and if I don't get on the ship, it will sail right by me.

I had the analytic skills from the math world, and I programmed a lot, so I had cryptography skills and I've known about a lot of the stuff because there's a strong overlap between number theory and cryptography. And then I also had all this monetary policy knowledge, so I got excited about the cryptocurrency space, but I didn't know anybody. I didn't know what to do in the space.

So, I said, 'All right, well, I'll go talk to one of my old professors and ask his advice' and that's Karl Gustafson over at the University of Colorado Boulder ... Karl said, 'Charles, those who cannot do... teach.' So I created a free course on Udemy about Bitcoin. It was called 'Bitcoin or how I learned to stop worrying and love crypto'^[32] and I got 70,000 students and thousands of emails and I met everybody. I met Roger Ver, Erik Voorhees and Andreas Antonopoulos and all the big names in the cryptocurrency space, before they were big.

Bitcoin was ahead of its time in 2009. It allowed for the creation of decentralized value, and for it to be sent and received like an email. It wasn't long until people wanted more. Just like when the web browser evolved from static to dynamic pages, programmability^[33] was required to meet the demand for more applications.

As well as moving value, there's also a story behind every financial transaction, because there are terms and conditions. For example, if you want to buy a book online, there will be a check to see if you have enough funds. If you pay the required amount, the book is sent to your Kindle if, and only if, payment is received. This is a contract; this is the story of a simple transaction. The first-generation blockchain, Bitcoin, wasn't equipped for this. Hoskinson, and others such as Vitalik Buterin, another future co-founder of Ethereum,^[34] wanted to improve Bitcoin. But they were met with resistance, and it wasn't easy to reach agreement on how to proceed.

Invictus Innovations & BitShares

Hoskinson met many people through his Udemy course. One of his students was Li Xiaolai who had founded *Bitfund*.^[35] Xiaolai offered funding to start a business together, so in June 2013, Hoskinson started a thread on Bitcointalk called *Project Invictus*,^[36] named after a [William Ernest] Henley poem. The post asked what could be done to make Bitcoin ‘undefeatable’ and solve existing problems. The feedback focussed on two industry needs. First was the need for a stablecoin,^[37] to limit exposure to volatility. The second was a need for a decentralized exchange.^[38] This was around the time of the Mt Gox^[39] collapse, so centralized exchanges were deemed a single point of failure. CH:^[40]

*I said ‘alright, well is there a way we can bundle both solutions together?’, and of all people, the very first person who replied on the thread was Dan Larimer,^[41] and he said, ‘I’m in!’ ...and he had this paper called BitShares.^[42] So I read the paper, we rewrote it together, his dad (Stan) was involved. Stan, Dan and I, we started a company called *Invictus* together. [...]it ended up being two Larimers and one Hoskinson, so I took a buyout.*

Around the same time, Buterin grew frustrated trying to expand Bitcoin’s functionality with colored coins^[43] and Mastercoin.^[44] Trying to augment Bitcoin proved to be more effort than it was worth. CH:^[45]

Let's be honest here, it (Bitcoin) is the least sophisticated ledger, the least sophisticated consensus algorithm and it consumes more power than the country of Sweden or Switzerland. It is the least sophisticated scripting language, it is not useful at the moment, and it requires enormous effort to innovate.

We created Ethereum on the bones of colored coins and Mastercoin. We didn't just go create Ethereum. Everybody in that damn project was trying to do something useful with Bitcoin and they couldn't! They spent millions of dollars, and months and months to do basic things like issue an asset, and then suddenly with Ethereum around, you could do it with a few lines of code that we could put on a f\$\$king t-shirt!

So this is my counterpoint to Bitcoin, and my primary issue with Bitcoin, is of the insular nature of the community, especially the maximalists,^[46] the inability to adapt and grow and adopt new technology, even when it's obvious that that tech is good like NIPoPoWs,^[47] the fact that they brutally attack people who are innovating and call those people criminals and scammers for having the audacity to try different things.

The fact that the monetary policy can never be updated or evolved, that's both a blessing and a curse, and the ignorance of science, especially when it comes to proof of stake,^[48] and this belief that what they've done is perfect and never can be changed and that cult of personality around the cult of Satoshi. That said, its digital gold, it's a standard, I think it'll always have value. It's done a huge amount of good. Bitcoin is why we're all here, it's why I'm here. So I never will say it's a bad project and I'll never say it's not worth holding BTC.

Origins of Ethereum

Hoskinson met Anthony Di Iorio through a contact of his. Di Iorio ran the Bitcoin Alliance of Canada (BAC)^[49] and asked him if they could use some of his educational material on Udemy. Hoskinson agreed and they started working together. Di Iorio shared Vitalik Buterin's white paper and Hoskinson read it and provided feedback. The white paper went through several iterations, the group converged together, and the result was Ethereum, deemed now to be the second-generation blockchain. Gavin Wood was credited by Hoskinson as the person who built it in a proper way that actually would work. Hoskinson helped set up the initial legal structure. The main point of Ethereum was to add programmability to cryptocurrencies. CH:^[50]

So in 2009, to about 2013, that was the experimental phase of Bitcoin and then in 2013, Bitcoin got to about a billion dollars, a stable industry formed around it and I said, 'Alright, well, it's not going anywhere.' Bitcoin is here to stay. The problem with Bitcoin though, is it's blind, deaf and dumb, and what I mean by

that is that you can't do much with it other than just push bitcoins around. You can't issue your own currency; you can't write applications.

It was similar to when JavaScript was introduced to the web browser. Before that, the web browser worked, but websites were dull and static. JavaScript allowed for the likes of YouTube, Facebook and Google to offer dynamic content with videos and e-commerce. Similarly, with Bitcoin, you could send, receive, and display transactions, you could use metadata for interesting things but DApps weren't possible, ICOs^[51] weren't possible, you couldn't issue your own custom token ... all the interesting and useful features that now make up the DeFi landscape of the industry.

Ironically, Ethereum was announced at the January 2014 North American Bitcoin conference. Bitcoin had just surged from \$100 to \$1,000, so the event was boisterous and rowdy. The first Ethereum t-shirt, made for the conference, had source code on the back of it for issuing your own token. It was so awkward to do that with Mastercoin and colored coins. So ironically, Ethereum was also born out of frustration, frustration with Bitcoin's rigidness and poor developer experience. By bringing a programming language to a blockchain, this allowed smart contracts^[52] to be written to have customizable transactions. So now when Alice sent value to Bob, terms and conditions could be embedded within the transaction, bespoke to her particular needs.



Figure 1: Ethereum T-shirt at January 2014 launch

Hoskinson wanted to set up a proper company, a for-profit and have Founders Agreements.^[53] After looking at the project's structure and direction, he was worried nobody had any incentive to stay involved after the project was launched. He wanted 'golden handcuffs', vesting, and standard things a normal company would have. There was a disagreement as Buterin wanted it to remain an open-source project. Hoskinson argued that if everyone was paid upfront, nobody would be motivated to commit long term. It didn't work out, Hoskinson left in June 2014.

There were no egos, or books written at that point. The group just wanted to produce 'something interesting and cool' to extend the functionality of cryptocurrencies. Ethereum went on to be a huge success. The term 'the Flippening' was even coined. It referred to the hypothetical moment of Ethereum overtaking Bitcoin as the biggest cryptocurrency. The main problem was scalability, it can't handle millions of users, and billions of transactions. Bitcoin could only manage 7 transactions per second, Ethereum 10-20.

Governance was also a problem. It became a victim of its own success. Every single time there was a major debate, instead of resolving it amicably, there were messy hard forks.^[54] Ethereum split in two, with one half forming Ethereum Classic. Likewise Bitcoin had a breakaway faction forming Bitcoin Cash.^[55] Sustainability problems emerged. After the ICO money runs out for a project, or its venture capital funds run out, who will step in and fund things? These gaping holes in Ethereum's design would be addressed by third-generation blockchains such as Cardano and Polkadot (founded by Gavin Wood).

The Ethereum platform forked into two versions: 'Ethereum Classic' (ETC) and 'Ethereum' (ETH). Prior to the fork, the token had been called Ethereum. After the fork, the new tokens^[56] kept the name Ethereum (ETH), and the old tokens were renamed Ethereum Classic (ETC). Ethereum Classic formed as a result of disagreement with the Ethereum Foundation regarding The DAO Hard Fork.^[57] Some people wanted to reimburse the funds. Others united under the 'code is law' philosophy, rejected the hard fork and split into Ethereum classic. Users that owned ETH before the DAO hard fork owned an equal amount of ETC after the fork.

Re: time at Ethereum. CH:^[58]

I don't imagine Vitalik has a super high opinion of me, and it is what it is. The reality is that we have very big philosophical disagreements about how things ought to be run. When I was there, I said, 'look if we are taking other people's money, we have to put that money into a structure that creates accountability. Furthermore we have to put golden handcuffs on the founders and keep them loyal to the project, because there's too many of them. There are eight founders and if they're not locked into something, then what's going to happen is they're all going to run away and create their own ventures.'

Which is what they did, Anthony (Di Iorio) did 'Decentral', Gavin (Wood) did PolkaDot^[59] and Parity, I did Cardano. Seven of the eight are gone, and furthermore the incentives were set up that

we got paid up front, with a founder reward, which I didn't take, the other seven did... basically if the projects successful, hallelujah, if it fails, hallelujah... but you've already got your maximum reward up front, whereas in an equity finance model, you have to build value over time, and you have a venture capital arm keeping you accountable.

So first, there was a fundamental disagreement about business strategy and execution vision. I felt a for-profit model with VC money, to build the protocol, made a lot more sense and then when the protocol was done, spin it out and have a governing foundation run it would be probably a much better approach.

That's one dimension, the other dimensions are interpersonal reasons. We had, for six months, been living like hippies in the Switzerland house and he was traveling around the world, and communication was very siloed, and paranoia and fear started building up. There are three books now written about this, and those books paint a portrait that there was a bunch of very brilliant people, that got two doses of brains and half a dose of social skills, myself included, and when you put them into a high-stress hippie-like situation, it breeds a lot of conspiracy theories and fear and these types of things.

...and frankly, there were just too many founders. So at some point you have to consolidate and there were really two different paths that Vitalik could choose, he was sitting in the middle, he could pick the business side, which is what I was advocating, and Anthony Di Iorio and Joe Lubin were advocating, or he could pick the tech, crypto anarchy, not-for-profit, egalitarian, meritocratic, open-source world.

Cardano is born

Now 0-2 as a crypto entrepreneur, Hoskinson felt disillusioned, but another door was to open. CH:[\[60\]](#)

After Ethereum I took some time off, about six months, and I was actually going to leave the space. I did a TED Talk,^[61] and I said ‘alright, this is my exit point, I’m going to tell everybody what the space is all about and then I’m just going to go do something else.’

Hoskinson’s talk focused on the matter closest to his heart, making finance universally accessible to everyone. He proffered that the main point of blockchain technology is about economic identity. That it should be geared towards the three billion people in the world without access to a bank account, who don’t have identity systems nor property systems and therefore, live in perpetual poverty as victims of geopolitical circumstance.

The talk was well received. Jeremy Wood, who had managed operations at Ethereum and stayed in touch with Hoskinson, invited him to Japan to talk about a new venture with local businesspeople. Negotiations went back and forth for a few months on the proposed structure, how funds could be raised, and they reviewed Hoskinson’s unused roadmap from Ethereum. Eventually a deal was reached with Japanese investors to start the ‘Ethereum of Japan’ which would become Cardano.

The Cardano Foundation (cardanofoundation.org), now based in the Swiss canton of Zug, was set up as a governance body and is the legal custodian of the brand. The Japanese people formed a company which later became Emurgo (emurgo.io), the commercialization arm of Cardano. In 2015, Hoskinson and Wood co-founded Input Output Global (iog.io), formerly IOHK (iohk.io). IOG is the development and science arm for Cardano. The rest of 2015 was focused on protocol development and a team of scientists were hired. The Cardano crowdsale^[62] ran from late 2015 to January 2017, managed by a Japanese company called Attain^[63] who aggregated all the funds. IOG got a 5-year contract to build Cardano.

Right from the start, their mission was clear: ‘using peer-to-peer innovations to provide financial services to the three billion people

who don't have them'. IO believed in the founding principle of 'cascading disruption' – the idea that most of the structures that form the world's financial, governance and social systems are inherently unstable and thus minor perturbations can cause a ripple effect that fundamentally reconfigures the entire system. The company committed to identifying and developing technology to force these perturbations in order to push towards a more fair and transparent order.

All of 2016 was devoted to science and research. The initial small team with massive ideas was Charles Hoskinson, Chief Executive; Jeremy Wood, strategy chief; Nikos Bentenitis, operations chief; Chikara Wakae, communications chief; Richard Wild, design chief; and Tomas Vrana, full stack developer.

November 4, 2020. What is IOG? CH:^[64]

With input output, what I wanted to do there was marry two things simultaneously. One, I wanted to have a company with a very strong philosophy about how to build products. I said, 'these products are born as a scientific method and of evidence, and we need to follow formal methods^[65] and evidence-based software and we need to follow a rigorous academic approach to protocol development'.

So that was one thing, the other thing was the types of products I wanted to build. What I believe in is the philosophy of cascading disruption. So basically what that means is that you're like the first domino, you're like the little pebble on the top of the hill that when you push it, it creates an avalanche. So you build a product, you embed in it all these processes and rules and then after a while, maybe a few years... you can actually walk away, and the product becomes self-evolving.

Back in 2015, IOG stepped back and asked a very simple question which was 'What is the consequence of Ethereum's success? If it works, what's going to happen to the industry?'

They identified three problems that were inevitable if Ethereum was to succeed.

- 1) **Scalability.** The problem with the way Bitcoin and Ethereum were designed, and Vitalik Buterin has basically admitted this by building Eth 2 (Ethereum 2.0),^[66] is that Ethereum can only get to a certain capacity, and at that point, it becomes untenable. Transactions get too expensive, system bloat sets in. A different protocol stack was needed so that, as you gain users, performance level is consistent. It needs to work similarly to centralized systems like Facebook or amazon where it can handle millions to billions of people. IOG sought to figure out how to solve that problem.
- 2) **Interoperability.** The world is made up of many standards, varying for different industry verticals and jurisdictions. It's likely legacy financial systems aren't going away, so it's best to work with them on bridging where possible. Wi-Fi standards would never work if they were tied to manufacturers. If your Huawei mobile could only talk to a Huawei router, it wouldn't be practical to roam anywhere. The reason Wi-Fi works is because it works for everybody regardless of your mobile manufacturer. Similarly, like with your funds and your identity, it would make life easier if information could flow seamlessly between the thousands of cryptocurrencies and legacy systems.
- 3) **Governance**, sometimes referred to as sustainability. Bitcoin and Ethereum have both encountered problems as they scale. There were no governance mechanisms to drive change. When they grew to millions of users, eventually it became impossible to make controversial decisions without fracturing the project. For example, Bitcoin had the 'Big blocks versus SegWit' debate which led to it splitting in two, Bitcoin cash and Bitcoin. Ethereum had similar upheaval with the DAO hack. This divisiveness is a big obstacle to government adoption, Fortune 500 adoption and mainstream adoption because everyday users

and corporations fear more infighting and hard forks every time a controversy, or hard decision arises.

Governance is not a sexy topic on Crypto twitter,^[67] but it's arguably the most important for a project's long-term viability. Who decides how to change the system? How and when should an update be executed? A blockchain needs to have a short-range microscope for near and present dangers, and a long-range telescope for technical challenges on the horizon. For example, if all hell breaks loose when debating a parameter change, what happens when quantum computers arrive? It is inevitable somebody in the next few decades will produce a commercializable quantum computer that can break cryptography. We know it's coming, so how does a fledgling protocol deal with this? IOG has had quantum resistance planned since the early days of the project and will implement it when appropriate.

There are also funding problems with first- and second-generation cryptocurrencies. There's a tragedy of the commons^[68] scenario where most people agree essential infrastructure, or critical updates, are required but there's no mechanisms to apply for, or approve, funding for development.

From 2015 to 2017, IOG took a big step back and just did academic research and asked foundational questions, without deciding on anything. They asked, 'what is a blockchain?' They didn't even decide on proof of work or proof of stake. They just tried to create definitions and models and understand enough foundations so they could reasonably approach these problems.

Professor Aggelos Kiayisis^[69] came onboard in 2016. IOG invented a new proof-of-stake protocol called Ouroboros, and proved it was possible and secure. They invented a whole gamut of interoperability protocols like NIPoPoWs (Non-Interactive Proofs of Proof-of-Work) and sidechain^[70] protocols, as well as a governance stack. IOG staff have written and published over 140 academic papers (latest count) cited countless times throughout the space, often by competitors.

IOG staff have appeared at most major Cryptography conferences in the world.

As well as seeking out the best academics, IOG also reached out to the best engineering teams at companies such as WellTyped, Tweag, and Runtime Verification, for people like Duncan Coutts, and Edsko de Vries, whose work includes the hard fork combinator discussed later. IOG (IOHK) feature prominently on Google Scholar, many of whom are professors or have professor-level citations, such as Dionysis Zindros, Kevin Hammond among many others.

IOG uses formal methods to implement rigorous security in theory and in development. All of IOG's research papers go through some form of peer review. The goal is always to eventually implement high assurance code, using the same techniques one would see with the Shinkansen,^[71] or in aircraft engines, where system failure results in human death. These techniques are applied to IOG's protocols, engineering and development, to garner a high level of trust in the quality of the code to avoid such debacles as the DAO attack, the Parity Wallet hack or the Solana Wormhole hack.^[72]

IOG chose one of the most scientifically oriented programming languages, Haskell,^[73] in use and stress-tested since the 1980s. Prof Phil Wadler,^[74] one of the creators of Haskell, led Plutus^[75] development alongside Manuel Chakravarty, Prof Elias Koutsoupias and Prof Simon Thompson. IOG has funded research and development at the Blockchain Technology Lab at Edinburgh University as well as University of Athens, Tokyo Institute of Technology, Stanford University and the University of Wyoming. Plutus and Marlowe^[76] were launched at PlutusFest in December 2018 by this cutting-edge research team.

Cardano Timeline

Sep 2015 Crowdsale funded development and treasury.

Aug 2017	Ouroboros paper accepted at Crypto 17 ^[77]
Sep 2017	Byron release
Dec 2018	Launch of Plutus and Marlowe at PlutusFest
Dec 2018	Sidechains paper ^[78] published
Dec 2019	Shelley Incentivized Testnet (ITN) ^[79]
Mar 2020	Byron Reboot, first Hard Fork Combinator event
July 2020	Shelley release (decentralization)
Mar 2021	Full decentralization (d=0)
Sep 2021	Goguen release (smart contracts)
Sep 2022	Vasil release

Note that there was no white paper in all this time, instead IOG focused on building on principles. In the next chapter we'll delve into more technical details and explain Cardano's roadmap and naming scheme.

Hoskinson often laments at being introduced as a former co-founder of Ethereum. He prefers to be known for his work at IOG:^[80]

I have six (in 2021) years of history at IOG, and I have six months of history at Ethereum. What's so disheartening is that Ethereum is the big project and Cardano isn't quite there yet, so Ethereum is what everybody knows me for. So they only had six months of data, where I had limited ability to influence and control things, and I was just one brick in the wall amongst many, and then at IOG, I've been the CEO, the big guy, so I've had the ability at my company to demonstrate what a vision would look like.

...and a lot of people often ask well what would have happened with Ethereum had you stayed? So we've already run that experiment. It would look a lot like Cardano, so how we built Cardano, the approach we took, that's exactly what Ethereum would look like. Similarly, they asked what would have happened to Ethereum had Gavin Wood had more say. Well, we already ran that experiment, we have PolkaDot.

Chapter 2: What is Cardano?

'We tell you what we're going to do, we write it down, we go do it, and then we tell you that we did it, and we show you the evidence and proof ... it's the Paul Halmos way of doing things'

- Charles Hoskinson



Alex Hammer
@AlHammer

...

Replies to [@IOHK_Charles](#)

Charles, please explain the essential value proposition of Cardano in one sentence.



Charles Hoskinson 
@IOHK_Charles

Replies to [@AlHammer](#)

Cardano is an open platform that seeks to provide economic identity to the billions who lack it by providing decentralized applications to manage identity, value and governance

Cardano is a decentralized, third-generation, proof-of-stake blockchain platform. It is the first blockchain to emerge from a scientific ethos and a research-driven methodology. Ada (₳, or ADA) is the 'ticker' used on cryptocurrency exchanges) is the first cryptocurrency built on Cardano.

December 12, 2020. How do you explain the Cardano project and its mission in a few minutes to someone not engaged in the cryptocurrency space or even the financial sector? CH:^[81]

The easiest way of explaining it is that the world is going through an upgrade, where we will go from a split system to a unified system. Right now we have two systems, the developed world and developing world system. The developed world system has banks, insurance, credit; it has identity, you can do business online. You can build trust with people, manage risk and be able to grow wealth. So any person born in a developed world country, if they work hard, has a good chance of getting to a point where they can retire and have a good life. That means a life where they have food, water, shelter, etc. They're able to pursue things that make them happy and have enough left over

that when they become weak and vulnerable, their savings can cover them to pay for those infirmities.

When you look at the developing world, for no fault of their own, they live in systems where wealth creation is very difficult. Even if you have some of it, you can't insure it and hedge it, so when an event happens, be it a war or natural event like a hurricane or a tsunami, they get wiped out. So the world is upgrading so that we'll have a unified system where all 7-8 billion people live under one financial operating system. So your identity is interoperable and universal. You can get a loan no matter who you are or where you are. You can get insurance no matter where you're at. You can do business with anyone in the world in a friction-free way.

The point of Cardano is to acknowledge this must be done with principles. So what are we trying to accomplish? We're trying to push power to the edges, and put you in charge of your own money, put you in charge of your own identity, put you in charge of your own voice and give you governance and these types of things. So that when we get to that universal system we get to an open, decentralized, principled system that can't be co-opted. Highly resilient to people trying to come and tamper with it, and then suddenly the richest people in the world, the Jeff Bezos's of the world, will use the same system as the poorest people in the world, and both will have a better system than the system that came before it, in both of those old systems. That's what we're trying to accomplish.

Foundational concepts

As discussed in Chapter 1, a blockchain is a form of database, in this case an accounting ledger,^[82] that is copied and distributed to all users of the blockchain. The blockchain consists of a network of nodes^[83] linked across the internet that store data or valuable digital files in blocks.^[84] Transactions verify these blocks, which are then

connected in a chain in chronological order. The details of these transactions are etched forever in the block and cannot be changed.

This blockchain technology, also known as distributed ledger technology (DLT), offers a decentralized and accessible data structure for digital files and documents. Financial payment and transaction data, as well as other sorts of information such as commercial records and information for supply chain management, might be included.

A blockchain is independent of centralized, controlling companies, institutions, or intermediaries because it keeps data in a decentralized way. This increases the visibility of data storage and administration. A fundamental aspect of blockchain is that records are stored immutably, which means they cannot be modified, falsified, or destroyed without causing the chain of records to be broken.

A blockchain may be likened to a book of permanent records, with each page serving as a data storage device.

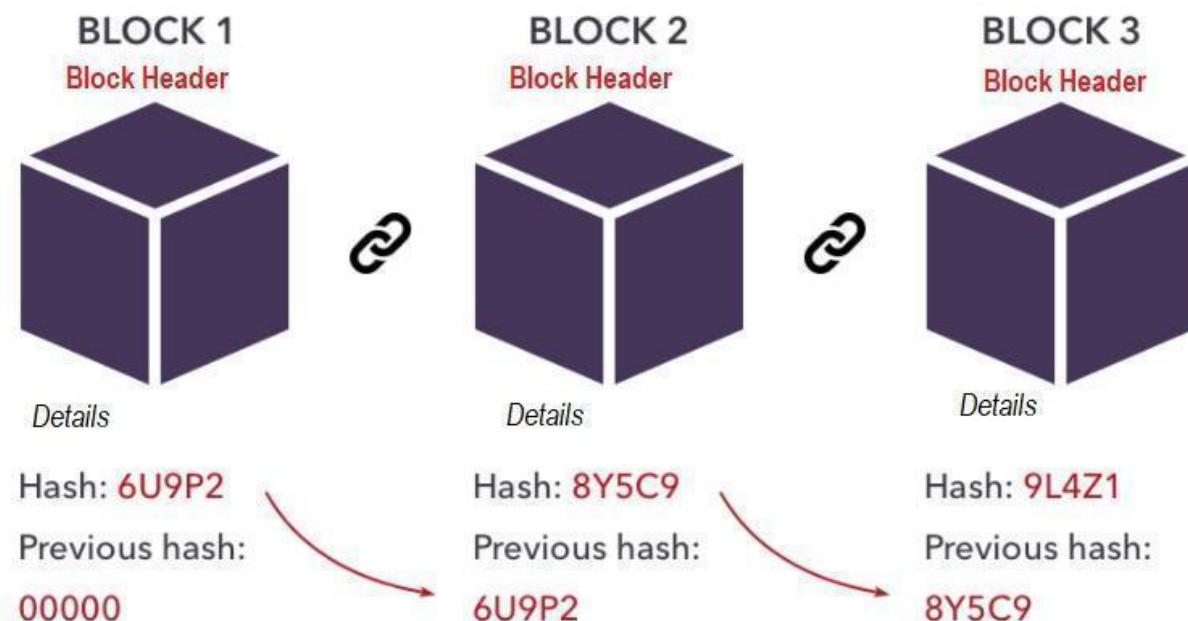


Figure 2: Infographic of blockchain blocks linked by hash^[85] pointers

Blockchain networks can be configured in several ways (see Figure 3):

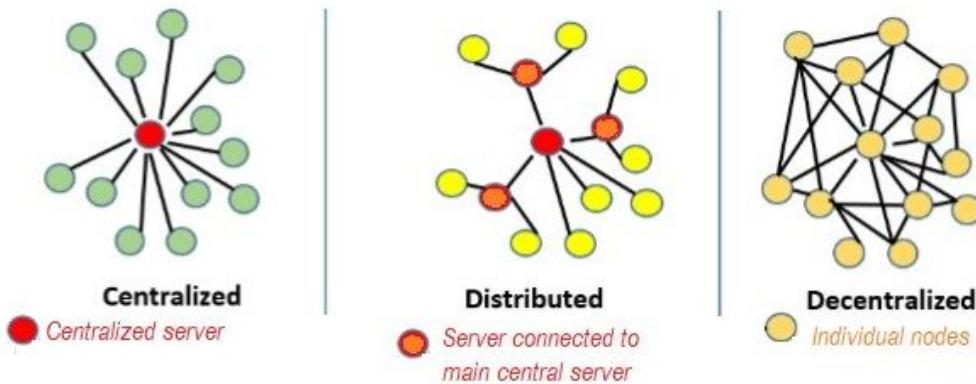


Figure 3. Three types of network structures.

With decentralized blockchains, users can deal with each other directly – peer to peer – without having to go through a central, controlling system

- Centralized systems: in most cases, a single central server manages all data and actions. This raises the possibility of a single point of failure while also implying that the controlling organization (typically a bank or a government agency) makes all the decisions.
- Distributed systems: these depend on several server nodes, each of which serves a portion of the total number of users.
- Decentralized systems: all data and transaction records are encrypted and kept over a network of linked, independent nodes and terminals, rather than on a single server. This assures security, transparency, and independence from centralized institutions.

In addition to providing an immutable and secure database, blockchains serve as a functional environment for transmitting cash, creating digital currencies, and processing complicated transactions,

including smart contracts (automated digital agreements).

What is a cryptocurrency?

A cryptocurrency is a digital asset that is recorded on a ledger and is usually intended to be used as a form of payment for products or services.

In a decentralized setting, blockchain ledgers serve as the foundation technology for cryptocurrencies. To allow the minting (creation) of cryptocurrencies and to safeguard and validate crypto ownership and money movement records, blockchain systems use stringent cryptography methods. A government or centralized financial institution has no influence over the price of a cryptocurrency. Its worth, links to real-world data, and market supply and demand are what define it.

When transmitting crypto payments, addresses^[86] are used. Each address is a one-of-a-kind identifier made up of a string of numbers and letters derived from each user's public keys.

Each blockchain ledger has its own cryptocurrency that provides the 'oil' to run the system. This cryptocurrency is 'native' to the blockchain because it interacts directly with the blockchain. Cardano's founding native currency, ada (₧), is the blockchain's primary payment unit. Ada may be used to pay fees, make deposits, and is the sole currency in which rewards^[87] are given out.

The smallest ada denomination is a lovelace. 1,000,000 lovelaces = 1 ada. Because transactions are calculated to six decimal places, it is easy to divide a single ada into fractions.

What is a native token?

Cardano allows users to generate (mint) their own tokens. These are digital assets, each of which is minted for a particular purpose. On

Cardano, tokens are native assets, meaning that they interact directly with the blockchain, rather than being generated using a smart contract. This means that users, developers, and companies may create tokens that reflect a value footprint on the Cardano blockchain (as defined by the community, market state, or self-governed entity). A token may be fungible (replaceable) or non-fungible (unique), and it can be used as a payment unit, a reward, a trade asset, or a holder of information.

Why is Cardano different?

Cardano is a durable blockchain that is designed to be secure, scalable, and interoperable.^[88] Importantly, Ouroboros, Cardano's proof-of-stake consensus protocol, has been shown to provide the same security assurances as proof-of-work blockchains such as Bitcoin.

Cardano is described as a 'third-generation' blockchain:

- first generation: Bitcoin, a proof-of-work blockchain;
- second generation: Ethereum brought programmable capabilities and smart contracts to blockchain. However, it was flawed because, like Bitcoin, it used a proof-of-work system that wastes huge amounts of energy to solve ever-more-complex mathematical puzzles that have no purpose apart from validating transactions. It is also not very scalable, so the more transactions are performed the slower the blockchain becomes, and the more expensive it is to make a transaction.
- third generation: Cardano uses proof of stake, which uses trivial amounts of energy, to provide all the capabilities of Ethereum. It is also designed to grow, work with other blockchains, and has a long-term funding system built in, and a structure for managing change in the future.

The blockchain engineers who wrote the open-source code for Cardano decided that the best way to produce high assurance software systems that users could trust to handle digital currencies was to employ formal methods such as mathematical specifications, property-based tests, and proofs. Cardano was designed using formal methods to get strong guarantees on the functional correctness of the system's basic components.

One of Cardano's central tenets is security. Haskell, a secure functional programming language, is used in its development. A functional language like Haskell promotes the use of pure functions^[89] in system design, resulting in an architecture that is easily tested in isolation. Furthermore, Haskell's sophisticated capabilities provide powerful ways to ensure the code's correctness, such as basing the implementation on formal and executable specifications, thorough property-based testing, and simulation testing.

Cardano must be able to grow and interact with traditional finance systems to provide a robust infrastructure on a global scale. Despite the fact that Cardano was built with resource efficiency in mind, scale is still an issue, as it is for all blockchain protocols. To address the problem of growth, IOG researchers developed Hydra,^[90] a protocol that can be run on top of Cardano^[91] and allows transaction and smart contract processing off the main chain. The whole system's capacity will be boosted as a result (see Chapter 9).

Performance engineering techniques were used to test which design choices helped IOG achieve resilience, performance, and scalability. Another important goal of Cardano's architecture is to prevent centralization by using economic incentives that encourage decentralization. Stake pools^[92] have an economic incentive to expand as soon as they are created, so it was critical to make it less appealing for a stake pool to become too large. However, a balance has to be struck because a limited number of big pools is more cost-effective than a large number of tiny pools.

A balance was accomplished by altering the reward formula. In a basic system, a pool's total rewards are simply proportional to its stake, hence the larger the stake, the better. With Cardano, if a pool collects more stake than a given threshold ($1/k$, where k is an adjustable parameter), the pool's payout will no longer rise. The pool is said to be saturated,^[93] and delegating more ada stake will not increase the rewards. The result is k pools of nearly equal size if everyone acts in their own self-interest to maximize their rewards.

Interoperability, or the capacity to communicate with other systems, is a fundamental architectural component of Cardano. The use of sidechains is one of Cardano's innovations. The design means that the system can be compartmentalized, and it enables interoperability inside the blockchain platform. A sidechain holds and manipulates data off the main chain. Many sidechains may function at the same time, and if one fails, the rest of the system remains operational. As a consequence, the blockchain has more certainty and trustworthiness. Assets can be moved between separate blockchains that run under distinct rules, procedures, or languages, as well as various methods of accessing the network, by using sidechains.

Cardano's architecture also prioritizes governance^[94] to maintain the system's long-term viability and flexibility. A well-developed governance structure allows Cardano's long-term development to be funded effectively and democratically. Cardano's treasury system is a long-term financing source for the cryptocurrency. It will be run by the community and will allow for a decentralized, collaborative decision-making mechanism to ensure Cardano's continued growth and upkeep. Various financing sources can be used to top up the treasury, such as the aggregation of newly minted coins, a portion of stake pool rewards, transaction fees, and donations. It will be able to support project development and pay for improvement recommendations using the funds earned. Additionally, Cardano improvement proposals (CIPs) are issued to stimulate and codify community conversations about new features and their development.

A voting system is at the heart of the treasury, allowing ada holders to decide on funding proposals and determine how funds are spent. This will guarantee that choices are taken democratically rather than by a small group of people. This voting method will decide on choices such as financing projects, allowing protocol upgrades, and implementing any constitutional changes such as decision-making process modifications. Project Catalyst^[95] (cardano.ideascale.com) is evolving into a fully on-chain democratic governance mechanism that will enable the project to expand over time while also allowing it to support itself in a sustainable manner through a visionary treasury system.

20 January, 2021. What is Project Catalyst? How can people get involved for future funds? CH:^[96]

So we're building a whole stack of voting into Cardano and we're partnered with a lot of great companies and think tanks. For example, we're partnered with an innovation management company called IdeaScale... they've been around for almost a decade. They work with Pfizer and Boeing ... so, yes, how'd Pfizer come up with that vaccine so quickly? They use IdeaScale. So we basically brought them in along with some decentralized tooling and we created a whole new voting system. We spent four years researching how to do a private blockchain-based voting system out of Lancaster University that can scale to lots of users.

Basically, what we've been doing is systematically launching funds... so the treasury of Cardano takes some of the inflation that normally you'd give to stake pool operators or miners... and it gives it to a decentralized account and then people submit ballots to get funded. Over time, people can vet those ballots and it goes through a process, like a gauntlet... and if they survive, they can vote... and if enough votes come in you get funded.

Cardano differentiators

The following aspects of Cardano are outlined in detail in later chapters, but here is a summary of the blockchain's innovations.

Academic research: formal methods, including mathematical specifications, property-based tests, and proofs, are the most effective means of delivering high-assurance software systems. They also provide users with trust in the management of digital assets. Cardano was created with formal methods to obtain strong assurances on the functional correctness of the system's key components. The research that supports Cardano is published at academic conferences and in journals, papers are available to the public and all Cardano development activity is documented on GitHub.^[97]

Only when the Ouroboros consensus algorithm had been proven to be mathematically secure by an academic team led by Prof Aggelos Kiayias at the University of Edinburgh did the software engineering work begin on implementing the blockchain in code.

System design: Cardano is built in Haskell, a secure functional programming^[98] language that facilitates the creation of systems using pure functions, resulting in a design that is easy to test in isolation. Furthermore, Haskell's sophisticated capabilities include powerful ways to ensure the code's correctness, such as basing the implementation on formal and executable specifications, thorough property-based testing, and simulation testing.

Security: Ouroboros^[99] (Cardano's proof-of-stake protocol) offers strict security assurances; it is based on peer-reviewed papers presented at top-tier cybersecurity and cryptography conferences and publications. Only around half of the users who are active in the network are required to follow the protocol; in fact, momentary rises beyond the 50% threshold can be accepted. As a result, Ouroboros is much more robust and adaptive than traditional Byzantine fault tolerance (BFT)^[100] protocols, which must forecast the degree of

expected involvement and may shut down if the prediction is incorrect.

Cardano's network protocol uses a pull communication method. If a node tries to push information, it is automatically disconnected.

- Unique built-in security capabilities:
 - VRF (verifiable-random function): used to prove that a node has the right to create a block in a given slot. [\[101\]](#)
 - VRF [\[102\]](#) use makes the consensus difficult to attack because it's impossible to predict the next producing nodes.
 - KES (key-evolving signature): keys are rotated after a certain number of epochs. [\[103\]](#)
- Plutus, Cardano's native scripting language, [\[104\]](#) uses a formal methodology to bring advanced smart contract capabilities to the blockchain without compromising security.
- DApp [\[105\]](#) certification program to be rolled out in 2022.

As is best practice, IOG rotates between various security auditors such as Bcryptic, R9B (root9b), Grimm, rpisec and Kudelski. The reports are available on the IOG GitHub page. [\[106\]](#)

February 4, 2020. Re: security. CH: [\[107\]](#)

So when we started the Cardano project we said, ‘well let's write software differently and let's think about science a little differently than how our industry thinks about it ...as opposed to writing some white paper or just writing ideas down or saying here's the code, enjoy it’. We said we will start with the peer-reviewed scientific process. So the first thing we did is that we hired a large group of scientists, and we asked a lot of hard questions and they thought deeply about security proofs, adversaries and security models and deeply about what had been done and where original innovation needed to exist.

Now that alone, at the time, was a major step forward because it had not simply been done at a large commercial scale by anyone in our industry. Now we're starting to see that with David Chaum and Silvio Micali entering the space, and others actually hiring real scientists, writing real papers, including Ethereum, that that's no longer a core distinction, but we didn't stop there.

In 2015, we also aspired to have this concept of formal methods, and this is something that very few software engineers in our space fully understand or appreciate the value of. So basically what a formal methodology is, it's where you say, 'okay let's write down in a very specific, detailed, rigorous, mathematical way what we intend on doing ...what is what'.

So we have this concept of Ouroboros, there's many flavors of it, but what does it actually mean to go from these dry, dead papers that our academics have written to something that an engineer can look at, and know with absolutely no ambiguity, that what they have created matches the intent of the authors of the system? So basically you have to write a specification for this, and specifications can then be analyzed in a rigorous way for correctness. You can use all kinds of techniques like model checking and SAT solving^[108] and so forth to verify that your specification meets some sort of collection of design requirements or tests.

So we chose to go down this road and unfortunately most of the time, when you write software in this way, it adds years to your roadmap and that's exactly what happened with us. When we went down this road we had to hire, in addition to a bunch of scientists, a bunch of formal methods experts and then we had to figure out how to do formal methods with cryptocurrencies. At the time, no one had actually done that before.

Power consumption: Cardano is a proof-of-stake blockchain. It requires far less power to operate than proof-of-work chains. The Bitcoin network grows by computers doing energy-intensive

calculations – a process known as proof of work – which is unsustainable in the long run. According to the Cambridge Bitcoin Electricity Consumption Index, [\[109\]](#) the machines that run Bitcoin use as much energy each year as a country such as Norway or Sweden. Ouroboros identifies the participants' leverage in the system using stake as the primary resource. Despite ‘costless simulation’ and ‘nothing at stake’ attacks, [\[110\]](#) which were previously regarded to be fundamental hurdles to stake-based ledgers, no physical resource is spent in the process of ledger maintenance. This distinguishes Ouroboros from proof-of-work methods, which need exorbitant energy consumption to establish consensus.

Seamless upgrades: in older blockchains, upgrades were done via hard forks. When a hard fork occurs, the existing protocol is disabled, new rules and modifications are introduced, and the chain is restarted – with all the history destroyed. Hard forks are handled differently by Cardano. Rather than making drastic changes, the Cardano hard fork combinator[\[111\]](#) (HFC) allow a seamless transition to a new protocol while preserving the history of blocks and causing minimal inconvenience to users.

Decentralization: Cardano is managed via a community-run network of over 3,000 distributed stake pools. Without relying on a centralized authority, network members verify all blocks and transactions.

Ouroboros includes a reward-sharing system to encourage participants to form operational nodes, known as stake pools, that can provide quality service regardless of how stake is divided among the user population. As a result, all stakeholders contribute to the system’s operation, guaranteeing resilience and democratic representation, while the expense of ledger maintenance is dispersed effectively across the user community. The system’s features discourage centralization. As a result, Ouroboros is inherently more inclusive and decentralized than other protocols, which either end up with a small number of actors accountable for

ledger maintenance or give no incentives for stakeholders to join and deliver quality service.

Ouroboros also provides a better staking^[112] experience. Cardano doesn't impose penalties such as stake slashing^[113] or lock-up (bonding). When you delegate ada to a stake pool from your wallet, it isn't locked up. Rewards are distributed every epoch (about 4% of the ada in circulation) and you can access or withdraw the stake at any time. Plus, staking on Cardano is non-custodial which means there's no risk of slashing either. As a delegator, your staked funds are never at risk of being taken by the stake pool.

- The Ouroboros protocol is highly efficient meaning that stake pool operators can run their nodes on low spec hardware, with less hardware investment required than other blockchains.
- Over 80% of tokens are held by the public and more than 70% of ada is staked in millions of wallets.

Websites such as AdaPools (adapools.org) and PoolTool (pooltool.io) give information about stake pools.

A functional environment for business: Cardano is laying the groundwork for global, decentralized finance by allowing developers to create decentralized applications (DApps) that run on functional and domain-specific smart contracts and provide multi-asset^[114] tokens for any need. Two smart contract language platforms are provided: Plutus,^[115] which is 'Turing complete',^[116] so can be used for any purpose; and Marlowe, a specialized language for banking and financial services.

Cardano adds programmability to Bitcoin's proven UTXO model^[117] with its extended UTXO (EUTXO) ledger model, offering smart contracts with increased scalability, while maintaining security. With EUTXO, metadata^[118] and scripts are bundled together in a single transaction for greater throughput. Transaction verification is simpler, so you can predict what's going to happen, including how much a

transaction will cost. And if a transaction fails, no fee is charged. The testing features provided in Plutus and Marlowe mean that developers can ensure their smart contract scripts operate as intended.

Fungible and non-fungible tokens (NFTs) are treated as native tokens, so no smart contracts are needed. This reduces complexity, making it easier for developers, and opens up new uses – and a superior gaming and metaverse experience.

Why choose Cardano?

Of the 18,000 cryptocurrencies^[119] around today, trying to grasp what differentiates one from another can be overwhelming. Are cryptos actually ranked on their merits? How is something as trite as Doge^[120] in the top 20 while a technical marvel like Ergo^[121] languishes outside the top 200? If you look at it long enough, CoinMarketCap begins to look like the odds for a horse race, and just as unpredictable.

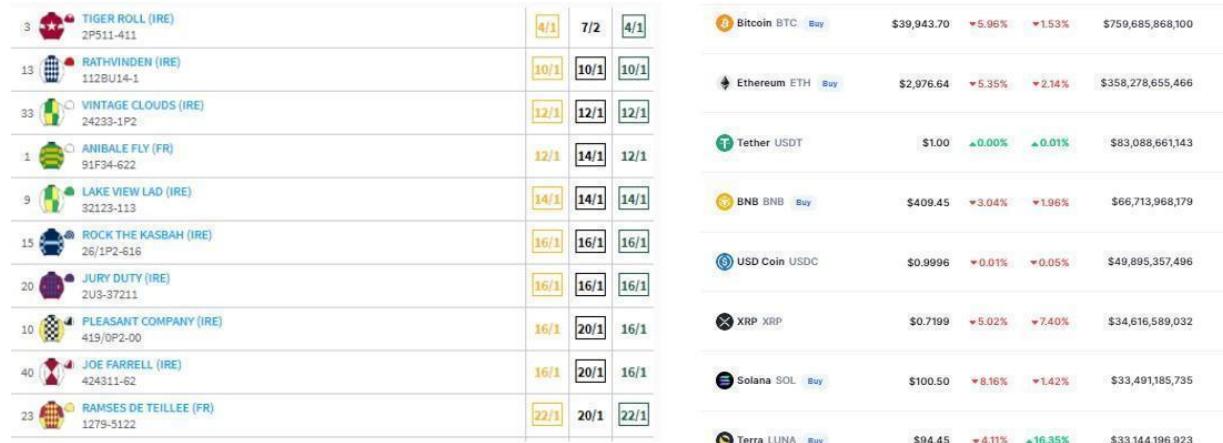


Figure 4. Horse racing odds vs Coincap.io

So what is so special about Cardano? The first generation of blockchains (Bitcoin) provided safe cryptocurrency transmission via decentralized ledgers. However, such blockchains did not offer a suitable environment for the settlement of complicated transactions or the creation of decentralized applications (DApps). The second

generation of blockchain technology (Ethereum) brought more advanced solutions for writing and executing smart contracts, application development, and the creation of tokens as blockchain technology evolved. However, second-generation blockchains were also built using energy-hungry proof-of-work mining and face scalability challenges.

Cardano is regarded as a ‘third generation’ blockchain platform because it incorporates the characteristics of previous generations but avoids their pitfalls and can adapt to meet all user demands. It is built on Ouroboros, a peer-reviewed^[122] proof-of-stake blockchain protocol that was published at the world’s top cryptology research conference (the International Association for Cryptologic Research 37th International Cryptology Conference – Crypto 2017).

The Cardano papers are open-access, patent-free, and give all the technical information necessary for anybody with the appropriate technical skills to verify the accuracy of the performance, security, and functionality claims (iohk.io/research). Other projects have borrowed heavily from IOG’s research, for example, Polkadot’s hybrid consensus protocol.^[123] You can inspect the citations themselves on Google Scholar: a search produces about 1,340 citations.^[124] Similarly, the ‘Bitcoin backbone protocol’ (GKL) paper, which has been the foundation for much of Cardano has more than 1,400 citations.^[125]

The ideal solution should offer the greatest levels of security, scalability (transaction speed, data scale, network capacity), and functionality to handle all aspects of business deal settlement, not just transaction processing. Furthermore, it is critical to guarantee that blockchain technology continues to evolve in terms of sustainability and interoperability with other blockchains and financial institutions.

To meet these demands, Cardano focuses on principles such as:

Scalability: assures that the Cardano ledger can handle a huge number of transactions without slowing down the network. Higher bandwidth possibilities are also provided through scalability, allowing transactions to transport a sizable quantity of supporting data that can be handled simply inside the network. IOG is gradually introducing Hydra (Chapter 9), which will allow sidechain capabilities, along with other solutions such as data compression.

Interoperability: guarantees a multi-functional environment for financial, business, or commercial processes by allowing users to engage with numerous currencies across multiple blockchains. Interoperability with centralized financial bodies is also critical for ensuring legitimacy and ease of use.

Sustainability: building a proof-of-stake blockchain necessitates ensuring that the system is self-sufficient. Cardano is designed to enable the community to sustain its development by engaging in, submitting proposals, and implementing system innovations to promote growth and maturity in a fully decentralized way. To maintain long-term viability, the community controls the treasury system, which is regularly supplied from various sources such as freshly minted coins held back as financing, a portion of stake pool rewards, and transaction fees.

Cardano roadmap

Cardano's development roadmap^[126] has been divided into five eras, each focusing on a different feature set:

- Byron focused on establishing a foundation.
- Shelley focused on network decentralization.
- Goguen is all about smart contracts.
- Basho is the drive to attain true scalability.
- Voltaire is based on implementing decentralized governance.

Each era is built around a collection of features that are implemented and improved over many code releases. While the work for each of these development streams is delivered in order, it is typically done

simultaneously, with research, prototyping, and development happening at the same time throughout.



Figure 5. from roadmap.cardano.org

Byron

Byron laid the groundwork for the creation of Cardano. It enabled users to purchase and trade ada on a proof-of-stake blockchain network. Initially, the Cardano ledger was set up as a federated network, with stake pools run by Input Output Global and Emurgo handling block generation and transaction validation. Byron saw the release of the Daedalus and Yoroi wallets,^[127] as well as a block explorer for examining the blockchain.^[128]

Shelley

The Shelley development era offered a decentralized ledger, resulting in a new economic structure that propels network growth and optimization. In the run-up to decentralization, an Incentivized Testnet (ITN) was set up to demonstrate that Cardano would be viable in the long term with only community-managed pools.

Shelley emerged from Byron's federated network, with the dispersed stake pool operator (SPO) community producing an increasing number of blocks until the network was fully decentralized in 2021. In terms of stake pool operation, delegation^[129] preferences, and incentives, Shelley focuses on essential processes that provide an improved user experience.

Goguen

The development of Goguen focuses on the creation of a worldwide, financial, and multi-functional system for the creation of decentralized applications (DApps), smart contract support, and custom token issuing. Goguen is a fundamental component in establishing a flexible platform for developing applications in areas such as supply chain, track and trace, finance, medical records, identity voting, property registration, and peer-to-peer payments.

Basho

Basho concentrates on Cardano's optimization in terms of network scalability and interoperability. While past rounds of development concentrated on decentralization and new features, Basho is all about enhancing the Cardano network's fundamental performance to facilitate growth and uptake for busy applications.

Voltaire

Voltaire is built on decentralized governance and decision-making, allowing the Cardano community to vote on network development updates, technological advancements, and project finance. To be truly decentralized, the Cardano network needs not just the distributed architecture developed during Shelley, but also the capacity to be maintained and enhanced in a decentralized manner over time. Project Catalyst is about putting the mechanisms in place so people can apply for funding and vote on proposals.

How does Cardano work?

The Cardano node is the network's top-level component. The networking layer, which is the driving force for supplying information exchange needs, connects network nodes to one another. For enhanced data flow, this provides new block diffusion and transaction metadata. Cardano nodes keep in touch with each other using a peer-selection method. You participate in and contribute to

the Cardano network by hosting a node. As with every aspect of Cardano, security is paramount. The network protocol uses a pull communication method so if a node tries to push information, it is automatically disconnected.

Stake pools are responsible for transaction processing and block generation and use the Cardano node to check how the pool interacts with the network. They operate as secure server nodes, storing and maintaining the pooled stakes of several stakeholders in a single entity.

Block production

The purpose of blockchain technology is to create a cryptographically connected, independently verifiable chain of records (blocks). A network of block producers collaborates to enhance the blockchain as a whole. A consensus protocol ensures that the chain is transparent and determines which candidate blocks should be chosen to expand it.

Valid transactions that have been submitted may be included in any new block. A block's producer signs it cryptographically and links it to the preceding block in the chain. This makes it hard to erase transactions from a block, change the order of the blocks, remove a block from the chain (if it has a lot of other blocks following it), or add a new block to the chain without notifying all network members. This protects the blockchain expansion's integrity and accountability.

Slots and epochs

The Ouroboros protocol is used by the Cardano blockchain to support chain consensus. Time is divided into epochs. An epoch is made up of slots, each of which lasts one second. There are currently 432,000 slots (five days) in a Cardano epoch. Slot leaders^[130] are elected randomly from among the stake pools. One node should be nominated every 20 seconds on average, for a total of 21,600 nominations every epoch. One of the randomly drawn slot leaders will be added to the chain if they create blocks. A node that goes offline will miss its chance, and another node will be chosen.

This means stake pools have to be very reliable and be online all the time. The remainder of the candidate blocks will be discarded.

There have been several versions of Ouroboros: Classic, Byzantine Fault Tolerance (BFT), Genesis, Praos, and Hydra. More about this in Chapter 3.

Slot leader election

The Cardano network is made up of a number of stake pools, or delegators, that govern the aggregated stake of their owners and other stakeholders. The slot leaders are chosen at random from the stake pools. The bigger a pool's stake, the more likely it is to be chosen as a slot leader and generate a new block that is accepted into the blockchain. This is the foundation of Cardano's proof-of-stake (PoS) approach. Cardano includes an incentive scheme that discourages delegation to pools that already control too much of the overall stake, to preserve a level playing field and avoid a small number of extremely large pools controlling the majority of the stake.

Transaction validation

A slot leader must confirm that the sender has included enough resources to pay for the transaction and that the transaction's requirements are satisfied while validating a transaction. The slot leader will record the transaction as part of a new block, which will subsequently be joined to other blocks in the chain, if it fits all of these conditions.

How to purchase ada?

Most people buy ada via centralized exchanges such as Kraken or Binance. The steps are documented in Cardano Docs and via a plethora of blogs and YouTube videos.[\[131\]](#)

How to Delegate and earn rewards

The number of ada you hold determines the size of your stake. Cardano users may receive passive rewards for verifying blocks if they have a stake in the protocol.

Because not everyone has the time, skills, or money to operate a stake pool, ada holders may delegate their stake to a chosen pool and have it managed on their behalf by an operator. This enables everyone to contribute to the consensus and receive rewards without having to keep a node online all of the time. The bigger the stake in a pool, the greater the rewards for its owners. You can spend your ada whenever you choose, regardless of whether it has been delegated.

Ada holders may use Daedalus from IOG (full node, desktop wallet) or Yoroi from Emurgo (light, mobile client) wallets to delegate their share. In June 2022, IOG announced a new light wallet, Lace. As the ecosystem has matured, there are now dozens of wallets to choose from.^[132] Here are a few guides recommended in Cardano Docs:

- How to choose a stake pool^[133]
- How safe is it to delegate to a stake pool?^[134]
- How to delegate to a stake pool^[135] (Daedalus)
- Staking and delegating for beginners^[136] (Daedalus)
- How to delegate from the Yoroi wallet^[137]

Cardano design decisions

Many people discovered Cardano by watching Charles Hoskinson's Whiteboard YouTube presentation^[138]. However, Cardano didn't start out with a detailed plan or even a white paper, as many open-source initiatives do. IOG explored the cryptocurrency landscape by adopting a 'first principles' approach.^[139] The Scorex project^[140] and IOG's vault of research papers^[141] were the product of this study.

Unlike successful protocols such as TCP/IP,^[142] most cryptocurrencies have no layering in their architecture. Regardless of whether it makes sense, there has been a desire to retain a single concept of agreement around facts and occurrences recorded in a single ledger.

For example, Ethereum has accumulated vast complexity in its quest to become a world computer, yet it is plagued by minor issues that might jeopardize the system's capacity to function. Should every DApp, regardless of its economic worth, maintenance costs, or regulatory implications, be treated as a first-class citizen?

Layered architecture

The focus of IOG's design is to accommodate the social features of cryptocurrencies, to create layers by separating value accounting from computation, and to answer the demands of regulators while adhering to the founding principles.^[143] IOG also assessed protocols via peer review and inspected code against formal specifications^[144] whenever possible.

February 8, 2019, Charles Hoskinson: In Defense of Peer Review^[145]

...unlike journals, which sometimes take years for research to actually get published, fully peer-reviewed and get through the system, conferences are very frequent. If you look at the cryptographic world you have Eurocrypt, CCS, Real World Crypto and dozens of other conferences every year. Almost every month there's some form of conference going on. So it doesn't slow you down to write a paper, in a very structured, thoughtful way, get it into a conference and then get some review from the community. Suddenly, now you have some of the brightest people in the world waking up trying to destroy your argument, because they know that it benefits their academic career if they can find a flaw in your paper.

Cardano is a cryptocurrency that acknowledges that 'money is social'. A social construct is something that comes through human interaction rather than objective reality. It exists because people acknowledge and believe in it. Countries and currencies are two examples of social constructs.

Flexibility and the capacity to handle complexity in any transaction are critical. If the Cardano project is successful in scaling up to be used by billions of people, massive computing, storage, and network resources will be required to handle billions of concurrent transactions. Cardano's architecture inherits the notion of separation of concerns^[146] from TCP/IP.

Blockchains are, at their core, databases that arrange facts and events based on timestamps and immutability to record asset ownership. It's non-trivial then to add complicated computation for storing and executing DApps. Do we need to know how much money someone is sending? Do we want to become engaged in deciphering the transaction's whole narrative?

To figure out what's happening, a single protocol must be able to comprehend arbitrary events, script arbitrary transactions, allow for fraud arbitration, and even reverse transactions when new information becomes available.

Then there's the issue of deciding what information to retain for each transaction, which is a challenging design choice. What components of a transaction narrative are relevant? Are they going to be significant in the future? When will it be safe to discard certain data? Is it illegal in certain jurisdictions to do so? Certain computations are by their very nature secret.^[147] It's always good to remember the difference between confidentiality and privacy.

Privacy and confidentiality are two separate concepts that protect different types of data. 'Privacy' is used in relation to data that is protected by law, whereas 'confidentiality' refers to different data contained in valid contracts and agreements.

A transaction consists of two parts: the mechanism for sending and recording token flows, as well as the reasons and circumstances for transferring tokens. The latter may be very complicated, including gigabytes of data, signatures, and the occurrence of unforeseen

scenarios. With a single signature moving value to another address, it can also be straightforward.

Modeling the motives and circumstances of value movement is difficult because they are personal to the parties involved in the most unanticipated ways. Contract law creates an even more complex picture, in which the actors may not even be aware that the transaction does not match commercial reality.^[148] This concept is known as the ‘semantic gap’.^[149]

The general lack of legal clarity around protocol participants’ legal safeguards is another gray area. There is no limit to what a sophisticated cryptocurrency may do. A blockchain such as Cardano can unwittingly facilitate all sorts of crime and malfeasance. Just how complex this is in practice is discussed in various academic papers, including ‘The Ring of Gyges.’^[150] using smart contracts for crime.^[151]

Cardano and Bitcoin have an advantage in that they have opted to split into layers. Bitcoin gave us Rootstock (rsk.co),^[152] while the Cardano Computation Layer is Cardano’s proposal.

IOG provides a reference library of Plutus code for application developers to use in their projects, similar to the Solidity-based^[153] Zeppelin project.^[154] IOG also created a set of tools for formal verification based on the Liquid Haskell project.^[155]

The ‘Why Cardano’ essay from 2017 describes the vision^[156] for The Cardano Settlement Layer (CSL) vs Cardano Computation Layer (CCL). The same functionality exists today, but it is implemented differently than outlined back then.

The layered approach was kept but computation is done on the main chain, Layer 1. This was implemented very carefully as the development of Plutus relied on formal methods and a secure design that would not endanger ‘simple’ non-script assets on the chain.

The code base was totally rewritten in a modular^[157] format in preparation for the implementation of the hard fork combinator (HFC) ^[158] in March 2020. The modular approach made it far easier to make changes with the HFC. The ‘Byron reboot’ and HFC in 2020, with the move to Ouroboros Praos, were fundamental in implementing code that would support the future of the blockchain. This was a watershed in the efficiency of the chain and for the productivity of IOG. It made possible the move to the quarterly update schedule in place today. Nobody had done anything like the HFC before; it made upgrades easy, another advantage of the third-generation approach.

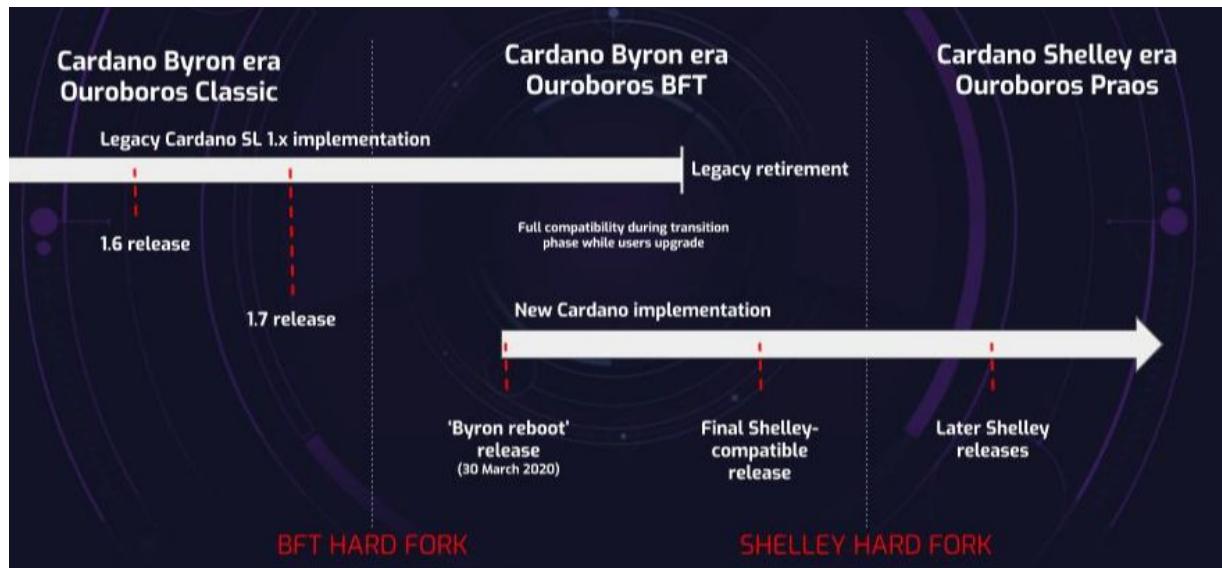


Figure 6: Mainnet Byron to Shelley Roadmap

Charles Hoskinson has explained the layered approach in many of his YouTube AMAs (ask-me-anything). Outtakes from some of these are included below for clarity.

April 21, 2019. Is Cardano going to be more of a sidechain host model? CH:^[159]

Cardano has always been a two-layer system, so this concept of the settlement system and a control layer idea ...so the control layers are either permissioned or permissionless^[160] and they can have arbitrary complexity. The settlement system has basically everything that you would need for a long-term

cryptocurrency ...so basically Cardano, at the settlement layer, is kind of like what I would like Bitcoin to look like ...had I built Bitcoin, if I was Satoshi years and years ago ...and I had unlimited resources and money and all the engineers that I have.... Basically what Bitcoin would have been in 2019 would have been Cardano.... we probably would have put a proof-of-work algorithm in just to create a distribution and then switch it over to Ouroboros... because you couldn't actually do an ICO back then...but basically that's where we'd like to be, and we're nearly done with that.

In terms of the conceptual design and actually the formal specification, we have a total understanding of what ledgers need to look like, the accounting systems behind them... we have an incredibly intricate understanding of what consensus looks like and the tradeoffs of consensus. We have a detailed understanding of interoperability; we understand how to extend the UTXO model to include pretty much as much scripting as you want... but do this in a very safe way where you have predictable gas cost

June 6, 2019. Re: Interoperability. CH:[\[161\]](#)

We've learned a lot along the way as a consequence of building Plutus we've learned a lot along the way in just the design of ledgers and accounting system like for example the Chimeric Ledger's design[\[162\]](#) that we came up with and so, as a consequence, it meant that we could make the base look a little bit more expressive than we anticipated in 2017... that doesn't mean the goal of the base layer of Cardano is to be a world computer and basically Amazon Web Services in the sky for blockchainsthis is not the point...

The point is it for it to be a beautiful place to put identity, metadata.... a beautiful place for it to coordinate financial stories of people and we hope in the developing world.... but ultimately across the entire world for all kinds of applications and then to

be a layer that allows you to move those stories into the domains that make the most sense ...whether those be permissioned private systems ...other public systems, ephemeral domains like MPC^[163] domains

July 9, 2020. Thoughts on Cross Chain Communication, Sidechains, NiPoPoWs and Litecoin^[164]

You can have a maximalist model ...and if they (Bitcoin) ever actually implemented this technology, it actually would be competitive. They've had since 2014 to do it but they haven't done it. This is this concept of primary - secondary chains. Used to be called master – slave, but that language is rapidly falling out of use even in different context. Basically we did this in our original white paper, we said SL (settlement layer) and the CL (computation layer) concept... so the idea is that there's one primary chain and that's where the token lives, ADA. Then that token ADA can be used to power different chains, that have different network logic, it has different consensus rules, it has different ledger rules, a different computational model and somehow these chains don't have their own native token ... rather they are at the service of the primary chain. So let's look at this in the context of the ITN (incentivized testnet).

So let's say that we modify Ouroboros....and Ouroboros now when you're a stake pool operator, instead of just getting one block, you get block Cardano... but then you'd also get block CL1, block CL2... block CLn... and so if you're a stake pool operator, when your job comes up to expand the state of the chain, you'll actually do that for each of these networks in addition to SL. So you'll generate the normal Cardano block, like all the stake pool operators do, but then you'll make the block for the next network, the block for the next network ... and you'll look up that network logic and those consensus rules and the ledger logic and you'll follow the computational model, and these will all be different.

So Cardano has one flavor but then there's a different flavor for CL 1... CL 2. For example, one of these can be an ITN running the EVM (Ethereum Virtual Machine), another one can be in ITN running IEL^E[\[165\]](#) ...and they don't have a native asset, so what happens is that ...wrapped^[166] ADA would be basically used to power transactions in these types of systems. So in practice you'd have SL, that's the main chain, that's where everybody lives right now ...that's what we're doing the hard fork on the 29th and so forth ...and then you would transact from SL to one of the CLs by a sidechain transaction, exactly like ...or spiritually similar like... what I was saying Litecoin^[167] into Cardano... and then once it's there you have wrapped ADA in CL. We'll call this X ...and then you can use that to run things.

So maybe you have an Ethereum smart contract, and we run that in a safety sandbox. Ouroboros has been built in a way that a modification of the protocol would allow stake pool operators to basically make blocks in all of these systems. So instead of running the state of one system, they can run the state of 'n' systems.... they get inflation for being the SPO for Cardano, so this is where ADA inflation would come from, so the state rewards that you have 6% right now ...and then the rest of these would be transaction (TX)^[168] fees that they would collect for.

Proof of stake actually makes this quite easy to do, it's not an overwhelming engineering or scientific challenge. There are certain things to think about, especially about how you synchronize all these systems and bla bla bla ...there are a lot of little details that need to be resolved but this is a model that you could have. This was kind of an envisioned model that came out of Blockstream^[169] when they were talking about sidechains. They said Bitcoin can be that version of SL, and it could be very simple and safe and secure, and then you could have Ethereum as a sidechain of Bitcoin, send your Bitcoin into that sidechain, operate and then send your Bitcoin back when you're done.

[...] After we finish up all the work in the first 5 years, one of our proposals will be to explore this captive sidechain model...so you can call it the 'capture sidechain model' or primary secondary or whatever we're going to end up calling it. We would like to re architect Ouroboros where it's self-evident on how to do this.. and also generalize the expression of ledger rules, computational models, consensus models and network logic so that it's easy to be re-express blockchains... even radically different systems, in a much more generic way. We explored this with the ScoreX project with Alex Chepurnoy ..who now created Ergo... but that work leaves a lot more to be done.

December 30, 2020. Is the distinction between the Cardano computation layer and the Cardano's settlement layer still relevant? CH:[\[170\]](#)

Yes, and in fact the sidechains that we're going to run are examples of what I call the computation layer. The difference is they're not ephemeral, they're actually permanently there ...but yeah that's exactly what we intended. You have a very stable secure settlement system which is the primary network with the stake pool operators ...and you have this collection of sidechains which do different things and have different computational models than the main chain.

Regulatory landscape

If a financial system grows and achieves adoption, it develops a need for regulation, or at the very least a desire for it. This is usually the consequence of periodic market breakdowns caused by the incompetence of some actor(s).

The Knickerbocker Crisis of 1907, for example, led to the establishment of the Federal Reserve System as a lender of last resort in 1913. Another example is the excesses of the United States in the 1920s, which ended in the Great Depression, a devastating

financial catastrophe. The Securities Exchange Commission was established in 1934 as a result of this collapse in an attempt to avoid a repeat of the incident or at the very least hold unscrupulous actors responsible. The Bitcoin Genesis block referred to ‘Chancellor on the Brink of Second Bailout for Banks’^[171] implying some inspiration from the events of the time.

One might question the need, breadth, and usefulness of regulation, but one cannot deny that it exists and that major governments have implemented it with enthusiasm, with many subsequently performing an about-turn once they realize the consequences.^[172] Cardano, like other financial systems, must have a viewpoint on what is fair and acceptable in its design. Cardano opted to distinguish between individual rights and market rights.

Individuals should always have complete control over their finances, free of coercion or civil asset forfeiture. This principle must be enforced because, as crises like Venezuela, Zimbabwe and Cyprus have shown previously, and the ongoing war in Ukraine shows today, not all governments can be trusted not to misuse their sovereign authority for the personal enrichment of corrupt leaders. Cryptocurrencies must be designed with the lowest common denominator in mind.

There should never be any tampering with history. Immutability is promised by blockchains. Introducing the ability to rewrite history or the official record offers much too much temptation to change the past to favor a certain actor(s).

There should be no restrictions on the movement of wealth. Human rights are harmed by capital restrictions and other artificial barriers. Aside from the impossibility of enforcing them, in a global market where many residents in developing countries migrate outside of their jurisdiction in search of a livable income, limiting capital flows frequently harms the world’s poorest.

According to these concepts, markets are separate from people. While Cardano believes in individual rights, markets also have the right to publicly express their terms and conditions. If a person decides to conduct business inside this market, they must be held to those T&Cs for the sake of the system's integrity.

December 30, 2020. Is the SEC (Securities & Exchange Commission) the enemy of Crypto? CH:[\[173\]](#)

No...the regulators are not the enemy of crypto ... let's be honest here our space created Bitconnect,[\[174\]](#) OneCoin,[\[175\]](#) Mount Gox,[\[176\]](#) Bitmex[\[177\]](#) ... thousands of scams that have hurt people. Regulators are like vampires, in a good way. They come in when you invite them. Okay, a vampire standing at the door says, 'can I come in?' ...what brings a regulator into an industry? Happy well-functioned industries where everything is going right? ... like how many regulators are there for mathematics? Is there a mathematics exchange commission? ...that sits down and says 'we really need to look into those topologists? they're slippery people, we are deeply concerned about statistics. Yeah, there's some problems there man, serious problems, 64% of people know that...'

No! because it's like... what scandals occur in the mathematical world? Occasionally we have an older fields medalist who claims he proved the Riemann hypothesis and turns out his brain's baked and it is a garbage paper! Okay we're pretty good at self-regulating in that industry. On the other hand, why is the pharmaceutical industry regulated? Because they make stuff that you put into people's bodies, and if they that up they break your penis, they break your brain, they break your eyes, you go deaf okay more than one person has gone deaf from the first reaction to an antibiotic. There are all kinds of bad things that can occur ...so you need to regulate it! Because there are perverse incentives against your health!

...

So let's look at crypto, you have the ICO (Initial Coin Offering) boom, you have tons of scandals and scams, you have rampant insider trading, you have wash trading on exchanges, you have exchanges failing and the principals of the exchange are stealing the money and fleeing abroad, you have software flaws that were made on purpose to steal people's money, you have massive misrepresentations... you have impersonations... you have people claiming they're using project capital for something but they're actually using to buy yachts and Miami houses and prostitutes and... rah-rah-rah

That is a big neon sign at the front of your door.... 'Vampire come in!' ...our industry did that, we didn't self-regulate, we didn't stop the agency failures, we created a neon sign and welcomed a vampire and now they're here! ...and we're going to complain that they're doing stuff... filing lawsuits, getting involved like a bull in a China shop... of course they are, and their ability to act is proportional to the sophistication of the tools and the modernity of the laws. The Howey test^[178] is an artifact of the 1940s ...it cannot work in 'stem cell' finance, where an asset can be everything... it can be a currency, a commodity and a security all at the same time, could be everything and nothing... it's like some f\$cking Buddhist Kōan^[179] ...Okay we've invited them in and now they're doing their best job to sort the whole thing through.

In June 2022, Charles Hoskinson spoke^[180] before Congress on the 'The Future of Digital Asset Regulation'. He didn't mention Cardano by name even once. The main message he delivered to representatives was cryptocurrencies, in general, should be treated as financial stem cells rather than be rigidly defined as a security, currency or a commodity. Future legislation should be based on principles, not focused on individual jurisdictions or bodies. His contribution was broadly well received.^[181]

Cardano Vision

Cardano is a long-term project that has benefited from the input of hundreds of the world's brightest minds, both within and outside the cryptocurrency sector. It entails constant iteration, active peer review, and leverages the findings of open-source research.

While no project can meet all goals or please all users, IOG intends to present a vision for what a self-evolving financial stack should look like for countries that don't have one. Realistically, cryptocurrencies will not replace current financial institutions. Legacy financial systems have always been able to absorb change. Instead, it's more fruitful to focus on jurisdictions where deploying the old banking system is just too costly, where many people survive on less than a few dollars a day, have no fixed identification, and credit is difficult to come by.

The ability to combine a payment system, property rights, identification, credit, and risk protection into a single mobile app is not just beneficial, but life-altering in these regions. IOG believes Cardano can build on the successes of projects like M-pesa^[182] and Kiva.^[183] If Cardano can transform the way cryptocurrencies are conceived, developed, and financed, then we are heading towards Dr Pangloss's 'best of all possible worlds'.^[184]

Behind the names

Why is it called Cardano? CH explains:^[185]

Girolamo Cardano was the ultimate Renaissance guy, he was a doctor, a lawyer, he was a mathematician, he was a gambler, a complete scoundrel. He was the personal physician of the Pope but then excommunicated but still hung out with the Pope even after being excommunicated, because the Pope liked him. He nearly killed one of his sons in a sword duel because they were sleeping with the same woman. Then he was also a gambler, and he invented a lot of probability theory just so he could be a better gambler. So he created all this advanced mathematics just so he could count cards and roll dice properly and so forth.

And he had a habit of getting kicked out of cities... And he also was a cryptographer because in Renaissance Italy, they had a lot of intrigue between the banking families. So he invented this wheel device to encrypt messages, so they kept secret communication between the families. So I just read about him years ago and thought he's one of the most interesting people I've ever read about in my life. So I was thinking of a cryptocurrency, it could do both good things and bad things, and it also does a little bit of everything and it's just all-around an interesting system, and I thought it'd be cool to name it after Cardano.

He was just one of those guys that lived a life that was unbelievably rich, wasn't nice, wasn't evil, he was somewhere in between. He basically built out modern probability theory because he wanted to be a better gambler. He also inadvertently created the Italian peer review process because, at the time, he was around most of the scientists in Italy who would guard their knowledge and not publish anything because it was a way to maintain employment. So how you would get a professorship in an Italian university is, you would go and present to the students and if they felt you were knowledgeable, they'd say yes, this person should be part of our system, so people didn't want to publish anything because it would ruin their brand, they kept things secret.

So what Cardano would do, he would get people very drunk and learn all of their secrets and he wrote them all down and then he eventually published books about this, which was super taboo and included how to factor quartic polynomial ...he got that from Tartaglia^[186] ...which means the stutterer. So he was a legendary guy and I think he was even a contemporary of DaVinci and I figured it'd be the perfect name for a cryptocurrency because the cryptocurrency is not good or bad, it's a neutral thing, it's brilliant and inspired, it's a bit of a polymath and everybody has an opinion about it and you'll

never get a clear and concise way, but it certainly has a huge impact and it's a man of its time.

But then the other thing is that when you have cryptocurrency, you have the protocol name, then you have the currency name. In Bitcoin, it's Bitcoin, it's the same, but in other systems they're different. So what I decided to do with Cardano is I named the currency, Ada, after Ada Lovelace.^[187] She was a pioneering figure in the 19th century, the first female programmer of note, good friends with Charles Babbage, and left a great legacy and inspired generations of women that came after her to enter into the sciences and become developers. I'd like to say the 20th century spiritual successor to Ada Lovelace is Grace Hopper, creator of COBOL (Common business oriented language) and also the gal responsible for the computer bug, there's a great legacy there as well.

When we were naming the Cardano ecosystem and thinking carefully about the name, the protocol, and what to name the currency, I wanted to connect every part of Cardano to historical figures who did something unique and special in their lives, not necessarily the best of people. Like for example, Cardano himself was a polymath and a brilliant mathematician, but he was also a little bit of a scoundrel from time to time. In fact, if you read his biography, it's a surprise to me that Hollywood hasn't made a book or a movie yet about Cardano, because he's an incredible guy, but Ada is one of the good ones and she lived an incredible life and left an incredible legacy.

And then I named every major release of Cardano after, either a famous poet or famous computer scientist, or somebody I was inspired by. So for example, Byron was after Lord Byron. Then the next thing, Goguen is a world-famous computer scientist, who did a lot of work I admire.

Lord Byron is one of my favorite poets, he wrote She Walks in Beauty.^[188] So I said it'd be cool to get a Byron connection and

bring this in. I also wanted a balance, if I named something after a guy, I'd like to name something after a girl. So always have a nice balance between the feminine and masculine inside the system. That's where that came from.

Where did the naming scheme come from in Cardano? CH explains:

They're just all people that I admired in my life... Voltaire's work, and I read Shelley's work, and some of the things were cautionary tales, - like Percy Shelley wrote Ozymandias^[189] for example.

The name Shelley is interesting, there's actually two famous Shelleys. There's Mary Shelley and Percy Shelley. A lot of people think it's Mary Shelley because she's the more famous of the two. She wrote Frankenstein and a lot of other books and her husband Percy was a famous poet, he was also a member of the Illuminati and he traveled the world and was an artist. He did a lot of cool things, so actually, I named Shelley after Percy, but at this point so many people confuse it for Mary. I say take your pick. The point of it was, that no matter how great a centralized system is, there's this concept that eventually time takes its place and so Shelley wrote a very famous poem called Ozymandias about a traveler who went to Egypt, and he saw all these ruined monuments from long long ago, and he was just commenting on the fact that they're all decaying now.

So I kind of looked at it the same way, that all things must change no matter how great your original ideas are. Time takes its place, so it's kind of a reminder these systems require constant vigilance, updates and maintenance to actually sustain themselves. It's now in the hands of not a leader, but the community to do that with Shelley. So I felt that was a proper way of naming it, but when I said the release was named Shelley, everyone just assumed it was Mary and they were quoting Frankenstein when it came out and I said, 'damn it.'

Okay, it's Mary if you want, they were married, so it kind of works.' Anyway, it's been overwhelmingly well received. [\[190\]](#)

Why the bull's head symbol for the Daedalus wallet? CH:[\[191\]](#)

That is not a bull's head, that is a minotaur's head. The minotaur was a mythological creature that lived in the labyrinth. We named Daedalus after Daedalus the historical figure, or mythological figure, the father of Icarus and the creator of the maze. The labyrinth was built because no chains could bind the minotaur and so, by basically building a giant maze and putting the minotaur in it, he couldn't escape the maze. So Daedalus is the name of the Cardano wallet. Daedalus is the creator of the labyrinth, and the minotaur is the most prominent creature within the labyrinth, that's why the symbol is a minotaur.

Byron is named after the Romantic poet who was the father of Ada Lovelace. The British Library[\[192\]](#) described him as 'Dedicated to freedom of thought and action, and anarchic in his political views and personal morality, the poet and adventurer Lord Byron was the personification of the Romantic hero.'

Lord Byron was an English poet, peer, and politician who became a revolutionary in the Greek War of Independence and is considered one of the historical leading figures of the Romantic movement of his era. He is regarded as one of the greatest English poets and remains widely read and influential. Among his best-known works are the narrative poems *Childe Harold's Pilgrimage* and *Don Juan*, a lengthy satiric poem where Byron portrayed Juan as someone easily seduced by women, reversing the legend of Don Juan as an actual womanizer.

He traveled extensively across Europe, especially in Italy, where he lived for seven years in the cities of Venice, Ravenna, and Pisa. During his stay in Italy, he frequently visited his friend and fellow poet, Percy Shelley. Later in life, Byron joined the Greek War of Independence fighting the Ottoman Empire and died of disease

leading a campaign during that war, for which Greeks revere him as a national hero. Often described as the most flamboyant and notorious of the major Romantics, Byron was considered a celebrity in his era both for his success as a romantic poet and for his aristocratic excesses, which included huge debts and many sex scandals – numerous love affairs with both men and women. One of his lovers, Lady Caroline Lamb, summed him up in the famous phrase ‘mad, bad, and dangerous to know’. His only legitimate child, Ada Lovelace, is regarded as a foundational figure in the field of computer programming. Cardano ticker, ADA, is named after her first name, and her surname Lovelace is used to describe smaller units of ada tokens. 1m lovelaces = 1ada

Goguen: Joseph Goguen was a US computer scientist. He was a professor of Computer Science at the University of California and the University of Oxford and held research positions at IBM and SRI International. Goguen’s work was one of the earliest approaches to the algebraic characterization of abstract data types and he originated and helped develop the OBJ^[193] family of programming languages. Goguen studied the philosophy of computation, formal methods, and functional programming. He inspired Cardano with his work to build the K framework to verify the code of smart contracts, so they can be automatically checked for errors. Goguen was an advisor to Grigore Roșu^[194] when Grigore was at University of California. Grigore is chief executive of Runtime Verification who continue much of this work^[195] today.

Basho: Matsuo Basho was the most famous poet from Japan’s 17th century Edo period. He wrote short 3 sentence poems. One of his most famous poems is called *Old Pond* which describes how a frog, by doing small jumps, can reach the big ocean. The analogy being, as Cardano grows and new users onboard, the system will scale and be seaworthy for the ‘ocean’. CH:

Basho went on this crazy journey during the Edo period in Japan when everybody lived in their silos there, you weren’t

allowed to travel, but he was a guy who traveled and somehow didn't get killed, and he wrote about all these crazy journeys.

Voltaire: Named after the French philosopher who prized criticism and argued for the separation of church and state. Voltaire was one of Charles Hoskinson's favorite poets:

He wrote Candide. He also wrote all these political commentaries and so forth. So I tend to name all the releases after major people who inspired me.

Voltaire was a versatile and prolific writer, producing works in almost every literary form, including plays, poems, novels, essays, and historical and scientific works. He wrote over 20,000 letters and over 2,000 books and pamphlets. He was an outspoken advocate of civil liberties, despite the risk this placed him in under the strict censorship laws of the time. As a satirical polemicist, he frequently made use of his works to criticize intolerance, religious dogma, and the French institutions of his day.

Yoroi is a ‘light client’ mobile wallet^[196] for Cardano. In Japanese, Yoroi means armor. It was built to protect the integrity of the samurai back in the Middle Ages.

Ouroboros is the name of Cardano’s network consensus protocol. The Ouroboros is an ancient symbol ('tail devourer' in Greek) depicting a snake or a dragon, eating its own tail, a fertility symbol also representing eternity and endless return.

Jörmungandr^[197] is a node implementation, written in Rust,^[198] with the initial aim to support the Ouroboros type of consensus protocol on the incentivized testnet in 2019. A node is a participant of a blockchain network, continuously making, sending, receiving, and validating blocks. Each node is responsible to make sure that all the rules of the protocol are followed. Jörmungandr refers to the Midgard Serpent in Norse mythology. It is an example of an Ouroboros, the

Ancient Egyptian serpent, who eat its own tail, as well as the IOG paper^[199] on proof-of-stake.

Plutus is the Greek god of wealth. He was made blind by Zeus, because Zeus wanted him to be able to disperse his gifts without any prejudices and discrimination. Plutus^[200] is the smart contract platform for Cardano. Plutus contracts consist of parts that run on the blockchain (on-chain^[201] code) and parts that run on a user's machine (off-chain or client code). Plutus draws from modern language research to provide a safe, full-stack programming environment based on Haskell, the leading functional programming language.

Marlowe. Named after Christopher Marlowe, an Elizabethan ‘forger, a brawler, a spy, but above all a playwright, a poet and the most celebrated writer of his generation’^[202] who was killed at the age of 29 in a drunken brawl over a bill but might have been assassinated. Marlowe, also known as Kit Marlowe, was an English playwright, poet and translator. He greatly influenced William Shakespeare, who was born in the same year as Marlowe. He was for anti-intellectualism, which is a form of hostility and mistrust of intellectuals.

In Cardano, Marlowe is a new domain-specific language^[203] (DSL) for modeling financial instruments as smart contracts on a blockchain. It is embedded in the Haskell language, which has its own established ecosystem and testing framework. You do not need programming expertise to use Marlowe and you can explore your Marlowe financial contracts with a browser-based contract editor and simulator.

Chapter 3: Proof of Stake

'He who has a why to live for can bear almost any how'

- Friedrich Nietzsche

What is proof of stake?

Proof of stake (PoS) is a consensus protocol, or methodology, that determines consensus based on the amount of stake (or value) retained in the system. A consensus protocol, in essence, is what governs the laws and parameters that regulate the behavior of blockchains, similar to a set of rules that each network member follows. Because blockchains aren't controlled by a single, central authority, a consensus protocol is employed to enable dispersed network users to agree on the network's history as recorded on the blockchain - to achieve agreement on what's occurred and move forward from a single source of truth.

Cardano is based on Ouroboros, an innovative proof-of-stake consensus system that was created via peer-reviewed research. Stake pools, which are server nodes maintained by a stake pool operator (SPO) to whom ada holders may delegate their stake, are at the core of this PoS technology. Stake pools are used to guarantee that everyone may participate in the protocol, regardless of technical expertise or availability to maintain a node. These stake pools are focused on upkeep and hold the pooled stakes of several stakeholders in one place.

Proof of stake vs proof of work

Proof of work (PoW), on the other hand, is a synchronous system^[204] that encourages miners to compete to solve problems inside the block first. This problem-solving is rewarded via a system of incentives. This strategy, however, comes at a cost: higher power consumption and longer time span to handle issues within the chain. These issues might cause the network to slow down dramatically, making it expensive to maintain.

One of the most important elements of proof of stake (PoS) is that as a user's funds grow, so does their ability to maintain the ledger. ie. the ability to create new blocks that can be put to the blockchain and timestamped correctly. A mix of random selection and a

determination of their stake, or money, determines who creates a new block. Within the chain, a form of leader election takes place. Under a proof-of-stake system, users earn transaction fees as they go, increasing their balance with passive income (staking). This strategy promotes the blockchain's steady and consistent expansion in line with the goal of the network becoming stronger as participants join.

Benefits of proof of stake

The following are some of the main benefits of PoS versus PoW:

- A proof-of-stake protocol incorporates stringent security procedures
- Decentralization - the danger of centralization is lowered by imposing penalties for selfish behavior inside the network
- Energy efficiency - energy consumption is incredibly efficient since the blockchain requires less power and hardware resources to operate. For example, 'Berry' is a Cardano Stakepool[\[205\]](#) running on a Raspberry Pi.[\[206\]](#) Markus Gufler[\[207\]](#) ran a Cardano node on a Rock Pi (single-board computer made by Radxa) at the IOHK Summit in 2019. A Rock Pi uses as little as 10W to function.
- Cost-effectiveness - proof-of-stake currencies are considerably more cost-effective than proof-of-work currencies.

Although using proof of stake for a cryptocurrency was a contentious design decision, IOG chose to embrace it since it offers a method for introducing safe voting, has more scaling capacity, and allows for more complex incentive schemes.

The Ouroboros protocol was developed by a skilled group of cryptographers from five academic institutions headed by Professor Aggelos Kiayias of the University of Edinburgh. Beyond being verified secure using a rigorous cryptographic model, the fundamental innovation it delivers is a modular and adaptable architecture that allows for the combination of multiple protocols to boost functionality.

Delegation, sidechains, subscribable checkpoints, improved data structures for light clients, [\[208\]](#) multiple types of random number generation, and even alternate synchronization assumptions are all possible thanks to this flexibility. The needs of a network's consensus algorithm will alter as it grows from hundreds to millions and ultimately billions of members. As a result, it's critical to have enough flexibility to handle these changes and, as a result, future-proof the cryptocurrency's core.

'The green blockchain'

The environmental effect of proof-of-work mining became a hot topic in 2021. Yahoo Finance, [\[209\]](#) EuroNews [\[210\]](#) and the Independent Newspaper [\[211\]](#) were just some of those to dub Cardano the 'green blockchain'. Cardano's staking mechanism avoids Bitcoin and Ethereum mining's huge energy consumption and hardware pollution. Bitcoin has been the subject of debate since Satoshi Nakamoto released the Bitcoin whitepaper [\[212\]](#) in 2008.

Cryptocurrency has been in the news a lot of times for all the wrong reasons. The most common objection is that Bitcoin mining, and other cryptos based on proofs of useless work [\[213\]](#) protocols like Ethereum, are harmful to the environment.

TABLE II: Ranking of Bitcoin and Ethereum among countries based on annual carbon footprint as of July 2021 [23, 26, 27, 30].

Rank	Country	Population (Millions) [26]	Emission (MtCO ₂)	Share (%)
0	World	7,878.2	37,077.40	100.00
1	China	1,444.9	10,060.00	27.13
2	U.S.A	332.9	5410.00	14.59
3	India	1,336.4	2,300.00	6.2
38	Nigeria	211.3	104.30	0.28
39	Czech Republic	10.7	100.80	0.27
40	Belgium	11.6	91.20	0.24
41	Bitcoin + Ethereum	N.A.	90.31	0.24
42	Kuwait	4.3	87.80	0.23
43	Qatar	2.9	87.00	0.23
49	Oman	5.2	68.80	0.18
50	Bitcoin	N.A.	64.18	0.17
51	Greece	10.3	61.60	0.16
76	Tunisia	11.94	26.20	0.07
77	Ethereum	N.A.	26.13	0.07
78	SAR	17.9	25.80	0.06

Figure 7. Table from Cornell University Paper

According to a recent paper^[214] published by Cornell University, Bitcoin and Ethereum's combined carbon footprint would rank 41st in the world.

Algorithms for mining take a lot of power. This problem was exacerbated until recently by the fact that 70% of mining took place in China, where energy is generated using fossil fuels, notably coal. A crackdown by Chinese authorities has resulted in a crypto mining migration, which only shifted the issue to other nations. And the problem has ramifications in other areas. Concerns over energy use, for example, led to the banning of mining in Inner Mongolia. ^[215]

Bitcoin and Ethereum's proof-of-work algorithms are their Achilles heel, yet essential to their operation. Mining rigs that are powerful and state-of-the-art create higher yields, but the quicker they are, the more energy they use. This raises the issue of long-term viability. According to a recent article on the Ethereum Foundation blog, ^[216] 'Ethereum's power-hungry days are limited,' and that the long-awaited switch to proof of stake would require 99.95% less energy, albeit the precise timing of this transition is unknown. 'Early 2022'^[217]

was the original date muted, and ‘the Merge’ is now set for September 2022. A more interesting discussion is ‘When Ethereum goes Proof of Stake, is Ergo likely to absorb most of the hash power?’^[218]

But what distinguishes proof of stake from other blockchains in terms of environmental impact? Because miners must answer increasingly sophisticated mathematical problems to produce blocks, proof of work is resource intensive. They’re on a high-energy race across the world to solve meaningless, randomly generated problems. This vast amount of computing power might be put to better use like programming wind turbines or solar cells. This PoUW (Proof-of-useful-work) paper^[219] discusses alternatives to proof of work. This squandered digital effort has real-world ramifications.

The need for powerful hardware creates a further issue: e-waste. Miners must continually stay up with their competitors, which necessitates the purchase of increasingly powerful mining equipment. ‘Old’ equipment, which is typically only fit for mining, soon becomes outdated. It is wasted, and Bitcoin’s e-waste is a growing problem. Because only 20% of electronic trash is recycled worldwide, the rigs’ plastics and dangerous elements, such as heavy metals, may wind up in landfills. By 2050, the United Nations predicts that the globe will create up to 120m tons of e-waste each year. This paper ‘Bitcoin’s growing e-waste problem’^[220] goes into greater detail.

So why is Cardano being dubbed the ‘green blockchain’? Cardano offers two distinct benefits when it comes to sustainability and environmentally friendly cryptocurrencies: considerably reduced energy use and staking. Network users run nodes in proof of stake, and the chain chooses a node to add the next block depending on the stake and other attributes of the node. The fundamental difference between these two algorithms (and hence their energy needs) is that block producers in proof of stake do not need to spend a lot of time and computer power solving random problems.

Cardano's energy consumption is projected to be 0.01% of Bitcoin's, [\[221\]](#) according to IOG chief executive Charles Hoskinson.

In a meaningless, energy-intensive arms race, proof-of-work cryptos need compute power to create blocks. A Cardano node, on the other hand, may operate on a low-power CPU like a Raspberry Pi. More than 40 million of these have been created, many of which are destined for schools in underdeveloped nations due to their low cost of \$40-\$70. This simplicity also cuts down on plastic and electronic waste.

Extreme weather and forest fires seem to increase each year, with the warnings from UN Climate reports becoming starker and starker. The latest report in April 2022[\[222\]](#) insists it's 'now or never'. Society is aware of deforestation, ice shelf depletion, and global warming. Heatwaves are wreaking havoc on the ecosystem in many regions of the globe, and forest fires are ravaging numerous places. As a result, everything that contributes to the sustainability issue is scrutinized. This encompasses the rapidly expanding cryptocurrency market.

When it comes to solving environmental issues, there are no simple solutions. Cardano is a decentralized platform that can replace older and legacy systems' inefficiencies. Cardano and other proof-of-stake protocols are considered to be contributing to the solution rather than adding to the issue produced by Bitcoin and Ethereum because of their sustainability credentials.

Although Cardano is a proof-of-stake blockchain and the focus of much of IOG's work, they do research other protocols. They have published extensively on Proof of work also. Their latest paper 'Ofelimos: Combinatorial Optimization via Proof-of-Useful-Work: A Provably Secure Blockchain Protocol' was presented at Crypto 2022.

Philosophy of POS

Decentralization is arguably Cardano's most important and fundamental goal. The basis of every blockchain is protocols and parameters. However, the community itself, how it perceives itself, acts, and establishes shared norms, is a major influence on the project's success. Cardano has been meticulously architected to have 'by design' all of the qualities required for a successful blockchain system. Cardano is a social construct, and as such, adherence, interpretation, and social conventions all have a part in determining its robustness and long-term viability.

Staking Principles

Since the debut of the Bitcoin blockchain, consensus-based on a resource that is disseminated over a population of users – rather than identity-based participation – has been the hallmark of the blockchain ecosystem. Proof-of-stake systems are distinct in this space because they employ a *virtual resource* called stake that is recorded in the blockchain itself.

Pooling resources for participation is unavoidable; some amount of pooling is generally advantageous in terms of economics; therefore resource holders will find a means to make it happen. Given this inevitability, the challenge is then to avoid the emergence of a dictatorship or oligarchy.[\[223\]](#)

Goal of Staking Rewards System

Unlike previous blockchain systems, Cardano employs a reward sharing mechanism that (a) permits staking without unnecessary inconvenience and (b) incentivizes resource pooling in such a manner that system-wide decentralization develops spontaneously through resource holders' rational engagement.

The mechanism's two main goals are as follows:

- Involve all stakeholders - The more people who are involved in the system, the more secure the distributed ledger becomes.

This also means that the system should have no participation barriers and should not cause friction by necessitating off-chain coordination amongst stakeholders to participate with the mechanism.

- Keep individual stakeholders' power to a minimum - For certain stakeholders, pooling resources increases their influence. The power of pool operators on the system is proportional to the resources managed by their pool, not to their own. Without pooling, all resource holders have a leverage of one. The stronger the system's leverage, the less secure it is (a 51% attack^[224] on the system is more likely).

A large pool size is not the sole cause of increased leverage; stakeholders may also gain leverage by forming several pools, either publicly or secretly (known as a Sybil attack^[225]). The greater the degree of decentralization of a blockchain system, the lesser its leverage.

From Theory to Practice

So, how does Cardano's reward-sharing mechanism achieve the aforementioned goals? Staking with Cardano allows for two options: pledging^[226] and delegating. Stake pool operators use pledged stake; pledged stake is committed to a stake pool and is expected to remain there for the duration of the pool's operation. Consider pledge to be a 'commitment' to the network. It's a way to 'lock up' a specific amount of stake to help protect and secure the protocol.

Delegating, on the other hand, is for individuals who don't want to be hands-on. Instead, individuals are encouraged to evaluate the stake pool operators' offers and delegate their stake to one or more pools that, in their judgment, best serve their and the community's interests. There is no reason to refrain from staking in Cardano since delegation does not involve the locking up of money; all stakeholders are welcome to do so. This is not a given with other proof-of-stake blockchains.

For example, with Polkadot, [\[227\]](#) your funds are ‘bonded’, which is a fancy word for ‘locked’. It takes a full 28 days to ‘unbond’ or ‘unlock’ your funds. Staking on Cardano is non-custodial, so there are no slashing [\[228\]](#) penalties imposed. As a delegator, your staked funds are never at risk of being taken by the SPO, significantly adding to delegator participation.

Two parameters, k and a_0 (*/a nought/*), are crucial to the mechanism’s operation. Pool rewards are limited to $1/k$ of the amount available thanks to the k -parameter. Adding X amount of pledge to a pool boosts its rewards by up to $a_0 \cdot X$, thanks to the a_0 option. This isn’t at the expense of other pools; any rewards that go unclaimed due to inadequate pledging will be restored to Cardano’s reserves and distributed in the future.

Creating a stake pool necessitates operators (aka stake pool operators, aka SPOs) declaring their profit margin [\[229\]](#) and operating expenditures [\[230\]](#) in addition to agreeing on an amount to pledge. The operating expenses are withheld first when the pool payouts are distributed at the conclusion of each epoch, ensuring that stake pools stay sustainable. Following that, the operator profit is determined, and all pool delegators are compensated in accordance with their investment.

This approach, when combined with the delegates’ evaluation of stake pools, offers the correct set of restrictions for the system to converge to a configuration of k equal-sized pools with the largest amount of pledge.

Cardano’s blockchain architecture, like many others, has an innovative and well-researched mechanism. The rewards system has been mathematically shown to provide an equilibrium that matches its goals. But, in the end, arithmetic alone will not be enough; only humans will be able to make it happen. The future of Cardano lies in the hands of the community.

Stake Pool Personas

A stake pool is a server node that aggregates and maintains the stakes of several stakeholders into a single entity. Stake pools are in charge of transaction processing and block production, and they monitor their interactions with the network via the Cardano node.

To manage a stake pool effectively, you'll need a stake pool operator and one or more stake pool owners. There are conceptual differences between these two jobs:

- A stake pool operator is someone who is in charge of setting up and managing the stake pool, which means they own or rent a server, manage and monitor the node, and have access to the stake pool. Stake pool operators may sign blocks, register, re-register, and retire stake pools, as well as upload updated certificates, using their key
- A stake pool owner is someone who offers their stake to the pool to boost the pool's reward earning capability and appeal. Sybil attacks are mitigated by the owner's capacity to pledge stake.

The stake pool operator and owner are normally the same person, although a stake pool might have several owners who commit their share to establish a larger pool and maintain it competitively. Stake pool activities are still managed by a single stake pool operator in this case.

The stake pool operator must have the trust of all stake pool owners. All operator and owner rewards are placed into a single shared reward account linked to the pool's reward address, and the protocol distributes them among the owner accounts. The reasoning for this is because if everyone could become a co-owner of a stake pool rather than delegating, the process would be rendered obsolete.

It's advisable to have a contract to specify when and how the collected incentives in a shared account should be divided. They can, for example, agree to have the operator manage the shared

account, or they can use a multisig^[231] account.

A bidirectional relationship and trust are required to run a pool properly. If this trust is betrayed, other parties may suffer losses in terms of accumulated or projected benefits, as well as the operator's reputation.

The **controlled stake** is the entire amount of stake held by a stake pool. It combines the pool operator's stake and any stakes that have been delegated to the pool by other ada holders. It may be expressed as a total quantity of ada (e.g., 2M ada) or as a percentage of the network's total ada supply (e.g., 2%).

Setting up and running your own stake pool

Stake pools are an important aspect of the decentralized Cardano network, since they enable the procedures that assure the network's long-term health and viability. Stake pool operators allow other users to participate in the system and earn rewards without having to host an active node all of the time. The scope of this book is to address the theoretical. More in-depth practical details are out of scope and covered in the following Cardano documentation sections:

- Creating a stake pool^[232]
- Establishing connectivity between core and relay nodes^[233]
- Operational certificates and keys^[234]
- Public stake pools and metadata management^[235]
- SMASH metadata management^[236]
- Stake pool performance^[237]
- Stake pool ranking^[238]

Cardano network

Federated nodes were solely responsible for block production and network connectivity in the Byron era. The Byron network was made up of federated core nodes, which were static nodes that created

blocks and kept the Cardano network running. With the launch of Shelley, the network initially went to a hybrid mode, with IOG-operated federated nodes (which configure connection between various stake pool operators) and SPO (stake pool operator)-operated nodes. The percentage of blocks produced by decentralized nodes steadily increased, while federated nodes progressively ceased operations, distributing network maintenance equitably across all stake pool operators. Using ongoing automated discovery and selection of peers, Shelley's network migrated to complete decentralization.

Nodes link to other nodes using a static configuration established in a topology file at the startup phase. It is critical to connect to dependable relay nodes to avoid a situation where relay nodes fall offline, rendering block-producing nodes unreachable. IOG provided SPOs with a list of all registered relays^[239] organized by geographical location for connecting reasons. SPOs should additionally produce a configuration that includes 20 other SPOs as peers. Many SPOs can employ more than 20 peers for connection reasons in practice. The list lets you choose peers both close by and far away, ensuring inter-region connection.

The node's network layer was altered to employ continuous automated discovery and peer selection as the network was shifted from federated to completely decentralized. Upgrades to the network stack were used to accomplish this. Initially, this allowed for enhanced automation of connecting SPO relays to one another, reducing the requirement for static setup. It eventually allowed all Cardano nodes to have a full peer-to-peer (P2P)^[240] architecture, eliminating the network's need for IOG-run relays.

More information regarding the Cardano network, node communication, and mini protocols that allow this capability may be found at this link.^[241]

Core and Relay Node Connections

You will have two sorts of nodes as a stake pool operator: core nodes and relay nodes. One or more relay nodes must accompany each core node. The distinction between the two kinds is that core nodes are in charge of creating blocks, whilst relays are in charge of connecting with other relays in the network as well as broadcasting blocks. This distinction influences how they are set up and linked to the network.

For block generation, a core node is set up with several key pairs^[242] and an operational certificate. It only communicates with the relay nodes it has set up.

Instructions to configure a node and create an operational certificate:

- About node configuration files^[243]
- Configuring topology files for block-producing and relay nodes^[244]
- Creating an operational certificate with key evolving signature (KES)^[245]

Because a relay node does not need any keys, it is unable to create blocks. It communicates with its core node, relays, and external nodes.

Each node should operate on its own server, with the firewall on the core node server set to only accept connections from its relays.

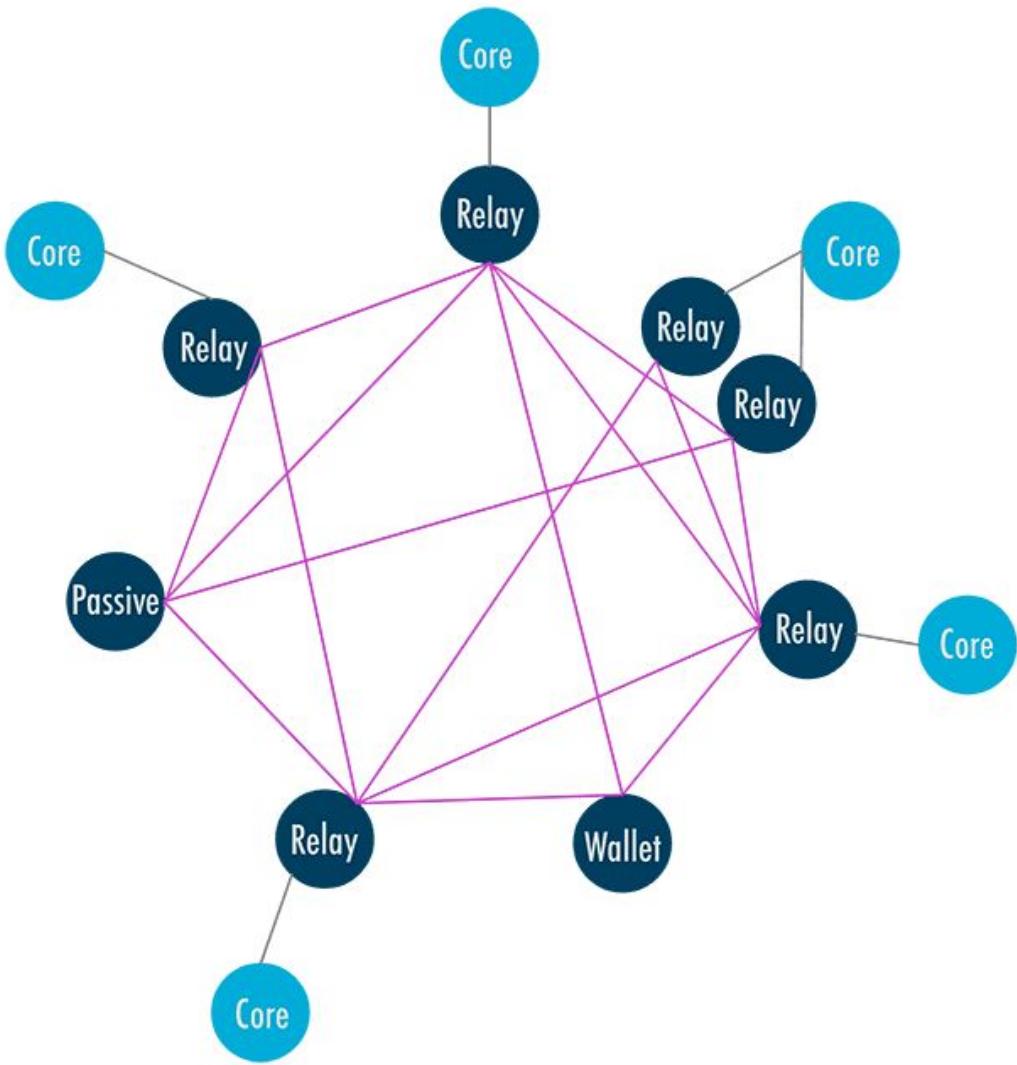


Figure 8: Core and Relay nodes

How to Research Stake Pools

SPOs (Stake pool operators) may be interested in getting specific information regarding their pools' activities after a successful stake pool registration and operation. [pooltool.io](#), which gives confirmed stake pool facts, may be used to get information about those pools that are active on mainnet. [\[246\]](#)

Exchanges and stake pool operators, in particular, are on the lookout for detailed information regarding their mainnet and testnet pools in certain circumstances. It's advisable to use `cardano-node`,

[\[247\]](#) cardano-db-sync, [\[248\]](#) and a cardano-graphql[\[249\]](#) to access data stored on the Cardano blockchain.

GraphQL is an open-source data query and manipulation language for APIs, and a runtime for fulfilling queries with existing data. GraphQL was developed internally by Facebook in 2012 before being publicly released in 2015. On 7 November 2018, the GraphQL project was moved from Facebook to the newly established GraphQL Foundation, hosted by the non-profit Linux Foundation. Here is a short video I recorded explaining ‘GraphQL in 6 mins’[\[250\]](#)

Docker[\[251\]](#) may be used to install and deploy each of the integration components described above.

Another alternative is the public Cardano Explorer, which is likewise built on the cardano-graphql instance and is often used by exchanges and stake pool operators who want to test stake pool functionality on testnet.[\[252\]](#)

Stake Pool Performance

The creation of new blocks for the Cardano network is the responsibility of a stake pool designated as a slot leader.[\[253\]](#) The slot will stay unfilled if the stake pool does not create a block, and the blockchain will not be extended. Although the Cardano blockchain may accept a few missing blocks, the bulk of expected blocks (at least $50\% + 1$) must be created within an epoch. Although missing blocks do not affect the blockchain’s overall extension, an unresponsive elected stake pool reduces the network’s overall speed.

The ratio of the number of blocks a stake pool generates in a particular epoch versus the number it was capable of producing is used to measure stake pool performance. For example, if a stake pool could create 100 blocks in an epoch (depending on its stake and likelihood of being elected), but only produced 50 blocks, its performance would be 50%. Poor stake pool performance reduces

the quantity of rewards received by a pool and its members, making it less appealing to delegators. A stake pool should have adequate network connectivity, be run on a dependable system, and engage in block generation and verification to increase its performance.

The stronger the pool's performance, the more appealing it will be to delegators, since higher rewards will be offered.

Ranking Stake Pools

Stake pools are ranked in the Daedalus wallet and Cardano Explorer depending on the amount of rewards users will get if they opt to delegate to them. The ranking indicates the saturation^[254] level of the pool, making pool selection easier. From the standpoint of a delegator, once a pool reaches a specific saturation threshold, delegating to it is no longer profitable. The most desirable stake pools are shown first, and they are sorted from top to bottom.

The ranking system is intended to let users pick the best stake pool for a greater return on investment (ROI), so that dependable stake pool owners can keep the system running and maximize decentralization.

Ranking parameters

The cost and margin of a pool, as well as the pool's performance and the amount of stake it has previously attracted, all factor towards its rating. These variables encourage the creation of dependable stake pools that are not yet saturated and provide low cost and margin.

The Cardano Docs includes guidelines for operating large stake pools^[255]

Types of Addresses in Cardano

The addresses are a blake2b-256 hash of the related verifying/public keys combined with some metadata stored on the Cardano

blockchain.

Shelley introduced four different types of addresses:

- base addresses
- pointer addresses
- enterprise addresses
- reward account addresses

Aside from those addresses, Byron-era bootstrap[\[256\]](#) and script addresses are still supported by Shelley. Only the new base and pointer addresses have stake rights. Addresses, such as a UTXO[\[257\]](#) address, are made up of serialized data described in the ledger specification stored in the blocks of the blockchain.

There are two pieces to the serialized data (address):

- Metadata for interpreting.
- Payload: raw or encoded data

Base Address

The staking key that should manage the stake for that address is explicitly specified in a base address. The owner of the staking key has the ability to exercise the staking rights connected with funds kept at this address. Without first registering the staking key, base addresses may be used in transactions. Only by registering the stake key and delegating to a stake pool[\[258\]](#) can the stake rights be exercised. After the stake key has been registered, stake rights can be exercised for base addresses used in transactions before or after the key registration.

Pointer Address

The staking key that should control the stake for the address is indirectly specified by a pointer address. It uses a stake key pointer to refer to a stake key, which is a place on the blockchain where the

stake key registration certificate for that key is stored. Even if the transaction's target isn't an active stake key registration, pointer addresses may be utilized in it. This includes the case when the key was unregistered after (or before) the transaction, as well as references to clearly bogus targets. The rationale for permitting such incorrect targets is so that nodes only have to keep track of the stake keys that are presently active.

The pointer does not have to be as long as the hash used in base addresses. Pointer addresses have a nuance to them. A stake key registration certificate referenced by a pointer address might be lost as a result of a rollback.^[259] To avoid funds from being lost in such a situation, the system treats incorrect pointer addresses as legitimate for the purpose of utilizing funds held there as inputs for transactions, but simultaneously ignoring them for the purpose of proof-of-stake participation. To avoid funds from being omitted from the proof of stake in the case of rollbacks,^[260] a wallet might refuse to make transactions to pointer addresses until the referenced certificate has become immutable.

Enterprise Address

Because enterprise addresses don't come with stake rights, adopting them implies you're opting out of the proof-of-stake protocol. Stake rights may not be exercised by exchanges or other entities that control substantial quantities of ada on behalf of other users. Exchanges may indicate that they observe this guideline by utilizing enterprise addresses. Enterprise addresses are automatically removed from the process that determines the slot leadership schedule since they are not connected with any staking key. Employing addresses with no stake rights reduces the overall amount of stake, which aids a prospective attack.

Reward Account Address

A reward address^[261] is a cryptographic hash of the address's public staking key. To pay rewards for participating in the proof-of-stake

protocol, reward account addresses are used (directly or via delegation).

They possess the following characteristics:

- Account-style accounting is employed rather than UTXO-style
- Transactions cannot be used to receive funds. Instead, when rewards are paid, their balance^[262] is just raised
- Registered staking keys and reward account addresses have a one-to-one relationship.

When funds are removed from the address, this key is used. Additionally, the stake connected with the funds in the address contributes to the stake of this key. The staking object for a reward address does not have to include any information, just as with enterprise addresses.

Pledging

Decentralization became a point of contention as Shelley approached on the Cardano mainnet. Proof-of-work cryptocurrencies like Bitcoin and Ethereum have grown increasingly centralized over time, regardless of their original founding aim. The days of Bitcoin fanatics mining blocks on AWS EC2 spot instances^[263] are long gone, and today's mining networks are dominated by a tiny handful of specialized, professional mining companies.

This isn't inherently a negative thing in and of itself, but it would go against Cardano's idea of a decentralized, proof-of-stake system if it occurred. Cardano was built from the bottom up with decentralization in mind, especially in terms of stake delegation and reward systems. Pools larger than a certain size will not be competitive on the Cardano network, and delegation rewards for everyone will be ideal when there are numerous medium-sized pools. Diversity is beneficial to all ecosystems. Similarly, this method strikes the optimal mix between promoting grassroots participation from experienced

community members and assisting individuals looking to start commercial stake pool firms.

How Pledging Works

A pool operator might pledge a personal investment in their pool upon registration to make it more appealing. The pledged sum may be modified epoch by epoch and will be refunded when the pool closes.

On the Cardano blockchain, anybody may run a pool. There is no minimum pledge. To make their pool more appealing, pool managers might pledge some or all of their stake to the pool. The more ada pledged, the more rewards will be given to the pool, which will attract more delegators.

It's also worth noting that there's also no maximum pledge, so a pool operator with a lot of ada to stake may maximize their own profits by filling up the pool with pledges and avoiding attracting any delegation. Of course, only a few operators will be able to do so; most will attempt to entice delegation with a mix of pledge, cheap costs, low profit-taking, and strong performance.

The appeal of a pool to delegators is determined by four interconnected factors:

- operating costs (lower the better)
- operator margin (lower the better)
- performance (higher the better)
- pledge (higher the better).

The pool operator might request a bigger operator margin while remaining desirable to delegators by offering a larger pledge.

Pledging rewards

Given two similar stake pools, the one with the higher pledge will receive more rewards and hence be more appealing to other delegators. The SPO (Stake pool operator) or other pool owners should work together to fulfill the pledge by delegating themselves. It's also crucial to make sure there's enough funds in the accounts that utilize the pool owner's address(es) as stake reference. Failure to meet the pledge will result in no rewards for the pool being earned by any owner or delegators. This will almost always result in a loss of delegation and, in the worst-case scenario, pool collapse.

Unlike delegation, the SPO is in charge of all pledge rewards distribution. This may be done in any way that is mutually agreed upon and is not governed by the blockchain.

Why do we need pledging?

Pledging on the Cardano blockchain is a technique for promoting a healthy economic environment. The pledge mechanism is also required to prevent Sybil attacks^[264] on the system. In such an attack, someone with very little personal stake establishes hundreds or thousands of pools with tiny margins and attempts to draw the bulk of stake to their pools. They can influence consensus and engage in double-spending^[265] attacks, create forks, censor blocks, and harm or even collapse the system if this succeeds. Such attacks are stopped by making pools with greater pledges more appealing, since an attacker must now divide their stake over many pools, making those pools less desirable and raising the inherent cost of executing a Sybil attack.

How to measure the impact of Pledging

Prior to the launch of Shelley on the Cardano mainnet, the parameter that affects pledging needed to be set. The parameter was created to be flexible and adaptable over time. The Shelley Haskell testnet^[266] was an excellent resource for fine-tuning this parameter and determining which values worked and which didn't. IOG also created a calculator^[267] to assist pool operators estimate

alternative pledge quantities and figure out how delegation could be affected.

Reasonable values are determined by a variety of variables, including: What percentage of a pool operator's interest does he or she own? How much does it cost to run a node? How many people want to run a staking pool? During the Incentivized Testnet, a lot of data was acquired.

IOG is committed to the scientific approach and that their architecture will result in a decentralized, stable, and secure blockchain— yet science and mathematics can only take you so far. Modeling assumptions must always be made, and no model will ever be as complex and colorful as what happens in practice.

On Reddit^[268] and on a ‘Cardano Effect’ episode, ^[269] there was insightful discussion on the matter. The Shelley Haskell testnets provided the ideal environment for continued debate. IOG evaluated, iterated and cooperated with stake pool managers to determine what is best for everyone. IOG enlisted the community’s support to put their findings into effect, much as they did with the Incentivized Testnet and Daedalus Flight^[270] user testing. ^[271]

Delegation

The practice of assigning individual stakeholders' ada to collective stake pools is known as stake delegation. Delegation is used in block production to guarantee that the block is created in accordance with the proof-of-stake consensus. Stakeholders do not transfer stake ownership, voting rights, or other rights when they delegate.

To maintain confidence in the blockchain, large SPOs will often own a considerable amount of third-party stake, making them accountable for:

- block production
- transaction processing

- Cardano network maintenance
- ensuring the owner makes a pledge
- pool security (protecting its private keys.etc)
- updating the community about anything related to the pool.

The blockchain handles the distribution of block production rewards to delegators, so large operators aren't concerned with it. SPOs are also not in charge of procuring delegated keys or acting on behalf of stakeholders in terms of delegation, voting, or other activities. Individual stakeholders must assume personal responsibility for their own security and make their own judgments on delegation, voting, and other matters.

Because Cardano is a proof-of-stake system, having ada gives you the right and duty to participate in the protocol and build blocks in addition to allowing you to purchase products and services.

Delegation of stake is a technique built into the Cardano proof-of-stake (PoS) protocol that enables it to grow even in the face of a widely dispersed group of stakeholders.

Anyone with ada may take part in the stake delegation process while keeping their spending power. Note that regardless of how you delegated your ada, you may spend it at any stage. In each epoch, the protocol allows stakeholders to engage in the slot leader election process.

Stake delegation creates 'stake pools,' which function similarly to the Bitcoin protocol's mining pools. When they are chosen as slot leaders, stake pool operators must be online in order to create blocks.

Stake delegation requirements

Delegating stake involves uploading of two certificates to the chain: a staking address registration and a delegation certificate. Because posting certificates necessitates funds, a user who is just getting started with their wallet needs a bootstrapping method. This

approach is based on the ability of base addresses using staking keys before publishing the key's registration certificate. The stake address can be based on a single key or a script like multi-sig.

Delegation Scheme

With the notion of delegation, any stakeholder may authorize a stake pool to create blocks for the Cardano network, and the protocol will subsequently distribute the rewards to all participants, including the stake pool operators' fees. A stakeholder is assigned to a specific pool ID, which is a hash of the operator's verification key.

The stakeholder may restrict the proxy signing key's^[272] valid message space to strings ending with a slot number in a certain range of values to limit the delegate's block generating capability to a specific range of epochs and slots. Due to the verifiability and abuse prevention qualities of proxy signature^[273] schemes, this basic scheme is reliable. This guarantees that every stakeholder can verify that a proxy signing key was granted to a particular delegate by that stakeholder and that the delegate may only use these keys to sign messages inside the key's valid message space.

A single transaction with a delegation certificate is required to post funds belonging to one staking key of a user's wallet. Only the standard transaction fees will apply. A stakeholder must pay a deposit to register a stake address, not for the stake delegation itself. After registering a stake address, the stakeholder will simply have to pay fees for their chosen delegation. During the rewards process, the stakeholders' stake will be considered part of the pool's stake.

Stake Delegation Example

Consider a user who is set to get their first ada, whether via redemption, an exchange transaction, or some other means. They'll generate a new wallet and an address for receiving the payments. This address will be a base address that will be used with a staking key created by the wallet but not yet registered on the Cardano blockchain.

The user may then engage in staking by posting a staking key registration certificate and a delegation certificate for their staking key. Newly created addresses may be pointer addresses to the staking key registration certificate after the key has been registered.

Pledging and rewards

Pledging is a critical method for fostering the development of a healthy ecosystem on the Cardano blockchain. You may pledge part or all of your ada to a stake pool when you register it to make it more appealing to others who wish to delegate. Although pledging is not mandatory when creating a stake pool, it may make it more desirable to delegators since the bigger the quantity of ada pledged, the higher the rewards given out. The $a0$ protocol parameter specifies how the pledge affects the pool reward. There is no optimal pledge amount, it depends on the pool and personal preference. The more you pledge the higher the rewards.

Rewards Distribution

Rewards are issued to all stakeholders who have delegated to a stake pool, either their own or another pool, at the end of each epoch. The protocol generates these rewards and does not rely on the stake pool operators to administer them. There are two types of rewards:

- All transaction fees: compiled from the collection of transactions contained in a block minted (generated) in that epoch
- Monetary expansion entails determining the difference between the total and maximal supply of ada. All ada now in circulation, as well as ada held in the treasury, make up the total supply. The maximal supply refers to the most ada that can ever exist (45 billion ada). The reserve is the difference between these two amounts. A predetermined (though parameterizable) proportion of the remaining reserve is withdrawn during each epoch and used for epoch rewards and treasury, with the amount

transferred to the treasury being a set percentage of the amount taken from the reserve.

IOG's chief scientist Professor Aggelos Kiayias discusses more in this *Rewards sharing and pledge on Cardano* video.[\[274\]](#)

Remember that the pledge is expressed (together with the cost and margin amounts) during pool registration and must be fulfilled by the pool owners who are delegating to the pool: Pool rewards for that epoch will be 0 if they collectively delegate less than the specified pledge. If the pool's operator margin is set to less than 100%, the pool will be public.

Pledging and Delegation Options

On the Cardano network, ada reflects a user's stake in the protocol, with the amount of the stake proportional to the number of ada possessed. Cardano users may receive passive rewards for verifying blocks if they have a stake in the cryptocurrency. The quantity of ada they pledge or delegate to a stake pool determines the amount of rewards they may receive.

Ada holders have 3 options when it comes to delegating their stake:

1. They are in charge of their own stake pool.
2. Rely on third party to manage a private stake pool on their behalf, such as Kraken,[\[275\]](#) one of the oldest Crypto exchanges.
3. Delegate to other stake pools

See the create transaction instructions[\[276\]](#) for advice on how to set up a stake pool, pledge, delegate and earn ada rewards.

Stake pools must maintain high availability, which means they must be accessible to verify and produce new blocks at all times. The quantity of ada committed or delegated, as well as the number of blocks a stake pool may build in a particular epoch, determine the rewards a stake pool can get. Based on the aforementioned criteria,

Ouroboros, the backbone of the Cardano protocol, elects the slot leader that grants permission to process transactions and mint new blocks.

Note: Before deploying to the mainnet, all stake pool functionality should be thoroughly tested on the testnet.

Pledging

When a stake pool is launched, the stake pool operator's pledge is the amount of ada that they 'delegate' to their own pool. The operator's commitment to maintain their pool and promote network activity can be seen in the pledge. It is not necessary to make a pledge, however it is suggested that you do so before starting the stake pool. The greater the pledge, the more rewards for the pool which is contingent on the pool's uptime and performance.

Delegation

Delegating to any stake pool accessible on the network might yield incentives for ada holders who do not have technical knowhow in operating a stake pool. The Daedalus wallet has a simple user interface that lets users start delegating to any registered stake pool straight away.

Note: holders of ada and SPOs (stake pool operators) who pledge or delegate will always have access to their ada. The rewards drop proportionately when the delegated ada is spent or withdrawn from the pool.

Rewards

For engaging in staking (either pledging or delegating), delegators earn rewards, which are immediately divided among the participants according to the rewards plan. Cardano's reward system is decentralized, meaning there is no one governing entity. Rewards are calculated by the Ouroboros protocol and generally are about 4-

6% assuming you have delegated to an unsaturated stake pool. If the amount of ada delegated to a given stake pool is over a set amount, the pool is deemed to be oversaturated. The delegating tab in Daedalus will display useful stats and details on each of the stake pool delegation candidates.

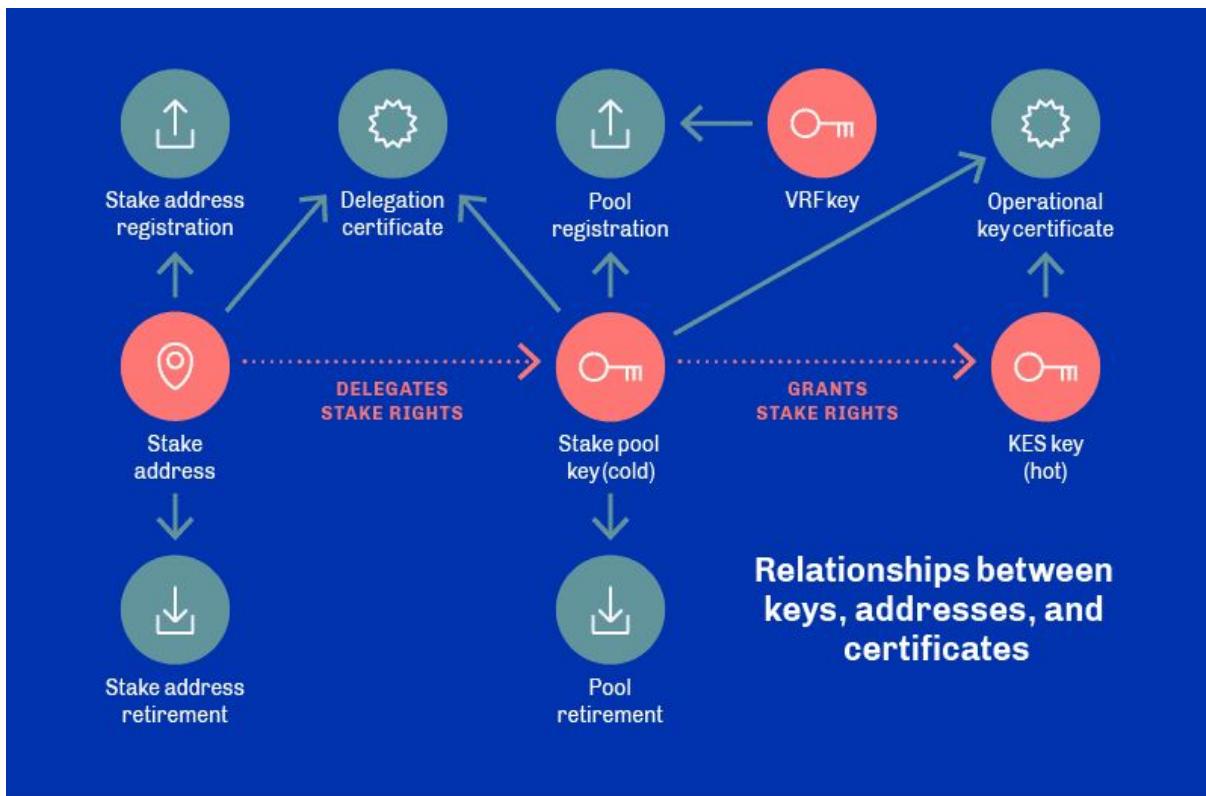
Rewards are distributed each epoch to stake pools for validating blocks. In 2022, about 4% of the amount staked is distributed. The staking and rewards should not be confused with *earning interest*. Interest is a fixed sum promised to a recipient, whereas there is a random element in distributing rewards, with the onus on the stakeholder to delegate to a pool that is not saturated, for example. Pooltool.io has a column ‘return on stake’; this varies between 0% and 18% for the 2,978 pools listed.

Types of Keys in Cardano

Asymmetric cryptography[\[277\]](#) key pairs known as keys are used for:

- Securing payments and staking certificates by signing and verifying them
- Identifying and defining addresses.

Figure 9. The link between keys, addresses, and certificates:



There are two main types of keys in Cardano:

- Node keys
- Address keys

Node Keys

The following keys make up the node keys, which constitute the blockchain's security.

- Operator/operational key
- KES key pair
- VRF keys

Operator/operational key

These are offline key pairs for operators that include a certificate counter for new certificates. The operator is responsible for managing both the hot (online) and cold (offline) keys for the pool.

Cold keys must be kept secure and should not be stored on a device that has internet access. Cold key backups should be kept in several locations.

KES key pair

A Key Evolving Signature^[278] (KES) key pair, which authenticates who you are, is required to establish an operational certificate for a block-producing node.

A KES key can only evolve for a set amount of time (a certain number of epochs) before becoming worthless. This is important because, even if an attacker compromises the key and has access to the signing key, he can only use it to sign blocks going forward, not blocks from previous epochs, preventing the attacker from rewriting history.

The node operator must produce a new KES key pair, issue a new operational node certificate with the new key pair, and restart the node with the new certificate when the specified number of epochs have elapsed.

VRF keys

Ouroboros Praos (Ouroboros versions are explained later, in Chapter 4) provided an additional degree of protection by using Verifiable Random Function (VRF) keys in block production. VRF makes the consensus protocol difficult to attack because it's impossible to predict the next producing nodes.

Because the slot leader schedule is known in other proof-of-stake blockchain protocols (such as Ouroboros Classic or BFT), it's known who has the authority to create the block in each slot. In this instance, you have to establish that you are who you claim you are, and anybody can verify this by looking at the public slot leader schedule. This process was subsequently improved in the Feb 2022 release, ^[279] with a new CLI tool for SPOs to check their own slot leadership schedule.

Ouroboros Praos' slot leader schedule, on the other hand, is kept private, which means that no one knows who will be the slot leader in advance, but once they are, they can verify to everyone else that they are using the VRF key.

The VRF key is a signature verification key that is recorded in the operating certificate. It establishes a node's permission to produce a block in a certain slot.

Address keys

The purposes of address keys are derived from the keys for identifying ada on the blockchain, which include the following keys:

- Payment key: a single address key pair that is often used to create UTXO addresses
- Staking key: a key pair consisting of a stake and a reward address that is typically used to generate account and reward addresses.

Signatures

If a cryptocurrency uses a single signature scheme, it must accept the risk that the scheme may be broken in the future, and that at least one entity will be unable to utilize the cryptocurrency owing to legal or industry constraints. However, a cryptocurrency cannot support all signature schemes since each client would have to comprehend and verify each scheme.

For Cardano, IOG chose to start with elliptic curve encryption, specifically the Ed25519 curve. [\[280\]](#)

Cardano will enable additional signature systems with the 'Vasil' hard fork. Quantum computer-resistant signatures will be included into the system. Cardano was built with specific features that enable a soft fork and the addition of new signature schemes. They will be

included when required and as part of the roadmap's major releases.

March 19, 2020, in response to the US Senate bill and prose to outlaw encryption. CH:[\[281\]](#)

I think that's equivalent to the ability to outlaw gravity or to change Pi to 3. I mean people can certainly say stuff and try to do things, but you cannot enforce something as crazy as outlawing encryption ...it's like how would the internet even work? SSL (secure sockets layer)[\[282\]](#) is now illegal? You have to have certificate authorities ...put a man-in-the-middle attack for every single website? Does the US government enforce that? It's old people who have no clue how the internet works, or technology works, playing and fiddling with things ...and they should be in diapers instead of voting.

Cardano RTView

RTView[\[283\]](#) is a real-time monitoring application that shows the status of Cardano nodes in real time. Even if the nodes are on separate computers, it offers multiple node monitoring.

Developers, testers, and end users with nodes connected to the actual cluster may use RTView to view what's going on and how the nodes are doing. It shows how much memory and CPU are being utilized, the status of the blockchain, how many blocks a specific node has forged, how many transactions have been handled, and so on.

It's a cross-platform program that works with Windows, Linux, and macOS, and it features a web-based user interface that lets you use any browser.

The key advantage of RTView is its ease of use. It's easy to set up; theoretically, there's no installation required; all you have to do is unpack the archive and run an executable. It's very straightforward

to set up since it has an interactive setup popup that tells the user which modifications to make in the node configuration files. It may also be used with any browser.

How to set up RTView

Follow the installation instructions to download, unpack, and launch RTView. RTView will be launched and ready to use after you've finished these steps.

Cardano tracking tools

Because Cardano is a public blockchain ledger, many tools may be used to conveniently follow all recent transactions, block information, and epoch data.

Exploring transactions and blocks

Cardano Explorer is a user-friendly application that pulls information from the main database and displays it in an easy-to-use online interface.

By selecting a single block, you may discover more about it, including its ID, size, epoch, and block data, as well as the number of transactions and confirmations contained. You may also use the search area to look for certain epochs, transactions, or blocks by pasting their IDs.

There's a whole gamut of tools and services listed under IOG's Essential Cardano, [\[284\]](#) the Cardano Developer Portal, [\[285\]](#) as well as third party sites like CardanoCube (cardanocube.io) and BuiltOnCardano (builtoncardano.com).

Exploring assets

Multi-asset generation and administration are supported by Cardano. You may use tools such as Cardano Assets (cardanoassets.com)

and Cardanoscan (cardanoscan.io/tokens) to view a list of assets and tokens:

Exploring stake pools

You can use these tools like Adapools (adapools.org) and Pool.pm (pool.pm/search) to get a list of all active stake pools, their tickers, pool names, and IDs. IOG has created a stake pool metadata aggregation server (SMASH) to give a list of validated stake pools with proper information to the community. Smash is connected with the Daedalus wallet, and under the delegation center page, users may view a list of eligible stake pools.

Chapter 4: Consensus (Shelley)

'If winter comes, can spring be far behind?'

Percy Bysshe Shelley

The Scalability Challenge

Distributed systems are made up of a group of computers (nodes) that have agreed to execute a protocol, or a collection of protocols, to achieve a shared purpose. This objective might be as simple as distributing a file using the BitTorrent protocol,[\[286\]](#) or decentralized storage.[\[287\]](#)

As more nodes join the network, the most efficient protocols acquire resources. If several peers are simultaneously downloading a movie file provided by BitTorrent, for example, it may be downloaded substantially quicker on average. Because peers both contribute and use up resources, the speed increases. When someone says a distributed system scales, they're usually referring to this feature.

The problem with most existing cryptocurrencies is that they were not built to be scalable in the first place. Blockchains, for example, are often a linked list of blocks that can only be added to. A blockchain protocol's security and availability are dependent on numerous nodes having a complete copy of the blockchain data. As a result, N nodes must copy a single bit of data. Additional nodes place a burden on resources required.

This is true for both transaction processing and gossip protocol[\[288\]](#) across the system. Increasing the number of nodes in the consensus system does not increase transaction processing power. It simply indicates that more resources are required to do the same task. More network relaying means that more nodes must send the same messages to keep the whole network in sync with the most recent block.

Cryptocurrencies cannot grow to a worldwide network, comparable to older financial systems, due to their structure. Legacy infrastructure, on the other hand, is scalable and can handle orders of magnitude greater processing and storage power. Bitcoin is a relatively tiny network in comparison to its payment counterparts

such as Visa, Mastercard, PayPal, etc and it is currently struggling to handle its present load.

The Ouroboros consensus protocol boosts scalability for Cardano. It allows for the decentralized election of a quorum of consensus nodes, which may then execute more conventional protocols to meet the demands of huge infrastructure providers like AWS, Google and Facebook.

For example, electing a quorum for an epoch implies there is a trustworthy group of nodes to keep the ledger up to date for a specified length of time. It is simple to elect many quorums at the same time and divide transactions among them.

What is a Consensus Protocol?

A consensus protocol is a collection of rules and parameters that regulate the behavior of distributed ledgers: a set of rules that each network member must follow. There is no one central authority in charge of public blockchains. Instead, a consensus mechanism is employed to enable dispersed network users to agree on the network's history as recorded on the blockchain - to achieve agreement on what has occurred and proceed from a single source of truth.

A single record is provided by that one source of truth. This is why blockchains are frequently referred to as 'trustless,' since trust is built into the protocol rather than needing users to trust one another. Unknown actors may communicate and trade with one another without requiring the mediation of a third party or the sharing of personal data.

Consensus is the method through which everyone participating in the blockchain's operation comes to an agreement. There must be unanimity on which blocks to generate, which chain to use, and how to establish the network's single state. Individual nodes examine the current state of the ledger system and form a consensus using the

consensus protocol ‘Ouroboros’. It has three key responsibilities: doing a leader check and deciding whether or not a block should be created, handling chain selection, and verifying blocks that have been produced.

Blockchains achieve consensus by enabling users to group transactions submitted to the system into blocks and add them to their own chain (sequence of blocks). The objective of the various consensus protocols is to determine who is permitted to generate a block when and what to do in the event of a disagreement. For example, what if two participants add different blocks at the same time? Ouroboros is a consensus mechanism based on proof of stake that has been shown to have the same level of security as proof of work.

Ouroboros

Ouroboros is a mythological creature represented as a snake, or dragon, devouring its own tail in a closed circle. The name ‘Ouroboros’ comes from Ancient Greek and literally means ‘tail eater’ or ‘tail devourer.’

Ouroboros is a symbol for infinity of time flowing back into itself in an endless circle, as if trapped in an unending loop. The first appearance of the Ouroboros was in Egypt in the 13th century BC. Alchemists later used Ouroboros in their mystical symbolism. Ouroboros has been understood and employed in a number of ways by many civilizations throughout history. One of the most prevalent interpretations of the symbol is that it signifies the Universe’s interconnection and infinity.

Charles Hoskinson named Cardano’s proof-of-stake consensus Ouroboros in 2017. In this sense, Ouroboros reflects the blockchain’s potential for endless growth and scalability. The core theme of Ouroboros is the provision of expanded possibilities for the planet, as well as its preservation through drastically decreased energy usage. [\[289\]](#)

Ouroboros was the first blockchain consensus system to be created via peer-reviewed research as a more energy efficient and sustainable alternative to proof of work, which is the foundation of previous cryptocurrencies such as Bitcoin and, more recently, Ethereum. Ouroboros and its various iterations give a new foundation for solving some of the world's toughest issues safely and at scale.

Ouroboros ensures and maintains the security and sustainability of any blockchain that uses it by combining unique technology and mathematically validated methods (including behavioral psychology and economic philosophy ideas). Ouroboros has demonstrated to be secure and capable of facilitating the spread of global, permissionless networks with little energy consumption. Cardano is the first network of its kind. Ouroboros enables users - in this example, stake pools^[290] - to establish new blocks based on the amount of stake they own in the network, and thus enable the creation of a distributed, permissionless network.

The different implementations of Ouroboros

Ouroboros Classic

Ouroboros Classic was the first implementation released in 2017. This original implementation established the protocol as an energy-efficient alternative to proof of work, provided a mathematical framework for analyzing proof of stake, and presented a unique incentive mechanism for proof-of-stake users.

What set Ouroboros apart from previous blockchains and, in particular, other proof-of-stake protocols was its capacity to provide unbiased randomness in the protocol's leader selection method, as well as the security guarantees that came with that. Randomness prevents patterns from forming and is an important aspect of the protocol's security. When a behavior can be expected, it may be manipulated — and although Ouroboros assures transparency, it

prevents coercion. Ouroboros is notable for being the first blockchain technology to undergo such thorough security testing.

The research paper on Ouroboros has in depth explanations of its functionality. The blockchain is divided into slots and epochs by Ouroboros. Each slot in Cardano lasts 20 seconds, and each epoch (which is a collection of slots) comprises around five days' worth of slots.

The awareness that attacks are unavoidable lies at the heart of Ouroboros' design. As a result, the protocol includes tolerance to prevent attackers from spreading other copies of the blockchain, and it assumes that an opponent may transmit arbitrary messages to any member at any moment. In reality, the protocol is guaranteed to be safe as long as honest players hold more than 51% of the stake.

Each slot has a slot leader who is in charge of adding blocks to the chain and passing them on to the next slot leader. To prevent hostile efforts to undermine the protocol, each new slot leader is obliged to treat the final few blocks of the incoming chain as transitory, with only the chain before the predetermined number of transient blocks being deemed resolved. This is also known as the settlement delay. This means, among other things, that a stakeholder may be offline and still be synchronized to the blockchain, as long as the latency isn't longer than the settlement delay.

Each network node in the Ouroboros protocol keeps a copy of both the transaction mempool, [\[291\]](#) where new transactions are inserted if they are consistent with current ones, and the blockchain. When a node becomes aware of a newer, more legitimate chain, the locally stored blockchain is replaced.

The disadvantages of Ouroboros Classic were that it was vulnerable to adaptive attackers — a real-world danger that was addressed in Ouroboros Praos – and that there was no safe means for a new member to bootstrap from the blockchain, which was addressed with Ouroboros Genesis.

Ouroboros BFT^[292]

Following ‘Classic’ was the Ouroboros BFT paper in 2018 (deployed in May 2020). Cardano employed the Ouroboros BFT (Byzantine Fault Tolerance) protocol during the Byron reboot, which was the transfer of the old Cardano codebase to the new. Ouroboros BFT aided in the preparation of Cardano’s release of Shelley and, with it, decentralization.

Rather than needing all nodes to be available at all times, Ouroboros BFT assumes a federated network of servers and synchronous communication between the servers, allowing for easier and more predictable ledger consensus.

Other advantages include immediate evidence of settlement, transaction settlement at network speed (i.e., the speed of your network connection to an OBFT node determines transaction settlement), and instant confirmation in a single round trip of communication. Each of these has a substantial impact on performance.

Ouroboros Praos^[293]

The Ouroboros Praos paper dropped in 2018 (deployed in August 2020) and is based on Ouroboros Classic, but with significant security and scalability enhancements. Ouroboros Praos, like Ouroboros Classic, divides transaction blocks into slots, which are then aggregated into epochs. Praos, on the other hand, is inspected in a semi-synchronous context and is safe against adaptive attackers, unlike Ouroboros Classic.

It presupposes two things: that adversaries may transmit arbitrary messages to any participant at any time, and those adversaries can delay honest participant communications for more than one slot. Praos assures that a powerful attacker cannot guess the next slot leader and conduct a targeted attack (like a DDoS attack) to pervert

the protocol by using private-leader selection and forward-secure, key-evolving signatures. Praos can also tolerate adversarial controlled message delivery delays and gradual corruption of individual participants in an evolving stakeholder population, which is critical for maintaining network security in a global setting, as long as an honest majority of stakeholder population is maintained.

Ouroboros Genesis[\[294\]](#) (paper 2018, due to deployed later in 2022)

Ouroboros Genesis was the fourth version of the protocol and built on Ouroboros Praos by including a unique chain selection mechanism that allows parties to bootstrap from a genesis block — without the requirement for trusted checkpoints or assumptions about prior availability. Genesis also proves the protocol's universal composability,[\[295\]](#) demonstrating that it may be used with other protocols in real world configurations without weakening its security posture. This boosts its security and long-term viability, as well as that of the networks that use it.

Ouroboros Hydra

Hydra is an off-chain scaling architecture that tackles three major scalability issues: large transaction output, low latency, and lightweight storage per node. The Hydra whitepaper proposes and details the inclusion of multi-party state channels,[\[296\]](#) which provide parallel transaction processing to greatly boost Cardano's transaction-per-second (TPS) output, as well as speedy confirmation of transactions. The paper refers to off-chain ledger siblings — state channels — as heads, reflecting the implementation's namesake. This makes the ledger multi-headed.

Instead of scaling vertically by adding more powerful hardware, Ouroboros Hydra allows Cardano to expand horizontally, enhancing performance by including extra nodes. Early testing indicates that each head is capable of 1,000 TPS. This might go as high as 1,000,000 TPS with 1,000 heads. Once in place, Ouroboros Hydra will enable Cardano to expand to unprecedented heights,

comparable to global payment systems. Hydra is being developed in collaboration with the Ouroboros protocol and the Cardano ledger, although it may be used with other systems as long as they have the same properties as Cardano. Hydra was later decoupled from Ouroboros and became an open-source project^[297] in its own right. More about Hydra later in Chapter 9.

The **Consensus Redux**^[298] paper was published August 2020. This paper discusses the concept of a self-healing ledger. How does the ledger recover when it's been attacked? How does a network recover when it's been attacked? The paper outlines solutions in both categories.

Ouroboros Crypsinous^[299]

The Crypsinous paper was published in 2019 but has yet to be implemented. Crypsinous is the first privacy-preserving proof-of-stake protocol. It boasts increased security features to protect against adaptive attacks including a coin evolution technique based on SNARKS^[300] and key-private forward-secure encryption.

Ouroboros Chronos^[301] (Paper 2021, not deployed at time of press)

Chronos delivered greater security and network resilience to communication delays by providing more accurate global timekeeping. To maintain the robustness of any dispersed network, global time synchronization is required. Time synchronization is critical in smart contract implementation, from guaranteeing up-to-date information amongst all participants to maintaining correct transaction processing and block construction.

IOG discovered a means to synchronize clocks across a blockchain in conjunction with experts from the Universities of Edinburgh, Purdue, and Connecticut to create a more secure and tamper-proof global time source. This includes time synchronization from internet of things (IoT)^[302] devices, such as supply chain monitoring tools, and general distributed systems, especially if a central clock failure poses

a security issue. The research is implemented as Ouroboros Chronos (Greek for ‘Time’).

Read more about Ouroboros’s design in Prof Aggelos Kiayias blog ‘The Ouroboros path to decentralization’

September 22, 2020, re: Chronos. CH:[\[303\]](#)

Ouroboros Chronos was a special paper. Leslie Lamport^[304] was one of the first guys to do major work in distributed systems and he wrote this beautiful paper on clocks and time in the distributed system from the 1960s or 1970s. It’s one of the most cited papers of all time in the systems world... ‘Time, clocks, and the ordering of events in a distributed system’^[305] and Chronos was like unfinished business in that respect. It’s fun to write papers like that and it has real use. You can completely decouple a dependency on NTP^[306] and these types of things, there’s a lot of theory there.

Timing is everything

Within computer systems and applications, the idea of time is critical. You wouldn’t be able to access any transport layer security (TLS)-based websites, exchange data, or use other cryptographic techniques without this notion.

Time tracking, on the other hand, is a challenging issue to tackle. Accurate time synchronization requires data transfer throughout the whole internet, which costs time as well. It’s also difficult to forecast how long a particular data transfer will take since the network status is continually changing and is influenced by variables like congestion and data size, among others. As a result, discrepancies are common, and it’s critical to supply the tools and solutions necessary for accurate timekeeping.

It’s easy to take timekeeping for granted with basic PCs. Behind the scenes, however, there is a strict protocol to follow. The Network

Time Protocol^[307] (NTP), for example, uses a worldwide hierarchy of servers to solve the timekeeping problem. This comprises up to 15 Strata, each with its own routing route designed to synchronize in the most efficient way possible. The development of a Bellman-Ford shortest-path spanning tree,^[308] which reduces latency and transmission time inconsistencies, also helps.

Time synching on the Blockchain

For distributed ledger technology, the idea of timekeeping is different. The network cannot verify that a transaction being processed is genuine, and does not reverse the prior one, without a correct timestamp. Different timestamping algorithms are employed across a variety of blockchain ledgers; however they aren't always reliable. Bitcoin, for example, employs timestamps for consensus security but not for timekeeping; while in Ethereum, on-chain timestamps are established by miners but are not technically blocked or verified for authenticity by the consensus.

Timekeeping is also necessary for smart contract execution. Decentralized finance (DeFi) smart contract attacks are vulnerable to inaccuracy. Vulnerabilities in smart contracts aren't necessarily caused by bad code; time discrepancies should be fixed to prevent any potential attacks on the ledger. Some blockchains, such as Solana, have experienced critical 'clock drift' issues.^[309]

Ouroboros Chronos Design

Ouroboros Chronos allows blockchain technology to securely synchronize clocks. Chronos is a cryptographically secure blockchain protocol that also offers an accurate source of time thanks to an innovative time synchronization technique that avoids the flaws of externally maintained clocks. This also enables blockchain to precisely time-stamp transactions, making the ledger more resistant to time-based attacks.

By syncing local time to a uniform network clock with no single point of failure, the new protocol may greatly improve the resilience of essential telecoms, transportation, trade systems, and infrastructures. This scientific accomplishment also represents a huge step toward building completely auditable and fraud-proof financial systems by providing exact time and hence full traceability of all transactions.

December 12, 2020. Is Chronos implemented? CH:[\[310\]](#)

We'd like to be reliant on nothing and no one and as decentralized as possible. So we were the first to address this in the very first paper of its kind, with something called Ouroboros Chronos, but it would be an unnecessary diversion to just go and chase 3 months of implementation to pull Chronos in, when we don't need it as a system right now. [...]

The other thing is that Chronos should be implemented with Consensus Redux, should be implemented with Genesis, and should be implemented with fast finality and high throughput enhancements to the system so Ouroboros 2 (subsequently named Ouroboros Omega)... a rollup of all the research that we've done which will make it considerably better than anything in market. So the name of deployment execution is saying 'what is a problem today? What's a theoretical but unlikely issue? Versus what is a practical and certainly problematic issue to resolve?' ...and understand how to balance things and create a roadmap accordingly.

Ouroboros Leios

The Leios paper is not published yet, but is previewed in this video[\[311\]](#) by Professor Aggelos Kiayias. The focus of Leios is Input Endorsers which leverage the aforementioned foundational Ouroboros functionality as well as Mithril (See Chapter 9). As input endorsers are quite technical and based on concepts not discussed yet, they are covered in the last section of Chapter 9, Basho (Scalability).

Ouroboros Omega^[312] will be the capstone of all the proof-of-stake research IOG have accomplished since 2016. There should be a paper soon on the ‘convergence of all the ideas.’

May 25, 2020. re: Ouroboros. CH:^[313]

The first thing we started with when we started the Cardano project is we actually didn't know if proof of stake would work or not. We didn't know if proof of work was the end-all be-all, and you could never synthetically create proof of work. So the first thing that happened was we wrote a model called GKL (The Bitcoin Backbone Protocol) where we rigorously defined what is a blockchain? What makes it secure? ...and then what are all the security properties you get for proof of work? So then you have a target and then the question is can proof of stake ever emulate that or not?

This is a very controversial thing, if you talk to people from Blockstream or the Bitcoin side of the world. The maximalists^[314] say that proof of work is holy, and nothing can compete with it, and we have all these strong arguments like ‘nothing at stake’ and long-range attacks and grinding attacks and so forth. So then the next part of the Ouroboros agenda, once we had a foundation, was to say could we synthesize consensus that proof of work does in unrealistic assumptions, meaning like everything works perfectly and everybody is reasonable. Can we even achieve the same things? That was the first version for Ouroboros.

The Ouroboros Classic paper, so it's synchronous, you had public stake pools and all this stuff, but it was not optimal, but because it worked, then we had a foundation we could build on and keep adding new security features and eventually bring it into line so we could replicate all the security and usability properties that proof of work has. So for example, partial synchrony... not everybody's going to show up on time because

it's a distributed system, so some nodes will be delayed and so forth ...so we did that.

Adaptive security... So we needed things because you don't know who won ahead of time. You only know after the fact and you can prove that, so people can't sell their votes or DDoS attack^[315] the next delegate, or something like that. You need to do a bootstrap from Genesis, so that's a property where when you join a proof-of-work system, you can know nothing, what you do is you just get history, and you weigh it. You look at the algorithmic weight in each chain, you say, 'well this one's the heaviest so that's the longest chain, I'm going to go with that' ...So you never need a checkpoint. You can just bootstrap from the very beginning the system and verify that. So we do that with Ouroboros Genesis, we achieve that property. So we've been systematically working our way through every security property they have.

We created a whole family of papers, there's more on the way, and that's what makes Ouroboros special was that we started with 'first principles'... what is a blockchain? We worked our way through and said what properties at the time do we really like? We'd like to replicate them in terms of how it operates, but then at the same time, we'd like all the benefits of proof-of-stake. Things like very fast finality, low energy consumption... You can run the whole system on 10 kilowatts of power. The fact you have endogenous security needs within the system. It's not exogenous, where security is outside of the system. That puts you in a good position to optimize around the stake pool model.

So you can use them for Layer 2 embedding, add lightning channels or Hydra channels or oracle solutions, etc. you can use them to accelerate the network stack and there's all these things you gain with the proof-of-stake side of the world in general. The delegation model is cool because it's a virtual resource, so if China was to ban mining tomorrow, it would be super difficult for the people running mining pools there to get

their miners out of China, into Mongolia or some other place, whereas with the virtual resource, you just click a button. You can rehost servers from China, Switzerland, Liechtenstein... New Zealand...anywhere with the click of a button. So you have a much more resilient system in that respect.

So there's a huge amount of benefits that proof of stake has from environmental sustainability, to performance, to the ability to layer additional services on that you get for free when you're in that model. Then there's this huge security menu you have to kind of worry about. We took years to work our way through to a point where we got confident enough, we had all those models.

Finally, this is a business, when you're running consensus. This is a business and Satoshi got it right. That's why we have giant mining warehouses in Georgia and Norway and these other places, so similarly if you build a business correctly, stake pools should be able to operate every day and make a profit and still sustain the network without being super expensive and requiring us to print billions of dollars of value every year long-term. So we had to figure out the business side of that as well.

That's what we did with the pioneers, it's what we did with the incentivized testnet, it's what we've been doing with Oxford University and the papers we published. We're trying to get the game theory^[316] right. That's been the single hardest thing for Ethereum 2. They've been working on that for years as well, and it's not trivial by any sense of the word.

So if I had to succinctly say .. 'well what is Ouroboros?'... I'd say it's a first principles-based, new way of doing consensus that keeps the stuff we've come to know and love from Bitcoin, that's very useful and great, but then does it in a much more sustainable energy-friendly way, that also allows you to layer on many more utilities than just mining to the system. It does so in a way that attracts lots of competition, lots of decentralization

and lots of businesses. Mining tends to centralize to a small group of actors because of economy of scale.

February 9, 2021. Can you talk about Ouroboros Omega? CH:^[317]

Omega is the culmination of all of our research of the last 6 years for Ouroboros: no reliance on external clock, self-healing so it can gradually recover 51% attacks, the ability to bootstrap from Genesis, semi-synchrony, adaptive security, instant finality... all kinds of stuff...multi-validation per block... there's so much stuff Things like the consensus Redux paper, the Ledger Combiners paper^[318] ... the Chronos paper, the Genesis paper, the Praos paper and then all the theory and then some of the engineering acumen, including an improvement to about a thousand TPS (transactions per second).

How the Consensus Layer Works

Abstraction^[319] is a key feature of the consensus layer.

The Cardano consensus layer is responsible for two major duties:

1. It uses the blockchain consensus mechanism to keep track of transactions. Consensus, or ‘majority of opinion,’ in the context of a blockchain, implies that everyone participating in its operation agrees on the one true chain. This means that the consensus layer is responsible for accepting blocks, selecting between rival chains if any exist, and determining when to create its own blocks.
2. It is in charge of preserving all of the information needed to make these judgments. The protocol must verify a block in relation to the state of the ledger before deciding whether or not to accept it. It must preserve enough history to be able to rebuild the ledger state on a different chain (a different point of a fork in the chain) if it chooses to move to a different chain. It must maintain a mempool^[320] of transactions to be placed into those blocks in order to be able to create blocks.

The consensus layer sits between the network layer below it, which deals with communication protocols and peer selection, and the ledger layer above it, which defines how the ledger should be updated with each new block and how it should be updated. The ledger layer is completely stateless^[321] and only contains pure functions. As a result, the consensus layer isn't necessary to understand the precise nature of the ledger state, or even the contents of the blocks (apart from some header fields required to run the consensus protocol).

The consensus layer makes extensive use of abstraction. This is significant for many reasons:

- When performing tests, it enables programmers to **simulate failures**. IOG may, for example, abstract the underlying file system and use it to stress-test the storage layer while simulating various disk errors. Similarly, they abstract across time and use this to see what happens to a node as the user's system clock advances or recedes.
- It enables IOG to **use a variety of ledgers** to create the consensus layer. They used it to run the consensus layer with the Byron ledger and the Shelley ledger for the Shelley Haskell testnet. They also utilized it to test the consensus layer using different types of ledgers developed expressly for testing, which are often simpler than 'real' ledgers, allowing IOG to concentrate their tests on the consensus layer itself.
- It **enhances compositionality**^[322] by enabling IOG to construct bigger components from smaller ones. For example, the Shelley testnet ledger only includes the Shelley ledger; but, after Shelley was launched, the actual chain had both the Byron and Shelley ledgers up to the hard fork point. This necessitated the creation of a ledger layer that switched between two ledgers at a predetermined moment. Rather than creating a new ledger, IOG created a hard fork combinator that solely implements these

features. This enhanced code reusability (no need to reimplement hard fork functionality for future hard forks), as well as separation of responsibilities (the hard fork combinator's development and testing aren't dependent on the details of the ledgers it flips between).

- The usage of abstraction **increases testability**. Combinators are variants of consensus methods that enable IOG to concentrate on certain areas. For example, IOG has a combinator that accepts an existing consensus protocol and merely alters the check to see whether a block should be produced. The consensus layer may then be used to establish testing scenarios in which many nodes produce a block in a particular slot or, conversely, no nodes at all, and verify that it performs properly.

Without a combinator to override this part of the consensus layer, such circumstances would be left to chance. Although 'chance' can be managed, it is hard to build up specific scenarios or to automatically decrease failed test cases to a minimum test case. The test may actually employ a schedule describing which nodes should create blocks in which slots using these testing consensus combinators. IOG can then construct such schedules at random, execute them, and if a flaw is found, reduce them to a single test case that still triggers the issue. A broken schedule with such a small number of steps is far simpler to diagnose, understand, and deal with than one with a random seed that causes 'anything' to happen at 'some' time.

Consensus Roles

The consensus protocol has three major roles:

1. Leader check (who should produce a block?)
2. Chain selection
3. Block verification

The protocol is designed to be independent of a specific block or ledger, allowing a single protocol to be used with a variety of blocks and/or ledgers. As a result, each of these three roles establishes its own ‘picture’ of the data.

Every slot has a **leader check** that determines whether or not the node should create a block. In practice, the leader check may need the extraction of certain information from the ledger state. The chance of a node being elected as leader (authorized to generate a block) in the Ouroboros Praos consensus protocol, for example, is dependent on its stake, the node’s stake.

The process of selecting between two competing chains is known as **chain selection**. The chain length^[323] is the most important selection criteria here, however other protocols may have extra requirements.

Blocks, for example, are usually signed using a ‘hot’ key that lives on the server and created by a ‘cold’ key that never appears on any networked device. If the hot key is compromised, the node operator may create a new one using the cold key and ‘delegate’ to it.

A consensus protocol will favor the newer hot key over two chains of similar length, ie. Each chain includes a tip^[324] signed by the same cold key but a different hot key.

Block validation is primarily a ledger problem; checks such as ensuring all transaction inputs are accessible to prevent double-spending are specified in the ledger layer. What’s within the blocks is mainly unknown to the consensus layer; in fact, it may not even be a cryptocurrency, but a distinct use of blockchain technology. IOG used the example of a Pokémon ledger^[325] on Ouroboros previously. However, block headers include a few items that are expressly designed to aid the consensus layer.

Node configuration

To execute, each protocol may need certain static data, such as keys

to sign blocks, a unique id for the leader check, and so on. This is referred to as the ‘node configuration.’

The ledger state

The consensus layer not only handles the ledger state but also operates the consensus protocol. It is unconcerned with the look of the ledger state; instead, it assumes that some form of ledger state is connected with a block type.

If a block is invalid, you may get an error while applying it to the ledger state. The ledger layer defines the precise kind of ledger errors, which are ledger specific. The Shelley ledger, for example, will have staking errors, but the Byron ledger would not since it does not enable staking; and ledgers that aren’t crypto ledgers will have quite different errors.

The Cardano consensus layer was created with the Cardano blockchain in mind, which initially ran Byron and was updated to run Shelley. It’s fair to ask why didn’t IOG developers create for that particular blockchain first? Then generalize when utilizing the consensus layer for other blockchains? However, there would have been significant drawbacks in doing so:

- It would obstruct IOG’s capacity to conduct tests. They wouldn’t be able to choose which nodes create blocks when, they wouldn’t be able to use a dual ledger, and so on
- It would entangle things that should be logically separate. The Shelley ledger, in the abstract method, is made up of three parts: a Byron chain, a Shelley chain, and a hard fork combinator that connects the two. Without abstractions, such separation of concerns would be more difficult to establish, resulting in code that was more complex to comprehend and maintain
- Abstract code is less likely to include flaws. For example, since the dual ledger combinator is polymorphic in the two ledgers it

combines, and they are of different types, IOG couldn't construct type correct code that attempts to apply the main block to the auxiliary ledger

- When the time inevitably comes to instantiate the consensus layer for a new blockchain, writing it in an abstract manner from the start forces IOG to think carefully about the design and avoid coupling things that shouldn't be coupled, or making assumptions that may or may not be true in general. It might be difficult to fix such issues once the design has been implemented.

To achieve all of this, a programming language with exceptional abstraction capabilities is required, and Haskell is well equipped in this regard.

January 10, 2021. Please explain Cardano being 100x more decentralized than BTC or others, how is this calculated? CH:[\[326\]](#)

It's calculated by those who produce blocks, so if you have a hundred times the unique entities producing blocks, then we say it's a hundred times more decentralized, but there are many measurements of decentralization. You can look at network propagation, so how many full nodes you have. You can look at unique development entities responsible for it ...you can look at the funding sources and see how many unique funding sources are there. You can see the totality of the user count....

You can see it by the total applications on the system but usually when we say decentralization, we strictly mean the amount of nodes participating in the consensus process and how many unique people are making blocks. In the case of bitcoin, 3 to 5 usually make the same blocks again and again... and we consistently have 300 to 500 stake pools consistently making blocks that are unique. There's over 1200 registered (currently over 3,000), so I feel very comfortable in the 100x statement, but reasonable people can have different definitions, there's no consensus in the industry of what decentralization is.

Hard Forking Business

In the context of the blockchain, a ‘hard fork’ refers to a significant change in the chain, such as switching from one protocol to another. A hard fork in most blockchains denotes block modifications or a change in their interpretation. Typically, when a hard fork is performed, the existing protocol is turned off, new rules and modifications are introduced, and the chain is restarted. A hard-forked chain will be distinct from the prior version, and that the pre-forked blockchain’s history will no longer be accessible.

The Cardano blockchain has hard forked from a federated Byron model to a decentralized Shelley model. This hard fork, on the other hand, was one-of-a-kind. IOG guaranteed a seamless transition to a new protocol while maintaining the history of earlier blocks, rather than making major modifications, the chain did not alter drastically. Instead, it included Byron blocks before adding Shelley blocks after a transition time. There was no ‘turning it on and off again’. The entire history was retained. There has been no downtime or restarts with Cardano, which is not always the case with other chains. [\[327\]](#)

Hard Fork Combinator

In Cardano docs and blogs, you may have seen a hard fork referred to as an ‘HFC’ or a ‘HFC event’. A combinator is a technical term that refers to the joining of two or more processes. In the context of Cardano, a hard fork combinator combines protocols, allowing the Byron-to-Shelley transition to be completed without the need for a system restart. It guaranteed that the ledgers of Byron and Shelley display as a single ledger. It was not necessary for all nodes to update at the same time when switching from Ouroboros BFT to Ouroboros Praos. Instead, nodes updated in stages; some running Byron blocks, others running Shelley blocks.

The hard fork combinator is intended to allow the integration of many protocols without requiring major changes. Byron and Shelley blocks are now combined in the Cardano chain. For future ‘hard fork

events', Basho and Voltaire blocks will be combined as well - all as a single property. By simplifying the prior Byron-to-Shelley evolution, this (HFC) hard fork combinator also made the transfer from Shelley to Goguen seamless with gradual, iterative upgrades rolled out as the *Allegra*, *Mary* and *Alonzo* updates.

HFC history to date

The Cardano platform entered a rapid development phase with the introduction of the Incentivized Testnet in 2019, which marked the beginning of the Shelley era. The Ouroboros Classic consensus system previously supported Byron and ada, and subsequently migrated to Ouroboros Praos. As Cardano decentralized, this was the version of proof-of-stake (PoS) protocol that first powered Shelley. It incorporated monetary rewards for ada holders and stake pool owners into the staking procedure.

In February 2020, IOG upgraded Cardano with a hard fork that moved the mainnet from Ouroboros Classic to Ouroboros BFT, an enhanced version of the original consensus mechanism. This BFT hard fork kicked off a transition phase under Ouroboros BFT, a pared-down version of the protocol aimed to ease the transfer to Praos while still avoiding malicious behavior. Users were unlikely to have noticed. It meant a routine software update for Daedalus wallet users. Exchanges were required to update manually, but they had many weeks to do it and IOG were available to assist.

The 'Byron reboot'^[328] followed that in March 2020. Many Cardano components received completely new code, including a new node to handle delegation and decentralization, as well as future Shelley features. The new code base was redesigned to be modular, which meant that many components could be updated without impacting the others.

In turn, the BFT served as a springboard for the Shelley hard fork, which happened after the Haskell testnet was complete. For exchanges, ada holders, and wallet users, this second hard fork was

similar to the first, a non-event in terms of user disruption. However, although everything seems to be in order on the surface, there was a lot of activity going on behind the scenes. IOG's developers were hard at work making it a seamless, benign experience for the end user. IOG chief architect Duncan Coutts^[329] explained at the time:

IOG's blockchain engineers believe in smooth code updates. Instead of trying to do the jump from Ouroboros Classic to Praos in a single update – which would be an incredibly complex task – it's been a two-stage approach using Ouroboros BFT as an intermediary. The BFT code is compatible with both the Byron-era federated nodes and the Shelley-style nodes released in the Byron reboot. It's like a relay race: one runner (in our case, running one protocol) enters the handover box where the other runner is waiting; they synchronize their speeds (so they're perfectly compatible with each other) and then hand over the baton (operating the mainnet), and then the new runner with the baton continues from the handover box for the next lap.

IOG were able to swiftly design and test a new wallet using Daedalus Flight, and once everyone was using it on the mainnet, and IOG finished changing over the core nodes, the old code was obsolete.

August 25, 2020. Re: Daedalus Flight. CH:^[330]

Well we have Daedalus flight and Daedalus mainnet. Both these wallets work on mainnet Cardano, just like Yoroi and Daedalus both work on mainnet Cardano but they're two separate wallets. The primary difference between Flight and mainnet is that Flight is for 'bleeding edge' experimental features that haven't been completely tested yet.... Hardware wallet center, voting center multisig, multi-asset... all of these things will come to Daedalus and we will release them first on Flight and the people who use Flight accept that, while they get features faster than everybody else, those features have not been as tested as the features that are deployed on Daedalus mainnet.

If you go to any Linux distribution, you'll see distributions that are considered to be older and more stable, or frankly any open-source software project, you tend to have the official release and then you tend to have a bleeding edge release that follows the software that gets features first. We're no different in that respect.

We will always release Flight first, that's our go-to for a release, especially if it's a big release and there's a lot of stuff to do we tend to beta test it with the Flight users before we release it on mainnet, because that's much more stable. That's much more tested and vetted software but if you're using mainnet, that means you don't get features first. You have to wait, in some cases weeks, to get those features. That's the difference between the two. [...] Flight is like our version of Chrome Canary.

In summary, the only real hard fork for Cardano was the switch from Ouroboros Classic to BFT (February 2020). The Byron mainnet was relaunched to run the BFT protocol, allowing for a smoother transition to Ouroboros Praos with fewer chain disruptions. The BFT protocol was meticulously built to preserve blockchain history and make the blockchain look as a single entity.

As IOG chief executive Charles Hoskinson discussed in his whiteboard video about the hard fork,^[331] the goal was to have a ‘graceful entry into Shelley.’ The hard fork combinator was crucial in accomplishing this transition.

Shelley Era Updates

Allegra (Token Locking)

Token locking was a feature introduced to the Shelley protocol to allow a variety of smart contract use cases, such as generating and transacting with multi-asset tokens and adding support for the Voltaire voting mechanism. Token locking is the act of reserving a

certain number of assets and agreeing not to sell them for a given length of time. This functionality was enabled in the *Allegra*^[332] upgrade in December 2020. *Allegra* was named after Allegra Byron, Lord Byron's daughter and sister to Ada Lovelace.

Token locking allowed for more complicated deal settlement and fund accounting. It's used in the following scenarios:

- **Contractual agreement** - when someone engages into a contractual agreement, such as to sell an asset like a painting, it is essential to guarantee that the painting will not be sold to anyone else save the person who pays the money. The token may represent both the painting and the 'promise', the actual token locking in this example. The contract becomes invalid if the painting is sold to a different third party
- **Vote registry** - Token locking will allow users to lock a set quantity of their tokens to reflect their voting rights inside the Voltaire voting system. Holders of ada tokens who participate in the voting process must 'lock' their tokens. This will reflect their voting rights in proportion to their investment and will prevent the hazards of double-counting votes, awarding more votes than is feasible, contradicting votes, or vote duplication
- **Multi-asset tokens** - In addition to ada, Cardano allows for multi-asset tokens, with the ledger supporting the creation and usage of several bespoke token types. Token locking enables ada tokens to be 'locked' to create a bespoke asset of equal value.

Mary (multi-asset support)

This then paved the way for the *Mary* (multi-asset support) upgrade in March 2021. It was named after Mary Shelley (the author and wife of Shelley). MAS (multi-asset support) means you can record that a particular token is being used for a specified purpose. The token may represent any object that is recorded on (native to) the

blockchain ledger, such as ada, and other custom tokens.

Mary enables users to generate (custom) tokens with unique characteristics and conduct transactions with them directly on the blockchain.

The ledger's accounting architecture now handles not just ada transactions, but also transactions that hold several asset types at the same time. Developers benefit from native support since they don't have to write smart contracts to handle bespoke token minting or transactions. Instead, the accounting ledger keeps track of asset ownership and transfers, minimizing unnecessary complexity and the risk of human error while also ensuring considerable cost savings.

To fulfill commercial or business goals, developers, enterprises, and apps can build general purpose (fungible) or specialized (non-fungible) tokens. Custom payment tokens or rewards for decentralized apps, stablecoins pegged to other currencies, and unique assets that represent intellectual property are just a few examples. All of these assets may then be traded, swapped, or used to purchase goods and services.

Alonzo (smart contracts)

Still part of the Goguen era, *Alonzo* was the next protocol update in Sept 2021. To enable functional smart contracts, *Alonzo* built on top of transaction metadata, token locking, and native asset functionality. By allowing the development of smart contracts and decentralized apps (DApps) for DeFi (decentralized finance), this update created a diverse platform that opened up options for enterprises and developers.

This functionality is available and enabled by the tools and infrastructure that make up the Plutus Platform.

Alonzo enhanced Shelley's basic multi-signature (multisig) scripting language with a rigorous methodology based on formal methods and verification. For more sophisticated and secure scripting capabilities,

Multisig was updated into the Plutus Core^[333] language. *Alonzo* enables this through extended unspent transaction output (EUTXO) accounting. More on this later.

Alonzo was named after Alonzo Church (1903-95). Church was a logician and mathematician who worked on logic and the foundations of theoretical computer science in the US. He is also recognized for establishing lambda calculus,^[334] a formal system that may be used to argue that the Entscheidungsproblem^[335] is unsolvable. Later, when working with Alan Turing, they realized that the lambda calculus and the Turing machine^[336] had equivalent capabilities, displaying numerous mechanical computing processes. Plutus Core (Cardano's smart contract language) is a variant of lambda calculus, which is one of the reasons for naming the smart contract upgrade after Church.

June 5, 2020. What is the best code in Cardano? CH:^[337]

The hard fork combinator code is the second most elegant code we have; the most elegant code belongs to the network code. We have lots of crazy stuff there, very elegant, very academic scary code ...but beautiful.

Path to Full Decentralization

Setting stable parameter settings, while being flexible for the future, is critical to Cardano's continued development and decentralization. IOG consulted with the community before setting initial values. Around 20 parameters regulate Shelley's behavior, and settings had to be specified for all of them before the mainnet could be launched. The majority of these parameters are technical in nature, so although they must be set appropriately to ensure system safety and improve performance, their specific values have little impact on user experience.

However, certain parameters are different. They determine the Cardano ecosystem's decentralization and long-term viability. They

also influence the cost of delegating and running a stake pool. IOG had to carefully balance a variety of essential issues, including security, performance, stability, sustainability, decentralization, justice, and economic viability, while selecting suitable values for these.

There are three primary points to keep in mind with all parameters on the Cardano blockchain:

- The protocol has to be truly decentralized, so that no single party can jeopardize the chain's integrity
- The protocol needs stake pool operators to be incentivized to keep supporting the chain; and
- It's not viable for incentives to change dramatically at any point in time, as this could jeopardize the operators' income stability.

Cardano aims to provide everyone who wishes to join in and manage a stake pool an equal chance. Parameter settings that seem fair and acceptable for smaller pools, on the other hand, might become difficult for bigger pools and vice versa. Large pools may find it easier to make a larger pledge than small pools. Small pools, on the other hand, may be able to run for a fraction of the expense of bigger pools.

Changing settings too often is risky, since it may jeopardize the operators' revenue stability and predictability. Democracy is a byproduct of decentralization. The Cardano community needs a voice in how the chain is run. As a result, these figures were just a starting point and IOG released a Cardano improvement proposal (CIP) in which the community can vote on the best chain settings. Finally, Cardano's governance will be in the hands of the Cardano community, who IOG believe are best placed to advise them.

K = number of stake pools

A crucial element is the desired number of stake pools, or the k

parameter. Cardano incentives have been intended to foster an equilibrium with k completely saturated pools, which means that when all stake is delegated equally to the k most appealing pools, rewards will be optimum for everyone.

The greater the value of k , the more decentralized the system. More k , on the other hand, results in a less efficient system (higher expenses, greater energy consumption) and fewer returns for both delegators and stake pool owners. IOG knew that the community would be motivated to build up pools based on what IOG learnt from both the Incentivized Testnet (ITN) and the Haskell Shelley testnet.

Decentralization occurred fast but decentralization alone is insufficient. Cardano requires long-term commitment from its operators, and operators must be appropriately rewarded for continuing to sustain the system. The initial proposal was $k=150$, to be progressively raised to create a balance between decentralization and rewards for stake pool managers. This guaranteed that the system was stable and efficient at first, and could progressively evolve over time to become more decentralized, and secure, in the future:

Cardano is an order of magnitude more decentralized than any other blockchain due to k stake pools of roughly similar size. And this was only the start. As of June 2022, there's 3,000+ stake pools running.

Monetary Policy

Transaction fees and monetary expansion are used to fund staking rewards for both delegators and stake pool operators. Every epoch, all transaction fees from all transactions from all blocks created during that epoch are collected and placed in a virtual ‘pot.’ A predetermined proportion of the leftover ada reserves, ρ , is also contributed to the pot. Then a portion of the pot, τ , is paid to the Treasury, and the remainder is used as epoch rewards.

This approach guarantees that the share of rewards taken from the reserves is large in the beginning, when the number of transactions is still relatively modest since users are only starting to create their businesses on Cardano. Early adopters will be enticed to act swiftly to reap the benefits of the high initial payouts. The higher costs compensate for declining reserves over time as transaction volume grows.

This technique also guarantees that the rewards provided are predictable and evolve over time. There will be no ‘jumps’ like the bitcoin halving occurrences that occur every four years. Instead, a steady exponential fall is guaranteed by a predetermined proportion deducted from residual reserves every epoch.

So, what kind of worth should ρ take? What percentage of the budget should go to the Treasury? This is also another trade-off: larger values of ρ indicate bigger rewards for everyone at first, as well as a faster-filling treasury. However, greater levels of ρ imply a quicker depletion of reserves. Paying big incentives and incentivizing early adopters is crucial, however, it is equally critical to present all stakeholders with a long-term view.

Cardano will never run out of reserves; instead, it will be an exponential decay. Calculate the ‘reserve half life,’ or the time it takes for half of the reserve to be used up, to obtain a sense of the effect of a certain value of ρ .

After careful consideration, 0.22% was the proposal for ρ . When the numbers are crunched, the ‘reserve half life’ comes out to be roughly 4 to 5 years. In other words, half of the remaining reserve will be consumed every four to five years. Because this is near to the four-year ‘bitcoin half life,’ Cardano holdings will diminish at a similar pace to bitcoin reserves.

It’s worth mentioning that Bitcoin took almost eight years to attain its highest level of popularity and pricing. As a result, it is reasonable to anticipate Cardano transaction volume and exchange rate to rise

substantially over the next eight years to more than compensate for the reduction in monetary expansion.

Funding the Treasury

IOG also recommends a starting figure of 5% for τ , the proportion of rewards that are automatically sent to the Treasury at the end of each epoch. Over the following five years, at least 380m ada will be transferred from the reserves to the Treasury.

The actual amount coming to the Treasury will be much larger. To begin with, it's unrealistic to anticipate that all ada will be delegated based on learnings from the Incentivized Testnet, but also anticipating future usage of ada. Some of it will be stored on exchanges, traded, and used in smart contracts. Unclaimed rewards will result from the ada that is not delegated. The treasury will salvage these unclaimed rewards.

IOG doesn't anticipate most pools' pledges to be extremely large, just high enough to make launching a Sybil attack undesirable. The difference between prospective pool rewards with a very high pledge and pools with a more realistic pledge level, ends up in the treasury as well. For the foreseeable future, the total of all ada going to the Treasury indicates that there will be enough funds to pay for new features and upgrades.

Pledge Influence Factor (a_0)

The ada promised by pool owners protects against 'Sybil' attacks by ensuring that delegated stake is not overly drawn to pools whose owners attempt to abuse the system by forming a large number of pools without owning a substantial amount of stake themselves. There was a lengthy debate, at the time, on this episode of the Cardano Effect.^[338]

The pledge influence factor has a direct impact on a pool's rewards: the higher the influence factor, the greater the impact of a bigger

pledge on rewards. A greater influence factor improves Sybil protection and makes the system safer and more secure, but it also offers stake pool owners who can afford a bigger pledge an advantage.

Increased pledges may be used to offset higher operating expenses, allowing a pool with relatively high expenditures to retain appropriate incentives and stay appealing to delegators by raising its pledge. IOG put a number of pledge influencing elements to the test in a range of real-world scenarios. The initial value of 0.3 was intended to strike a compromise between the amount of Sybil protection and the pledge needed.

However, there is no minimum pledge. The pledge may be made as low or as high as the pool operator decides. Their choices impact the rewards, but there is no ‘hard’ rule requiring them to pledge a certain amount. This means that pool pledges will eventually go as high as pool owners are willing to go, and it will be up to the community to strike a balance between security, economic concerns, and the desire for justice and equal opportunity.

By eliminating a ‘race to the bottom,’ when pool owners claim extremely low running expenses to obtain a competitive advantage, the minimal operational cost setting guarantees that the pledge influence factor is effective. While this may help ada stakeholders in the short term, it may end up jeopardizing the Cardano network’s long-term health by discouraging professional pool operation.

In May 2020, a survey of experienced pool operators yielded a distribution of typical pool operating costs per pool per year. Genuine low-cost operators may gain a lot from the lowest operating cost since the gap between it and their actual cost gives them extra money on top of their margin and staking rewards. According to IOG’s study, normal annual running expenses for a pool are projected to be in the \$2,000-\$15,000 range. As a result, IOG set the minimum operating cost at \$2,000 per year.

Finally, IOG estimated stake pool anticipated returns under a variety of real-world conditions (about 150,000 pools in total). IOG utilized the above-mentioned values for the impact factor, monetary expansion, and minimal cost, and modified the intended number of pools from 150 to 500. Using ada to dollar translation rate at the time, IOG's findings demonstrated that stake pools would produce sustainable ROIs of between 6% and 6.5 percent. Naturally, if the value of ada increased, the ROIs would be much greater.

First Draft

Choosing good values for all the initial Cardano Shelley parameters was a non-trivial, complicated task with many concerns to be weighed up. IOG were navigating uncharted waters and moving at the cutting edge of science and technology, so there wasn't any dependency on existing data, statistics, or prior experience, and instead relied on educated estimates and mathematical models, which can never be flawless. IOG tried to come up with sensible settings but recognized that they will need to be refined over time. The values outlined were just a starting point and IOG intends to work closely with the community to improve and adapt them as the Basho and Voltaire roadmap eras come to life.

Stake Pool Diversity

First and foremost, Cardano's rewards-sharing method attempts to equitably compensate users for long-term support of the platform, rather than as a one-time windfall. One of the purposes of staking has always been to promote long-term ada holders: those who care about the ecosystem's sustainability.

The system can only be effective in the long run if it is broadly decentralized. The rewards plan is designed in such a way that it encourages a broad range of stake pool operators. This protects the platform from attacks, distributes any available rewards equitably among the community, and makes the system more change resistant.

Blockchains can only succeed if power is decentralized. Smaller and medium pools may contribute substantially to the ecosystem because of the rewards-sharing mechanism, which prevents them from being swallowed up by bigger operators, as has occurred with other blockchain systems, notably Bitcoin.

Introducing counterincentives to a pool's expansion is one way to resist a tendency toward a few giant pools controlling the system collectively. This innovative notion is exemplified by the rewards-sharing model IOG devised. When stake delegation to a single pool reaches a certain level, the benefits automatically decrease, pushing ada holders to choose a new pool to enhance their returns. This approach restricts the amount of delegation that may be made to each pool and distributes delegated stake among a wider number of pools.

Special k

k is the reward scheme parameter that determines the soft limit on the pool size. At equilibrium, assuming rational participants and no external influences, the mechanism is constructed such that the stakeholders' optimal response behavior converges to k pools of equal size, each delivering the same amount of rewards per unit of stake to their delegates. IOG began with $k=150$ for the mainnet deployment of Shelley, which restricted pool size to 210m ada. This was a little improvement over the parameter choice in the incentive testnet (ITN), which was $k=100$. This was seen to be a cautious approach at the time, aimed to enable a seamless transition of the ITN environment to the mainnet. The debut of Shelley drew a lot of attention from the community and a lot of pools. IOG watched how the staking pools worked and realized that k had to be raised.

Tiny, progressive increases in the k -parameter aren't possible (unlike, for example, the decentralization d parameter, which lent itself to a gradual reduction). Each rise in k necessitates action on the part of pools and delegators. For pool operators, this entails fine-

tuning their settings, particularly their margin; for delegators, it entails selecting new pools to delegate their ada to, particularly if their existing selection becomes oversaturated.

As a result, the optimal method for increasing k is to do it in bigger, less frequent increments – and as quickly as realistic network dynamics and economics will allow. The question of ‘how much’ and ‘how soon’ sparked heated debate and discussion. The optimum option is one that causes the least amount of disturbance to successful pools and their delegators while increasing the chance for medium and smaller pools to mint blocks and attract additional stake. It’s also critical to have a long-term strategic aim in mind as a community: to spread decentralization as broadly as possible.

The $k = 500$ change

IOG’s plan has always been to make gradual and thoughtful adjustments and use the information they acquire to guide future choices. As a result, they want to execute the k modification in stages. At epoch 234, an adjustment to $k=500$ was made on December 6, 2020. Small-to-medium-sized pools that were having trouble attracting delegation benefited from the change to $k=500$. It also restricted pool size to 64 million ada, meaning that more than 100 of the biggest pools would overfill.

Before the transition, ada holders could redelegate at any time. You may have needed to transfer your ada before epoch 233, on December 6, 2020, if you were delegating to one of the larger pools and wanted to continue collecting optimum staking rewards. It’s always best practice for delegators to monitor their preferred pools. In the Daedalus wallet, there is a tab that displays pool saturation levels. You should definitely redelegate if you see your chosen pool becoming oversaturated. It’s crucial to remember that rewards will still be paid out from relatively saturated pools, but they’ll decrease when the pool’s saturation rises. No one who delegated to an oversaturated pool ever lost any ada. It’s only that if one remains in a saturated pool, their return on investment will be diminished.

IOG discovered that a k value of 1,000 was stable in the long run when modeling the long-term survival of stake pools. As a consequence, the plan was to reach $k=1,000$ by March 2021. IOG realized the significance of economic elements that have a significant impact on pool profitability and continue to interact extensively with the community; the network's social dynamics should never be overlooked.

The bigger picture

Despite a time of upheaval and change, IOG felt that adjusting k to 500 would improve the ecosystem. It is not, however, the whole story. They worked to refine their ideas in additional ways that will help Cardano become more decentralized. Hardware wallet delegation support aided in the expansion of ada supply, benefiting everyone. Stake pool server improvements will eventually enable community members to curate their own pool lists to assist influence and drive delegation decisions. All but one of the public IOG pools was retired, and delegators were encouraged to convert their ada to community pools, while IOG built their own delegation plan. On the parameter front, IOG did some modeling concerning pool operator pledging, which is another aspect that shifts network dynamics in favor of ada's wider distribution.

IOG acknowledged that the transition to $k=500$ caused major adjustment for some people. Some pools became oversaturated when delegators to bigger pools did not respond, and rewards went unclaimed. Note that no rewards are lost; everything goes back to the system's reserves for the community to draw from in the future. As a consequence, pool operators needed to modify their margins and costs in the near term in order to remain viable and attract delegators to act. While this took some community work, it is a necessary step for the Cardano ecosystem to achieve maximum decentralization. Cardano's high degree of decentralization is the jewel of the ecosystem, and a huge competitive edge over other blockchains.

Any rise in k will be a major step forward in carrying out Cardano's objective. IOG wants to give the community plenty of time to alter their plan and absorb the changes since such a shift will create some inconvenience. Furthermore, they want to assist the community in making the best choices for Cardano's long-term viability. As IOG continues to enhance the experience, they will be posting additional information to support this strategy. For example, they included a guide^[339] in the docs on selecting smart delegation choices.

$d (=0)$ Day and beyond

Cardano hit a milestone at the end of March 2021 when d , the parameter that determines what proportion of transactions are processed by the genesis nodes, reached zero. The duty for block creation was totally decentralized at this time. Cardano's network of 1,800 (March 2021) community pools were fully responsible for the generation of blocks.

The day d reached 0 was a watershed point for Cardano. When IOG released the Shelley update in July 2020, they set d to 1.0, which meant that every block was generated by IOG's federated nodes. Of course, this was the polar opposite of decentralization, but it was a prudent (secure) strategy in the short term until the stake pool operator (SPO) network was set up and mature.

Steady and Deliberate Countdown

IOG steadily lowered d at a rate of 0.02 each epoch over time, an increase of two percentage points in community block production every 5 days. When d dropped, the community created more blocks, and more stake pools were able to generate blocks. The network's diversity and geographic dispersion grew as d decreased.

d hit zero on March 31, 2021, at the end of epoch 257. That day was memorable because, although d is a modest number, its importance is enormous. That zero was the most crucial external signal of

decentralization, a parameterized symbol confirming a major principle of Cardano's ideology of pushing power to the edges.

There are various factors that have shaped the Cardano network's history. More than 20 parameters influence network function and health, including the d number. This collection of settings serve as 'levers' for managing and steering a decentralized proof-of-stake system's^[340] effective functioning. The community will eventually determine Cardano's progress via Voltaire governance rules, but IOG maintains this set of parameters until then. IOG's stewardship compels them to make modifications as needed to create and maintain the network's health.

Why k (# of stake pools) matters

Apart from technical reasons, IOG continues to encourage smaller stake pools because they feel this strategy corresponds with their long-term aim of establishing the most decentralized and economically viable stake pool ecosystem possible. This is mirrored in their delegation strategy, which strives to encourage stake pool diversification.

Pledge

IOG keeps track of stake pool activity, gets feedback, and applies what they learned when making modifications. Pools will divide up when it is economically feasible for them. The more promise a pool has, the more valuable it is, and the more incentive SPOs have to maintain their pledge together. If, on the other hand, a pool has a low level of pledge, there is little reason not to divide it apart and form new pools. While there are costs connected with administering a tiny pool, IOG felt that the financial motivation for splitting pledge was increasing, given the gain in the value of ada. Ada hit a record high of \$3.10 in September 2021.

Pledge update

SPOs that concentrate their pledge into a limited number of pools are rewarded with the $a0$ parameter. This has worked well in encouraging pools with high levels of ada pledge to combine into big private pools (like IOG do), giving smaller pools a better chance to recruit delegators.

However, IOG felt the existing method could be improved, therefore debated and modeled ideas to make pledge more successful at resolving pool splitting for lower pledge levels. IOG realized they needed to adapt the rewards formula, which their research team worked on for some time. IOG thanked community member Shawn McMurdo for his important contribution to the development of this area's thinking with his Curve Pledge Benefit improvement proposal. [\[341\]](#)

IOG's research team developed a strategy. Their team decided that $a0$ should be changed. This modification, they felt, considerably improved the network by making it more sustainable, broadly spread, and internationally diversified. It also boosted the revenues of all public pools (those that hadn't yet been fully 'saturated' with pledge).

While there has been much internal debate, IOG came to the conclusion that any change in k should be only made after revising the formula for $a0$ to get the desired outcomes (especially encouraging stake to flow to smaller single pools rather than split pools). Because this was a complete formula change rather than just an epoch boundary change, it had to be issued as part of a hard fork. IOG planned to make this adjustment in the third quarter of 2021, given their product pipelines and their team's focus on the Goguen rollout.

Other factors

Other aspects must be taken into account. The provision of multi-pool delegation, which allows ada holders to distribute their stake over many pools from a single wallet, is one of the most important of these features. This will need extensive backend work from the core

development team. IOG want to provide better pledging alternatives for Daedalus SPOs in a comparable period (now only accessible through CLI or AdaLite), which would need extra development work not just for internal teams but also for the Ledger (ledger.com) and Trezor (trezor.io) wallet firms.

As smart contract technology became available, IOG continued to investigate various aspects such as minimum fees (designed to avoid a ‘race to the bottom’, but biased towards smaller pools), as well as measuring and improving node speed. IOG’s goal is to maintain a delicate balance between the network’s reliability, scalability, and general health, as well as a thriving ecosystem of pool operators and delegators.

Constantly Evolving

IOG continues to monitor and explore additional factors and values as they try to improve the network and stake pool ecosystem’s health. This study takes into account both tactical and strategic methods.

IOG continued to examine and revise the Cardano fee structure as the price of ada rose, native tokens were implemented, and smart contracts followed. For example, IOG contemplated taking the tactical approach of instantly cutting certain prices in response to community comments. The stake pool minimum fixed cost of 340 ada was an obvious adjustment; network transaction fees and smart contract deposits were also discussed.

IOG researchers and analysts were also collaborating with an outside economic consulting firm to formulate an optimization strategy that maintains fee stability and predictability over time. As IOG expands, optimizes, and grows the network, the findings of this assessment will include a governance model with a clear mandate regarding when and how fees should be established in the future.

June 4, 2019. Re: Ouroboros parameters. CH:[\[342\]](#)

What is the protection mechanism against too many stake pools? So you have to delegate to the stake pools ...so there's only a finite amount of ada and the financial incentives are basically set up in a way where you will have a ceiling of stake pools, and if you have more than that, you actually make less money. So I'd highly encourage you to read our paper, we wrote out of Oxford with Alexander Russel.^[343] The paper covers how you parameterize that model and that's why we can believe that there'll be a stable thousand stake pools after a while.

The 3 different sides of full Decentralization

Decentralization is the transfer of power from a central authority to smaller entities. However, in the context of cryptocurrencies and blockchain, this definition merely scratches the surface. Cardano's technological road to complete decentralization gradually unfolded, with stake pool operators (SPOs) producing varying degrees of blocks, peer-to-peer (P2P) network discovery, and 'gossip' with peers trading information among themselves. It entails the implementation of sophisticated community-led governance and decision-making mechanisms, with completely decentralized software and protocol changes as a result.

Pushing power to the edges

The balance of power has moved from the people to businesses like Facebook and Google, resulting in a virtual information monopoly. Centralized authority has data hegemony over their customers due to their unassailable market positions.

Decentralization is the antidote to power concentration and the dangers it entails. Decentralization allows individuals to make choices and decisions, restores personal information ownership to the individual, pushes authority to the margins, and gives every network member (or ada holder) a stake. Cardano's decentralization

is built on three principles: block production, networking, and governance. These are inextricably intertwined and work together to produce a cohesive result: complete decentralization, which lies at their intersection.

1. Decentralized block production

To develop and prosper, every blockchain depends on the creation of new blocks. Core nodes – maintained by IOG, Emurgo, and the Cardano Foundation – were solely responsible for building blocks and maintaining the network throughout the Byron era deployment. Shelley and the Incentivized Testnet, which launched in 2019, served as a testbed for decentralized block production. The Incentivized Testnet experiment demonstrated that Cardano could be supported by a network of community-run stake pools. There were 1,299 registered stake pools as of epoch 170 on June 3, 2020, with 413 of them producing blocks.

The number of stake pools continues to grow and grow, with a good number of them forming blocks and rewarding delegates. Exchanges control some, while single-pool community operators handle others. Everyone contributes to the network's worth. The former because of their capacity to attract new ada holders into the ecosystem, and the latter because of their contribution to decentralization and grassroots involvement. IOG is dedicated to promoting decentralization, and tweaks to parameters like k (maximum pool size) and pledge, as well as their community delegation plan will help achieve that goal.

2. Decentralized Network

The introduction of peer-to-peer (P2P) networking is the second pillar of Cardano's decentralization. The goal is to connect geographically dispersed pools to create a safe and reliable blockchain platform.

This feature will leverage a collection of mini protocols^[344] and a categorization of cold, warm, and hot peers on mainnet to allow a

node to make the best connection choice possible. In terms of networking, there was a hybrid era where SPOs had to use manual methods to maintain network connections. As SPOs took over block production at $d=0$, all core nodes were decommissioned. IOG continued to maintain relays, but the SPO network gradually took over this duty. To learn more about this, watch March 2021 Cardano360 episode, [\[345\]](#) in which IOG's principal architect Duncan Coutts outlined the P2P future.

3. Decentralized Governance

Cardano has already got transaction metadata and native tokens thanks to the Goguen rollout. Since the Shelley launch, this has perhaps been the most visible evidence of Cardano's development and success.

At the same time, something even more powerful has emerged with Project Catalyst: an active community of builders, innovators, and entrepreneurs. The Catalyst community has a worldwide membership of entrepreneurs, professionals, and specialists from a variety of fields that make up this pool of decentralized talent, which offers a broad reservoir of innovation to guarantee the greatest and brightest ideas receive the financing they deserve.

Cardano's ultimate goal is to create a blockchain where a community of stakeholders make practical choices regarding the chain's protocol and growth, which is supported by a layer of robust governance. Catalyst is the forerunner of Voltaire, the development era that will usher in the third and ultimate degree of decentralization by integrating governance and on-chain decision-making/voting.

Voltaire will introduce:

- Access to funds through a decentralized treasury under a governance framework in which the community will have the authority to influence Cardano's future path via their ada stake

- Decision-making on enhancements, network improvements, and parameter modifications is decentralized
- Fully decentralized software updates: a procedure that allows for decentralized, open voting on choices concerning system and protocol developments.

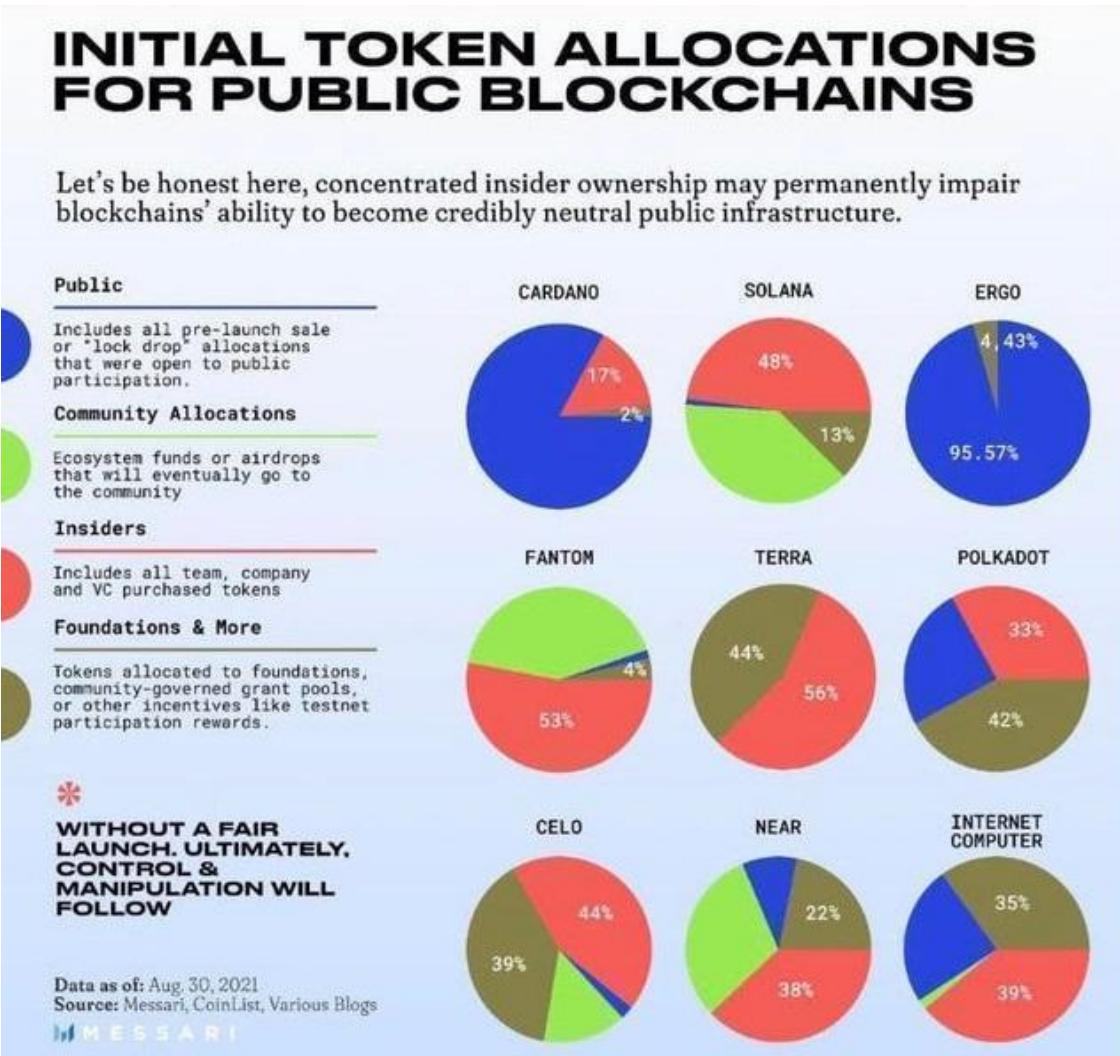


Figure 10. Messari Initial Token Allocation Chart

September 8, 2021. Re: Catalyst. CH:[346]

The cryptocurrency space, as a whole, is not aware of this yet, they're still thinking that it's just all centralized and top down, and there's a few people floating around who make all these

calls. They don't really understand that we've silently built one of the world's largest decentralized organizations and decentralized decision-making machines, and it's in its infancy.

We have constructed this meta brain, that runs this meta machine in the sky, and all these people whether in the south of France, or an island, or right here in Colorado with a lobster on the mic... we somehow just come together, with different values, different languages, different perceptions of reality and we converge to a point where we actually can vote on, and move forward, and make change and get funding behind people... more and more of the community is going to be involved in deciding the direction and governance of Cardano in general.

What's so cool about this is it's completely bottom up. There's not a lot of top down here, the top down stuff is just ensuring that there's best practices and good infrastructure ...and asking questions about what tools we need to construct and how do we improve things? ...but the solutions are coming bottom up, and it's growing rapidly, and more and more people come in every time we do a fund, it just massively increases... 250,000 unique votes, 33,000 wallets ...we don't even have the mobile interfaces in yet, or the Daedalus integration in yet.

Half a million, million people are going to be in this club next year, if not more. So this is a great opportunity for us to kind of explain where this is going, and why this is the heart of Cardano and what's going to make Cardano frankly not only here to stay, but the dominant protocol of all the protocols.

Centralization is ripe for disruption

The evolution to decentralized block production has been completed. Starting in April 2021, P2P networking was available. On the governance front, Project Catalyst continues to grow and grow with much more to come.

From a federated chain with centralized block production to one with entirely community-minted blocks, Cardano has come a long way. IOG will have produced something genuinely unique after they have finished constructing all three pillars. A network that is both strong and durable, as well as flexible and adaptable to future expansion. A platform that meets the needs of its users today while also allowing them to provide new value and features in the future. All of this takes place within a democratic framework in which the community makes the decisions. The result of these three principles is complete decentralization.

Ouroboros lays the foundation for the Basho Era

Cardano is built to service millions of users across a worldwide network. This means that, like any other decentralized blockchain, it must provide a predictable and steady supply of new blocks that collectively develop the chain and transparently record user transactions. It is critical that the system utilizes compute, memory, storage, and network resources economically in order to guarantee that new blocks are propagated over the network in an effective and safe manner.

Because flexibility is so crucial, the Cardano protocol was built with genuine scalability in mind. Its parameterized technique is meant to bend and respond to price swings, network saturation and rising demand. There are a number of protocol options that may be used to fine-tune the system's behavior without requiring a hard fork. But even then, larger modifications that do need this may be handled neatly using the hard fork combinator (HFC). These are important differentiators for Cardano, since they provide it with durability and dependability, as well as very flexible upgrade options as the network develops and the user base grows.

Cardano's roadmap was similarly designed in eras, taking in one step at a time toward the final objective. Within a federated network, Byron was about fundamental transactional capacity. While working

on the following phase, IOG were able to start establishing a community and relationships. The Byron reboot laid the groundwork for an increase in capabilities, while Shelley introduced stake pools, which helped to grow the community and enable 100% decentralized block production.

IOG debuted a slew of new, much-anticipated features in 2021. Cardano has enabled multi-assets and non-fungible token (NFT)^[347] generation on the ledger since the ‘Mary’ upgrade. There was an explosion of activity in this field due to cheap fees and the lack of a requirement for smart contracts.

Support for Plutus smart contracts was added with the ‘Alonzo’ update in September 2021, allowing for the construction of a broad variety of decentralized apps (DApps). Smart contracts on Cardano are still in their infancy, but with many projects working on DApps and several already released, momentum is building. These additional features have an impact on how the ledger handles new scripts and transactions, as well as putting new demands on the system’s resources. As the volume of activity increases, Cardano’s design will enable it to bend and adapt as needed.

Network bandwidth

All Cardano activities are built on top of networking. The Cardano network distributes transactions and blocks among nodes all around the globe that build and validate the blockchain. This is known as data diffusion, and it is necessary for the consensus protocol to make judgments by providing the necessary information to nodes. These choices move the chain forward, since node consensus guarantees that all transactions are confirmed and approved, allowing them to be included in a new block in a transparent manner.

The speed with which the system as a whole operates is influenced by network performance. This covers things like:

- *throughput* (amount of data transferred)

- *timeliness* (time for block adoption)

These two needs are in direct opposition to one another. When the created blocks are used as effectively as possible, throughput can be increased. This, in turn, requires adequate buffering to offset latency, reducing the negative effects of a globally distributed system. When the system is saturated, more buffering may frequently suggest greater block (and network) usage, but it comes at the expense of higher latency (time to adoption in the chain).

A block's budget

To comprehend how quickly Cardano transactions and scripts may be completed, the concept of the block budget is key. A block's total size was originally restricted to 64 KB, which struck a compromise between maximizing network use and reducing transaction latencies. A single block may include a variety of transactions, including smart contracts written in Plutus, native tokens, metadata, and straightforward ada transactions (payments). A single transaction was also restricted to a maximum of 16KB at first. This guaranteed that a single block always included numerous transactions (at least four, but usually many more), hence increasing transaction throughput.

Another attribute is the block time budget, which is a set amount of time allowed to complete all of the transactions in a single block. This is split between the amount of time available for Plutus script execution and the amount of time available for other transactions. This attribute guarantees that transactions containing Plutus scripts do not consume the available time budget, and that basic payments may always be processed in the same block as Plutus scripts.

The entire time budget for creating each block (including networking overhead) is set to 1 second, with a Plutus script execution budget of around 50 milliseconds. In actuality, this is a reasonable provision; IOG's testing has demonstrated that many scripts on a testing environment will run in 1 millisecond or less.

The block time budget was set initially at 1 second. Due to security concerns, the Praos consensus process picks just a small proportion (1 in 20) of the blocks that might possibly be added to the chain. The maximum transaction throughput (for basic transactions) with the protocol settings was around 11 transactions per second (TPS). Obviously, the size and effective payloads of various transactions will change. A single transaction, for example, may close off an entire Catalyst voting round, moving millions of dollars in value.

As previously stated, each block contains a number of transactions submitted by end users through wallets, the command-line interface (CLI), and other means. These transactions are stored in the mempool, a temporary in-memory storage space, until they are ready to be processed and included in a block. As a block is minted, pending transactions are removed from the mempool, allowing new transactions to be added. The potential of nodes being overwhelmed during high-demand times was eliminated by employing a fixed-size mempool, although this meant that a wallet or application may have needed to re-submit transactions. The mempool size was 128 KB, which was double the block size at the time. This was determined using queueing models.

Stress testing the network

Ouroboros is built to manage massive amounts of data, as well as transactions and scripts of various sizes and complexity. With the settings in place the Cardano network was still only using around 25% of its capacity on average in October 2021. Of course, the most efficient option is for Cardano to operate at or near 100% capacity (network saturation). While many networking systems would suffer in such circumstances, Ouroboros and the Cardano network stack have been engineered to be fair and very durable even in the face of extreme saturation.

Benchmarking data reveals that even at 200% saturation, overall performance remains stable and no network failures occur. Even

with stress tested at 44x, there were no problems in the entire network capacity (though some transactions may be slightly delayed). Backpressure^[348] is used to regulate the overall system load, which is how the network is meant to function.

While certain users participating in a big NFT drop^[349] may suffer lengthier wait times for their transactions or may need to resubmit the rare transaction from a large batch (or spread the drops over a longer time period), this does not indicate that the network is not coping. It really signifies that the network is working properly. It's referred to as 'graceful degradation,' and you can understand in more detail by reading the network design paper.^[350] See 'Cardano Upcoming NFT drops'.^[351]

Wallet types

End-user wallets upload payments and other transactions to the blockchain on their behalf, as well as monitor the blockchain's progress. One of the most important functions of a wallet is to submit transactions on behalf of the user, validate that they have been approved into the blockchain, and retry them if the first attempt fails. That is, when the network saturates, the wallet should consider the implications of backpressure as well as other network effects (temporary disconnection, possible chain forks, etc). Wallets may be one of two types:

- Full-node wallets (like Daedalus), which operate a node that connects directly to the Cardano network using local compute and network resources
- Light wallets such as Yoroi and Flint, on the other hand, take advantage of pooled processing and networking resources to service a large number of users.

Both kinds of wallets may need to retry transactions during times of strong demand (e.g., an NFT drop). Light wallets may need to temporarily scale available compute and network resources to meet

user demand since they share resources across numerous users. Full node wallets, on the other hand, may be unaffected.

Transactions may be somewhat delayed, but each wallet will have the dedicated resources, including its own network connections, to attempt the submission. DApp providers should follow similar principles: if particular network endpoints are offered, system resources should be adjusted to match demand.

Network optimization

IOG appreciates the NFT community's creativity and excitement. To enhance the user experience, development methods must be optimized so that, for example, the process of creating NFTs functions effectively even when the system is saturated. For example, many NFT developers use batch minting to increase efficiency.

IOG encourages creators to consider how they might improve their own efforts to reduce network congestion. They also encourage everyone to participate in their Discord discussions.^[352]

Chain v transaction confirmation

'*What is Cardano's TPS (transactions per second)?*' must be one of the most common questions on Crypto Twitter. How many network confirmations does Cardano require before a transaction goes through? These are often asked questions about Cardano. The solutions to these concerns necessitate a more in-depth examination of the principles of chain confirmation and transaction confirmation, as well as their relationship to the protocol.

Chain confirmation

This is the threshold at which the protocol guarantees that the chain will not change any further due to randomness or random occurrences. After a sufficient number of future k blocks have been issued, chain confirmation happens at some point in the future. The

stability window is the period of time between now and when chain confirmation for a certain transaction happens (that is, the number of slots required for a block to become stable, where stability is defined as a block that cannot be rolled back). The formula for calculating this window is:

$$3k/f$$

- where k is the parameter that restricts a pool's growth by lowering its rewards yield beyond a particular threshold,
- f is the parameter that determines a pool's maximum size

Transaction confirmation

When a transaction is accepted into the chain, it becomes immutable at this point. The terms 'block depth' and 'settlement window' are used here. If the block containing the transaction is deep enough in the chain, it is deemed confirmed. Deep enough is a relative term: the depth of a block shows how many further blocks have been added to the chain since that block was introduced. Because blocks have depth, the transactions included within them have depth as well.

The transaction is deemed verified when the depth of a specific block exceeds a certain threshold, and the assets in that transaction can be used 'safely' (i.e., the protocol can guarantee the transaction is immutable, so the assets can be traded, exchanged, etc).

The settlement window is the amount of time between when a transaction is confirmed and when the transaction's assets may be utilized to swap with other assets.

The chance of immutability

Another factor to examine when deciding whether or not a transaction is verified is its possibility of immutability. The likelihood of a transaction being immutable is proportional to the number of

blocks added to the chain since the transaction was approved. The bigger the number of blocks added, the more likely the transaction will become immutable. When a transaction's depth exceeds 3k/f slots, it becomes immutable. The Ouroboros Praos protocol guarantees this.

In most cases, however, 3k/f slots surpass the criteria, therefore a more realistic way is to assess the likelihood of a transaction being immutable. In this scenario, we consider a transaction to be verified if the likelihood of it being immutable is sufficiently high.

P2P (peer-to-peer)

Due to Cardano's decentralization, stake pools are in charge of maintaining the blockchain. Reliable and effective connections between all dispersed nodes, as well as guaranteeing the network's resilience to failure, are critical components.

With the Byron version of the blockchain, the Cardano Foundation, Emurgo, and IOG were solely responsible for monitoring block creation and network connections via federated nodes. This kept the network running while constructing a system of thousands of dispersed nodes controlled by stake pools. Cardano has finally achieved decentralization by ending the need for federated nodes, which have maintained the system since its inception in 2017.

The **networking layer** of Cardano is a physical infrastructure that unifies nodes and their interactions into a single system. The network disseminates transaction and block generation information to all active nodes. The system validates and adds blocks to the chain in this manner, as well as verifying transactions. As a result, a distributed network of nodes must have minimal communication latency and be robust enough to deal with outages, capacity restrictions, and hackers.

Nodes were linked in the former federated system using a static configuration described in a topology file. With Shelley's inception,

the system had operated in a hybrid mode, with nodes connecting to both federated and other SPO's relays. SPOs may share block and transaction information without depending on federated nodes since this connectivity is somewhat manual. If there is to be complete decentralization in terms of block generation, it's also critical that there is decentralization of network connectivity as well. Cardano will do so by switching to peer-to-peer (P2P) networking.

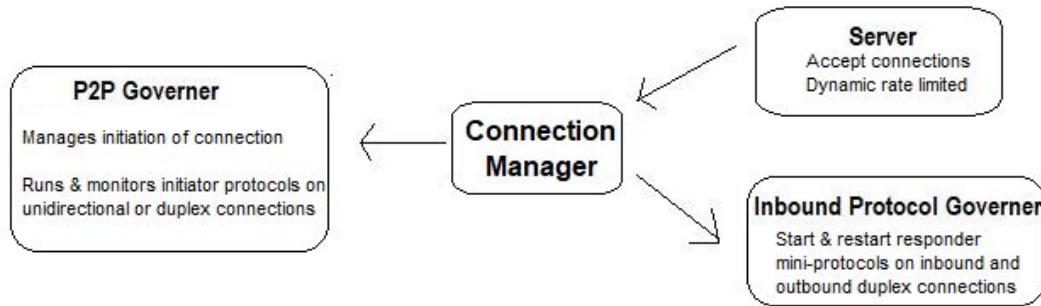
Peer-to-Peer networking

The network 'stack' is a collection of software tools that IOG's engineering team has improved to deal with a bigger, more dynamic, and sophisticated network.

P2P communication has improved the flow of information between nodes, eliminating the network's dependency on federated nodes and allowing Cardano to become fully decentralized. IOG's networking team has been hard at work enhancing the network stack with enhanced P2P capabilities to achieve the needed resilience. These enhancements don't need a protocol change, but they do make peer selection and communication more automatic.

Figure 11. The components used to support peer-to-peer networking

The Network- Peer-to-Peer Architecture



Peer-to-Peer architecture

The following section looks at the process of establishing node connections and how innovations have simplified data sharing

between nodes.

Mini protocols

Communication between nodes is enabled through a variety of mini protocols. Each protocol implements a fundamental necessity for information transmission, such as notifying peers of new blocks, sharing blocks, or processing transactions. The following protocols have been used to distribute chains of blocks and transactions for node-to-node communication in the network: chain-sync, block-fetch, and tx-submission

- block-fetch accesses the chain database for information
- chain-sync synchronizes data that has been fetched across the network
- tx-submission consumes peer mempool transactions and adds them to the local mempool, allowing peers to submit transactions to the node. This is a tweak to the existing tx-submission protocol.

The Ouroboros consensus protocol is supported by these mini protocols. Additional protocols have been introduced by IOG to support a reliable networking service:

- keep-alive: this maintains the connection between nodes and reduces performance issues
- tip-sample: this offers information on which peers provide best performance in terms of connectivity.

Learn more about the network architecture and mini protocol in the Cardano documentation.

Connection management

Linux, Windows, and macOS are all supported by the networking service, however the number of connections supported by each operating system varies.

A multiplexer^[353] combines numerous channels into a single Transmission Control Protocol (TCP) connection channel to minimize system overload. This has two benefits: bidirectional peer communication (any peer may commence communication with no constraints since both parties have read and write rights inside the same channel), and improved node-to-node communication without compromising performance.

IOG's networking team built a bidirectionally aware 'connection manager' that works in tandem with the P2P governor. The API for the multiplexer has also been updated to detect new connections and protocols. This upgrade makes connection management more efficient and improves troubleshooting.

P2P governor

Multiple peer nodes make up the Cardano network. Some are more active than others, while others have established connections and should be supported to maintain optimal system performance. Peers are divided into three kinds, as explained in 'Cardano's path to decentralization'

- **cold peers**: peers that are known of, but where there is no established connection
- **warm peers**: where a bearer connection is established but it is used only for network measurements and not for any application level consensus protocols
- **hot peers**: peers where the bearer connection is actively used for the application level consensus protocols.

It is critical to know which connections are active to build bidirectional connections between them.

Peer Discovery on Cardano

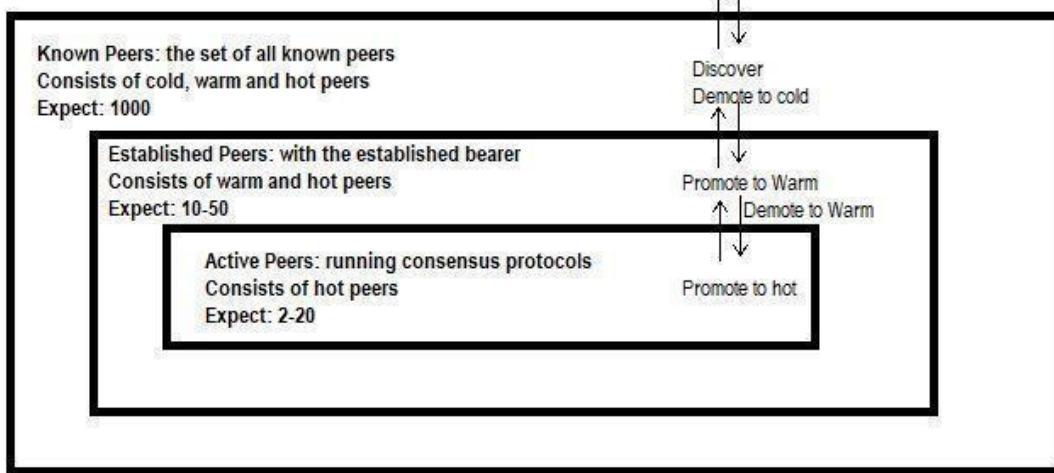


Figure 12. Peer Discovery on Cardano

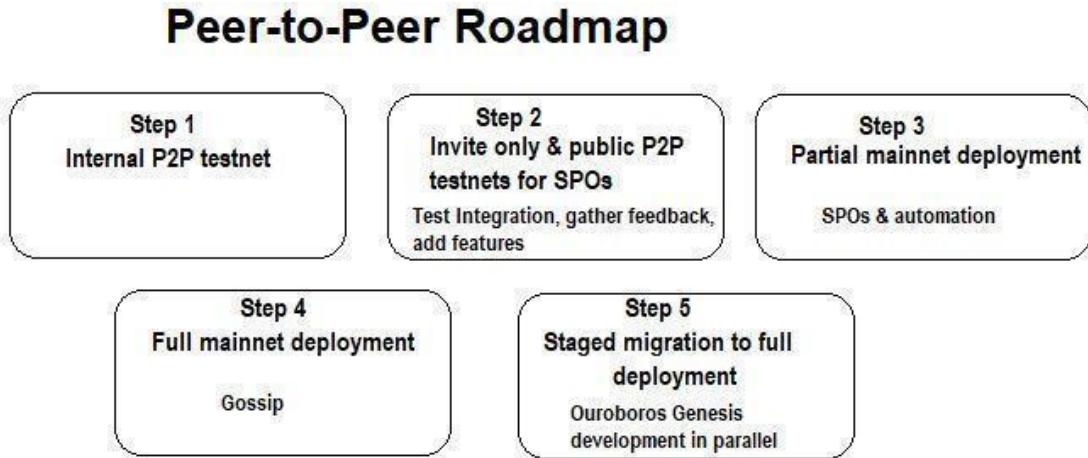
The P2P governor^[354] keeps track of connections and tells you which peers are active and doing well. This feature encourages peer connections to improve system efficiency and gives visibility by creating and maintaining a network connectivity map. The governor automates the process of connection definitions, eliminating the need for a few central stake pools to manually set them. The governor moves peers between the cold, warm, and hot states, as well as interacting with the connection manager to create new connections or reuse old ones.

Peer-to-Peer roadmap

The P2P governor interaction with the node was quality checked by the IOG networking team. After that, the team added further protocols to the network stack, including gossip, which allows for frictionless data sharing between peers and aids in the creation of a decentralized communication map.

IOG was able to simplify Cardano node interfaces and enhance the system's setup because of these technical enhancements. Following the completion of testing, all SPOs were allowed to update and simplify their setup settings in order to improve connection.

Figure 13. These were the stages before full P2P deployment



Check out the March 2021 Cardano360 episode for an overview of the plan from head architect Duncan Coutts.

While governance plays a significant part in the network's creation and ongoing maintenance, genuine network sustainability can only be accomplished via decentralization, which guarantees a fair chance for all stake pools. As a result, the purpose of stack enhancements is to enable all stake pools to operate the same configurations, ensuring that all stake pools have the same capabilities in a decentralized system.

The release of a private P2P testnet in April 2021 was made possible by the activation of the peer-to-peer (P2P) governor and the deployment of the connection manager. Before releasing a semi-public P2P testnet for a set of invited SPOs to assist them test and tweak, IOG evaluated this testnet first.

IOG evaluated how the connection model had progressed to the point where automatic peer connectivity was possible, as well as the outcomes of the private testnet launch.

Evolution of network connectivity

The Byron network connection mechanism was in a federated form when Cardano was released. IOG maintained core and relay nodes, which were linked to around 200 additional relays.

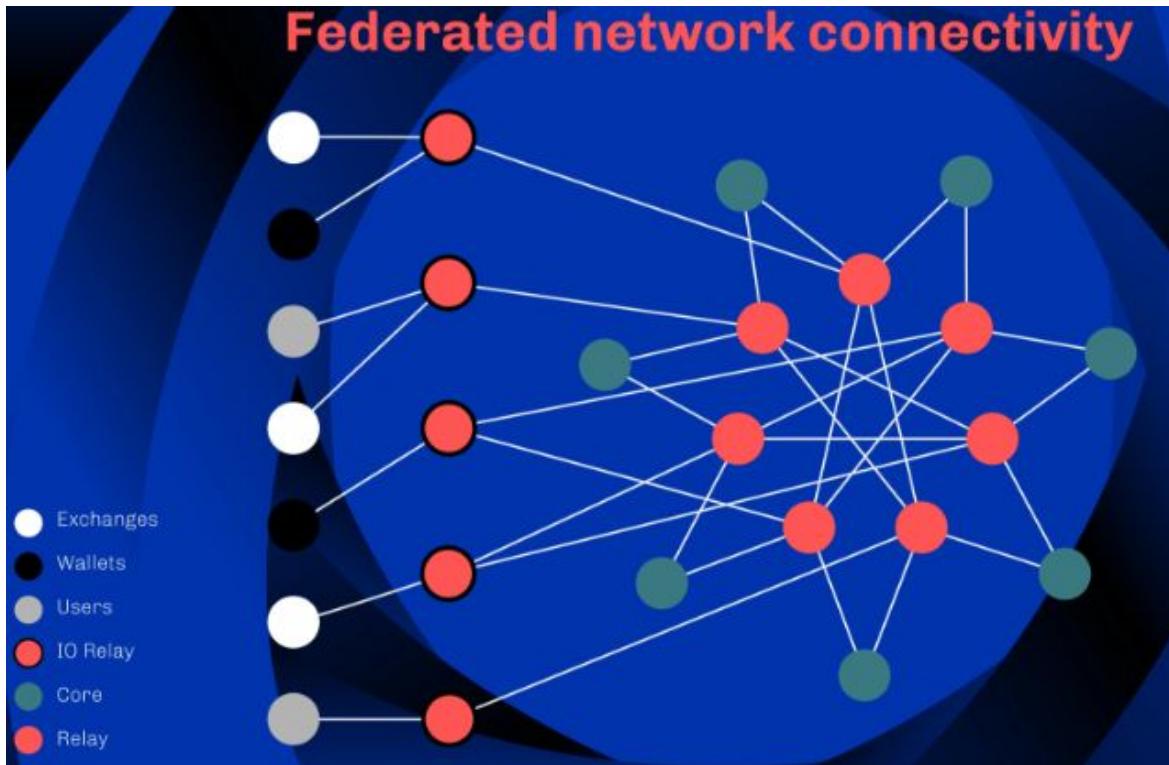


Figure 14. Federated Network Connectivity

Cardano began operating in a hybrid context with the introduction of Shelley in 2020. This enabled stake pools to manually build their P2P network by connecting to core and relay nodes, as well as the seven federated relays that assisted with network maintenance throughout the transition.

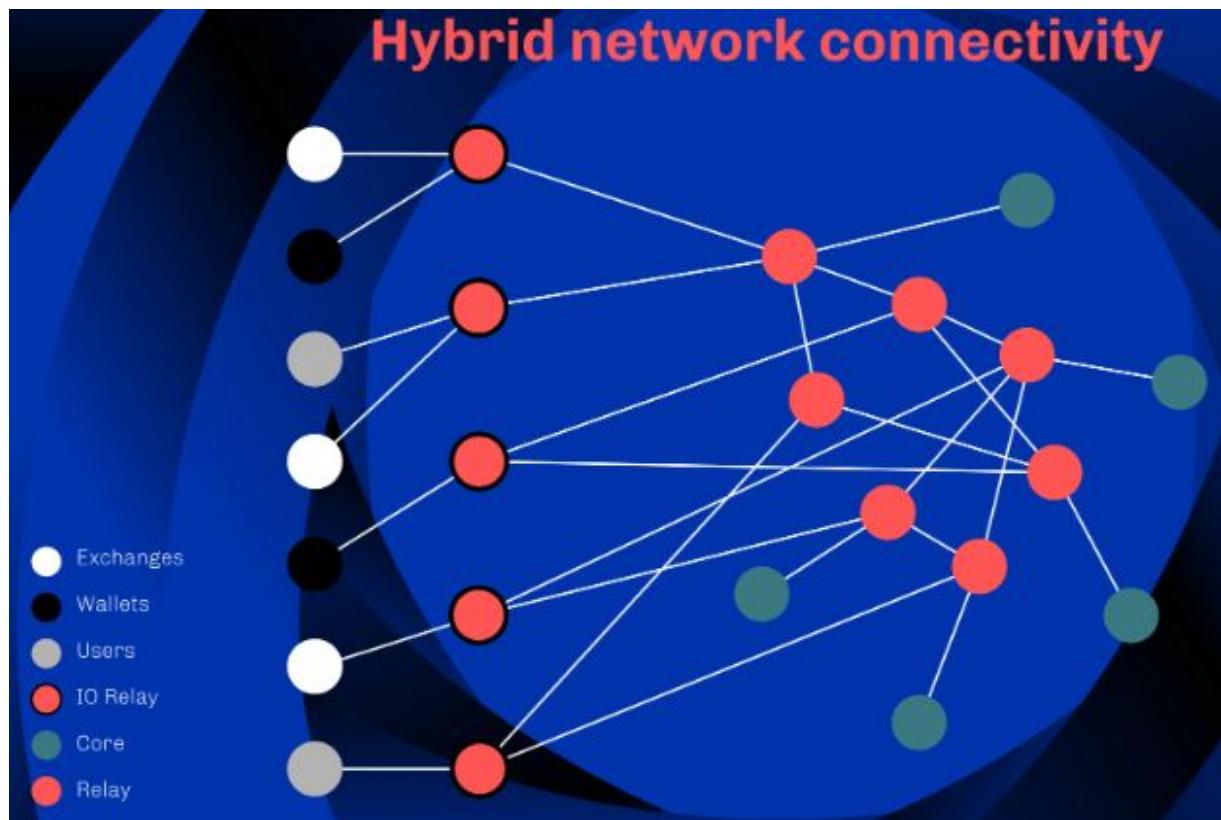


Figure 15. Hybrid network connectivity

Block production has been completely decentralized since March 2021, with stake pools using manual topologies for P2P connections. This meant SPOs had been generating their configuration for connections with other peers using a list of relay nodes registered worldwide. It was critical to allow automated node communication without relying on IOG-run relay nodes to improve efficiency. As a result, the IOG networking team delivered automated P2P code, allowing pool owners to build and operate a more decentralized network.

Cardano will be maintained completely by community-run nodes after the P2P mainnet is launched.

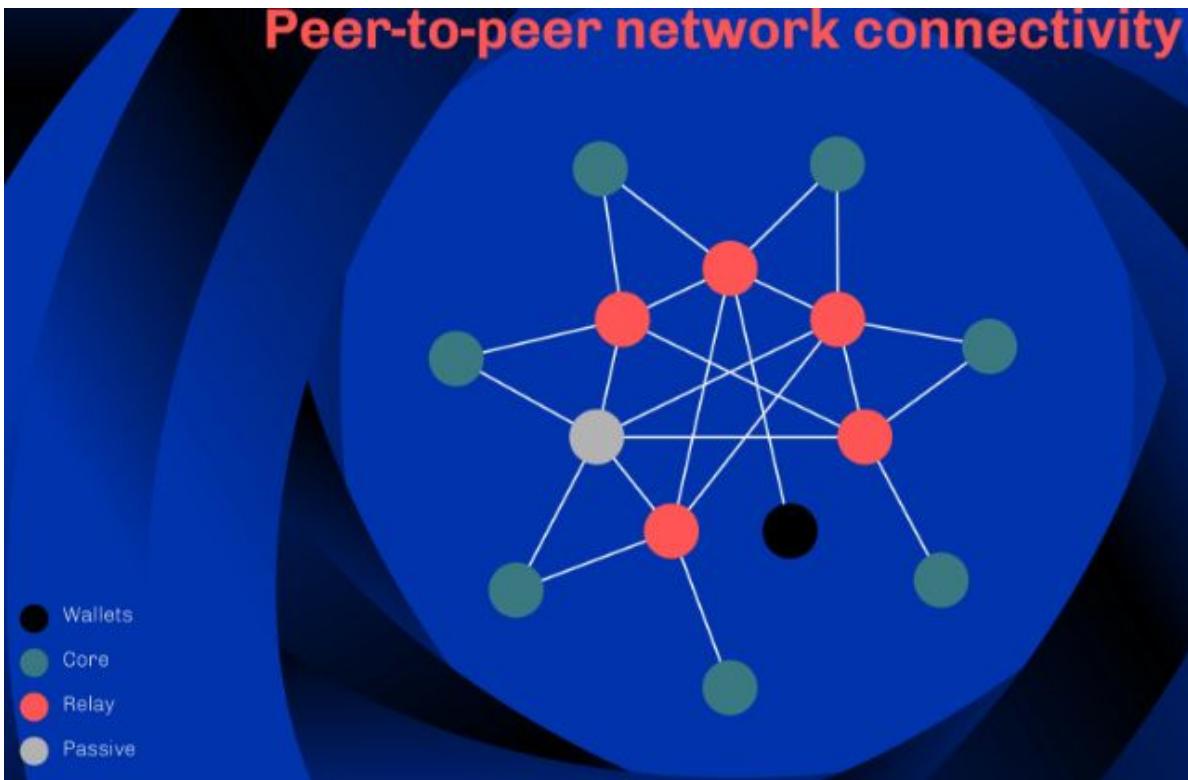


Figure 16. Peer-to-peer network connectivity

Peer-to-Peer testnet

The introduction of the private P2P testnet in 2021 was the first step in the P2P deployment. This was used to test the components' fundamental capabilities:

- P2P governor: oversees hot, warm, and cold sets of peers, ensuring that the node satisfies the required number of each kind of peer
- Connection manager: establishes or registers incoming or outgoing connections, records their status, and enables full-duplex TCP connections to be reused
- Server: receives connections and limits them dynamically
- Incoming protocol governor is in charge of operating and monitoring the inbound connection side. This involves keeping track of each remote peer's temperature as well as the condition of each incoming mini-protocol.

The P2P system was tested between eight nodes that connected to the mainnet and established connectivity with active SPO relay nodes, which then connected to further relays and block-producing nodes in a private environment. The system allowed nodes to find stake pool relays by leveraging the on-chain stake pool registry, which contains each relay's DNS name or IP address.

The nodes were able to choose peers for communication at will, including those from the mainnet, according to the findings of the tests. The adoption of an 'upstream' metric allowed the worst-performing peers to be discarded and new peers to be randomly selected for connection. This approach has been proven in large-scale simulations (10,000 nodes) with near-optimal outcomes. IOG saw numerous rounds of the optimization during live testing. They also saw a variety of peer connections, with both close and far-away peers from various places, which was common to all eight nodes operating in different regions of the globe.

All SPOs invited to the semi-public testnet were able to establish direct peer connections after the IOG networking and DevOps teams collaborated to enhance the testnet environment. This included work on additional functionality and test procedures to ensure the best outcomes. In order to introduce new targets for local root peers, the IOG team looked for related features as targets for known, established, and active peers.

IOG created the semi-public P2P testnet with the cooperation of a select set of SPO partners for early testing before making it available to the rest of the SPO community. Early community input and ideas were crucial in testing, iterating, and improving procedures as the Cardano mainnet moved closer to a fully automated and decentralized P2P architecture.

December 2021 Testnet

With the introduction of a new peer-to-peer (P2P) testnet in December 2021, IOG launched an essential step to help their

continued push toward complete decentralization.

Cardano's Ouroboros algorithm uses proof-of-stake consensus to maintain trust and security in a decentralized context. Over 3,000 stake pools are managed by operators (SPOs), who are in charge of the network's scattered nodes. Clearly, reliable communication between these nodes is required in a decentralized and distributed network. Data diffusion — the process of disseminating information about transactions and block distribution – is important to this and essential for validating blockchain operations. This is also how the Ouroboros algorithm makes decisions.

From the early days of the Shelley incentivized testnet to the Alonzo testnets initiative, IOG has prioritized community-supported rollouts. They invited several pool operators to a semi-public testnet to enhance testing of the P2P modifications. Operators assisted in the testing of the automated P2P components before IOG expanded the program.

P2P was still considered a beta function in December 2021. Despite the fact that it would be included in future versions, IOG did not include it into all of their work at that stage. By organizing their nodes for direct contact with one another, the pool operators evaluated the environment. The cardano-node master branch^[355] and merged pull requests to 'ouroboros-network' on GitHub will have P2P capabilities.

The P2P mode allows for 'churn' to guarantee that peers are dynamically promoted and demoted. SPOs will find it easier to update network settings since their nodes do not need to be rebooted. The node's Prometheus^[356] interface will also be improved thanks to the semi-public testnet. The following data will be included:

- outbound connections: warm (active connections that do not participate in the consensus) and hot (active connections that do participate in the consensus)
- inbound connections: warm and hot
- uni-direction/duplex connections.

P2P rollout

IOG was able to get vital input and identify unexpected concerns by assessing network connections on the semi-public testnet. They'll invite all SPOs to test P2P node communications on the public testnet once they're satisfied. This will be the first time a smart peer selection policy has been implemented. This policy will allow for the definition of final metrics that can be compared to the prior, non-P2P configuration. Above all, they'll keep testing to ensure that all of the components perform perfectly in isolation as well as in combination under a variety of network scenarios.

Nigel Hemsley, Head of Delivery at IOG, confirmed in the May mid-month update^[357] that P2P decentralization is nearing completion and there will be further updates soon.

P2P Progress Update

Marcin Szamotulski, team lead for Cardano Networking, provided an update in the Cardano360 May 2022.^[358]

P2P, peer-to-peer, brings to the network automatic discovery of available peers that are registered on the network, on the chain, and automatic creation of connections between the peers we want. So it's both discovery from the chain, and then constructing connections between the peers.

What does gossip bring to the network?

So gossip is about discovering nodes on the network, beyond the nodes that are registered on the chain. Let's say that I'm running a node without running a stake pool. How can other nodes connect to my node and take its resources to be contributed to the network? Gossip answers these questions.

The gossip (protocol) gives a chance to non-SPO to contribute to the network. Their nodes, that they operate, can be discovered by relays, run by SPOs, or some other non-

associated relays, to connect to your node and take blocks from you and distribute to the network.

Current state of private testnet:

We're actually feature-complete as the networking stands. We also finished all our essential tests that we really wanted to finish, before any release. We're also engaging right now with Haskell consultants. They are reviewing our design and our implementation. They had very encouraging comments about how we write software and how we wrote the network code specifically. In the coming weeks, you'll hear about the rollout of peer-to-peer nodes. It will be a gradual rollout. We will first ask SPOs to start running a single one of their relays as this peer-to-peer node. That will be the initial deployment of peer-to-peer nodes on the mainnet.

Cardano Entropy (Randomness)

It shouldn't be possible to anticipate or influence future blockchain states if the system is genuinely decentralized. All future on-chain events must be fully random. Cardano makes this possible by including an extra entropy mechanism that may be applied to assure the system's randomness. Any complicated cryptographic system relies on true randomness. A source of pure, unexpected randomness must exist for a cryptographic environment, like the Cardano blockchain, to operate and be accepted by the community as truly decentralized and fair. This assures that the chain's future path cannot be altered by anybody with knowledge of the past.

The entropy parameter specifies Cardano's randomization source. Outside of the Cardano ecosystem, this signifies something unexpected, ensuring that no one can 'hijack' the blockchain's randomness. This parameter's value was computed based on occurrences that could not have been predicted in advance or about which anybody might have had insider knowledge.

Entropy addition mechanism

To appreciate the entropy addition mechanism, one must first comprehend completely decentralized block generation and how the transition nonce^[359] will impact this process.

The Ouroboros protocol uses an evolving sequence of leadership nonces to decide which pools are chosen as block producers (cryptographic seeds used to generate a sequence of values using a repeatable random number generation algorithm). These nonces determine the block production schedule. This timetable is determined by each leader nonce for a whole 5-day epoch, during which the nonce controls the stake pools used to guide the development of each block. To achieve the basic ledger features needed, the leadership nonces and stake distributions develop in lockstep.

Nonce Value

IOG added a transition nonce to the running leadership nonce just after March 31, 2022. When the stake distribution for the April 10 epoch was decided, the transition nonce then had to depend on random values (which are introduced by on-chain transactions) that can't be anticipated. This emphasizes transactions that emerge on the blockchain between the 12-hour mark — when the stake distribution is settled — and the 42-hour mark, when the hash value is removed.

The transition nonce is a reflection of entropy generated by a multitude of external, uncontrollable elements. All transactions posted to the blockchain before Wednesday, April 7 at 15:44:51 UTC play a significant role in Cardano's history: the transactions' accumulated hash value (reflected in the 'previous-block hash' from the first block created on-chain on or after this time) will determine the transition nonce, and thus contribute directly to Ouroboros' perpetual cycle of randomness generation.

A user gives a nonce for a transaction when using the Cardano

command line interface (cardano-CLI), however the nonce retrieved when viewing the details of the transaction is different. You can review more details and the relevant command line options in Cardano docs here.[\[360\]](#)

February 2, 2021... How can you explain verifiable randomness to a layman? CH:

That's easy so imagine your gambling against the server, you know, like for example you're playing Blackjack. So when you play Blackjack in human life, you have the dealer and the dealer playing against you and he's giving you cards, you want to believe that the deck is randomly shuffled but it doesn't have to be. What if the dealer had pre-set the cards up so he always gets good cards and you get bad cards? So what does a dealer do to give you some faith in the process? He shuffles the cards in front of you. If you believe that shuffling is a randomization process then you will be satisfied that you're playing a fair game, but the problem is what happens if you can't see them shuffle the cards?

This is the problem when you gamble with central servers, so you're playing blackjack against blackjackstarz.com or whatever the hell these sites are. Well, how do you know that that's a fair deck? Well, they have a random number generator, but how do you know it's not biased so that they win more than you win? Well, you trust that maybe a regulator stepped in and did that. What if you had a cryptographic protocol, you could verify the person's running and you trust the protocol to produce true randomness, then that protocol would guarantee that they're shuffling correctly.

That has to be done for a proof-of-stake system. Why? Because we are replacing traditional proof of work, where it's a meritocratic thing where your computer is chipping away at computations with a synthetic lottery proportional to your amount of stake you have in the system. So if you have 25% of

the total stake in the system, you should win on average 25% of the time. But what if randomness is biased? Then what can happen is even though you have 25% (of the stake), maybe you only win 8% of the time, because I biased the numbers in a way to reduce your chance of winning. So you have to have faith that the randomness in the system is secure, it's true.

That was the point about heavy vs light, dirty vs pure. What is okay from a probabilistic point? So generally, how cryptographers do this is that they compare your pseudo-random number generator to true sources of randomness, and they make a probabilistic argument. So they say, 'can we differentiate between the true stuff versus the pseudo random number generator?' If you can't tell the difference, does it matter? So that's what they're looking for as cryptographers. They're really interested in whether we can quantify that? ...and also, is it always the case? Are there special cases where you lose some of that for a variety of reasons?

So it's a really involved topic, cryptographers have studied this for over 40 years and there are dozens of protocols that exist to produce truly random numbers, usually through some form of distributed process, like a multi-party computation protocol or a collective work problem involving commitments and so forth, and it just so happens that the VRF (verifiable random function) is a really good one for a protocol that has adaptive security in a semi-synchronous network. What that means is that it's a protocol where you know after the fact, but you can't predict it beforehand. It's a protocol where your network conditions are suboptimal.

So in an optimal network, you're like the Googleplex^[361] and your local network and all the networks are connected to each other, you own those computers, you're using high-quality fiber to connect them. They're not going to go down, that's not how it works. You're in Costa Rica, what if there's a hurricane? I'm here in Colorado, what if there is a snowstorm? Cables get cut;

you have to go through seldom-used backend things. So networks are very finicky in that respect. So all the time, you have people who have high latency, packets get dropped, EMI (electromagnetic interference) comes in and distorts and turns bits around. So fault tolerance, the ability to handle an adaptive network is very important.

The problem is that with consensus protocols, when you start introducing semi synchrony and asynchrony, they don't tend to work. In fact, we've had things like the FLP impossibility theorem^[362] that make predictions about what is your capability in a truly asynchronous sense, in a network? So your randomness, that you generate, can't be reliant on synchronization as well. So it has to be deterministic and survive bad network conditions and adversarial connections.

So an example of a protocol is one that Intel came up with that only runs on trusted hardware. So it's trivial for any person to break if you don't have trusted hardware. So there's something called proof-of-elapsed-time^[363] (poet) that's part of the Hyperledger Sawtooth project. It's Intel's contribution to enterprise blockchain and basically how it works is you have a random number generator, and everybody gets together and they run random numbers. Whoever has the lowest number wins. Now if that protocol wasn't running on trusted hardware, you could guarantee you always win. Why? Because you could just set your random number generator to always return the minimum value, right? So that's not byzantine resistant. But because it's running on SGX,^[364] you can't manipulate the hardware to change the code. So that's why Intel gets away with it and it's a super-efficient protocol.

So the operating environment has a lot to do as well with randomness and trust and surety. It's a big topic and it's one that cryptographers have really fallen in love with, and the math there is quite elegant and there's a lot of beautiful things about it.

Fees on Cardano

Cardano has a transaction fee scheme that covers the cost of transaction processing and long-term storage.

Fees are not paid directly to the block maker in the Cardano ecosystem, which makes it unique. They are instead pooled and given to all pools that produced blocks during an epoch. There are no costs for the memory cost of keeping track of the accumulated chain state, specifically UTXO.

Halting economic attacks

The Shelley hard fork changed the Cardano blockchain from federated to entirely decentralized, thus increasing the incentive for bad actors to carry out economic attacks.

When the expenses paid by the operators of a system are not compensated by fees imposed on the system's users, an economic attack could occur. These conditions enable users to impose charges on operators without incurring the whole cost themselves, possibly resulting in a significant decline in operator involvement and, eventually, the system's collapse.

To avoid a scenario like this, it's critical to handle both the current unaccounted operator costs as well as the additional expenses.

Cardano's fee structure is straightforward.

The structure of fees is based on two constants (a and b).

- a/b are protocol parameters, and the method for determining minimum fees for a transaction (tx) is $a * \text{size(tx)} + b$
- size(tx) is the size of the transaction in bytes.

Protocol parameters

Cardano's update system may adjust protocol settings to respond and adapt to changes in transaction volume, hardware pricing, and ada valuation. Changing these settings is considered a hard fork since it affects which transactions the system accepts.

Parameter a

The transaction cost is dependent on the transaction size, as indicated by parameter a. Larger transactions require more resources to store and complete a transaction.

Parameter b

Regardless of the magnitude of the transaction, the value of b is the fee that must be paid. The purpose of this option is to avoid Distributed Denial-of-Service (DDoS) attacks. b makes such attacks extremely costly and removes the chance of an attacker flooding the system with millions of small transactions.

Parameter x

x represents the size in bytes of the transaction

From Twitter Space, April 18, 2022, 'Sunday Chat with Charles' **Re: Rewards going down, compensated by Transaction fees.** [\[365\]](#)

Well there's a formal curve in the specification, so if you look at the inflation, it's over a 140 year period, I think, so it goes down. But it's bounded and there's precise formulas for how that works. It's unlike Bitcoin, which has a step function which reduces every four years by half. This is a continuous emission decline, so it's a nice gradual monotonically decreasing curve that's quite smooth.

Now Cardano is unique, unlike Bitcoin, where sidechains are going to really change things. So what people don't seem to understand is that when a sidechain comes out, the sidechain is going to do its quorum sampling from stake pool operators. And when you mine that sidechain, you have to pay a block reward

to get those stake pool operators interested in it, but then that gets paid to the operators and to the delegators, just like ada rewards are.

So as a sidechain ecosystem starts building up, and we have dozens and eventually hundreds of sidechains, that means when you hold ada, in addition to getting ada rewards, you'll also get tokens from all the sidechains that are supported. So that plus transaction fees is really going to change the calculus. The other thing is that ada is a very volatile asset. So yeah, block rewards are worth something, but you know, ada was \$3 less than seven months ago. It could be \$5 in seven months. It could be \$0.05 in seven months. So percentages certainly matter, but the real value does as well. And there's some elasticity there. So I think the introduction of sidechains increases the transaction volume, and then also the volatility of the price of the underlying asset is going to really be a game changer for the return for holding in that respect, and this is what makes it fun.

You know, the other thing is multi-resource consensus is going to come at some point. It's one of our proposals for the long-term road map, and there, you'll have different ways of creating resources for consensus, and those could either be directly monetized with ada or they could be monetized with a different asset. So there's a lot there. That said, ada is a deflationary asset. Bitcoin Maxis (maximalists) seem to hate us, but we actually have the same monetary policy in that respect.

Fixed supply 45 billion, we're gradually earning our way up to it and it's monotonically decreasing inflation. So it's a deflationary asset, at its core, and that's one of the reasons why a lot of people like ada. But there's going to be a whole ecosystem of tokens, a constellation of them, and lots of utility and things to do. DeFi also changes the equation as well, because you can use your ada and DeFi at the same time, so you can also augment your yields to offset the decline in yields. So it just basically comes down to what your risk profile is from that respect.

November 18, 2020. Re: Bitcoin maximalism. CH^[366]

So first off let's be clear about something, there's nothing magical or special about Bitcoin. It has great security properties and for its design, it's certainly a colossal system and there's a lot of faith in it because the cost of attacking the system is quite high, but through innovations and improvements in cryptography and social structures, we can accommodate the same security properties at potentially a significantly lower cost, and in a significantly more scalable system. That's the point of science, we have old ciphers like DES,^[367] they've been superseded by AES so you don't just say, 'hey let's do more of the old and that somehow is better than these new ciphers.'

Similarly we have old consensus algorithms like proof of work and proof of stake which certainly had to go through a lot of significant scientific rigor and analysis to get to a point but now it's a done deal. There's Algorand, there's Tezos... there's what we've done with Ouroboros. There are protocols like Snowwhite, there's Polkadots nominated proof of stake, there's what Ethereum is doing with Eth2 (Ethereum 2.0) and all of these approaches have undergone enormous public engineering, infosec and academic scrutiny over a period of more than 6 years.

...and the trade-off here is that because we can now create a synthetic resource instead of an actual resource. You don't have to use all the energy of a country to be able to build a ledger. You just use like 10 kilowatts of power, 20 kilowatts of power ... the system runs and that's just one dimension of it. There are dozens of other design dimensions that exist and that you can improve things from recursive SNARKS and roll-ups, to better signature schemes, a lot of threshold signatures ...to more programmability at the base ledger.

Now Bitcoin doesn't incorporate any of this. It's the first mover and therefore it's the least sophisticated of all cryptocurrencies

by design and its appeal is that it's simple, and its appeal is that it's durable and reliable, and for a whole class of applications where simplicity, reliability and utmost confidence is required, like digital gold.

It makes a lot of sense if you want to build DApps or get into the DeFi space, if you want to do a whole litany of other things, then it makes a lot more sense to use a different system. In many cases there are permissioned systems that make sense, like for example when you're dealing with closed supply chains, but you need audibility in those supply chains and the people within the chains don't trust each other.

That's where a federated blockchain makes sense. It's funny when you see these maximalists come around and say 'oh that's all just mickey mouse, use a database'... you can't use a database because you have 12 people, 12 unique companies that don't trust each other. So which one of them is going to own the database? 'oh we have to federate access to the database', well that's what a permissioned ledger is all about you dummy.

You see a lot of these say because we do a lot of business with supply chain management and these types of things and you also have varying levels of privacy, where one group will have audit access to the ledger but the other groups you have, for commercial reasons, to restrict their view of it. Like for example, price transparency when you have many vendors competing, you don't necessarily want the vendors to see what the other vendors are charging or bidding, or what they had to pay to access the supply chain.

..but the audit and oversight people need to see all of these things, and be able to put them together for accounting purposes or tax purposes. It's really hard to do that in a permissionless system, where everybody is equal. So it's just a situation using the right tool for the right job and one of the things we do as a company is we try to sort out fact from fiction

and we start with basic science and we write papers about that like the GKL model, where we built a notion of a secure blockchain. We say ‘this is what Bitcoin does and properties of blockchain should have...’, and then we do very specific protocols for very specific use cases, whether they be voting, or a new programming language for financial contracts, or a SNARK for user updatable privacy or these types of things.

We do that stuff and then by doing the basic science we at least know what the trade-offs are and what you can do and what you can’t do with these systems.... and then based upon your needs, we can make recommendations of what type of system to use. Now systems like Cardano, for example, are kind of the ‘goldilocks’ of our research where what we did is we took the best case of each of these trade-offs and we stitched them together and we said, ‘a system built like this should have a minimal set of trade-offs and still benefit from a lot of the lessons and advancements that the space, as a whole, has made and be maximally useful to the largest group of businesses and consumers that exist, but you certainly can build different systems with different trade-off profiles that are highly optimized for certain use cases.

...and that’s what (Hyperledger) Fabric does and (Hyperledger) Sawtooth does, and these other systems so it’s a very nuanced conversation and I think maximalism is a cult, and the people who subscribe to it, they’re like people who say the earth is 10 thousand years old and Jesus is going to come tomorrow on a dinosaur.

You get adoption in baby steps, and this sort of notion that one blockchain is going to solve all those problems, it seems very short-sighted to me.... and that’s always been the point, it’s like any piece of technology, you have graph databases, NoSQL databases... you have Java versus Haskell versus Prolog. I mean every one of these are tools and they have their benefits and their drawbacks.. and what you have to be asking is ‘what

problem do I want to solve?’ That’s what you have to be asking and then you work your way backwards to what makes sense from a technology perspective. What maximalists do is say, ‘well if this doesn’t solve your problem, shut up it’s not a problem, or make your problem fit our solution’... which is insane, it’s absolutely insane.

Further Reading

You can read in much more detail about topics like Multiplexing[\[368\]](#) and Connection Management in *About the Cardano Network*[\[369\]](#) and the Network protocol design overview[\[370\]](#) in the Cardano Docs or Go to *Ouroboros Network* in the GitHub repo

Chapter 5: Smart Contracts (Goguen)

*'The most damaging phrase in the language is...
it's always been done this way'*

- Grace Hopper



Erik Voorhees ✅
@ErikVoorhees

...

Noise: Bitcoin doesn't have smart contracts

Noise: Bitcoin does have smart contracts

Signal: Bitcoin has some smart contract ability, but it's far more limited than other protocols such as Ethereum.

Signal: Ethereum has greater complexity & attack surface due to this.



Charles Hoskinson ✅
@IOHK_Charles

...

Signal: Cardano's EUTXO and Plutus have the expressiveness of Ethereum with the attack surface of Bitcoin.

Extended UTXO – the basis for Cardano's DeFi strategy

Blockchain networks are complicated data structures. Transactions traverse the chain on a regular basis, leaving digital fingerprints [\[371\]](#) that must be carefully tracked and managed to maintain the underlying ledger's integrity and trustworthiness. In the blockchain world, there are two types of accounting ledgers: UTXO-based blockchains (like Bitcoin) and Account/Balance chains (Ethereum, and others).

The accounting models of these two models vary in many ways. The Unspent Transaction Output (UTXO) model is used by Bitcoin, while the Account/Balance model is used by Ethereum.

Cardano aimed to create an Extended UTXO (EUTXO) accounting model by combining Bitcoin's UTXO model with Ethereum's capacity to handle smart contracts. The adoption of EUTXO makes it easier to integrate smart contracts into the Cardano network.

How does the accounting model work?

The analogy of a balance sheet is often used to explain the account model. A balance sheet is required by any commercial entity to maintain an accurate record of profit, loss, cash flow, and other factors. Companies can visualize their financial situation at any moment in time by keeping meticulous records of all this information. Another benefit of a company's accounting ledger is the ability to track the origins and ownership of funds. Blockchain networks also need an accounting model to establish who owns what currencies, monitor where those coins move, which ones are used up, and which ones are still accessible for spending.

Account/Balance model vs. UTXO model

Accountants used to maintain records of the transfer of funds in physical ledger books with handwritten entries. Electronic versions of the same thing are being used by businesses. To monitor provenance and ownership, blockchains employ transactions as records (much like entries in a ledger book). These transactions include a lot of information (where the coins came from, where they're going, and how much change is left over).

UTXO

An unspent transaction output (UTXO) is the term for the amount of digital currency that remains after a cryptocurrency transaction. The flow of assets is documented in a UTXO model as a directed acyclic graph^[372] with nodes representing transactions and edges representing transaction outputs, with each successive transaction consuming some UTXOs and adding new ones. Users' wallets

determine the users' balance by keeping track of a list of unspent outputs connected with all addresses held by the user.

In many respects, UTXO is identical to currency. 'Cash in cash out' is the commonly used analogy. If you pay a restaurant bill of €15. You forgot your credit card so pay in cash. You pay with a €20 note (input) and want to leave a €2 tip. The waitress puts €15 in the till (output 1) and gives you back a €2 coin (output 2) and a €1 coin (output 3). She puts the €2 tip (output 4) in the tip jar. Regardless, if you decide to leave a tip or not, or give exact change, the inputs and outputs must match.

If you have €100 in your cash register. This sum might be made up of a variety of different banknotes: four €20 notes and two €10 notes, eight €10 notes and four €5 notes, and so on. The sum (€100) stays the same regardless of the permutations. The same is true for UTXOs. Any balance you have in your blockchain wallet may be built up using a variety of UTXO combinations depending on prior transactions, but the total value stays the same. In other words, a wallet address's balance is the total of all unspent UTXOs from prior transactions.

Concept of 'change' in UTXO models

UTXOs introduce 'change,' much like currency transactions at a shop. You can't cut a €50 note into smaller pieces to pay for anything that costs €15, for example, when you take it out of your pocket. You must hand over the whole €50 money and the clerk will give you your change. The same is true for UTXOs. A UTXO cannot be 'split' into smaller pieces. UTXOs are used in their entirety, with the remainder being returned to your wallet's address in the form of a smaller UTXO.

UTXO advantages

One can derive reliable information regarding the blockchain's use and financial activities by examining and tracking the size, age, and

number of UTXOs being moved around.

Other benefits of UTXO models may be found like better scalability, especially for state channels and sharding solutions. On privacy, UTXO makes it difficult for a malicious actor to link transactions. A user can constantly change their receiving address, with new addresses having no previous owner. Also, since each UTXO may only be consumed once and in its whole, the transaction logic is streamlined, making transaction verification considerably easier.

To summarize UTXO:

- A UTXO is the result of a prior transaction that may be spent in the future
- There are no accounts in UTXO chains. Instead, coins are kept as a list of UTXOs, and transactions are made by consuming existing UTXOs and creating new ones in their place
- Balance is the total number of UTXOs possessed by a certain address (UTXOs are used whole).

The Account/Balance model is a method for keeping track of, and balancing, your finances. An account (which may be managed by a private key or a smart contract) is used to keep a coin balance in blockchain models that employ an Account/Balance accounting model, as the name implies. Assets are represented as balances inside users' accounts in this architecture, and the balances are saved as a global state of accounts maintained by each node and updated with each transaction.

Account/Balance chains (such as Ethereum) function similarly to regular bank accounts in many ways. When coins are deposited, the wallet's balance rises, and when coins are moved elsewhere, the wallet's balance falls. The key distinction is that, unlike UTXOs, you may only utilize a portion of your balance. So, if you have 50 ETH in your account, you may transmit a piece of it to someone else (for example, 15 ETH). As a consequence, your account balance will be 35 ETH, and the address to which you delivered the coins will be

increased by 15 ETH. In Account/Balance accounting models, the idea of change does not apply as it does in UTXO accounting models.

Transaction sizes are generally smaller with the account model, compared to UTXO, as only basic data regarding sender, receiver, amount and signatures are captured. Onboarding new nodes is therefore easier as there is less data to sync.

To summarize the Account/Balance concept:

- This accounting approach works similarly to how a bank does
- Users have accounts that keep their coin balances
- Partial balances may be spent
- The idea of change is irrelevant
- Account models are suited for Layer 2 deployments as transaction size/metadata is light.

Transactions Outputs and Inputs

The word ‘transaction’ frequently conjures up images of money. While this definition applies to Bitcoin (since the Bitcoin is used to transfer payments between peers), many other blockchains (like Cardano) are more flexible. The word ‘transaction’ is significantly more complicated in these circumstances. Transactions may be thought of as value transfers.

Each transaction in a blockchain system may have one or more inputs and one or more outputs. If one wishes to grasp how a transaction works and how it connects to UTXO, one must first comprehend the notion of inputs and outputs. Consider a transaction to be the operation that unlocks past outputs while also creating new ones.

Transaction output

An address (which you might view as a lock) and a value are included in the transaction output.^[373] In line with this analogy, the

address's signature is the key that unlocks the output. An output may be used as an input after it has been unlocked. New transactions use previous transactions' outputs while also producing new outputs that may be consumed by subsequent transactions. Each UTXO may only be used once, and it must be consumed in its entirety. Only one input may spend each output.

Transaction input

The output of a preceding transaction is referred to as a transaction input. A pointer and a cryptographic signature that serves as the unlocking key are included in transaction inputs. The key unlocks a prior transaction output, and the pointer refers back to it. The blockchain labels an unlocked output as 'spent' when it is unlocked by an input. New inputs may then refer to new outputs produced by a given transaction, and the chain continues. The UTXOs are the new outputs (which have not yet been unlocked, i.e., spent). Unspent outputs are just that: outputs that haven't been used yet.

How UTXO works

Transactions consume unspent outputs from earlier transactions and create fresh outputs that may be used as inputs for future transactions under a UTXO accounting model.

These UTXOs are managed by the users' wallets, which also start transactions using the user's UTXOs. At all times, every blockchain node keeps track of a subset of all UTXOs. This is called the UTXO set. In technical jargon, this is the chainstate, which is kept in each node's data directory. The chainstate is changed whenever a new block is added to the chain. The list of recent transactions is included in this new block (including of course a record of spent UTXOs, and new ones created since the chainstate was last updated). Every node keeps a duplicate of the chainstate.

Why Cardano chose EUTXO

Cardano's UTXO accounting mechanism is not the same as Bitcoin's, since Cardano is meant to do more than only manage payments. The necessity for increased programming expressiveness in the Alonzo era's smart contracts feature required a unique ('Extended') approach.

The 'basic' UTXO concept has a restricted programmability expressiveness. With the establishment of an account-based ledger and related contract accounts, Ethereum's Account/Balance accounting model addresses this particular challenge. However, the contract code's semantics grew significantly more sophisticated as a result, which had the unintended consequence of compelling contract writers to fully comprehend the semantics to prevent the insertion of potentially extremely expensive flaws in the code.

An 'extended' UTXO solution would need the inclusion of two features that the current UTXO model lacks:

1. To be able to keep the contract in its current state.
2. To be able to ensure that the same contract code is used throughout the transaction sequence. This is what is referred to as continuity.

The EUTXO model has the advantage of being able to forecast the fees necessary for a successful transaction before it is processed. This is a characteristic that account-based models do not have.

Why is it called EUTXO?

UTXO is 'extended' by allowing for extra 'locks' and 'keys' controlling under which conditions an output may be unlocked for consumption by a transaction (in addition to value), and by allowing for custom data to be added to outputs. In other words, rather than having public keys (hashes) for locks and accompanying signatures serve as 'keys,' EUTXO allows arbitrary logic to be implemented using scripts. This arbitrary logic examines the transaction and data to determine whether or not the transaction may use an input.

What's so great about EUTXO?

Cardano's ledger architecture extends on the UTXO model to accommodate multi-assets and smart contracts while maintaining the UTXO model's benefits. Groundbreaking research allows Cardano to do functions that no other UTXO ledger can, making it a unique contender in the blockchain space.

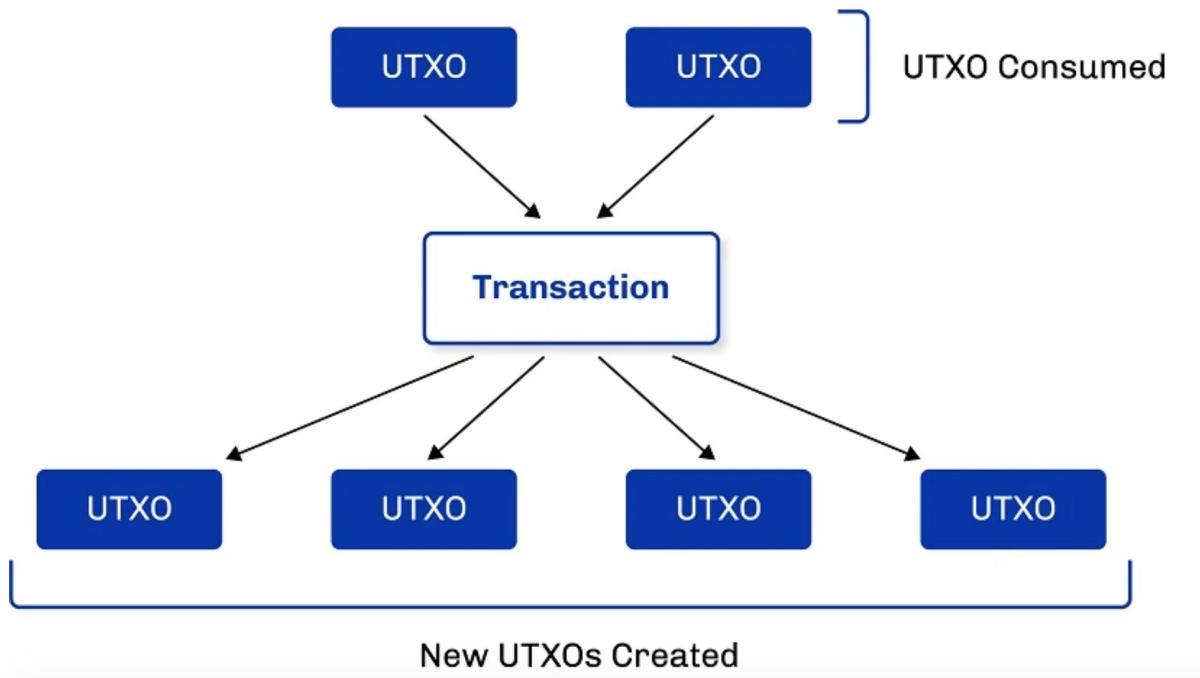


Figure 17. UTXO

The extended UTXO model

The UTXO model is extended in two ways by the EUTXO model:

1. The lock-and-key analogy is used to extend the idea of 'address.' Addresses in the EUTXO model may include arbitrary logic in the form of scripts instead of confining locks to public keys and keys to signatures. When a node verifies a

transaction, for example, it evaluates whether the transaction may utilize a certain output as an input. If the output can be used as an input, the transaction will look up the script supplied by the output's address and run it.

2. The second distinction between UTXO and EUTXO is that, in addition to an address and a value, outputs may contain (virtually) any data. By enabling scripts to carry state, they become considerably more powerful.

Furthermore, EUTXO expands on the UTXO concept by enabling output addresses to include complicated logic to determine which transactions are allowed to unlock them, as well as by allowing custom data to be added to all outputs. When verifying an address, [\[374\]](#) the script will look at the data carried by the output, [\[375\]](#) the transaction being checked, and some extra data known as redeemers [\[376\]](#) that the transaction supplies for each input. The script [\[377\]](#) provides enough context to deliver a 'yes' or 'no' response in what may be very complicated circumstances and use cases by uncovering all of this information. [\[378\]](#)

EUTXO allows for arbitrary logic to be expressed in the form of scripts. This arbitrary logic examines the transaction and data to determine whether or not the transaction may use an input.

The graph structure of the UTXO paradigm differs significantly from the account-based model employed by several current smart-contract enabled blockchains. As a consequence, design paradigms for DApps on account-based blockchains do not easily adapt to Cardano. Because the underlying representation of the data is different, new design patterns are required.

The per-branches architecture of the UTXO (Bitcoin) model is carried over to EUTXO, where one branch is defined as a series of transactions requiring a succession of validations. Building DApps and other solutions with numerous UTXOs is vital for splitting the functionality over various branches and enforcing additional

parallelism.^[379] This has scalability advantages, just as creating Bitcoin services necessitates breaking one wallet into sub wallets.

EUTXO Advantages

Compared to other accounting models, the EUTXO model has a number of distinct benefits. The transaction's success or failure is solely determined by the transaction and its inputs, not by anything else on the blockchain. As a result, before a transaction is posted to the blockchain, the legitimacy of the transaction may be confirmed off-chain. A transaction may still fail if another transaction consumes an input that the transaction is expecting at the same time, but if all inputs are still available, the transaction will succeed.

This is in contrast to an account-based approach (such as Ethereum), which allows a transaction to fail in the middle of its execution. In EUTXO,^[380] this will never happen. Also, transaction execution costs may be calculated off-chain before transmission, which is something that Ethereum does not allow.

Cardano's EUTXO paradigm provides a safe and flexible environment for processing many operations without causing system issues. This architecture provides superior scalability and privacy, as well as more straightforward transaction logic, since each UTXO can only be used once and in its entirety, making transaction verification considerably easier.

A significant degree of parallelism is feasible due to the 'local' nature of transaction validation. In theory, a node might verify transactions in parallel if they did not attempt to consume the same input. This is beneficial for both efficiency and logic, since it simplifies the study of various outcomes and demonstrates that 'nothing untoward' can occur. This functionality was enhanced with the Vasil hard fork, with multiple DApps now able to access the same input. More about the Vasil update later. You may read more about the EUTXO model in IOG's blog.

The EUTXO model has the advantage of being able to forecast the fees necessary for a successful transaction before it is posted. This is a feature that account-based models do not have. Account-based blockchains, such as Ethereum, are indeterministic, meaning the impact of a transaction on the chain cannot be guaranteed. This ambiguity raises the danger of financial loss, unexpectedly expensive costs, and a broader attack vector for hackers to exploit.

To recap, EUTXO provides increased security, predictability in smart contract execution costs (avoiding unpleasant shocks), and more powerful parallelization.

The DeFi Revolution

The number of ada users and software developers working on Cardano is steadily increasing. Sites like *CardanoCube*, *Built on Cardano*, *Building On Cardano*, and *Essential Cardano* are busy mapping a fascinating ecosystem with projects currently in final testing and beginning to deploy. As Charles Hoskinson observed in his recent AMA^[381] (ask-me-anything), there was so much going on, it's hard to keep up.

Cardano was designed to be a safe and reliable platform for developing blockchain-based assets, services, and systems. Decentralized finance, or DeFi, has risen in popularity in recent years, introducing a slew of new financial products ranging from practical to dubious. DeFi's ultimate purpose, as the market develops, is to assist people and businesses in conducting financial transactions without the need of a central, costly intermediary such as a bank, or in achieving greater returns on their assets in an era of inflation and negative interest rates.

Cardano has extended this further. The goal is to provide low-cost banking and insurance services to the millions of individuals throughout the globe who do not have access to such services. This would aid in the dismantling of barriers between developed and poor

countries. This concept is dubbed ‘RealFi’ by IOG.^[382]

Despite the spike in Cardano’s popularity, general blockchain awareness and acceptance remain low. Not least, due to the mound of jargon that any crypto-curious individual must wade through. DeFi, RealFi, DApp, DEX, liquidity, and other terms are synonymous with the most recent blockchain products.

Why do we need DeFi?

How can we utilize blockchain in everyday life? Why is it important? Blockchain is all about trading or exchanging funds under certain circumstances for an almost limitless variety of uses. Blockchain technology is already used by companies across all verticals.

	Traditional Finance	DeFi
Custody	Held by institution or custody provider	Held directly by users in non-custodial accounts or via smart contract
Unit of Account	Fiat Currency	Denominated in digital asset or stable coin
Execution	Facilitated via intermediaries	Facilitated via smart contract
Settlement	-3-5 business days depending on transaction, during M-F business hours.	Seconds to minutes depending on blockchain, 24/7 operating times.
Clearing	Facilitated via clearinghouses	Facilitated via blockchain transaction
Governance	Specified by exchanges & regulators	Governed by the protocol developers & users
Auditability	Authorized third-party audits	Open source code & public ledger, can be audited by anyone
Collateral	Transactions may involve no collateral, intermediates take on risk	Over-collateral generally required.
Risks	Vulnerable to hacks and data breaches	Vulnerable to hacks and data breaches of smart contracts

Figure 18. Traditional Finance v DeFi. Courtesy of CoinYuppie^[383]

What is DeFi?

Decentralized finance, often known as DeFi, is a blockchain-based type of finance that serves the same functions as conventional finance. You may use cryptocurrencies to make and receive payments, pay for goods and services, and invest in projects rather than bonds or equities. DeFi, on the other hand, does not rely on a middleman and instead relies on smart contracts to settle transactions equitably. RealFi is created by combining an

identification layer, such as Atala PRISM,^[384] with a ‘bridge’ to the actual world.

Means of exchange

We traditionally pay for goods and services with money. The most common form of this medium of trade is coins or banknotes issued by central banks. The word fiat has become common among cryptocurrency users to denote real-world money. Fiat money includes the US dollar, the British pound, and the Japanese yen. Since governments no longer have to back their currency with gold, this term has been adopted. Instead, they designate their currencies to be legal tender by a formal decree known as a fiat.

On the blockchain, crypto assets are used instead of fiat currency.

How it all works together

Before we get into the nitty gritty of DeFi nomenclature, let’s have a look at how it all works. Smart contracts are the driving force behind security and fair agreements. Assume you’ve downloaded a DeFi app and want to lend Bob 10 ada. We need to know that Bob will pay it back, and we’d want to be able to collect some interest if he does so later than expected. Traditionally, users sign contracts that include such terms. This is done on the blockchain as well but using smart contracts.

Smart contract: a code-based automatic digital agreement that monitors, validates, and executes the legally binding portions of a trade between two or more parties. When preset criteria are satisfied, the smart contract algorithm automatically executes the contract steps.

Smart contracts do not access particular data on their own. For example, let’s assume we agree with Bob that he will repay us by February 23rd. The date, whether Bob completed a transaction, and whether the supplied amount equals the amount due are all required

for a smart contract to execute. Smart contracts make use of oracles to do this.

An Oracle is a tool for interacting with real-world data. Oracles link to trustworthy external data sources, allowing smart contracts to run by reference information like accurate time, weather, election outcomes, sports statistics, and cryptocurrency markets. Oracles guarantee that data is accurate, timely, and unaltered.

With Cardano, users can work with **Plutus** or **Marlowe** contracts:

- Plutus is a suite of programming tools for creating Cardano smart contracts. Plutus Core and the Plutus programming language, which is based on Haskell, have been running on Cardano since September 2021. The Plutus Playground^[385] allows developers to test their code before it's deployed on the main chain
- Marlowe is a programming language created specifically for the creation of financial smart contracts. It is restricted to financial applications and is intended for financial specialists rather than programmers. Users may also leverage the [Marlowe Playground](#) via a web browser to create, amend, simulate, and analyze Marlowe contracts. There are plans to deploy Marlowe on Cardano later in 2022.

Broader DeFi ecosystem

Users leverage a variety of DeFi systems and apps for a variety of reasons. For example, asset management solutions (or simply wallets) allow customers to store, transmit, and receive cryptocurrencies. There is a plethora of decentralized apps (DApps) available:

With the fast-growing Cardano ecosystem, more and more DeFi goods are coming to Cardano. For their financial requirements, users may now utilize new DApps and platforms. As a result, IOG is

focusing on the following to guarantee that users and the developer community can provide and consume high-quality products:

- The DApp Store is a user-friendly store where all Cardano DApps may be found. It'll also be a site where individuals with less blockchain understanding may learn about how the technology might help them
- DApp certification: certification and assurance ensure items satisfy quality standards. While certification is optional (Cardano is open source and decentralized), it helps both developers and consumers since it contains security checks that aid in smart contract audits. There are three certification levels, each of which is useful in conjunction with the others.

DeFi systems and DApps are mostly used for financial transactions. These may be used for investing, lending, and borrowing in addition to funds transfer. In reality, on the blockchain, users may borrow crypto without paying interest:

- Flash loan: operates as a quick loan with no collateral (funds required to secure a loan of other cryptocurrencies or tokens) or know-your-customer (KYC) checks. The flash loan, on the other hand, requires payback inside the same block that it was provided to the borrower. The original transaction is rejected if the loan is not repaid, and the lender keeps the funds.

Let's have a look at a few more of the most often used phrases in DeFi:

Exchange: a cryptocurrency exchange that allows users to purchase and sell cryptocurrency. There are two different kinds of exchanges. A CEX (centralized exchange) is run by a distinct company or structure that is governed by rules and regulations. Users may purchase and sell their assets in a safe, peer-to-peer manner on a DEX (decentralized exchange), which has no middleman.

Another phrase you'll come across is liquidity. It tracks the amount of circulating supply and trade activities on a particular DEX, CEX, or another network. Users' trade demands need the circulation of supplies. Alice, for example, wants to sell some bitcoins she possesses and replace them with ada and tokens for her new retail app.

Bitcoin trading is quite popular so she will have no problems there. If the exchange she chooses supports ada, she'll most likely purchase it as well. But what if there's not enough of the tokens she wants available? For example, what if she needs 50 tokens for her app but there's only 15 available? This is what liquidity refers to: having a sufficient quantity of coins or tokens to meet the needs of users.

Liquidity encompasses the following actions and concepts that go along with them:

- **Liquidity mining** refers to the practice of producing or adding new currencies or tokens to meet transaction demand. Liquidity miners (providers) are often compensated in order to sustain the user base and create liquidity pools. Yield farming is another name for liquidity mining
- **Liquidity pools:** a collection of deposited cryptocurrencies that serves as a source of liquidity for the network when the currencies are in high demand
- **AMM** (automated market maker): a pool of cryptocurrency that acts as a liquidity provider between 'trading pairs.' A trading pair is a match between two parties, such as Fred who wants to sell his bitcoin and Barney who wants to purchase it. AMMs are decentralized and rely on the liquidity that their users provide.

Decentralized exchanges are more than just handy trading platforms for cryptocurrencies. They may also be used to generate revenue.

Some key terms:

- **Return on investment (ROI)**: the profit or loss on an investment, usually stated in percentages
- **Yield farming** is sometimes known as liquidity mining. Farming is a term used to describe a process in which rewards are exchanged for making funds available
- **Yield**: the amount of rewards earned by staking crypto or mining liquidity
- **Leverage**: the act of borrowing with the expectation of making a profit higher than the interest paid.

Ada holders may make a passive income from their ada in a secure manner:

Staking and delegating on Cardano: each ada holder has a stake that is proportional to the quantity of ada they hold. A tech-savvy individual may create a stake pool and operate it to assist in the verification of Cardano transactions in exchange for rewards. To get a portion of these rewards, anybody may delegate their ada to a stake pool. There is no danger with this as no ada leaves your wallet. Ada may be delegated, or spent, at any point from your wallet.

August 30, 2020, DeFi ‘network effect’. CH:[\[386\]](#)

The reality is that the first mover advantage is actually a disadvantage in DeFi. Those network effects were ephemeral and often covered with mistakes, scars and explosions.

You actually want to be in the imitator, the second mover category for DeFi, and I think we'll have a lot more luck than the first movers did in the space and there'll be a mass exodus because those first mover architectures and designs are just too inflexible and Cardano is much better suited as a platform.

DeFi vs RealFi

IOG can provide value and opportunity for individuals all around the world by merging digital identification with Cardano. When it comes to the evolution of blockchain, all the hype has been around decentralized finance. DeFi makes use of smart contracts on the blockchain to provide everybody with access to banking via a public, decentralized ledger. DeFi has attracted a new generation of consumers by eliminating the middlemen, bankers, and brokers, and the industry has grown at a breakneck pace, currently worth an estimated over \$75bn.^[387]

DeFi is a financial network that is available to everyone. To transmit, borrow, or lend money, people do not need to go via a private corporation like PayPal, Western Union, or a bank. Instead, this is done on a peer-to-peer basis, with blockchain serving as the underlying ledger to support and facilitate the transaction.

The core premise of DeFi is solid. Typically, loans are completely, or over-collateralized because little (or nothing) is known about the borrower, and there is minimal recourse if the loan is not paid. Borrowing is often re-invested in further crypto prospects. Users engage in a peer-to-peer way, with no central governing authority, instead relying on smart contracts and blockchain-based systems' inherent transparency and immutability. Most of the standard regulatory restrictions on lending and borrowing do not apply in this manner, and costs are often substantially cheaper.

DeFi has emphasized the potential for blockchain to disrupt banking 'legacy' institutions and offer access to new consumers looking for higher returns and shifting funds around in developed economies. It has created a whole new financial paradigm, and the \$75 billion DeFi industry is anticipated to expand dramatically in the coming years as models improve.

However, although the DeFi era is spawning new markets and exciting new use cases, it is also highlighting the economic

difference between those who have easy access to financial services and those who do not.

DeFi for the masses

The goal of credit pricing is to analyze and minimize the risk of default. Traditional consumer finance and credit decreases risk by gaining a better knowledge of how borrowers act, such as how much they spend, how much they earn, and so on. This falls under the umbrella of KYC, Know Your Customer. DeFi takes a unique approach to risk management.

In first-world economies, a well-established credit rating system is essential for granting credit. In developing markets, though, it is much more important. In developing economies, banks often decline credit or loans because they lack sufficient information about the individual or entity seeking credit. Either the systems aren't advanced enough, or they don't exist at all. A credit score cannot be used to build a realistic financial picture.

However, by querying proxies tied to an identity, it is possible to build up a credit score. You may call utility providers to see whether the consumer has always paid their bills on time, or you could call a phone company to see how often the potential borrower bought credit for their phone. There is an identity out there; the challenge is tying data to it. After that, the data may be offered to a local bank, a microfinance project or a decentralized pool of funds contributed by Cardano community members all around the globe.

We've finally arrived at a stage where crypto technology can help us do this. Through an Atala PRISM DID, all relevant financial metadata may be kept and communicated in a reliable way. DeFi's monetary building blocks may be used to organize these loans and mitigate currency risk, while Cardano's scalable payment rails and other layer 2 solutions will enable frictionless money transfers throughout the globe.

Time to get RealFi

IOG announced two big blockchain partnerships in 2021. In collaboration with the Ethiopian Ministry of Education,^[388] they are developing a national attainment tracking system to validate grades, track school performance, and improve education throughout the country. Another partnership announced is with World Mobile^[389] who are using Cardano as part of implementing local mobile nodes in Africa (2021). They are also using balloons^[390] in Zanzibar (2022). World mobile has made rapid progress^[391] evolving from ‘smart cities’ to ‘smart countries’ and are now launching their ‘dynamic network technology’ to areas of the US that don’t have mobile coverage. Charles Hoskinson speaks more about the importance of the partnership in this update.^[392]

These kinds of transactions serve as a springboard for Cardano’s objective to establish RealFi: real finance targeted at those who actually need new methods to access finance, bringing the true value that DeFi frequently lacks. RealFi is a product ecosystem that eliminates friction between crypto liquidity and real-world economic activity to provide crypto investors with attractive returns and real-world consumers with lower-cost credit and financial services.

Cardano completes the financial jigsaw by unleashing genuine economic value in a transaction chain: personal identification. Everything revolves around one’s identity. A lot of potential and inclusion opens up once someone has an economic identity. Real opportunity comes from having access to key services that were previously unavailable. And there’s actual funds, like loans to start a company or keep one going.

In the sense that it may be used as a replacement for collateral, identity can become an asset. The primary concern of a lender is to guarantee that loans (plus any accumulated interest) are repaid. Collateralizing the loan is one method to enforce this, however if the lender has adequate and unambiguous information about a borrower

(for example, if they know the borrower is on a large salary or a long-term client), the lender may be willing to forego the collateral.

~~DeFi~~ RealFi for the masses

Microlending platforms like Kiva (kiva.org) provide a profitable business model that is well-suited to Africa's expanding economy. Small loans may be life-changing for farmers, entrepreneurs, and anybody with the will to create and flourish in this environment.

However, financial access is simply one aspect of a wider picture. People would still be at danger if they didn't have access to insurance, education, and health care. RealFi offers an alternative to this conundrum by combining the power of blockchain with a digital identification platform like Atala PRISM. Digital identity allows individuals to get access to services that allow them to compete on an equal footing with their counterparts in more developed regions of the globe, and not only financial services.

RealFi will usher in a new era of credit activity on the blockchain. Cardano 'Whales'^[393] presently own billions in ada and tokens, and many of them may soon be seeking other ways to earn money beyond staking. Cardano's potential and originality may be lit up by the tangibility of this real-world application of crypto, the distribution of real funds to real people. This is the real-world use of cryptocurrency that many people overlook. RealFi ushers in a new age of on-chain financing. Someone in London, for example, could be able to make an uncollateralized loan to a Kenyan enterprise if their identification has been verified. Charles Hoskinson often stated that his measure of success is if something like Kiva could run on Cardano^[394] as it would bookend his vision laid out in his Ted Talk^[395] in Bermuda in 2014.

To get started on this path, IOG has teamed with Pezesha (pezeshacom) to help small and medium-sized enterprises get short-term working capital loans. These loans have a 2% default rate, but owing to a lack of local liquidity, they are difficult to finance

in the Kenyan market. The idea is to provide easy, frictionless technologies that allow crypto holders to lend to real-world opportunities while getting repayments in cryptocurrency straight into their wallets.

RealFi is already happening

RealFi is the polar opposite of financial exclusion, ushering in a new age of financial and social inclusion throughout Africa and across the world. Cardano becomes a bastion of identity provision with RealFi, allowing individuals to assist themselves. The objective of RealFi is to create real financial value for real individuals, and this is what sets it apart from other blockchain platforms.

The initiatives in Ethiopia, Tanzania, and Kenya are only the beginning of a much longer path toward global justice and inclusion. The beginning of a campaign to remove marginalization of the poor while also providing attractive returns to cryptocurrency investors. RealFi, like DeFi, will be a product and technology ecosystem that reduces the friction between cryptocurrency liquidity and real-world economic possibilities. The aim is to shrink the globe by linking everyone to a global community of wealth and opportunity that is now available and welcome to them via RealFi.

In April 2022, Catalyst launched its incubator Ariob (ariob.io), in partnership with iceaddis, a pan-African business accelerator. Cardano's roots in Africa are deep as they showcased during their 'Africa Special' in 2021. Their partnership with the Ethiopian Ministry of Education^[396] to provide five million Ethiopian students with a means (Atala PRISM, atalaprism.io) to verify their academic credentials. IOG is also collaborating with World Mobile in Zanzibar to connect the unconnected. IOG's blog post^[397] describes how Ariob will build on this momentum with new projects joining all the time.

November 24, 2020. Re: motivation behind Cardano. CH:^[398]

You've got to have passion and you have to be willing to take the hits. I've been in this space for 8 years and I've seen everything. I've been at conferences where Onecoin and Bitconnect people have come up to me to try to pitch me these projects. I've heard everything and you just burn out listening to these schemes. Money cannot sustain you in this space, you get attacked viciously every day, on twitter, on reddit, on telegram, etc. You deal with assholes every day. There are setbacks every day, complications, research realities...the only way you can stay in it long term is that you need to have a mission, a long term goal. You have to go somewhere. You have to want to do something.

So why does Cardano exist? I did a TED talk in 2014 and I have not deviated since I did it. I said I care about economic identity. Every day we wake up, there's three billion people who don't have economic identity. They're unbanked, they're outside of the global economy. They get screwed...they pay 85% interest on loans. When their kids go to London and work as maids and wire money back, there's a 15% charge for that. When they get money, they can't hold on to it. They have no insurance, so when a disaster happens, they've nothing to cover it with. So one bad event, one monsoon, one hurricane...they're done. That's the reality for three billion people.

. . . So what's the solution? You can be a bleeding heart liberal and go around donating...telethons don't work. You need an economic solution and the only way to have such a solution is to give people economic identity. You have to give them their own identity, banking system, insurance and lending systems. What are we doing? We are giving people stablecoins, exchanges, the ability to securitize their business interests, peer-to-peer lending, the ability to quantify knowledge with oracles, new business models like decentralized media, decentralized content sharing, new venture capital models... that is what our industry is about at its core.

'Neither smart nor a contract'

While Vitalik Buterin and others^[399] have opined that smart contracts are neither smart nor a contract, let's not be pedantic for the sake of brevity. A smart contract is a code-based automatic digital agreement that records, validates, and executes the contract's binding transactions between numerous participants. When preset criteria are satisfied, the smart contract code automatically executes the contract's transactions. A smart contract is just a brief program whose inputs and outputs are blockchain transactions.



vitalik.eth ✅
@VitalikButerin

Replying to [@CleanApp](#) [@cryptoecongames](#) and 4 others

To be clear, at this point I quite regret adopting the term "smart contracts". I should have called them something more boring and technical, perhaps something like "persistent scripts".

6:21 PM · Oct 13, 2018 · Twitter Web Client

Smart contracts are self-executing and dependable, requiring no third-party intervention or presence. The smart contract code is kept on a decentralized blockchain network and spread throughout it, making it transparent and irrevocable.

Smart contracts are immutable because they cannot be modified, they are distributable and tamper-proof, they are quick and cost efficient because there is no middleman, saving money and time, and they are secure because they are encrypted.

Cardano enabled smart contracts with the Goguen hard fork in 2021, utilizing programming languages such as:

- Plutus is a platform for developing and executing smart contracts. Plutus contracts are made up of on-chain (code that runs on the blockchain) and off-chain (code that runs on the user's workstation) components. Plutus is a secure, full-stack

programming environment based on Haskell, the functional programming language.

- Marlowe — a domain-specific language (DSL) for defining and executing financial contracts that allows for both visual and conventional code construction. It may be used by financial institutions to create and deploy unique instruments for their customers and clients. The Marlowe language is now integrated in both JavaScript and Haskell, giving developers a variety of editors to choose from, depending on their preferences and expertise.
- Glow is a domain specific language (DSL) for creating blockchain-based decentralized apps (DApps). Users may create secure DApps using Glow, guaranteeing that smart contracts function securely in a hostile environment.

Why smart contracts?

Intermediaries are engaged in many commercial procedures that include the exchange of value (such as money, property, or shares) to ensure that the conditions of the agreements are comprehensive, clear, and met before the exchange may take place. The cost of a transaction is increased by these middlemen. Smart contracts have evolved as a technique of decreasing the time, third-party participation, and expense of reliably executing an agreement.

Smart contracts are software programs that are stored on the blockchain in an immutable format. They're run on virtual computers, and their data is stored in the same immutable architecture. Businesses aiming to improve their operations might profit greatly from smart contracts. Many sectors, including automotive, supply chain, real estate, and healthcare, are investing in research to see how this technology might help them compete more effectively.

Metadata on Cardano

The need for metadata

Remember, money is a social construct. It is only valuable if people acknowledge and believe in it. Most transactions have a context that needs to be captured in metadata. Bitcoin and its contemporaries have abandoned the requirement for reliable identities, information, and reputation in commercial transactions in their quest to anonymize and disintermediate central players. Adopting centralized methods to add this data loses the auditability, global availability, and immutability that is the whole idea of using a blockchain.

Transactional information is abundant in legacy financial systems such as those based on SWIFT. Regulation often involves attribution of individuals engaged, compliance information, reporting suspicious behavior, and other records and activities in addition to knowing how much value transferred between accounts. The metadata might be more essential than the transaction in certain instances. The metadata is the story of the transaction.

As a result, it appears logical to conclude that tampering with metadata may be just as dangerous as counterfeiting money or changing transaction history. Making no allowances for actors who want to freely participate in these domains seems to be detrimental to mainstream acceptance and consumer protection.

Adding metadata to transactions was the first step in preparing Cardano for DeFi. Cardano evolved into a smart contract platform with the launch of Goguen. This began by including metadata — information about the data being processed — in transactions, which was introduced to the blockchain. Cardano has evolved from a transaction-focused platform to a utility platform available to partnerships, businesses, and commercial applications that may be used for the complex processes that will characterize the decentralized financial future (DeFi).

With the growing number of cryptocurrency transactions, having access to immutable data that cannot be changed is critical,

particularly for applications like wealth management. The Cardano blockchain keeps permanent records of completed transactions, guaranteeing a transparent and auditable history of financial activity. However, to give financial operations greater responsibility and visibility, context must be given to these transactions. Facts such as sender and recipient information, processing circumstances, and processing time are examples of additional information. This is accomplished by including transaction metadata.

Data about data

The term ‘metadata’ refers to information about information. It defines the context, content, and structure of records, in other words. Metadata promotes confidence through permanent data attestation, since blockchain technology offers a transparent ledger for preserving information immutably and securely.

Whether it’s a purchase for a product or service or a money transfer to a family member, all transactions have a definite purpose. When making an online purchase, for example, there is a lot of information that can be gathered about the transaction. Metadata may help convey the tale of a product purchase by revealing information about the customer and seller, the date of the transaction, the product maker, and the supply circumstances. All of these details, as well as the wealth transaction, are necessary to keep.

March 31, 2019. On metadata. CH:[\[400\]](#)

We are exploring contingent settlement ...so basically the idea is that you have Alice and Bob and under a push transaction system, Bob pushes a transaction to a known address of Alice... Now Alice can be a pseudonym or anonymous... it can just be numbers but it's some sort of payment address ...so Bob just pushes it in ...now here's the thing, Alice did not consent to that that was just received, the payment ...furthermore Bob had to pay the transaction fee to push the value to Alice ...so when you take a step back and you deconstruct this... you'd really

rather have the ability to do transactions where you have some sort of interaction between Alice and Bob in that process.

...so for example, at the base level, you'd like perhaps to capture the commercial intent between Alice and Bob ...so Bob isn't just pushing money to Alice for just the sake of sending money ...some people do that, we see that with 'dust transactions' with Bitcoin^[401] for example.... but for the most part, Bob is buying something, or Bob has some commercial expectation... or Bob is making a donation... but in all these cases there is an understanding between Bob and Alice that relates to the transaction ...at the moment that's meta - that's abstracted from the system ...so the base layer doesn't record that.

So while the layer said an event happened ... the nature of the event, terms of the amount of value and the actors involved... it's going to timestamp it and that records are immutable ...the contract, the social dynamics of that event are not captured in the system which means they're subject to debate.

...so give me an example of this.... let's say that Bob goes to an ATM and withdraws \$300 of value out of an ATM ...now that's a transaction ...now let's say Bob did that next in an Italian restaurant on his birthday and all of his friends happen to be there ...you would say 'oh it looks like Bob's pulling money out to pay the check'or in some way is connected to this event, he's at a celebration, there's people there.... it's expensive and let's say it's at 12 o'clock ...it's lunchtime yeah... Bob can then go take 300 dollars from an ATM, so the same type of transaction but now I've changed the metadata....

let's say it's 2:00 a.m. right next to a known brothelso basically the exact same type of transaction ...the same type of value, the same actor involved... this is his account and his money, but because you've changed the metadata it has vastly different implications.... So what if you could swap these

metadata and then suddenly you can now make the Italian restaurant look like a brothel? whoever controls that story has a lot of power.

With the advent of Bitcoin, developers began using blockchain technology to add small amounts of new data to the chain, knowing that the data would be accessible for the rest of time. In 2015, the University of Nicosia^[402] became the first university to issue academic certificates whose authenticity could be verified through the Bitcoin blockchain.

Adding information to the chain became the norm over time. Cardano is a third-generation distributed ledger. In terms of metadata, Cardano is significantly more efficient than previous blockchains in adding transactional data. Cardano's initial transaction size was approximately 16KB (80KB as of Feb 2022), while previous blockchains permitted just 40-80 bytes of information. Even after subtracting the size of the remainder of the transaction (UTXOs, inputs, and outputs), the metadata still takes up the bulk of the 16KB.

Transaction metadata

Metadata is a useful tool for certifying and validating information. It lets cryptocurrency assets save information about their previous owners, transfers, and values. This is especially useful when dealing with non-fungible assets that reflect value, such as property or intellectual property. A public key may also be used to sign and certify a variety of documents, proving the document's authenticity.

One of the most well-known applications of metadata is in the supply chain. Factories, customers, suppliers, and delivery services are all part of the supply chain. Participants must give proof of interconnected services that are available to everyone for verification in order to allow effective data tracking. In this situation, metadata may give a full view of supply chain activities by combining fixed data

on the blockchain ledger with metadata. For all parties, this ensures openness, immutability, and confidence.

Atala

IOG's Atala product suite, which includes Atala PRISM, Atala Trace, and Atala Scan solutions, saw early commercialization of metadata deployment on Cardano. The IOG team is developing metadata support while connecting with the Cardano ledger to improve the entire product functionality in terms of data feasibility, accountability, and traceability.

Atala PRISM^[403] is a decentralized identification system that allows individuals to control their personal data and communicate with organizations in a seamless, private, and safe manner. On Cardano, the Atala PRISM team is using metadata to certify and store DIDs and DID documents. It will also be able to cancel credentials such as university certificates, in addition to creating them.

Atala Trace and Atala Scan are being developed to help brand owners get a better understanding of supply chain operations while also establishing product provenance and auditability. Metadata integration will be employed in these circumstances to store tamper-proof supply-chain information.

Both organizations and the developer community have varied approaches to dealing with metadata. Using the metadata service established by IOG's Professional Services Group is one such method. IOG have been working on integrations with a number of partners and have a lot more planned. Transaction metadata was an early component of Goguen utility and smart contract capability, which were expanded and developed by a variety of additional features.

Cardano's metadata strategy

Metadata has a wide range of applications. With this in mind, IOG

has been trying to make it as simple as possible for developers to include metadata into their applications. IOG also want to ensure that ada holders have a simple means to see information about their transactions.

Differentiators

Metadata conveys a transaction's narrative, and there are several methods to engage with it. Ada users may search for particular information in the Cardano Explorer, and developers can make use of metadata by embedding details directly into a transaction. The data may be directly contributed, or a Merkle tree^[404] of the data can be created and the root hash of the Merkle tree placed on the blockchain for larger data sets. Once this is completed, it can be shown that the data exists at a certain moment in time and that it is permanently stored on the chain for future use.

It's also worth noting that transaction information is recorded on the blockchain and sent with every transaction. The fact that it is kept on-chain rather than in the ledger state is advantageous since it has no impact on transaction validation and does not degrade ledger performance.

Metadata service

Business consultancy and technology services are provided by IOG's Professional Services Group (PSG). The PSG is creating services to assist businesses in designing and implementing blockchain solutions by connecting their systems with distributed ledger technology in a simple and easy manner. The metadata service was created with a range of uses in mind, but particularly for commercial purposes.

This interface manages wallet interactions, sends low balance alerts to users, and wraps everything up in a Docker container. This removes the complication of manually providing information in the wallet's backend API. Before a transaction is declared complete, the

metadata service just needs the requested information and the number of blocks in which it should be stored.

One may add the following in the metadata request:

- The actual metadata, which includes the sender and receiver's identities, as well as comments and tags.
- The depth: the number of blocks in which the metadata-containing transaction should be kept before being declared complete.
- The wallet to be utilized is indicated by the client identification.
- Transaction identity: in the event of failures or restarts, this functionality is helpful.

It enables clients to re-examine metadata that has already been supplied. The metadata service stores a transaction on the blockchain after incorporating all of the details, allowing transaction information to be accessed via the Cardano Explorer. All that is required is the specification of a transaction identification.

PSG metadata service may also be supplied via language-neutral protocol buffers. Client generators support a wide range of programming languages, including Python, Java, and Scala, which enhances the number of possible applications. The process of integrating with the Cardano blockchain is made easier by these expanded options.

Accessible metadata

IOG also created a Scala and Java client for the Cardano wallet API, which groups calls to the API together and makes them more accessible to developers. IOG supplies an executable jar file in addition to a Java and Scala API to allow basic access from the command line. On GitHub, you can learn more about the PSG Cardano wallet API[\[405\]](#) and how it lets clients execute tasks like transaction submission and listing, wallet management, and node monitoring.

Wallets and the Cardano-CLI

Submitting metadata straight from a wallet or the Cardano command-line interface (CLI) is another way to deal with it. These procedures need some coding skills as well as familiarity with the Cardano node and CLI. Because developers may verify important data in their own way, direct interaction with metadata unlocks enormous opportunities for creating decentralized apps on Cardano.

The format of the metadata is established in the Cardano wallet and CLI via a mapping from keys to values (key-value pairs) that integrate info for many uses into a single transaction.

- Metadata keys serve as a schema identifier for the metadata value they represent
- Metadata values are simple terms, consisting of integers, text strings, byte strings, lists, and maps; keys are unsigned integers with a maximum size of 64 bits; and metadata values are simple terms, consisting of integers, text strings, byte strings, lists, and maps. Values need to be structured so that they can be viewed and controlled more easily, especially by scripts.

The sole additional cost is that metadata increases the transaction's size in bytes, and the processing price is depending on transaction size. The Concise Binary Object Representation (CBOR)^[406] and Concise Data Definition Language (CDDL)^[407] notations may be used to create metadata. Check the Cardano wallet's transaction metadata and how to use transaction metadata schemes in Cardano CLI.^[408]

Cardano's growth into a multi-functional smart contract platform will need transaction metadata. Metadata was added during Goguen to define transaction conditions for smart contracts, expanding the possibilities for commercial adoption.

April 21, 2019. Metadata use case: contingent settlement. CH:[\[409\]](#)

The other thing that hasn't been discussed and this is something that really needs to be carefully brought out in the cryptocurrency space, is the notion of contingent settlement as well as metadata embedding. It's a controversial topic but it's a topic that is being forced upon us... for example the state of Texas is right now debating whether to pass a law that would require someone who receives Bitcoin, or any cryptocurrency, to know the identity of the person that they've received it from. So this actually means all of you could make every Bitcoin holder in Texas a criminal just by sending them a small transaction, because they don't know your identity. So it's a fundamental misunderstanding of how cryptocurrencies work, but the writing is on the wall that these systems have to be more intricate and complicated.

So there's two components, one is the idea of permission to send ...so I have an address and Bob has an address and right now the way things are, I can just push a transaction to Bob, with or without his consent. However, what if Bob has a specially constructed address that says you have to go and get my permission before the transaction will settle. So for example, let's say your exchange and Bob is withdrawing from an exchange. The exchange would really love to have an audit log that showed they gave you your money, so you pull your 100 Bitcoin out that you've made from trading and normally they just push a transaction to you and that would be it...but what if the exchange forces you to use a contingent address that then could be connected to an identity? For example, the DID (decentralized identifiers) standard which is basically a URN (uniform resource name) that connects to an identity document ...called a DID document.

So they could say 'look before you're able to withdraw your money, you basically have to sign the hash of an agreement that this is a withdrawal from our exchange in that you've been

totally settled for this particular transaction' ...then that hash can be embedded along with the DID, or an encrypted DID... so you can encrypt it with an audit key into the transaction itself and the transaction won't settle until that's been satisfied. So the exchange gets an auditable, non-reputable guarantee that they can show to the regulator, they can show to their third-party staff ...that you have consented to the withdrawal and it was you.

....now the advantages is that it's an added layer of security from an exchange because you now have separate credentials... the login credentials that get access to the exchange... as well as the KYC (know your customer) credentials which are connected to your identity ...and these are separate ...so they can basically have additional security, and if your account gets hacked, the person wouldn't be able to withdraw from the account.

So there's a consumer benefit but that very same infrastructure could be used for compliance for people in Texas. You could populate a Texas-flavored wallet that has contingent addresses and basically it means nobody can send me any money until I have their DID, or something like that. Now everybody's in compliance and there's no way to make them non-compliant. So there's all kinds of primitive structures that you can build and by using Marlowe, you can put very sophisticated financial contracts on top of these things, for all kinds of financial products, whatever they may be, and this is portable.

Furthermore, with the notion of metadata embedding, basically what you're doing is saying you have some commercial understanding of the transaction between Alice and Bob, and you're taking that entire understanding and you're transmitting it through a pub-sub (publish-subscribe) interface. So you send out-of-band to Bob, that metadata ...and then they sign it, with the hash, so the transaction has the hashes which are not reversible so they're secure. Nobody can know what you did, but yet you possess a copy and Bob possesses a copy. So if the

taxman comes or the regulator comes calling, you can show a time-stamped, non-repudiable, auditable, immutable record. That's what that transaction was about, and nobody can be the wiser about it.

In addition to that, with DIDs you can encrypt the DID and embed it within the transaction as well. So again you have a time-stamped, audible, immutable and non-repudiable way of verifying that that transaction's connected to that identity but the encryption keys are up to the parties of the transaction to be shared with whomever they care. So either you can just possess it for your own internal records. You can have an audit key for a regulator, the taxman... whoever you care about, or it can be part of a larger commercial understanding between different parties.

These capabilities . . . they're actually not hard to integrate because we designed things the way we did. By the way, that was another reason we had slight delays because we've discovered these types of patterns, as we were building the system, and we thought it'd be really cool to build these types of things and put these types of things into Cardano, and it would make Cardano kind of a a system that could absorb a lot of the innovation that's been brought out in the permissioned ledger space, or in policy groups.

Furthermore, contingent settlement also allows for receiver-pays transaction fees. So you see certain systems say that transactions are free. Well you can now absorb that with receiver pays, basically say that the receiver has to contribute some of the transaction fee and if they don't, then the transaction doesn't execute... in which case you have a free transaction at the sender side... so we can absorb the credit card use case into the system as well.

Regulation should follow the identity and the asset ...we've moved beyond regulation being global for everybody and we've

moved into individual transaction, from a vending machine and a 500 million dollar transaction ...it's really crazy, and so instead, we should move to a world where the transaction itself has metadata, identity connected to it, and a smart contract capability within it and then it inherits its regulatory standard from the geographies it touches, the identities it touches, and ultimately the amount ...and then you can have an auditable, time-stamped, immutable and non-repudiable proof that you've complied with the regulation ...and then what you do is you click one button in your wallet software, it bundles everything together at the end of the year, and that's what you give the government and the taxmanand you're done...

Your cost of paying taxes and filing taxes, your cost of compliance is automated, and then the burden is on the government to write the smart contracts and the regulatory standards. I'm really tired of these unfunded mandates where they say 'you must, you shall, you will, you do', and then they leave it to the industry to figure it out... not realizing that they're costing all of us millions to billions of dollars... which in turn gets pushed to you, the consumer.

Token Locking on Cardano

Cardano's growth has been envisioned as a journey encompassing five overlapping development eras, each of which is supported by the Ouroboros consensus system. As Cardano developed, the protocol adapted as well, as new features and functionality were added to the platform. Upgrades need progressive modifications to the network protocol.

Traditionally, when a hard fork occurs, the existing protocol ceases to function. All block producers must update to the latest version of the software, which includes the new block production regulations as well as additional improvements. The chain history is then cleared, and block manufacturing is resumed. This means that a hard-forked chain will be different from the prior version, potentially raising

worries about the blockchain's integrity or possibly causing chain splits.

The introduction of token locking

Token locking was the main feature of the second Goguen protocol upgrade. *Allegra* was the name for this development stage. This was the next major update for Goguen, after the network integration of metadata.^[410]

This was a minor technical adjustment to the consensus process that had little effect on the ledger. It was crucial, though, since it prepared the platform for smart contracts and the production of Cardano-based assets (in addition to ada). It also supports voting, an essential piece of Voltaire (governance) functionality. System modifications ensure IOG can continue to progress through future hard forks.

Token locking is a method of locking the usage of a single token for a defined purpose. The assets that are tallied by the blockchain ledger are referred to as tokens. There was just ada before this, but many more custom tokens were able to utilize the Cardano platform since. In this scenario, locking means 'reserving' a particular quantity of tokens for a certain length of time so they can't be sold for a profit (such as voting, or running a smart contract).

This is comparable to receiving RSUs (Reserved Stock Units) from your employer. An employee who works for a corporation may be entitled to receive shares when they vest after an agreed time period. For example, 500 shares, with 100 vesting each year for 5 years.

This model is often referred to as the 'golden handcuffs'. This is perhaps a bland example, much more imaginative and innovative ideas were discussed on the Twitter Space chat between Snoop Dogg, his son Champ Medici, Clay Nation & Charles Hoskinson.^[411]

Re: Snoop Dogg, '4/20 Hangout with Charles' Twitter space. CH:
[\[412\]](#)

Snoop Dogg, that was an interesting one. Josh Miller contacted me, said 'hey, you want to do a Twitter space with Snoop?' and I said sure and then we went back and forth for about two months and did a promo video[\[413\]](#)

I was actually flying back at the time. And so I found a little quiet area and we had the conversation. He was just a great guy and his son Champ's a great guy too, and they really have just demonstrated what you ought to do. It's very easy, when you're older and very successful, to rest on your laurels, but what Snoop has done is he's always been able to embrace and stay relevant decade by decade. And it's paid huge financial dividends and also has kept his fan base ever renewing. And now they're entering in the NFT space and that's really great to see them do that. They're also thinking how we can apply these fundamental capabilities towards our particular industry.

So the lesson of Snoop is less about Snoop and it's more about how crypto should work. Which is you start with what is important to you? ..and then you try, with that, to enable a solution that is new and exciting and brings something different to the table. Where it goes wrong, is what's happened, for example, in the gaming industry where they've applied NFTs. Where they look at as the next LoopBox or micro transaction... and basically, it's just a new way to monetize something, but it adds nothing new to the experience. It doesn't improve the games, it doesn't make anything better, which is why many gamers have actually rejected that.

So there's both a light side and a dark side to it, and I think what Snoop is doing, is he's trying to be on the light side, which is end to end... How do you put all these pieces together in a way that not only creates more profit, but changes the business model in a way, so it's less predatory to new musicians entering? Which is something he personally had to deal with.

*Prince had to deal with.... almost every musician has a story about how they got f**ked at some point, and it's really good and cool to see that they're thinking along these lines. And there's many means to that end.*

Token locking enable smart contracts

Token locking is required to implement sophisticated smart contracts and certain circumstances, such as when completing a purchase. When someone gets into a contractual arrangement to sell a painting to an art gallery, the seller promises that the painting will not be sold to anyone else. In this scenario, the token might represent the painting, while the ‘promise’ represents the real token locking. If the painting is sold to a third party, the contract’s guarantee will be breached, and any penalties will apply. With the introduction of token locking and the use of ada coins as tokens, contract providers will have access to this exact capability. As usual, the ada may be delegated to a stake pool.

Those ada holders who participated in the Catalyst Fund2 voting process had to ‘freeze’ ada. This indicated their voting privileges, based on how much ada they had locked. It proved each person had a certain amount of votes and avoided the chance of votes being tallied twice. Individuals were unable to assign more votes than they had, vote on opposing proposals, or duplicate vote.

Unseen work

Token locking was implemented in a behind-the-scenes manner. It had no impact on ada holders’ experience since Daedalus and Yoroi wallets were automatically updated.

To use the new version of Ouroboros, which featured token locking, all of the network’s nodes had to ‘agree’ on it (that is, reach consensus). Stake pool operators and exchanges with operational nodes just needed to download the latest version of the code and test its functionality to do this. To guarantee a seamless transition,

IOG's dev teams assisted stake pool operators and monitored the network throughout the process.

Following the implementation of token locking on the mainnet Cardano ledger, future hard forks included multi-asset and other smart contract features. These features leverage token locking as well, giving Cardano users a plethora of additional options. This paved the way for non-fungible (unique) tokens to be created on the Cardano blockchain.

Cardano has a safe, seamless route to frequent protocol changes, each of which adds new value and usefulness to the network while reducing interruption and risk, thanks to IOG's hard fork combinator.

Native Tokens

Tokens on Bitcoin

Protocols were built early in Bitcoin's existence to enable users to issue assets that piggybacked on Bitcoin's accounting system to monitor numerous currencies at the same time. The Bitcoin protocol does not support these protocols natively, but they were created through hacks. Light clients are forced to depend on trustworthy servers in the case of Bitcoin overlays like Colored Coins and Mastercoin (now Omni). Transaction fees must still be paid in bitcoins. These characteristics, together with the fact that transactions are approved via a single pipeline, render Bitcoin unsuitable for multi-asset accounting.

Tokens on Ethereum

In July of 2015, Ethereum was launched. Despite the fact that Bitcoin had been in existence for six years at the time, the cryptocurrency world was a nascent industry. When Ethereum first appeared on the scene, its schtick was smart contracts. This meant that third-party developers could create their own apps and run them on the

Ethereum blockchain in a decentralized way. Ethereum outperformed Bitcoin in terms of marketability and adaptability.

On the Ethereum blockchain, smart contracts allowed for the creation of user-defined tokens. The ERC20^[414] standard allowed for the creation of fungible Ethereum tokens, whereas the ERC721^[415] framework allowed for the creation of unique, non-fungible tokens. However, since the Ethereum chain did not enable native token support, user defined Ethereum tokens (both fungible and non-fungible) had an inherent inefficiency: they required the construction and execution of custom code.

What is Tokenization?

Tokenization is the process of converting physical objects into digital assets. Tokenization replaces a non-sensitive data element for a sensitive data element. This non-sensitive equivalent is known as a token, and it has no intrinsic or exploitable value or meaning.

Reduced transaction costs, transparency, higher liquidity, decentralization, and increased efficiency are just a few of the benefits of this. Tokenization is a very adaptable feature that may be used to achieve a variety of goals. Tokens^[416] are programmable; thus they may be made unique, which adds to their usefulness.

Tokens may, for example, be designed to provide holders access to unique material, personalized items, or even a vote stake. It makes no difference what the aim of the voting process is. Finally, tokenizing the capacity to vote provides individuals the sense of being a part of something bigger than themselves, and that their opinions may be heard.

Financial goods and economic models may be created via tokenization. Collectibles, alternative investments, gift cards, sports betting, in-game assets, commodities, video clips of your favorite NBA star^[417] and a variety of other areas are all possible examples.

This has the ability to link physical products, services, and activities to the virtual world.

Tokenization on Cardano

Goguen added a technique that handles tokenization natively. Rather than depending on smart contracts, the logic is based on the Cardano ledger. IOG created an efficient tokenization technique that is superior to the Ethereum blockchain's ERC20 and ERC721 standards by following this approach.

On the Ethereum blockchain, user-defined tokens (both fungible ERC20 and non-fungible ERC721 tokens) are non-native, meaning that the underlying ledger does not directly support them. ERC20 and ERC721 tokens are fundamentally distinct from Ether, Ethereum's native coin.

The Cardano approach to tokenization allows for the representation of custom assets on the blockchain without the use of smart contracts, as well as for those assets to behave similarly to the primary currency, ada, with the exception that:

- native tokens, unlike ada, can be minted and destroyed; and
- Ada is the only currency that can be used to pay fees, rewards, and deposits.

Native tokens parlance

In the crypto industry, the phrases 'coin' and 'token' are often employed. These words are sometimes interchangeable, and sometimes they aren't. And, in other cases, the word 'token' is used to refer to all digital assets.

Cardano's tokenization strategy is as unique as the blockchain itself, therefore here's a glossary to help you grasp the native tokens architecture.

- A token is defined as a representation of an asset kept on the Cardano blockchain
- An asset is defined as anything that can be quantified
- A token bundle is a representation of numerous tokens in Cardano
- Token logic that runs on the Cardano ledger rather than smart contracts is referred to as *native*.

Native tokens on Cardano vs Ethereum

Token code for both standards (ERC20 and ERC721) is copied and modified, rather than being part of the system itself, therefore Ethereum needs custom code for user-defined tokens to be supported on the chain. This adds a layer of complexity, expense ([gas](#)^[418] is required to pay for the execution of the code), and inefficiency. This is an inherent flaw in the Ethereum blockchain since it allows for human error. If coding best practices are not followed, dodgy custom code might bring problems that can result in significant financial loss. Software vulnerabilities contributed to the loss of \$300m worth of ether in one especially memorable^[419] occurrence. Solana^[420] has been restarted several times and suffered an expensive Wormhole hack. Cardano seeks to avoid such debacles.

The native tokens framework in Cardano enables user-defined tokens natively, that is, without the requirement for special programming. Native tokens are a kind of accounting system that is inherently provided by the ledger. This eliminates the complicated, unpredictable and expensive aspects of tokenization on Ethereum.

Cardano is a kind of decentralized ledger. Typically, a distributed ledger can only track a single asset type when it is created (usually its own cryptocurrency). However, as the ledger gets more decentralized, the requirement and capability of monitoring different kinds of assets on the same infrastructure emerges, which is why blockchains need to handle numerous assets such as stablecoins, utility tokens,^[421] credential tokens, and security tokens. Native

tokens, unlike ERC20, do not need extra event-handling logic or specific transfer costs to monitor transactions.

The accounting infrastructure established in the ledger model, initially intended for processing ada-only transactions, was extended to support transactions that employ many kinds of assets at the same time. Native tokens have the advantage of not requiring smart contracts to transmit their value and may be traded alongside other kinds of tokens.

Security is another benefit of native coins over ERC20. ERC20 tokens have been shown to be subject to a variety of security problems that are well documented.^[422] This is due to the fact that creating ERC20 tokens requires manual changes of the contract standard, which might lead to mistakes and flaws. Because the ledger manages the token logic, creating and transacting tokens natively eliminates this risk. Additionally, native tokens do not suffer the same overflow and underflow vulnerabilities as ERC20 tokens since Cardano's scripting language does not employ fixed-size integers and the ledger itself (as opposed to the ERC20 user code) monitors token movement.

Four Differentiators of Native Tokens on Cardano

Lightweight Architecture

The native token architecture is constructed around token bundles and is based on a multi-asset ledger structure. A token bundle might include a mixture of ada and other tokens. Instead of ada, these token-containing structures are recorded as outputs on the ledger. The asset ID of each kind of token contains a hash reference to the token's minting policy. The minting policy is only verified during the minting or burning process, and it is not maintained on the ledger, making this method very light.

The asset ID also captures the fungibility connection in a lightweight way: tokens with the same asset ID are fungible with one other, but

not with tokens with different asset IDs. The asset ID of unique tokens is coupled with a quantity of precisely one.

Within a single token bundle and throughout the whole ledger, the asset ID identifies each kind of token. It also indicates the token's position inside the token bundle's internal two-level map structure. This underlying data structure makes it possible to express fungible and non-fungible tokens in the same way. It also allows the system a lot of flexibility in terms of the types of asset use cases that can be tokenized. It's simple to represent, say, a collection of one-of-a-kind works of art covered by a single minting policy set by the artist.

When we examine how Ethereum's ERC20 handles asset transfers between two contracts, the inherent simplicity of native tokens is underlined even more. Smart contract code is necessary in this scenario, which adds complexity, as well as possibility for mistake and expense. Because several kinds of tokens may be traded in a single transaction, the structure of token bundles allows for a more lightweight approach to asset transfer.

Inexpensive

Transferring any amount of tokens between two peers in an ERC20 token ecosystem necessitates the execution of a smart contract, which comes with an execution charge (gas). The transfer of assets (tokens, ada, custom currencies, and so on) in Cardano's native multi-asset ecosystem does not need a smart contract and does not incur an execution cost.

More Security, less custom code

Native tokens have a lighter and less expensive design than Ethereum's ERC20 and ERC721 protocols. These two elements, however, would be useless without a strong security layer to ensure the system's integrity.

System integrity with native tokens is based on the ledger attribute of value preservation (that is, that the sum of all the inputs is equal to the sum of the outputs). Unlike user-defined smart contracts, all native token transfer logic is embedded in the ledger. This guarantees that the system behaves predictably and consistently, and it eliminates the need for users to master smart contracts, which can often be vulnerable to exploitation by hackers.

While the ledger ensures accounting accuracy, the minting and burning of tokens is governed by their user-defined minting policies. A minting policy is hash-linked to the tokens it covers indefinitely, and there is no way to modify it. This ensures that an issuer's policy cannot be amended to enable the minting or burning of a token that was not permitted under the initial policy. The policy for each kind of token being minted is verified and must be met whenever a minting transaction is put to the ledger. Except for ada (Cardano bans minting new ada), every token in circulation must have a minting policy and must have been minted pursuant to that policy.

As a result, the policy is the only custom code necessary to alter tokens in Cardano. Because the policy hash is linked to the asset identification, there is no need for a global asset registry, making asset creation cheap and simple. The technology is still basic, light, and simple to operate.

Simplicity

Now that Goguen's native tokens are implemented, the ledger treats all tokens in the same manner. To avoid ambiguity and any errors or flaws, a token may only be minted in one method. This streamlining of development via the use of a uniform methodology resulted in speedier development and a better overall development experience.

IOG has provided more detail on GitHub under native tokens and how they compare to ada and ERC20. [\[423\]](#) There is also a native tokens explainer video. [\[424\]](#) Momentum built steadily after the *Mary* and *Alonzo* upgrades, with developers realizing the benefits of

deploying native tokens and NFTs on Cardano. Cardano blockchain insights^[425] report almost 3.3 million wallets, over 4.5 million native tokens, 5,000+ NFTs, and more than 900 projects deploying to Cardano as of April 2022.^[426]

Multi-Asset Support (MAS)

Single asset ledgers

Single-asset ledgers are cryptocurrency ledgers that track just one kind of asset.

Multi-Asset support

When a blockchain, ledger, or cryptocurrency enables recording the transfer and ownership of several kinds of assets on its ledger, it is said to have multi-asset (MA) support. The native tokens feature in the Cardano ecosystem provides this capability.

This feature extends the accounting infrastructure specified in the ledger model, which was intended to handle ada-only transactions, to transactions that employ a variety of assets at the same time. Ada and a range of user-defined custom token types are among these assets.

Native versus non-native

Some cryptocurrency ledgers have features that allow you to monitor the ownership and transfer of many types of assets. Native MA (multi-asset) support is the name given to this sort of MA support. The MA functionality of Cardano is built-in or ‘native’.

It is possible to monitor assets for which there is no ledger accounting support if a cryptocurrency platform has sufficiently sophisticated smart contract capabilities. This is accomplished utilizing a Layer 2 solution based on smart contracts. This is a non-native form of MA support.

Assets

On the blockchain, an asset is an item that represents value. A digital asset like ada, a position, a certificate, or a number of products are all examples of these items.

The word asset might refer to one of two things:

- the identifier of a class of objects, such as ada or ‘johnCoin’; or
- an exact amount of a certain thing, eg. ‘10 lovelace’, ‘33 johnCoin’, ‘this book’ or ‘these jars of marmalade’

An asset ID is a combination of the policy ID and the asset name that uniquely identifies it. It’s worth noting that, although ada may be used as an asset, it doesn’t have an explicit policy ID.

Tokens with the same asset ID are fungible with each other, however they are not fungible with tokens with different asset IDs. An asset ID is a fungible token collection’s unique identifier.

PolicyID - The unique ID linked with a minting policy. The ID is a sequence of letters and numbers that is generated by applying a hash function on the policy itself.

Asset name - an asset’s (immutable) property that is used to differentiate amongst assets within the same policy. The asset name, unlike the policyID, does not correspond to any code or set of rules and may be any common term, such as ‘tickets’ or ‘VIPTickets.’ Valid asset names may, however, be limited by the policy that defines how an asset is scoped.

For distinct tokens, various policies might use the same asset names.

Tokens

A token is a short word for ‘asset token,’ which is an asset’s on-chain representation and accounting unit. One ada, one home, or a ton of tea, for example, may be represented by a token.

Currencies

Currency is a term used to describe a monetary unit that serves as a means of exchange for goods and services. Cardano accepts ada and native tokens, both of which function equally on the network.

However, at this moment, ada is the only currency used to pay fees and make deposits, and it is also the only currency in which rewards are issued. The architecture of the underlying consensus protocol is responsible for this attribute of ada (and no other sort of asset).

Native tokens are a kind of accounting unit that may be used for payments and transactions, as well as being transmitted to an exchange address. Because the Cardano accounting ledger has built-in functionality for tracking ownership and transfer of several types of assets, these tokens are supported by the ledger without the need for extra smart contracts. While both ada and native tokens have value and may be used to pay and transact, only ada is utilized for fees and rewards, and only native tokens can be customized.

Conditions when using ada

Cardano’s main currency is ada (A). Because each address must have a minimum ada value, having ada (along with other currencies) is required to transfer multi-asset tokens between addresses (min-ada-value, currently set at 1 ada).

As a result of its design, the following conditions apply:

1. Creating outputs that exclusively include custom tokens is not possible.
2. The quantity of each kind of token in an output has no effect on

the output's min-ada-value, but the number of types of tokens raises the min-ada-value. (This is because the names and policy IDs of each of the different sorts of tokens take up extra space in the output.)

3. When sending custom tokens to an address, the min-ada-value of ada is always sent together with the custom tokens (by including the ada in the same output). The ada supplied with the tokens no longer belongs to the sender if the address is not spendable by the person sending the tokens.

Users may opt to employ off-chain dialogue to discuss who gives the ada to cover the min-ada-value in the output created by the transferring transaction before transferring custom tokens.

4. To retrieve the ada placed along with custom tokens in an output O, the user must either:

- Spend the output O and burn the custom tokens that it contains
- Spend an output O and an output O', then combine the tokens in those outputs with the same set of custom tokens stored in another output (spent within the same transaction).

5. Because some ada must be provided in each output, splitting custom tokens into more outputs than they were before the transaction was run needs more total ada to cover the min-ada-value.

What are Token bundles?

A token bundle is a collection of tokens that is heterogeneous ('mixed'). Tokens of any kind may be packaged together. On the Cardano blockchain, token bundles are the standard - and only - method to represent and store assets. Token bundles group tokens into a certain data structure, ensuring which tokens are fungible with other tokens is clearly defined.

Ada amounts were stated in transaction and UTXO outputs in prior versions of the Cardano ledger. These amounts have been expanded with token bundles, which may define an ada amount with quantities of other assets in a single output, thanks to the addition of multi-asset functionality.

Token bundles are stored in transaction outputs and mint fields, as well as the UTXO set outputs, which are monitored by the ledger. Certain elements of a transaction, such as the fee field, must still explicitly state ada amounts.

Token bundle storage

Token bundles can be found:

- As a transaction's mint field, indicating that the transaction is producing the bundle's tokens
- In a transaction's output or an output in the current UTXO recorded by the ledger, alongside the address of the output, e.g. Multi { MyAddress, value: TB_Example }

Splitting and combining token bundles

Token bundles may be split and combined arbitrarily by transactions.

Minting policy

A minting policy is a collection of rules that control the minting and burning of assets that are within the policy's control. A minting policy specifies the circumstances under which tokens are minted (or burned). The rules might, for example, describe who has authority over the asset supply through minting and burning.

Users that wish to produce a new asset establish the minting policies. For example, a user may choose to limit themselves to just minting a certain kind of token. This is something that would be outlined in the policy.

The following are the rules for minting:

As a very simple set of rules, it consists of the following (ANDs and ORs):

- A list of the signatures required to enable the mint to operate (e.g., a multisig specification, where no code is needed)
- With a Plutus Core script, a specification of when the script may be spent (e.g., after slot 10 and before slot 30).

When a transaction is executed, the node checks for compliance with minting regulations by executing the code or validating the appropriate signatures. All minting policies for all assets that the transaction is seeking to mint must be followed.

Minting: Terms & Conditions

- A minting policy is required for all assets. Ada's minting policy, for example, states that 'new ada can never be minted'
- A token has just one minting policy connected with it
- A single policy describes the requirements for both minting and burning tokens that fall within its ambit. Its compliance is monitored both during minting and during burning
- An asset's related minting policy cannot be changed at any time, it's irreversible. Current tokens cannot be linked to a new policy. With a new minting policy, users may purchase back and burn all current tokens while still minting new ones. This is by design, it's not a fault in the system
- An existent asset on the ledger that is scoped under a certain policy is guaranteed to have been minted in accordance with that policy

- The actual policy is unimportant until tokens of that policy are generated in a transaction. Its only purpose is to serve as a unique ID for the asset
- Assets related with various minting policies are never interchangeable. They can be exchanged in the same manner as USD can be used to acquire Euros: the quantity of Euros you can buy with a specific amount of USD is determined by the exchange rate.

Relationship between an asset and its minting policy

For security reasons, the link between an asset and its minting policy is permanent. This feature protects users and the system against falsely minted tokens.

When a token's minting policy changes, it's no longer the same token, and its value can't be compared to the original token's. In order to define high-assurance policies, this permanent asset-policy association method is essential. Cardano's MA (Multi Asset) technique becomes vulnerable to a variety of attacks if this identification is loosened. It's best to ensure that every token was minted in line with its minting policy, not any other policy it may have previously been linked with, by having a permanent link between them.

Minting policy Types

There are several more sorts of minting policies to consider.

Single-issuer policy

A single-issuer minting policy states that only the entity with a certain set of keys may mint tokens for a specific asset group. For example, the minting transaction must have been signed by the set of keys provided in the minting policy.

Tokens representing Panini soccer cards are an example of an asset category that would adopt a single-issuer policy. The firm that makes authentic collectors' cards would provide the keys needed to mint

fresh soccer cards, as required by the minting script. This means that no new soccer card tokens may be produced without the approval of the firm. There is no need to use Plutus smart contracts when creating this form of policy.

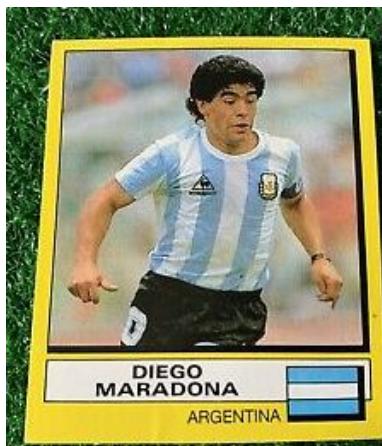


Figure 19. Panini soccer card

Time-locked minting policy

AKA token-locking. This policy may be used to limit the amount of tokens that can be spent from a certain address.

- only during or after a defined time slot
- only before a defined time slot

Typically, this form of policy isn't employed on its own. It is often used in combination with a multisignature or single issuer policy, for example. Only a transaction signed by key 'k' may spend this output after slot 's'.

This form of policy may be created without the need for Plutus smart contracts.

One-time minting policy

In a one-time mint policy, a single transaction mints the whole set of tokens for a specified asset category. This indicates that there will never be any more tokens in that asset category. This sort of policy necessitates the use of Plutus smart contracts.

For example, a one-time mint policy may be used to create ticket tokens for the Super Bowl. Because the venue's capacity is known ahead of time, there will be no need to issue more tickets.

Minting transactions

Each transaction has a mint field that may be used to add fresh amounts of new tokens to the ledger (minting) or to remove existent tokens (burning). Minting transactions are transactions in which the mint field is not empty. The usage of this field must be strictly regulated to guarantee that tokens are minted and burned in accordance with the token's minting policy.

Minting transactions must include the minting rules for the tokens they are minting, in addition to the mint field, so that these tokens may be inspected during validation.

The ledger will record the assets contained in the mint field, which is included in the transaction's balancing: if the field is positive, then the transaction's outputs must have more assets than the inputs supply; if it is negative, then they must contain fewer.

It's worth noting that a single transaction might result in the creation of tokens with numerous minting rules. For instance, (Policy1, SomeTokens) or (Policy2, SomeOtherTokens). A transaction might also mint and burn tokens at the same time.

The metadata registry

Metadata is a description of native assets that anyone may read in Cardano. These assets are held on-chain using non-human-readable IDs. The readable version of this data is held in public token registries, not on the blockchain. These registries, which will first be controlled by the IOG, will eventually be owned and configured by the community, allowing Cardano to achieve another degree of decentralization. IOG guarantees that the community can completely trust the datasets by allowing the community to own and

configure these registries. Because the users are the owners of the data, it is in their best interest to behave honestly.

Creating native tokens on Cardano

Users are able to select between simple and sophisticated tools to bring their assets to life on Cardano. Tokens are becoming more popular for financial transactions. They reduce fees while boosting transparency, increasing liquidity, and, of course, remaining independent of centralized corporations like the banks. Tokenization is the process of converting actual assets (such as fiat currencies, equities, precious metals, and real estate) into digital tokens that may be used to build commercial financial instruments.

Many tokenization options^[427] are available in Cardano. The ledger's accounting architecture handles not just ada transactions, but also transactions that hold several asset types at the same time.

Utility

To fulfill commercial or business goals, developers, enterprises, and apps may build general purpose (fungible^[428]) or specialized (non-fungible) tokens. Custom payment tokens or rewards for DApps, stablecoins tied to other currencies, and unique assets, like eBooks, that represent intellectual property are just a few examples. All of these assets may then be traded, swapped, or used to purchase goods and services.

Users will be able to transmit, receive, and burn their tokens without paying transaction fees or installing event-handling logic to monitor transactions since native tokens do not need smart contracts to transfer their value. Users are able to produce, distribute, trade, and store tokens in one of four ways, depending on their preferences and technical expertise:

1. Cardano CLI

Advanced developers may create (mint) assets and submit test transactions to various addresses using the native tokens testing environment.

Because of the nature of working with the CLI, it is assumed that you are comfortable with setting up and administering a Cardano node, as well as dealing with transactions and managing addresses and values. To generate native tokens using Cardano CLI, follow the steps outlined in the documentation.^[429] At a high level, the steps are as follows:

- Create and start a Cardano node
- Generate verification and signing keys
- Generate a payment address, fund and check the balance
- Start the minting process, create a policy and mint a new asset
- Lastly, build the raw transaction, submit and sign transactions to send the tokens to the target address.

On the Cardano docs site^[430] IOG provides native token tutorials and exercises to enable developers create tokens, implement monetary rules, and understand how to conduct multi-asset transactions.

2. Token builder GUI

The CLI requires a certain amount of programming expertise. As a result, IOG established other methods for less technically adept individuals to generate tokens. After the mainnet CLI launch, IOG deployed a token builder to do this.

The token builder is a graphical user interface that simplifies the process of creating tokens. The token builder may assist you in building tokens for your decentralized application, tokenizing your property, making NFT collection cards represented as specialized assets, or establishing a stablecoin tied to the value of other currencies.

To make a token, just fill in the following fields:

- The token's name (for example, CardanoForTheMasses)
- the token's symbol (for example, CFTM)
- the token's icon (generated automatically)
- Amount to be made (eg, 10m)
- Cardano wallet location (your address to host newly created tokens).

The monetary policy is generated automatically by the token constructor, so you won't have to describe it yourself. This accelerates and simplifies the token generating process for non-technical users.

Initially, the token builder allowed for the generation of fungible tokens (while non-fungible tokens were created using Cardano CLI). IOG eventually expanded the capability to enable users to create non-fungible tokens and change the monetary policy according to their preferences. Meaning, for example, that users are now able to determine the circumstances under which tokens are created (or burnt), as well as who controls the asset supply.

Finally, after tokens have been minted, the 'Mint more' option will allow you to mint more. This may be done using the same policy to produce additional tokens of the same kind or using a new policy to create tokens that represent various values. You might, for example, make CardanoForTheMasses tokens for each edition of this eBook. Initially only minting for the 'Vasil Edition'. When the 'Chang' HFC event occurs, no more 'Vasil edition' tokens are minted. New tokens are now minted for the 'Chang Edition' with new cover art and an updated eBook. Each edition will have a different minting policy.

The token builder seeks to simplify token production while simultaneously emphasizing the improvement and visual display of functional procedures. As a result, users want to be able to see all of the tokens that have been produced, their values, amount, and the addresses to which they are being transferred — all in one spot.

3. Daedalus

Users that do not want to generate their own tokens but want to use current ones for payments, purchases, or exchange can use Daedalus and Yoroi wallets.

The Policy ID and the Asset Name are two hexadecimal integers recorded on-chain that uniquely identify native tokens. IOG generated fingerprints to make it simpler for users to identify native tokens since these numbers aren't 'human-friendly.' Fingerprints are 44-character alphanumeric strings with the prefix 'token' at the start.

The Cardano token registry, which was controlled initially by the Cardano Foundation, includes additional token data presented in the wallet UI (name, description, and acronym). adaHandle (\$handle, adahandle.com) was one of the first projects to launch after Goguen as '*An NFT-powered naming solution for your Cardano wallet address, secured entirely on-chain via the Handle Standard*'.

4. Third party platforms.

For example, Driptdropz (driptdropz.io), the 'Cardano Token Distribution System' has added great value to the ecosystem.

The lifecycle of native tokens on Cardano

The native token lifecycle will be complete after all of the required components have been deployed. It is divided into five stages:

- Minting
- Issuing
- Using
- Redeeming
- Burning.

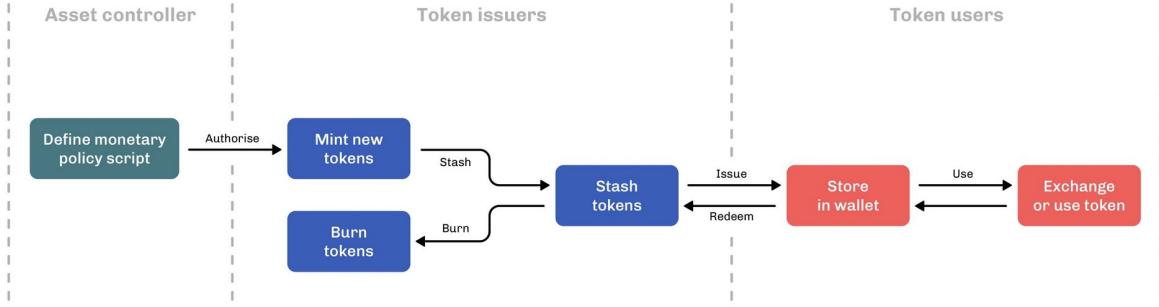


Figure 20. Lifecycle of native tokens on Cardano

Each of these logical processes includes Cardano blockchain transactions, which may result in ada fees. The following are the primary actors:

- Asset controllers, who determine the asset class's policy and authorize token issuers to mint and burn tokens. They might also retain co-signing rights for any tokens that are minted or burned
- Token issuers, who create new tokens, keep a reserve of them in circulation, distribute them to token holders, and destroy them when they're no longer useful
- Token holders, who keep tokens, send them to other users, use them for payment, and then redeem them with the issuers when they're no longer needed. Normal 'Joe Soap' users, exchanges, and other entities may be token users.

The lifespan of multi-asset tokens begins with their creation – minting, which is the process by which one or more token issuers generate new tokens in line with the monetary policy script provided by the asset controller. In most cases, new tokens will be issued to serve a particular function. Tokens that are fungible or non-fungible (unique) may be developed for particular payment, buying, or exchange requirements, for example. When a new token is created, the overall token supply for that token grows, but the ada supply remains the same. Minting coins and transferring them to new

addresses may need the payment of ada, which might be proportional to the quantity of distinct tokens possessed.

Token holders will store tokens in their wallets and will be able to transfer them on to other users, swap them for objects of value (including non-native tokens), and so on, just like they would with ada. When a user's token has been used up, they may opt to redeem it. Meaning tokens are returned to their original issuer (perhaps in return for a product, service, or some other currency, for instance). Tokens may then be re-issued to other users as required after they were redeemed. To pay for transaction fees, token holders will need to keep some ada in their wallets.

If required, tokens may be burnt when they become redundant, in line with the underlying monetary policy script. The act of burning these tokens eliminates them (removing them from circulation), reducing the overall token supply. At this time, any deposits will be refunded. Fungible and non-fungible tokens are both burned in the same way.

The multi-asset token lifecycle may enable tokens to be acquired and reissued by other parties, such as token holders acting as reissuers. This may be done to facilitate trading across different asset classes, maintain liquidity in one or more tokens (by serving as a broker), or reduce the effort/cost of token minting, issuance, or metadata server maintenance, for example. As a result, such a transaction benefits both reissuers and issuers by reducing costs and effort, preserving separation and integrity, and infusing value into the asset class.

Min-ada-value requirement

On the ledger, UTXOs may contain a mixed bag of tokens, including ada. The maximum total size taken up by UTXO entries on the ledger at any one moment is limited by requiring some amount of ada to be included in every UTXO (where that amount is dependent on the size of the UTXO, in bytes).

By increasing and reducing the min-ada-value setting, the maximum permissible UTXO size (the total of the sizes of all UTXO entries) is implicitly modified. The limitation prevents the Cardano ledger from going above a specific size in this manner. A ledger without size restrictions is prone to becoming overburdened with data to the point that users will be unable to process it (or operate a node) on devices that satisfy the required node criteria.

There is more detail in Cardano Docs on the ‘ada-only’ case, ‘min-ada-value’ calculation and with worked examples.

As a result of this strategy,

- It’s difficult to create outputs that exclusively include custom tokens
- The number of each kind of token in an output has no bearing on the output’s min-ada-value, but the number of token types contained in an output raises the min-value
- This is due to the fact that the names and policy IDs of each kind of token take up extra space in the output
- When sending custom tokens to an address, the min-ada-value of ada is always sent together with the custom tokens (by including the ada in the same output). The ada supplied with the tokens no longer belongs to the sender, if the address is not spendable by the person sending the tokens
- Before the transfer of custom tokens takes place, users may utilize off-chain communication to determine who provides the ada to cover the min-ada-value in the output created by the transferring transaction
- To recover the ada stored alongside custom tokens in an output O, the user must either:

- a) spend the output O and burn the custom tokens therein; or
- b) spend an output O and an output O' and consolidate the tokens therein with the same collection of types of custom tokens stored in another output O . (spent within the same transaction)

For example, in a new output created by the consolidating transaction, (CryptoBisonPolicy, AmericanBison, 2) in O may be consolidated with (CryptoBisonPolicy, AmericanBison, 4) in O' , for a total of (CryptoBisonPolicy, AmericanBison, 6)

- Splitting custom tokens into more outputs than they were before the transaction was executed necessitates using more ada in total to meet the min-ada-value, since ada is required in the extra outputs.

Native Token FAQ

Q. What does ‘multi-asset (MA)’ support mean, and does Cardano have it?

A. Multi-asset (MA) support refers to a collection of features that a ledger (blockchain / wallet / cryptocurrency / banking platform) may provide that enables it to account for and interact with several types of assets.

Native Tokens is Cardano’s MA support feature. Users may transact with ada and an infinite number of user-defined tokens using MA. This is native support, meaning tokens may be transacted with using the accounting system established as part of the cryptocurrency’s ledger capabilities, without the need of any smart contracts.

Q. What is the definition of (asset) tokenization?

A. Tokenizing an asset entails generating a digital version of it on the blockchain.

Q. What does it mean to ‘mint’ a token?

A.'Minting' refers to the process of creating or destroying new tokens. That is, the overall quantity in circulation of the token type being minted grows or decreases (i.e. when all addresses on the ledger are put together). Token creation is when a positive number of tokens is minted, whereas token destruction occurs when a negative number is minted.

Q. What does it mean to 'burn' a token?

A. The term 'burning' refers to the process of destroying tokens. It's the same as 'negative minting.'

Q. What does token redeeming entail?

A. Token redemption entails returning tokens to the issuer to be burnt. This is often done when the tokens being redeemed no longer serve a function on the ledger and the user or contract in possession of them is unable to burn the tokens (according to the minting policy). Although the token issuer/minting policy may not give any reward for redeeming the tokens, the user may opt to do it nevertheless to avoid having useless tokens in their wallet.

Q. What is a minting transaction?

A. The arrangement of transactions differs across the Shelley, ShelleyMA, and Goguen eras, although it is the identical within a single epoch. The Shelley MA (multi asset) and Goguen transactions may include information about the tokens they are minting. Minting transactions are those in which this piece of transaction data (called the mint field) is not empty. These transactions must additionally include the minting policies for the tokens they're minting, so they can be verified during validation.

The assets contained in the (mint) minting field of the transaction will now be added to the ledger as a consequence of performing a minting transaction. If the quantity of a given asset in the mint field is negative, the total quantity of that asset on the ledger will be lowered by the amount indicated in the mint field when the transaction is processed.

Note that a single transaction may mint tokens associated with many different minting policies. It's also worth noting that a transaction may mint and burn tokens at the same time.

Q. What is a minting policy?

A. A minting policy is a collection of regulations that govern the minting of assets linked to it. For example, who controls the currency's supply (and under what circumstances), as well as its minting and burning. These rules apply to the content of the transaction data for the transaction that the mint is attempting. For example, a minting policy may specify that the minting transaction be signed by a certain set of keys.

The user who desires to mint a new asset defines this set of rules. For example, a user could want to limit themselves to just minting this kind of token. This would be specified in the policy. When a transaction is executed, the node checks for conformity to minting regulations by executing the code or validating the appropriate signatures. All minting policies of all assets the transaction is seeking to mint must be satisfied by transaction data.

Q. What is a token builder and what is its functionality?

A. A token builder is software that enables a user to specify the tokens that will be created and include them in a minting transaction. It also guarantees that the transaction has the necessary extra data to verify that the transaction is authorized to execute the mint.

Q. What is ‘multisig’ and what does it have to do with minting policies?

A. The multisig scripting language (which existed before Cardano's introduction of Multi Asset capability) sets a minimum number of signatures necessary for a transaction to complete a certain operation, typically spending a UTXO entry.

Multisig scripts may also be used to define the most fundamental minting rules, such as those that need a specified set of keys to sign

the minting transaction. A multisig script, for example, may be used to specify a single-issuer minting policy.

Q. What is the relationship between Plutus smart contracts and native tokens?

A. The Plutus smart contract language may be used to write minting policies. This enables users to specify a far broader variety of policies than the single issuer policy that multisig may convey. Plutus, for example, may specify a one-time minting policy (but not just as multisig).

Q. What is the definition of a single-issuer minting policy?

A single-issuer minting policy states that only the entity with a certain set of keys is permitted to mint tokens under that policy. For example, the minting transaction must have been signed by the set of keys provided in the minting policy. Multisig may be used to provide this sort of policy.

Tokens resembling an artist's paintings are an example of a single-issuer policy use case. This would rule out the production of new painting tokens without the artist's signature. The insurance, on the other hand, establishes that all of the existing paintings covered by the policy were properly produced by the artist and nobody else.

Tokhun^[431] is just one NFT marketplace where artists can sell their paintings as artist Jonathan Dickson^[432] explained in this video.^[433]

Q. What is a one-time minting policy?

A. A one-time minting policy mints the whole set of tokens covered by it in a single transaction. This means that under that policy, no further tokens will ever be minted. Smart contracts are required for this form of policy, which cannot be represented via multisig. Minting ticket tokens for the SuperBowl is an example of a one-time minting policy in action. Because the venue's capacity is known ahead of time, there will be no need to issue more tickets.

Q. What is the difference between fungible and non-fungible?

A. Fungibility is the relationship that exists between two assets or tokens. When two tokens are interchangeable, they are said to be fungible. A €10 note, for example, is interchangeable with all other €10 notes (as well as all ten €1 coins and all pairs of €5 notes). Non-fungible assets can't be swapped for one another. Two precious jewels, for example, or two on-chain tokens that represent two real-world jewels. If a token is not fungible with other assets, such as a token representing a home, it is considered unique (non-fungible).

Q. What is a token bundle, and how does it work?

A. A mixed set of tokens that are subject to one or more minting policies. Tokens of any kind may be bundled together.

Q. What is the appearance of native tokens in a user's wallet?

A. A user's wallet stores both outputs with addresses that belong to the user and the quantities of ada that these addresses have prior to the introduction of MA (multi asset) functionality into the Cardano system. (Users address1, someAdaAmount) is an example.

The user's wallet can now include many kinds of assets in a single output with multi asset (MA) support, i.e., the wallet will be able to contain a token bundle. This means that wallets may include the following items:

- Assets covered by many policies in a single UTXO (including ada)
- Assets covered by a single policy and dispersed over several UTXOs

Q. Do native tokens contain IDs and other information that can be read by humans?

A. Instead of lengthy Policy ID strings and asset names, human-readable names for assets may be registered on a metadata server. When a user looks at their assets in a wallet that is connected to a metadata server, they will be able to see the human-readable names. Users will be able to upload the names of their tokens, as well as any other token-specific information, to a metadata server.

Users will have to pick which server(s) to upload or download their metadata from if more than one metadata server is active at the same time. Users may also enter names and other details directly into the transaction's metadata field. Transaction costs will rise in proportion to the amount of metadata added.

Q. What are the expenses of generating native tokens and exchanging them?

A. There are two types of costs associated with multiple assets:

- Fees: Sending and minting tokens has an impact on the fees that the transaction's author must pay. Fees are determined depending on the entire amount of the transaction, just as in an ada-only ledger. There may be extra costs for verifying minting policies, however only multisig policies are currently available, which do not incur additional fees on top of the transaction size-based ones
- Minimum ada-value: Every transaction's output must contain a minimum amount of ada, which is computed depending on the output's size (the number of different token types in it, and the lengths of their names).

Min-ada-value:

Keep in mind that outputs may include a mixed bag of tokens, including ada, which is a scarce resource. The inclusion of some amount of ada in every output on the ledger (where that amount is dependent on the size of the output in bytes) prevents the Cardano ledger from getting too large.

Q. What kinds of assets can I leverage to pay the expenses of native tokens?

A. At this time, only ada may be used to pay fees or make deposits.

Q. How does bespoke native token coin selection work?

A. It works similarly to ada coin selection in that the user chooses the tokens and amounts they want to spend, and the wallet selects suitable inputs and pays fees.

Q. Is it possible to send tokens to an address?

A. Yes, sending native tokens to an address is accomplished in the same manner as sending ada is accomplished, namely by submitting a transaction with outputs containing the token bundles the transaction author desires to send, as well as the addresses to which they are delivered.

Q. What level of control over custom token assets does the user have?

A. Multi asset tokens may be spent, sent, traded, and received in the same manner as ada tokens. Users may mint and burn native tokens, unlike ada.

Users may spend tokens in their wallets or tokens in outputs that are locked by scripts that let this user spend the output. Sending tokens to other users: Users may send (spend) tokens in their wallet to any address.

Minting tokens: Users may mint custom tokens in accordance with the asset's policy. These tokens may be sent to the user's or anybody else's address during the minting transaction. The policy may limit the specific output address for the tokens if required.

Note that, depending on the policy rules, even if a user has specified a policy, that user may not be allowed to mint or burn assets covered by that policy. Regardless of the identity of the user who developed the policy, a minting policy governs the minting of any assets covered by it.

Burning tokens: The policy linked with the asset also controls the burning of tokens. The user must be able to spend the tokens they are trying to burn in addition to being able to burn them (always in compliance with the minting policy).

Even if the minting policy clearly allows it, users cannot burn tokens over which they have no control, such as tokens in someone else's wallet.

Q. Is there a decentralized Exchange for Cardano native tokens?

A. No. DEX feature is not supported by the Cardano ledger itself. Many DEXs built on Cardano are in the works now that smart contract capability is enabled, like SundaeSwap, which was one of the first to launch but there are now many more as listed on CardanoCube.

Q. Is there a Cardano native token asset registry?

A. No. The deployment of Cardano's Native Tokens functionality does not need the use of an asset registry. If a user wants to list tokens they've minted, they may utilize the metadata server.

Q. How do Cardano native tokens compare to Ethereum custom tokens ERC721 and ERC20?

A. Cardano's approach to custom token creation varies from non-native implementations of custom tokens, such as ERC721 or ERC20, which use smart contract capabilities to mimic the transfer of custom assets (i.e., a ledger accounting system). Because the ledger architecture permits accounting on non-ada native assets, Cardano's technique for creating custom tokens does not need smart contracts. Another significant distinction is that, unlike ERC721 or ERC20, the Cardano multi-asset ledger allows both fungible and non-fungible tokens without the need of specialized contracts and is flexible enough to incorporate a mix of fungible and non-fungible tokens in a single output.

Multi-assets on Exchanges

Native assets are defined by its *minting policies*, which are set by users when creating (minting) new asset(s). These policies specify the maximum and lower bounds of what a token may do, as well as who can do it and when it can be done throughout the transaction lifecycle.

The network protocol and ledger-defined rules bind a minting policy. The minimum UTXO value^[434] is one such guideline (the minimum

amount of ada that must be sent in a single transaction). Because the value is presently fixed to one ada, a minimum of one ada must be included and accounted for in each native asset transaction on the Cardano network.

[cardano-graphql](#) or [cardano-rosetta](#) may be used to validate and locate these unique native asset transactions.

Multi-Asset Management

Exchanges that list ada are likely to face one of two scenarios:

Scenario 1: Spending a UTXO with a multi-asset attached

This situation is only relevant for exchanges that control their own UTXOs.

How do I discover UTXOs with a native asset attached? Local block explorers (cardano-graphql or cardano-rosetta, for example) are often used by exchanges and third-party wallets that maintain their own UTXOs.

cardano-graphql is a query language and runtime component for the Cardano API that allows you to satisfy queries using data from the cardano-db-sync PostgreSQL [\[435\]](#) database. It offers customers the ability to request the information they need by giving them a clear and comprehensible description of the data. As a result, both the growth of client APIs and the deployment of developer tools are simplified.

Getting started

After you've seen how a native asset transaction works, you may wish to produce or burn some native assets or tokens on the testnet. To begin minting native assets, check out these requirements [\[436\]](#) and follow the steps below:

- Connect cardano-node to testnet
- Build cardano-node and connect to testnet
- Download cardano-cli prebuilt binary or use build from source
- Follow the steps in docs[\[437\]](#)

How do I spend a UTXO with native assets attached?

It's critical to account for two factors when using cardano-cli to generate a transaction using native assets, as described in this section:

1. The value of the ada you want to send
2. The number of tokens

Any exchange or third-party that wishes to spend, refund, or store any multi-asset must follow the same rules. Getting a multi-asset transaction is, by definition, the same as receiving any other Cardano transaction. The only distinction is that the transaction may include additional data, such as multi-asset.

It's best practice for all exchanges and third-party wallets to check and process any multi-asset transactions in the block. It is up to the user to decide how these sorts of transactions are handled.

What about unwanted tokens? The function of any multi-asset may be anything you want it to be, but it's crucial to remember that, like ada, it's part of the transaction and must be managed and balanced accordingly.

Multi-assets will not present any problem, whether they are in the wallet of the issuer or the wallet of the exchange. Until it is redeemed, utilized, or burnt, it will be 'live'.

The exchange or third-party wallet is ultimately responsible for deciding what to do with a multi-asset.

To handle and maintain UTXOs, cardano-wallet employs a UTXO algorithm. On the blockchain, a multi-asset managed via cardano-wallet might easily go undetected.

Choosing a UTXO means taking into account the asset associated with that UTXO. An out-of-balance error will result if this additional input is not handled appropriately.

You have complete control over the native asset. You have two options: return it to the sender if you know the address or transfer the native asset to an address in your wallet while complying with network conditions and the minimum UTXO value.

For more information on establishing and balancing a transaction with a native asset attached, see the *native tokens* section of Cardano Docs.

Scenario 2 – Surprise receipt of multi-asset in cardano-wallet .

Note: This scenario only applies to exchanges that use cardano-wallet .

Confirm you have received a multi-asset

1. Check the wallet information to confirm
2. To confirm the wallet information, use the curl command below:

Shelley

```
curl http://localhost:8090/v2/wallets
```

3. Confirm in the assets section:

```
"assets": {  
    "total": [  
        {  
            "asset_name": "2e7444437f696e",  
            "quantity": 10,  
            "minting": {  
                "script": "sha256:  
                    2e7444437f696e  
                ",  
                "quantity": 10  
            }  
        }  
    ]  
}
```

```
        "policy_id":  
        "f325fdd8f936d76d3d9944358380cff64d0db66e545f99a3cc01ab97"  
        }  
    ],  
    "available": [  
        {  
            "asset_name": "6e7466636f696e",  
            "quantity": 10,  
            "policy_id":  
            "f125fdd8e336d56d3d9943117380cff64d0db66e545f99a3cc01ab97"  
            }  
        ]  
    }  
}
```

What about token redemption or getting rid of unwanted multi-assets from cardano-wallet? Tokens generated using a minting policy adhere to a set of guidelines. For example, the minting policy might enable token holders to burn or produce new tokens. If you obtain undesirable tokens, you must usually return them to the issuer or sender, or store them someplace else for protection. For further information on minting policies, see minting policies docs section. [\[438\]](#)

Note that transmitting any quantity of native asset costs one ada plus the transaction fee as a minimum. For more details on the minimum UTXO requirements, see the minimum ada value requirement section in the docs. [\[439\]](#)

Option 1: Return tokens to the sender or issuer:

1. Confirm the sender's / issuer's address.
2. In cardano-wallet, create a JSON transaction with a minimum UTXO of one ada and include the native asset.

Sample transaction for sending a multi-asset:

```
curl -XPOST http://localhost:8090/v2/wallets/{wallet_id}/transactions
\H "Content-Type: application/json \; charset=utf-8"
d "{"
  "payments": [
    {
      "address": "{destination_address}",
      "amount": {
        "quantity": 5000000,
        "unit": "lovelace"
      },
      "assets": [
        {
          "policy_id": "asset_policy_id",
          "asset_name": "6e7436436f646e",
          "quantity": 5
        }
      ]
    }
  ],
  "passphrase": "mylittlepony"
}
```

Confirm that the multi-asset transaction is complete, and that the assets have left the wallet.

Shelley

```
curl http://localhost:8090/v2/wallets
```

4. You should see the following result:

```
"assets": {
  "total": [],
  "available": [] }
```

Option 2: Move tokens to an address inside the existing wallet:

1. Confirm you have native tokens in the wallet.
2. Specify an address from the wallet to send the tokens.
3. Follow the steps in Option 1 to send the tokens to an address.
4. Keep track of the address containing native assets.

Listing native assets on an exchange

Many native assets are now functioning on Cardano, and new ones are being added on a regular basis. Some of these native assets have performed well in the market, where community members and financial institutions have shown interest and invested. There is a non-exhaustive list of native assets that are on *CardanoAssets.com*.

Going public with native assets

Token creators have two options for making their tokens available to the public:

1. Sell the native asset privately in a token sale, or
2. List the native asset on an exchange while adhering to the exchange's policies and guidelines.
3. Third party platforms like Dripdropz, the 'Cardano Token Distribution System'

Private token sale

Native asset producers who want to sell their tokens privately should do their due diligence and research first before deciding on the best way to do it.

Listing on an exchange's marketplace

Native asset developers may choose to list and sell their tokens on an exchange. When it comes to token listing, each exchange has its own set of regulations, standards, and laws.

From a technical standpoint, IOG can assist with any queries. IOG can help with things like token generation, minting, and burning, but any inquiries about the listing process should be handled to the appropriate exchange. Listing processes vary by exchange, eg. Kraken^[440] or Binance.^[441] If you are planning to list a native asset on an exchange, it's best to speak with the exchange directly first.

Technical support: When it comes to technical assistance for exchanges, the Cardano Foundation is the initial point of contact. If you have any technical problems or difficulties, contact them through the standard support channels, or submit a support request.

The Different Devnets

A blockchain ecosystem isn't one that sits still for long (writing a book about it is an exercise in constant revision). Cardano, like other blockchains, evolves as its community grows and learns. Cardano has a thriving and knowledgeable community, one of the most powerful and intelligent in the crypto field. IOG aims to reach out to other communities and get them on board, in keeping with their avowedly non-'maximalist' and open approach.

Cardano's strategy, as detailed in Charles Hoskinson's video 'The Island, The Ocean and the Pond,'^[442] is the creation of a variety of devnets to attract new developer communities into the Cardano ecosystem. These devnets serve as 'bridges' connecting developer communities, offering development environments, virtual machines, and developer tool suites so that new applications may be tested in a realistic setting.

KEVM

IOG have worked on and off with Runtime Verification on the K Ethereum Virtual Machine (KEVM) initiative. After some early exploratory work in 2018, the KEVM devnet^[443] was to be the first of many to be launched. The EVM is implemented in the K Framework,^[444] which has been dubbed 'software that can't afford to fail.' The

Ethereum Virtual Machine (EVM^[445]) is responsible for Ethereum smart contracts.

For the greatest levels of assurance, K uses formal logic and mathematical rigor. It allows programmers to specify or implement a programming language's formal semantics in an understandable and modular manner. K additionally creates a 'correct by construction'^[446] VM executable from its formal specification, which is fast and powerful enough to execute actual applications and smart contracts. This simply means that software should execute just the functions requested and provide verifiable proof for all conceivable inputs.

IOG's long-term goal, in collaboration with collaborators at Runtime Verification, is to create a K environment that allows them to simply 'plug-and-play' additional virtual machines. The KEVM devnet, which was geared for the Solidity/Ethereum community, was to provide complete Ethereum backward compatibility. Solidity, like JavaScript and C++, is a high-level language that cannot be directly run by the EVM. To execute on the KEVM, Solidity applications must first be converted to assembly language (EVM bytecode).^[447]

IOG states on their Goguen roadmap page^[448] they have:

paused its collaboration in the K framework project in order to focus on other priorities, but is enthusiastic about the vision and may participate again in the future.

IELE

While full compatibility with the EVM is easy and appealing to many experienced Ethereum developers, KEVM also inherits the EVM's flaws.

As a result, IOG were to provide a more sophisticated and secure option in the shape of the IELLE devnet. IOG partnered with Runtime Verification to work on the IELLE virtual computer, which is comparable to the EVM but significantly more secure. It employs

arbitrary precision numbers, for example, which instantly eliminates many of the EVM's flaws. IELF is also register-based, rather than stack-based like the EVM, which makes writing IELF bytecode by hand considerably simpler.

The acronym IELF (pronounced YELL-eh) stands for two things:

- The IELF Virtual Machine (VM)
- The IELF Assembly Language

IELF is a human-readable blockchain low-level language used to build third-generation blockchains. IELF was built using state-of-the-art formal methods to handle Ethereum's security and accuracy problems while also providing the mathematical correctness of smart contract code verification that KEVM adds to Ethereum. IELF was to be the next phase in the development of autonomously produced, correct-by-construction implementations. It's designed to be the cornerstone of a full compiler backend, allowing for extensive gas optimization, including contracts written in a high-level language like Solidity, or Plutus, that uses IELF as its compilation target.

IOG have a similar status for IELF on the same Goguen roadmap page:

After significant contribution to the project, IOHK has paused its collaboration on IELF to focus on other priorities for the time being, but is enthusiastic about potentially returning to the project in the future.

Glow

The next devnet to be deployed was Glow in early 2021. Solidity is the most common higher-level programming language that compiles to EVM bytecode, although it is far from the only one. Glow, created by IOG partner MuKn (Mutual Knowledge Systems - mukn.io), is an alternative to Solidity.

Glow is a ‘high-level’ language (other examples include JavaScript, Python, and others) that allows for intuitively constructing extremely secure financial contracts. To prevent mistakes and possibly expensive defects, Glow adheres to the ‘correct-by-construction’ approach. Glow may show that contracts created in this language have certain desired features, regardless of what the other contract parties do or do not do. Glow was created with the goal of interoperability in mind. Glow compilers are available for a variety of platforms and blockchains, making code reuse easier and more practical.

Connecting developer communities

Goguen’s major aim for the KEVM, Glow, and IELE devnets was to provide Cardano usage and usefulness, as well as to form strong, long-term collaborations that contribute to the continued expansion of the Cardano developer ecosystem. To encourage adaptability and diversity, IOG wants to recruit as many developers from as many fields as possible.

While work with Runtime Verification was put on hold, the mission is still the same. Cardano shifted to focus more on a sidechains model. In a sign of a thriving ecosystem, there are more and more third-party sidechains being launched. Milkomeda^[449] went live in March 2022, an ingenious Layer 2 Protocol (Rollups^[450]) delivering EVM capabilities to non-EVM blockchains. It runs on Cardano, Solana and Algorand. Milkomeda was born from collaboration with dcSpark (dcspark.io). dcSpark was founded by former Emurgo and IOG developers and have already, in a short space of time, made significant contributions such as the Flint wallet. dcSpark are trailblazers for Cardano, attracting developers to enter the space and ensure there is diversity in the ecosystem, and not an over-reliance on IOG.

April 2022. IELE update from twitter space ‘Sunday Chat with Charles’. CH:[451]

So ‘the island, the ocean in the pond’ was really a segregation of three different strategies. So one was saying ‘how do you create a really end to end beautiful, well curated development experience, which is built for applications that should not fail?’ I frankly feel DeFi, identity, ... These types of things should not fail. \$10.5bn last year was lost because of poor code.

And so we created Plutus based on an extension of what we learned from the Haskell ecosystem. We kind of brought the old crew who created Haskell back together and said, ‘hey, now that you’ve been thinking about this for 40 years, let’s do it again.’ And they created a really wonderful thing and this year (2021) we’re seeing that mature rapidly.

So in June (2022) the extended UTXO Plutus development model is going to get much better, and there’s probably going to be another six months to a year of enhancements and upgrades to get to the idealized form that includes certification and a litany of other things. So that alone is a phenomenal achievement, and that’s our only achievement in this space, I think we’d win a lot of the Fortune 500 and governments and other people to use Cardano because they care about it not failing, and it’s fine for an engineer to go spend two to three months to learn something because, at the end of the day, that they already have the users, it’s not about being first to market.

Then you have to recognize that there’s tremendous progress with solidity and EVM, and that the ecosystem has a lot of adherences. A lot of developers and you need to be able to get interoperability there. So we call that ‘the pond’, and so we’re chasing that. And that’s also being chased by dcSpark who recently released Milkomed. EVM interoperability is a priority, and it’s already achieved on Cardano and more to come. So the pond and the island strategies are both well underway and there’s enormous progress in both cases and we’re really getting it done.

Your question was about the ‘ocean’, which is the intoxicating thing, and the ‘ocean’ is all languages, so IELE was the platform

that we created out of University of Illinois with Runtime Verification, and that was a derivative of LLVM, which was created by Apple in 2003. The idea was that IELF would kind of be like a universal language using this framework called K. What you would do if you wanted to support new programming languages, you would write the case semantics of that language.

This would be done by the language group themselves. So Python was wanted. Do people maintain Python? Would it deliver for Cardano Python fans or whatever, and then you'd submit it as a transaction and then use what's called semantics-based compilation to convert one k specified language into another k specified language. So basically you get universality and over time you'll have thousands of programming languages that are supported.

Now we chased this dream, off and on for four years. My company personally invested, I think, probably more than \$10m into R&D. Papers were written involving Reachability logic and other things. And we just kept chipping away at it and this year we got to a point where we were no closer to that dream. Despite the assurances we got. And despite the academic progress we got, than we thought was reasonable for the money that was invested.

So what we did is we took a step back and said, 'is there a less ambitious, but still quite nice strategy that could get us most of what we'd like to get with the ocean, which would be effectively interoperability with mainstream programming languages?' So about the main programming languages...the top 15, top 20 and so forth, so the best option there would be Web assembly support, WASM (webassembly.org).

And we've been exploring that and having some discussions there. But to be frank, we're under-resourced. RV was doing heavy lifting with IELF, which meant that we didn't have to touch the 'ocean' strategy and our engineers were primarily involved in the sidechain strategy, which gives us multiple computation

layers. So that's the basic infrastructure to get new environments and also improvements to Plutus itself and working and building out the Plutus ecosystem.

So we had kind of a divide and conquer, and now that we can't rely on RV for the 'ocean' strategy, we have to kind of go back to the drawing board on what's a better approach for it now. Some of this is theoretical computer science. It's been the Holy Grail of computer science... universality. The easy program translation from one language to another, it's a super hard problem and then part of this is also just practicality. So web assembly, for example, already has mainstream support for most programming languages that matter, and if you're downstream of that, then you may not have to actually build anything proprietary or any infrastructure for Web Assembly. You just have to create the metering system for it.

Then there's a question of the accounting model and a litany of other concerns and considerations. So this is something the Ethereum space has been chasing for quite some time because it wasn't lost on Vitalik (Buterin) ...universality is very important. So we're certainly looking into it. We certainly had a lot of conversations. I've spent a lot of my own money on this, and I continue to spend money on it, but it looks like the 'ocean' strategy will get kind of pushed over into the Cardano roadmap for the community to kind of think about and my hope is to get a little bit more diversity and strategy.

This kind of shows you the nature of research and development. So with R&D you go and reach for the stars, and you go and fund a bunch of different approaches, and some of them work spectacularly well. Like for example, the Ouroboros research agenda where we knocked it out of the park and we got a perfect proof-of-stake system.

And other things you know they didn't work as well, like IELE for example, where I was extremely bullish about it in 2017, I really was excited about it, I thought it was frankly a better design. But then the minute we started pushing for universality, we were

having difficulty even getting some of the rank-and-file engineers at RV to get excited about it. And we were like ‘guys, this is the product you created.’ It seems to be a disconnect between the leadership on both sides and the rank and file who were actually accountable for this. The other thing is that we’re heavily represented in our organization by functional programmers and so they don’t pay as much attention, nor have the domain competence for the imperative side of the world.

So you know, it’s something I’d still like to do, and I see the huge commercial value in it, and you know, solving a subset of it is still a humongous leap forward, and regardless of the strategy, you still have to have the sidechains infrastructure. Regardless of the strategy, you still have to have a good ‘island and pond’ play.

But it just shows you how hard these things can be in practice and how many moving pieces there are and when you’re actually trying to go and do this, what can happen. That said, we did learn a lot. We gained K competency and that’s now being applied for certification of Cardano smart contracts. So when you look at the wallet that’s coming out, with the DApp store, you’re going to have certification levels: level 1, Level 2 and Level 3. A lot of that is inspired from that four-year journey, all that verification work and formal semantics work and so forth. We also learned an enormous amount about how the Ethereum virtual machine was written because we subsidized the first set of formal specifications for the KEVM, which gave us an enormous amount of knowledge and that world, but unfortunately IELI itself still is a very elusive thing.

Smart Contracts Rollout

Alonzo built on Cardano’s token improvements to provide developers with the tools they needed to create commercial DApps. IOG launched Mary, a multi-asset protocol update in March 2021 that enabled users to create native tokens for Cardano transactions. They laid the groundwork for Cardano to become the premier smart

contract platform by introducing transaction metadata,^[452] token-locking^[453] with *Allegra* in December 2020, and native token issuance.^[454]

These features were built into Alonzo, the following protocol update. Alonzo contributed functionality for smart contracts (digital agreements) to Cardano leveraging IOG's hard fork combinator technology. By facilitating the construction of smart contracts and decentralized apps (DApps) for decentralized finance (DeFi), it offered up new possibilities for developers.

Why smart contracts when we have Bitcoin and Doge?

Cardano's progress as a global distributed ledger continued with smart contracts. When it comes to regular commerce, a blockchain must ensure that people can transfer their money and pay for goods in a safe manner.

Smart contracts may be used to settle complicated transactions, keep the funds in escrow, and secure funds transfer under predetermined criteria. DApps may interface with Cardano's ledger to keep track of their actions and execute smart contracts. These digital agreements tell the tale of a transaction, specifying where money should go and under what circumstances they should be transferred, and only finalizing a deal if all of the requirements have been satisfied. Cardano is able to handle such applications thanks to *Alonzo*.

Alonzo presents a flexible framework for constructing smart contracts, while multi-asset support lets users design unique currencies that fulfill business demands. Collectibles, crowdsourcing, and auctions, for example, are now possible.

Deployment of escrow-based decentralized cryptocurrency exchanges (DEX) or the development of sophisticated apps supporting centralized stablecoins might be explored. Users may utilize token-locking to create utility tokens with vesting periods,

which means that tokens can be locked, or frozen for a certain duration of time, before being released.

Plutus Scripting

IOG developed the essential tools and infrastructure with *Alonzo* to enable Plutus Platform application development. *Alonzo* enhances Cardano Shelley's basic multi-signature scripting language (multisig) with a rigorous methodology based on formal methods and verification. For more sophisticated and secure scripting capabilities, Multisig was updated to the Plutus Core language. The *Alonzo* ledger uses Plutus Core to enable advanced scripting leveraging the extended unspent transaction output (EUTXO) accounting model.

The foundation for smart contracts must be both safe and dependable. As a result, Haskell was selected as the programming language for Plutus Core smart contracts. Haskell is a high-level programming language that is used by developers to code, which is then compiled into Plutus Core.^[455]

Haskell has been around since 1987, and it stands out among computer languages because of its high degree of trustworthiness. Smart contracts written in Haskell, and Plutus, are designed to accomplish precisely what is expected of them and can be checked for correctness before being implemented. This ensures that smart contracts written on Cardano will be simple and secure, which is critical for applications that manage automated trading or large-scale money transfers.

Tools and APIs

On Cardano, developers can test and adapt transaction validation using functional tools. The Plutus Core code is deployed and run on Cardano while communicating with wallets and the ledger, coupled with the an extension of the API library.^[456]

Alonzo's deployment is an iterative process. On the mainnet, working smart contracts are available, and IOG is working to strengthen the off-chain infrastructure to offer software development kits (SDKs).

The IO Global team eventually linked the Alonzo rules with the Cardano node and ledger code during Spring 2021. Cardano supplied API tools and command line interface (CLI) support after Alonzo integration with the node was complete.

IOG continued to work on Plutus development by launching a private testnet. Partners (advanced developers) tested the platform throughout this phase, producing and deploying non-fungible tokens (NFTs), marketplaces, and DApps that ran smart contracts on Cardano. This process emphasized incremental changes to ensure that everything ran smoothly.

IOG began working with the Plutus pioneers^[457] in May 2021. These certified program trainees proceeded to test the platform by creating Plutus apps and deploying them for DApps and DeFi in production. IOG completed the ledger, node, and wallet backend integration during this phase. IOG also made documentation available, which included specification examples and development tutorials.

Quality assurance and user testing were undertaken during the summer of 2021, followed by a feature freeze.^[458] This allowed cryptocurrency exchanges and wallets to upgrade and prepare for the Alonzo protocol update in September 2021.

What smart contracts technology is currently available?

Of the 18,000^[459] cryptocurrencies around today, with only 70 having smart contracts according to CryptoSlate.^[460] PolkaDot, Solana and Ethereum are among the participants on the market that support smart contracts. Technology is changing to suit the market needs for systems that are quick, secure, accurate, and dependable. Many firms have attempted to install large-scale apps on these platforms

and have run across ‘issues’. For example, the DAO hack,^[461] the Parity bug and the shambolic Solana Wormhole hack^[462] where \$320m went missing. Despite bad press, the most critical problems in smart contracts continue to surface.^[463] There is plenty of space for innovation here, and IOG is working hard to establish itself as a technological leader.

Predictable Transaction Validation

Cardano’s EUTXO model enables the deterministic nature of Plutus script execution. Cardano fulfills the rising need for decentralized solutions since the Alonzo hard fork introduced core Plutus smart contract functionality to the network. The Cardano ledger is designed with high certainty, security, and formal verification in mind. In line with this philosophy, it’s also critical to make sure transaction processing is deterministic, which means a user can anticipate the effect and result of a transaction before it’s executed.

With the addition of smart contract capabilities, the ability to ensure transaction execution costs and how the transaction acts on the ledger before it is submitted becomes even more important. Such features are provided by blockchains based on Unspent Transaction Output (UTXO),^[464] such as Cardano. Account-based blockchains, such as Ethereum, are indeterministic, meaning the transaction’s impact on-chain cannot be predicted. There is a danger of financial loss, extortionate fees, and potential for adversarial conduct as a result of this. Cardano’s deterministic architecture allows for secure transaction and script evaluation before execution.

What is transaction determinism?

In the context of transaction and script processing, determinism is synonymous with predictability. This ensures that a user may forecast locally (off-chain) how their transaction will affect the ledger’s on-chain state without:

- surprising script validation outcomes or failures

- surprising fees
- surprising ledger or script state updates.

Even if written properly, a transaction in a deterministic system may still be rejected. The transaction is rejected because it could not be applied to the ledger and so had no influence on its state, hence no fees are paid. The reason for this is because additional transactions completed between the time the first transaction is generated and the time it is processed cause ledger revisions. Even basic transactions might result in this. Another transaction, for example, may spend a UTXO that a user was also going to spend. When a transaction is accepted, determinism assures that it will only have predictable consequences on the ledger state.

Indeterminism (unpredictability)

We can't foresee what consequences a transaction will have on the ledger until it's executed, which is known as indeterminism. It's critical to consider indeterminism while developing the ledger and a smart contract interpreter. Access to changeable ledger data, or data that may be updated or altered, is one of the major risks in such a scenario. Indeterminism may arise when the changes made to the ledger by a transaction, or a smart contract are determined by the state of the ledger at the time of processing rather than the contents of the transaction.

Ethereum is particularly vulnerable to this issue. Between the moment a user makes a transaction and the time it is executed, for example, gas prices or a decentralized exchange (DEX) rate might vary. As a consequence, unanticipated gas expenses or price fluctuations in the assets being acquired occur. Alternatively, a script might simply fail, resulting in significant execution fees (hundreds of dollars) with no further consequences. This may happen, for example, if the money available to pay the gas fees run out during the time a smart contract is running. These possibilities are ruled out by deterministic ledger design.

Other possible sources of indeterminism include allowing scripts to see:

- data in the transaction block that isn't included in any transaction, such as system randomness, block headers, or the current slot number
- data that has been tampered with or replaced by an attacker, potentially changing the result of script validation while the transaction itself continues to be processed.

Improved script-writing processes, or layer-2 solutions, can probably reduce these shortcomings in most systems. Cardano is built to ensure that all scripts and transactions have predictable consequences.

UTXO and determinism

The Cardano ledger uses a UTXO accounting model, meaning that assets are held in unspent outputs rather than accounts on the ledger. Each of these outputs defines the number of assets held as well as their address. Unspent outputs are immutable, so a transaction may consume all of them but not modify them.

A transaction that transfers assets consumes one or more outputs and generates new ones that contain the same amount of assets as the ones consumed. These values, as well as their UTXO addresses, are stated in the transaction's outputs. The only means for a transaction to impact the effect of another transaction on the ledger is for it to spend the same UTXO as the later transaction, forcing the node to reject it. This is the essential characteristic that allows the UTXO paradigm to preserve determinism.

Compared to an account-based model, a UTXO ledger offers both advantages and disadvantages. For example, there will be fewer instances of transactions blocking one another in account-based models. Accounts, unlike UTXOs, are mutable (modifiable) ledger data. So, depending on whether it was executed before or after

another transaction that updates the same account, a transaction may show a different number of assets in an account. This situation may not result in the transaction being refused, but it may cause the ledger to change in unexpected ways.

A transaction may perform a variety of actions, including spending a UTXO. But what exactly is a transaction? How can they be verified? Modifications to the action validation process were the most substantial changes made by the Alonzo update.

Validating with signatures and scripts

Validating the actions that are being taken is a vital part of executing a transaction. When data in the particular field to that action is provided in a transaction, it is deemed to be taking action. When a transaction has a reference to 'U' in its input field, it is spending UTXO 'U', and when its mint field contains 'X', it is minting a token 'X'.

When a node processes a transaction, it checks to see whether it is capable of doing the action. For this, the transaction's creator must give necessary data, such as scripts, redeemers, or signatures. Spending a UTXO locked with a public key is a typical example of an operation that needs validation. To accomplish this step, the transaction must give a signature from the associated private key.

Cardano validates actions via scripts. The code in these scripts implement Pure functions with True or False outputs. The process of calling the script interpreter to execute a given script with given parameters is known as script validation.

Validation of scripts may be done for the following actions:

- To spend a UTXO that has been locked by a script address: the script that is executed is the one whose hash generates the address

- Minting a token: the script that is executed is the one whose hash is used to generate the token's policy ID
- Withdrawal of rewards: the script that is executed is the one whose hash is used to generate the staking address
- When applying a certificate, the script that is executed is the one whose hash creates the credential of the certificate issuer.

All transaction actions describe how to assemble parameters provided to that script, in addition to letting the node know which script to execute.

Simple multisig and timelock scripting languages are supported by Cardano's multi-asset ledger. Users may define the signatures necessary to undertake an action as well as the time period during which it can be completed. The actual slot number in the transaction that contains it is never visible to a timelock script. Timelock can only observe the carrying transaction's validity interval. Allowing a timelock script to view the current slot number (that is, data from the block rather than the author) would violate determinism. This is assured by the fact that a user cannot foresee how the script will function since they do not know the specific slot in which the transaction is executed.

Unlike Plutus contracts in *Alonzo*, *Mary* scripts had a very restricted range of expression. The Alonzo hard fork ushered in a new age of rich, stateful contracts that don't undermine the ledger's determinism.

Plutus scripts

Due to the deployment of Plutus scripts, Alonzo presented a new strategy to transaction validation on Cardano. Plutus contracts are supported through the extended unspent transaction output (EUTXO) paradigm, which was implemented as part of Alonzo. A high-level summary of ledger and transaction modifications is provided below. Check out the Plutus Pioneer program^[465] (in its third iteration at time of this book) for greater depth on working with the ledger and Plutus scripts.

Alonzo makes the following adjustments to the ledger data:

1. Plutus scripts have the ability to lock UTXOs.
2. Script state-like functionality is enabled via a new component added to the contents of the output bits of UTXOs. A UTXO locked by Plutus scripts includes a datum in addition to assets and an address. A datum^[466] is a piece of information that represents an interpretation of the script state.
3. A number of new protocol parameters have been added to enforce extra transaction validation requirements. These include upper restrictions on how much processing power scripts may use.

Transactions have been updated to support Plutus scripts as follows:

1. The transaction now has a redeemer, which is a user-specified parameter for each of its actions. A redeemer may fulfill a variety of functions depending on the script. It may, for example, serve as the user's decision to give a thumbs up or down on social media, or the handle adopted by a gamer, among other things.
2. The transaction contains each script's computational execution budgets.
3. Alonzo provides extra bits of data to verify that a transaction can pay its execution fee (more on this later).
4. Transactions include an integrity hash, which is used to confirm that it hasn't been tampered with, isn't expired, and so on.

In comparison to Mary, there are certain differences in the technicalities of Alonzo transaction validation. The node assembles script parameters required by the Plutus interpreter for each action, including:

- datum
- redeemer
- execution budget
- transaction summary

The node runs new Alonzo-specific checking to guarantee that the transaction is built properly. It must not, for example, exceed the maximum execution resource budget. It also executes the scripts using the Plutus script interpreter.

Datum objects vs script state

Mutable script state, like mutable accounts, belongs to the ‘mutable ledger data’ category of indeterminism sources. The UTXO paradigm overcomes the indeterminism of mutable accounts. It may also assist in reimagining the idea of script state in a deterministic manner. If a Plutus script locks a UTXO, the script code for that UTXO is connected with its address. The datum contained in the UTXO is the script’s state-analog. When a transaction spends that UTXO, the transaction, including the datum, is erased from the ledger. The Plutus script’s contents, on the other hand, may require that the transaction carrying it produce a UTXO holding a certain datum that may be seen as the updated script state.

Execution budget

The non-deterministic gas model has the tendency to charge consumers unexpectedly high costs. This form of indeterminism is addressed in Cardano scripts by requiring that both the resource budget and the fee necessary to cover it be included in the transaction. When creating a transaction in Alonzo, a user may forecast both locally. Script execution will always return True or False, and it will not loop endlessly. This is because every action a script does consumes a non-zero amount of resources, which the interpreter keeps track of. If the transaction’s budget is exceeded, the script is terminated and False is returned.

Transaction validation since Alonzo update

The following essential elements address potential causes of indeterminism and make the results of script and transaction validation predictable:

- When applied to the same parameters, the script interpreter will always finish and deliver the same validation result
- During validation, a transaction must correct all parameters that will be provided to the script interpreter
- A transaction lists all of the actions it's taking that need script validation
- On a transaction, compulsory signatures guarantee that it cannot be tampered with by a malicious actor in a manner that causes scripts to fail
- In the EUTXO ledger model, implementing a transaction is deterministic.

The final point is inherited from the UTXO model, since Alonzo ledger protocol upgrades are essentially consistent with prior era updates (including the delegation scheme, etc.). Since the Alonzo upgrade, script validation failure or success has an impact on how a transaction is handled. For a particular transaction, however, the True or False returned, as well as the ledger modifications associated with either outcome, are predictable.

Cardano's script and transaction validation exhibits deterministic behavior, but this is not a natural result of using EUTXO. To guarantee this feature, the IOG team had to trace the source of every piece of data that a script is permitted to see.

Cardano's two-phase transaction validation process.

Alonzo transaction validation is performed in two phases to ensure fair compensation for validation work. IOG have devised a custom two-phase validation approach based on the assurances offered by the Alonzo ledger's deterministic architecture. It is intended to reduce the amount of resources used by nodes to verify network transactions while also avoiding unexpected charges for the user.

Transaction validation was a one-step operation throughout the *Shelley*, *Allegra*, and *Mary* eras. Before it was implemented, the impact of a valid transaction on the ledger was completely

foreseeable. A transaction was included in a block and added to the ledger if it was valid. If not, a node would reject the transaction after a failed validation attempt, and it would not be included in a block. Regardless of whether or not the transaction ended up in a block, nodes that verified incoming transactions needed time and resources.

Plutus scripts, which Alonzo introduced, may need substantially more resources to verify than simple scripts from past eras. *Alonzo* offers a two-phase validation solution to alleviate the problem of nodes investing effort verifying scripts of transactions that are rejected. This approach assures that transactions are applied to the ledger in a predictable manner, as well as those nodes are fairly compensated for their effort and resource use.

Validation over two phases

On Cardano, transaction validation is split into two stages. The basic goal of implementing two-phase validation is to reduce the amount of uncompensated validation work performed by nodes. Each phase has a specific role to play in reaching this aim. In general, the first step determines if the transaction is properly designed and capable of paying the processing fee. The transaction's scripts are executed in the second phase. Phase-2 scripts are executed if the transaction is phase-1 valid. If phase 1 fails, no scripts are executed, and the transaction is rejected right away.

As a result, even if the transactions are not phase-2 valid, nodes are assumed to add processable transactions to a block. This signifies one of two things:

- A node does some uncompensated effort to determine that a transaction is not processable, but no costly phase-2 validation is performed, or
- the transaction can be completed. After that, the node can do phase-2 script validation, designate the transaction as phase-2 valid or phase-2 invalid, and add it to a block. In any instance,

the fee or collateral acquired from this transaction will be used to reimburse the node for both phases of validation.

Phase-2 failure should be minimal, since a user who submits a transaction with failed scripts would lose ada while accomplishing nothing. Because this is a locally predicted occurrence, it can be avoided. The phase is a needed precaution to ensure that scripts' possibly resource-intensive computations are compensated for. Let's take a deeper look at each phase.

Phase 1

The initial step in the validation process should be straightforward. Because it cannot take processing fees from unprocessable transactions, if this phase fails, a node is not rewarded for the work it has done. Phase 1 validation ensures that a transaction has been accurately constructed and that it may be added to the ledger. The following checks, as well as a few more, are included in this validation:

- It pays the necessary fees and provides the appropriate collateral (i.e. ada collected in the case of script failure)
- it contains all of the information needed to run Plutus scripts
- It does not exceed any of the protocol parameters' limits
- Its inputs are UTXOs that already exist on the ledger
- The transaction's stated computational budget does not exceed the transaction's maximum resource limit
- integrity hash checks, etc.

A node must conduct all phase-1 validation tests before adding an incoming transaction to the mempool (and, subsequently, to a block). If any of these checks fail, the transaction is refused, and no fees are collected. This was the sole validation step in past eras, and Cardano handled all validation failures in this way.

Honest, non-compromised nodes are unlikely to create unprocessable transactions deliberately. Nodes may also drop

connections that are disseminating phase-1 invalid transactions in an adversarial way.

Phase 2

Plutus scripts are used in the second phase of validation, which can be more computationally intensive. As a result, fees are charged regardless of whether the second phase was successful or unsuccessful. The ada that is collected is put into the fee pot, which pays nodes for the resources they consumed in the validation process. Phase-1 validation does not promise that all of the transaction's actions will be processed, simply that the collateral can be collected. Phase 2 validates Plutus scripts, and depending on the results, the decision is taken whether to proceed with full processing or only collect collateral:

- completely apply the transaction (before Alonzo, this was the only option) – if the Plutus scripts verify all of the transaction's actions, or
- if one of the Plutus scripts fails, collect the collateral ada and discard the remainder of the transaction.

Remember that script validation has a locally predictable result and will always terminate. Users may evaluate the results of script validation locally, and there will be no dispute among honest nodes on how to process a transaction and its scripts.

Collateral

Even if the scripts do not validate, nodes must be rewarded for their efforts. However, you can't just remove funds from the transaction inputs since they may have been locked with scripts - the ones that failed. As a result, Alonzo makes a particular provision for it. The amount of ada that will be collected as a charge in the event of a phase-2 script validation failure is the collateral of a transaction. In order for the transaction to be processed, this sum must be at least a

specific percentage of the transaction fee, as stated in a protocol parameter.

This amount is set while the transaction is being created. Not directly, but indirectly by adding collateral inputs into the transaction. The transaction's collateral amount is the entire balance in the UTXOs corresponding to these specially marked inputs. These UTXOs must hold no tokens other than ada and are required to have public key addresses (rather than script).

Only if any script fails phase-2 validation does the collateral inputs get deleted from the ledger UTXO. As in past eras, if all scripts pass, the set transaction fee amount is paid. The funds come mostly from ordinary, non-collateral inputs, whereas collateral inputs are disregarded. Only one of the two sets of inputs is ever taken from the UTXO, so it is allowed to use the same inputs for both collateral and ordinary non-collateral.

The signatures necessary to verify the expenditure of collateral inputs are also necessary to guarantee the transaction's integrity. They accomplish this by prohibiting adversaries from modifying its contents, resulting in a processable transaction that fails phase-2 validation. An adversary taking the place of a redeemer is an example of this. To make such a modification, the signatures of collateral key holders are needed. If script validation fails, the collateral key holders are the only users who would lose any ada.

The collateral key holders may verify locally whether the transaction will pass phase-2 validation on-chain before signing it since script evaluation is deterministic. If it does, they may be certain that it will do so on-chain as well, and they will not risk their collateral. A user should never lose their collateral if they are behaving in good faith. They may also reuse the same collateral inputs for several transactions while ensuring that the collateral is not collected.

The concurrency non-issue

Shortly after the Goguen hard fork there was a spate of accusations of Cardano being only able to process one transaction at a time due to concurrency issues.^[467] An objective analysis can only conclude this was FUD (fear, uncertainty and doubt) spread mostly by Cardano competitors.

Addressing the concurrency FUD, Charles Hoskinson used the analogy of single core processor vs multi-core processor:^[468]

The analogy I like to use here is when we went from single core processors to multi-core processors. You'd see the marketing dual core, quad-core, 8 core, 16 core, that meant software under the hood actually had to be written a little differently to take advantage of parallelism. If you didn't do it you could have 16 cores, 32 cores ..but only one would actually be engaged, one thread would be engaged in that application, unless the application was rewritten for it. It's a bit disingenuous then to say, 'oh well intel's a scam ...ARM is a scam and AMD is a scam... they lied to us they said 16 cores, but I only use one core'. Well, that's a software contingent thing, those are there, you can access them, there are design patterns to do that. We've gotten a lot better today than we were when the dual core world came out, but you still need to introduce parallelism into your code in order to do that.

One or more inputs may be used in a blockchain transaction, as well as one or more outputs. If one wishes to grasp how a transaction works and how it pertains to the Unspent Transaction Output (UTXO) accounting model, one must first comprehend the idea of inputs and outputs. Consider a transaction to be the operation that unlocks past outputs while also creating new ones.

Transaction output

An address (which you might regard as a lock) and a value are included in the transaction output. In line with this analogy, the address's signature is the key that unlocks the output. An output may be used as an input after it has been unlocked. New transactions

use previous transactions' outputs while also producing new outputs that may be consumed by subsequent transactions. Each UTXO may only be used once, and it must be digested in its entirety. Only one input may spend each output.

Transaction input

The output of a preceding transaction is referred to as a transaction input. A pointer and a cryptographic signature that serve as the unlocking key are included in transaction inputs. The key unlocks a prior transaction output, and the pointer refers back to it. The blockchain labels an unlocked output as 'spent' when it is unlocked by an input. New inputs may then refer to new outputs produced by a given transaction, and the chain continues. The UTXOs are the new outputs (which have not yet been unlocked / spent). As the name implies, unspent outputs are outputs that haven't been spent yet.

Multiple transactions

There are some pointers to keep in mind when submitting multiple transactions. When the mempool fills up, users that need to submit several transactions one after another may have issues. This is referred to as 'high throughput.' Some transactions may not be approved if the user continues to submit transactions after the mempool is full. The system has never guaranteed a transaction can be submitted reliably. In a distributed system like Cardano, such a guarantee is difficult to offer. Resubmission logic must be handled appropriately by submitting agents.

The cardano-submit-api is the proper endpoint to utilize. The thread is halted when the mempool is full. As a result, the API user may queue several transactions, which will be handled as soon as mempool capacity is available. However, the application must account for the fact that the number of in-flight transactions is restricted by the operating system's maximum number of open files. If this limit is reached, cardano-submit-api simply quits, and no more requests are processed. Using *ulimit*^[469] to raise the number of open

files permitted by the operating system will increase the number of in-flight transactions available, reducing UTXO congestion.^[470]

To avoid the requirement for complex queue management, you may use the cardano-submit-api serially or with extremely low concurrency.^[471]

It is a general rule that simplicity promotes resilience; if your use case allows, just submit one transaction at a time and wait for it to be verified before moving on to the next.

How EUTXO handles concurrency on Cardano

The EUTXO paradigm in Cardano offers a safe and adaptable environment for processing many operations without experiencing system problems. Cardano is a UTXO-based blockchain that uses a different programming model than existing account-based blockchains like Ethereum for decentralized applications (DApps). Cardano employs the Extended Unspent Transaction Output (EUTXO) paradigm, which was implemented with the *Alonzo* update. As a consequence, EUTXO provides a distinct solution to parallelization, allowing for increased security and cost predictability (without nasty shocks) in smart contract execution.

The per-branch architecture of the UTXO (Bitcoin) model is carried over to EUTXO, where one branch is defined as a series of transactions requiring a succession of validations. Building DApps and other solutions with numerous UTXOs is vital for splitting the functionality over various branches and enforcing additional parallelism. This has scalability advantages, much as creating Bitcoin services necessitates breaking one wallet into sub wallets.

Cardano DApps aren't restricted to only one transaction per block. In actuality, the block budget (the max number of transactions it can carry) permits hundreds of simple transactions and numerous complicated scripts to be executed simultaneously. The EUTXO approach, on the other hand, only permits a transaction output to be

spent once. Because users may experience contention while attempting to access the same UTXO, it is critical to employ a range of UTXOs. This is significant unless the architecture would gain from a rigorous ordering of clients. Design patterns that involve semaphores^[472] may be implemented using sets of UTXOs.

Furthermore, several users may interact with a single smart contract without causing a concurrency problem. This is because a smart contract can manage a variety of UTXOs that make up its present state, as well as off-chain metadata that enables those UTXOs to be interpreted.

Parallelism

Blockchains provide transaction processing immutability and transparency. To address the ever-increasing requirement for safe but efficient operation processing, every blockchain system should have the following properties:

- Throughput: the number of processes a system can complete in a given amount of time. This refers to the number of transactions or smart contracts completed in a second, for example
- System performance: how quickly the system operates. The execution time of a transaction or smart contract is measured by performance.
- Scalability: the system's capacity to handle many processes without overburdening the network or affecting performance.

The system's throughput can be raised while maintaining the speed of individual operations by boosting parallelism, but this kind of scalability will always be restricted by some degree of contention.

Concurrency, parallelism, and contention are all system considerations when it comes to scalability. Concurrency is required

in order for several actors to work on a job without disturbing each other. Parallelism enables such development to be made simultaneously without interfering with each other. Contention happens when different actors work concurrently, or in parallel, and interfere with one another.

What is concurrency?

Concurrency may enhance or harm a system's performance, throughput, and responsiveness. The max number of simultaneous operations that may be executed is limited by the level of concurrency. Processors or other agents in a UTXO-based blockchain should be able to do several activities at the same time to achieve real performance benefits. The max achievable parallelism rises as the amount of concurrency increases. As a result of this strategy, performance and throughput increases. It also has a number of benefits over account-based systems such as Ethereum.

Launching DApps on a UTXO ledger

Cardano's approach to DApp deployment is unique, with a steep learning curve requiring a new approach. Choosing from multiple programming languages is a similar analogy: there is usually a single end goal to implement something, but there is a plethora of languages you could use to get to this goal.

Concurrency optimization is a competence that must be mastered. Developers must code in such a manner that contention is limited (e.g., avoiding shared states and watch for accidental dependencies). This concurrency must then be turned into parallelism by the system. A number of developers (such as SundaeSwap^[473]) have previously found approaches to this problem, while others are currently working on them. In April 2022, WingRiders (wingriders.com) innovative DEX was successfully launched.^[474] It is not possible to simply apply the same skills learnt on another blockchain directly to Plutus smart contracts. The learning curve is steep, but the benefits outweigh the effort.

In any case, it's vital to remember that a developer can't simply use an adapted Ethereum contract to build a scalable DApp on Cardano. Cardano uses the UTXO model rather than the account-based one. As a result, a single on-chain state will not satisfy the concurrency property on Cardano. DApps should instead distribute their on-chain state across several UTXOs. As a result, their application's concurrency will grow, enabling greater throughput.

In the Plutus Pioneer program, Dr. Lars Brünjes^[475] previously presented a basic AMM-style^[476] DEX implementation. While this design is educational, it would not be fit for purpose for a commercial DEX that requires an order book approach and more concurrency. If a developer wants to deploy on the Cardano mainnet, they will need to increase the architecture's scalability.

A solution is outlined in the Djed stablecoin paper^[477] (covered shortly). An order book modeling pattern is preferred for the Djed^[478] implementation on Cardano, in which an order maker is responsible for sending any minting or burning orders to the stablecoin smart contract, with a separate incentive fee levied on each would-be buyer or seller of stablecoins and reserve coins. Several security techniques (eg. widespread use of non-fungible tokens) are also leveraged to ensure the uniqueness of transactions, the validity of each submitted order, and to thwart front-running^[479] attacks, NFT tokens are also used to indicate whether or not minting and burning orders were successful.

Re: WingRiders, Thinking Crypto Interview, May 21, 2022. CH:
[\[480\]](#)

I like the WingRiders team a lot, we talked to a lot of the different DEXs, because they had to kind of figure out how do you port something from a mindset of an accounts model to the extended UTXO model. It's a great model, but it does require translation and it's quite hard, in certain respects, to wrap your mind around it. It's kind of like when you go from a Java

programmer to a functional programmer. You start falling in love with functional programming, but there's kind of this translation time, where you have to get used to these new paradigms... you're like 'wait, i can't change the variables?!... how do i program anything?, this is crazy'

So WingRiders is the most advanced, at the moment, of the DEXes that are hitting the market, and they've really spent a lot of time and effort into building a great product and the team's pedigree is impeccable. It's vacuum labs (vacuumlabs.com) and they were the ones who did the Ledger (hardware wallet) integration and Trezor integration for Cardano. They created the AdaLite (adalite.io) wallet and so forth, so they've kind of been around for a long time and we've worked with that team a lot on these different integrations, and we came to respect their technical acumen.

...and just how they think, and how they work, so we got pretty excited when we heard that they're getting into that market, building a DEX... and you know it's launching and it's just one of many from Minswap to SundaeSwap ...and people have a lot of options now on Cardano, and usually settlement time is under a minute for all the DEXes that are here and there's tons of asset pairs that are trading, and there's good liquidity inside these things.

So this is what you look for, and it'll take probably another six months to a year for everything to completely stabilize, and for winners and losers to be selected, wallet integrations to be done and these types of thingsbut it's very encouraging overall to see the levels of advancement. SundaeSwap feels like a lifetime ago but that was really only six months (ago)... you know and now we're in a situation where you have something that's like an order of magnitude better entering market, but you know Sundae's gonna upgrade and the rest of these guys are gonna upgrade as well and then so so there's this Darwinism to the DEX space... and they're forced to either get better or die,

and every one of these teams are writing a lot of code, they're building very quickly...

Deploying DApps on Cardano

Cardano's EUTXO paradigm provides a strong foundation for decentralized finance (DeFi) and decentralized applications (DApp) development because it allows for parallel transaction processing, which allows for higher scalability than account-based models while also offering increased security.

When developing decentralized exchanges, utilizing a design suited to account-based systems, rather than the EUTXO model, may result in contention difficulties. This causes delays since a new transaction is reliant on the output of a prior transaction, particularly when there are a high number of transactions. To overcome this problem, programmers should avoid adopting a single-threaded state machine approach and instead write code with EUTXO features in mind.

A deep technical analysis of EUTXO ledger's architecture is beyond the scope of this book, however, you can get 'into the weeds' by reviewing IOG's blog 'Architecting dApps on the EUTXO Ledger'^[481] where they provide a sample architecture. SundaeSwap^[482] and Maladex^[483] also blogged about their solution while ERGOdex^[484] talked about their philosophy on 'Cardano with Paul'^[485] YouTube channel.

There are also some code samples from IOG on avoiding concurrency using multi signatures in the Lobster Challenge.^[486] IOG analyze a sample order book pattern^[487] architecture in their blog.

Babel Fees

Cardano is introducing a novel mechanism (muted for late 2022 in a recent update^[488]) that allows the payment of transaction fees in user-defined tokens on Cardano. Babel fees are named after the Babel fish,^[489] a creature in Douglas Adam's book *The Hitchhiker's*

Guide to the Galaxy that enables you to hear any language translated into your own. Despite the galaxy's many varied languages, this vision of global translation provides for meaningful communication.

Smart contracts allow for the creation of a wide range of unique tokens in the cryptocurrency sector. Babel fees are based on the idea of using your preferred token to interact with the platform. Similar to how you would interact with legacy financial systems, where you would use your local currency by just making a selection in a dropdown. 'Babel fees' convert the token you're using to the one required by the platform for transactions or whatever trade you want to execute on the platform. IOG's chief scientist, Prof Aggelos Kiavias, [\[490\]](#) was ahead of the curve when introducing this concept early in 2021. IOG also produced a video whiteboard walkthrough^[1] on their 'IOHK' YouTube channel at the time. The paper 'Babel Fees via Limited Liabilities' was subsequently published in April 2022. [\[491\]](#)

In most blockchains, it's typical that a legitimate transaction must come at a cost to the sender. Without such a limitation, anybody may overwhelm the system with minor transactions, overflowing its capacity and leaving it worthless. On that basis, a common implication is that for any blockchain that supports user-defined currencies, paying transaction fees in such tokens should be forbidden. Instead, transactions should be charged a fee in the platform's native token, which is seen as valuable by all of the token holders (hodlers^[492]). It's arguable that such a limitation is bad for adoption and interoperability with other blockchains and legacy systems. How are IOG planning to work around this shortcoming?

EUTXO enables innovation

Cryptography and game theory have a history of making the seemingly impossible achievable. Cardano's Extended UTXO (EUTXO) architecture enables a solution because of how native assets function on the platform.

Tokens may be generated using a minting policy, and they are regarded similarly to ada on the ledger. Creating a valid transaction requires the consumption of one or more UTXOs. On Cardano, a UTXO may hold more than simply ada; it can also handle a token bundle containing numerous distinct tokens, both fungible and non-fungible. It is therefore feasible to use a single UTXO to construct transactions that transfer many distinct tokens. Ergo, underrated pioneers in the crypto space, have already delivered 15k outputs per transaction using EUTXO and rollups.^[493]

The ledger's transaction fees are priced in ada, using a function fixed as a ledger parameter. The costs necessary for a successful transaction may be anticipated accurately prior to execution, which is a key strength of Cardano's EUTXO architecture. This is a unique property that other ledger configurations do not have. It's well documented how frustrating and unpredictable the Ethereum gas fees can be to process a transaction. Not only that, but the fees can also vary throughout the time it takes for the transaction to settle, since other transactions may modify the state of the ledger in the interim, influencing the required gas fees to process the transaction.

How will Babel Fees work?

Babel fees enable a transaction to announce an ada-denominated debt equal to the amount of fees the transaction issuer is required to pay. A transaction like this would be rejected by the ledger. However, it might be seen as an open offer in which the debt is taken on. Why would someone accept such a burden? To make this attractive, the transaction may give some quantity of token(s) to whoever covers the debt. The assumption being the token bundle is already existing in Cardano. This would be a one-to-one transaction between ada and the given token(s) at a fixed rate.

Consider a block producer who notices a transaction like this. The block producer may generate a matching transaction and claim the tokens on offer by absorbing the debt and covering it with ada. The transaction with the debt, as well as its matching transaction,

become admissible to the ledger as a group. The set of two transactions becomes priced in ada as a whole as a result of the debt absorption, and so it does not violate the ledgers' accounting requirements in terms of ada fees. As a consequence, the transaction with the debt is settled.

Users can propose transactions priced in whatever token(s) they own and have them settle in the ledger as normal transactions if a block maker is ready to take them up on the spot trade.^[494] This shows how native assets, the EUTXO architecture, and the small but powerful change of adding liabilities in the form of negative values in token bundles can handle Babel fees, allowing users to price transactions in any token that the system supports natively.

For the above concept to work, Cardano must have liquidity providers who have ada and are ready to issue matching transactions. The ecosystem of thousands of stake pool operators (SPOs) are obvious initial candidates to make the market by advertising exchange rates for their preferred tokens, etc.

Following the introduction of native assets with the *Mary* hard fork, the possibility of negative amounts in token bundles can be incorporated into Cardano's ledger rules. Aside from Babel fees, this opens up other use cases such as atomic swaps^[495] for spot transactions. It's just another example of how Cardano innovates instead of forking and copying first and second-generation blockchains.

A worked example

Below is an example transaction in human readable format. This is about Bill, Ted and Barney exchanging ada and a new native token, JohnCoin (JCN).

Transaction:

< Receive 20 ada from Bill
> Send 10 ada to Ted

> Send 9.66 ada to Bill
–Use 0.34 ada as the transaction fee

Bill has received 20 ada in the past, so has a UTXO worth 20 ada in Daedalus. He takes that UTXO, sends 10 ada to Ted, 9.66 ada back to himself, and uses the leftover 0.34 as the transaction fee. For it to be a legitimate transaction, the inputs and the outputs must be equal, ie. $20 = 10 + 9.66 + 0.34$

Now let's look at a transaction that uses JohnCoin, JCN as well as ada.

Transaction:

<Receive 20 JCN from Bill
<Receive 4 ada from Bill
>Send 10 JCN to Ted
>Send 10 JCN to Bill
>Send 3.66 ada to Bill
–Use 0.34 ada as the transaction fee

This time Bill wanted to send 10 JCN to Ted. He also had to include some 'extra' ada to cover the transaction fee. It worked fine, but it was inconvenient and not really sustainable if we were dealing with hundreds, or thousands, of transactions.

Here's how this same transaction would work with Babel fees.

Transaction:
<Receive 20 JCN from Bill
>Send 10 JCN to Ted
>Send 8 JCN to Bill
>Send -0.34 ada and 2 JCN to whomever takes on the debt
–Use 0.34 ada as the transaction fee

This poses some questions:

How can Bill pay the 0.34 ada fee if he didn't have any ada in

Daedalus begin with? With babel fees, this isn't a problem. So long as the inputs equal the outputs, the transaction is legit. The negative and positive ada in the outputs cancel each other out.

How can Bill send a negative amount of ada to just anyone, as a valid transaction? It isn't a valid transaction until someone 'volunteers' to take on the debt. It has to be voluntary as no one can be sent negative ada without their permission. Why would anyone 'volunteer' to take on the debt? They would not only take on the debt, ie. the negative ada, they would also receive the additional 2 JCN.

So the first user to 'volunteer' to take on the debt, Barney in this example, will make a transaction as follows:

Transaction:

<Receive 4 ada from Barney
<Receive -0.34 ada and 2 JCN from Bill's transaction
>Send 3.32 ada to Barney
>Send 2 JCN to Barney
–Use 0.34 ada as the transaction fee

Barney has volunteered to take on the debt of -0.34 debt, in doing so validating Bill's transaction. All fees were technically paid in ada, however, the way Bill sees it, he only paid using JCN.

If Barney wants the 2 JCN, he must also accept the -0.34 ada. They cannot be separated. Note that since two transactions were needed for this process to work, the total amount of fees paid was double than normal, 0.68 ada.

This means that the amount of JCN that Bill pays has to be greater than or equal to 0.68 ada to make it worth it for Barney. Since fees are relatively small on Cardano compared to other chains, doubling them shouldn't be a major issue.

This system works as long as there are users who consider the

asset ‘JohnCoin’ JCN to be of value. They will compete in a fair and open market to offer the best exchange rate for fees. Tokens not considered valuable are useless in this system and can’t be used to pay fees, but that’s the way it should be.

Research comes to life

Babel fees is just one area where IOG are bringing research into reality. IOG research engineer Paulina Vinogradova presented the elegant solutions being considered, competitive analysis of other chains’ solutions, as well as some of the remaining challenges in this presentation. [\[496\]](#)

February 27, 2021. Re: Babel fees. CH: [\[497\]](#)

...basically what that does is it gives every token issued on Cardano the ability to pay in the native asset, if there is a market for it. So it solves all the problems at the same time and you, as token issuers, now have your own network. It used to be that either you had to go borrow another network and pay in that network’s fees, or you had to launch your own network and build a network effect behind it. This is the third option. The space currently does not allow that to exist. There are some clever hacks here and there, but for the most part, it’s a new thing. It’s an elegant thing and it’s a thing that’s brought uniquely because of Extended UTXO.

And that’s the magic of doing things correctly. When you do things correctly, it’s very easy to just innovate, and just add and say, ‘here you go’. What that means is we’re probably going to be the ultimate stablecoin platform for all the stablecoins because you pay the transaction fee in the stablecoin. You don’t have to pay 100 of Eth to send a dollar of Tether. [\[498\]](#) you know that’s the point, and that’s what we’ve been looking for and that was just one of many things that came.

Stablefees

Cardano has a novel technique for making fees more equitable, stable, and predictable over time. Enabling transactions on cryptocurrency platforms runs afoul of the platform's underlying asset's dual purpose. Users may keep and trade it as part of their investment portfolios on one hand. On the other hand, it provides the 'gas' required for transaction processing. Because of this duality, the system should have a process for changing transaction prices so that they stay competitive and acceptable. The system should also enable users to identify the optimal fee for fast transaction processing, based on their particular demands.

Transaction fees are required for three reasons: For starters, transaction processing costs the system in terms or resources consumed. Allowing transaction processors, stake pool operators, to offset their expenses is only fair. Secondly, even with theoretically limitless capacity, transaction issuers must be prevented from flooding the network with worthless transactions in a DDoS attack. Thirdly, incentivizing transaction processors to deliver high-quality service is good practice.

The above issues may be addressed by charging transaction fees.

Learning from the past

The first system for pricing transactions on distributed ledger was introduced by Bitcoin. This system works in the same way as a first-price auction: transactions bid for a spot in a block with a certain reward, and block producers choose which transactions to include. Block producers are also granted the power to mint new coins, meaning that their operations are funded by the whole community via an increase in the overall currency supply. Over time, inflation decreases linearly, and transaction fees become more prominent in the rewards. This process has been challenged for its inefficiency, despite the fact that it has allowed Bitcoin to function for well over a decade. Over time, transaction fees have also increased.

In the Summer 2021, IOG introduced a new mechanism that complements the Babel fees^[499] idea and expands on Cardano's approach to ledger rules and system assets. The goal is to make fees fair, consistent, and predictable over time. The mechanism is described in the context of Cardano but it may be applied to any other cryptocurrency with equivalent properties.

What are Stablefees?

Stablefees' central concept is to provide a base pricing for transactions by tying them to a basket of commodities or currencies. Stablefees include native 'decentralized reserve' contract which produces and administers a stablecoin tied to the basket.

The idea mirrors the workings of the International Monetary Fund's SDR (Special Drawing Rights)^[500] which is a fiat currency that is evaluated against a basket of five currencies: the US dollar, the euro, the Chinese renminbi, the Japanese yen, and the British pound sterling. The stablecoin, or 'Basket Equivalent Coin' (BEC), is the currency that is used to pay transaction fees (and other pricing needs of the platform like Stake pool operator costs).

Ada has a dual purpose in this system: it serves as a reserve asset for the decentralized reserve and as a reward unit for staking. In severe cases when the reserve contract's liquidity is depleted, it may also be used as a fallback currency. The issuer will need to receive BECs before completing a transaction, either via third parties or directly by transferring ada to the decentralized reserve contract.

What criteria will the reserve use to distribute BECs? In return for ada, the reserve contract will also issue equity shares, referred to as decentralized equity coins (DECs). The decentralized reserve will often change the value of BEC to be tied to the underlying basket of commodities by leveraging the value of DECs. DECs will absorb ada vs. the basket fluctuations to keep the real-world value of BECs consistent. The AgeUSD^[501] stablecoin has already been implemented on Ergo (sigmausd.io). Ergo (ergoplatform.org) is an

innovative proof-of-work blockchain (also EUTXO-based) co-founded by the prodigious Alex Chepurnoy.^[502]

These three coins, which are issued by the system natively, will appeal to various groups. The security and liquidity of BECs (Basket equivalent coin) may appeal to risk-averse, transaction-heavy investors. DECs (decentralized equity coins) will get the most benefits if ada rises but will suffer the greatest losses if ada falls. DECs may be more appealing to long-term investors. Furthermore, since decentralized reserve pricing these currencies in ada, both BECs and DECs may make staking and governance easier. Returns may be provided at various rates, depending on the type of the coin. Ultimately, all rewards will be priced and paid in ada, which will continue to be the most adaptable of the three currencies.

Oracles

An on-chain oracle is at the heart of this system, determining the price of the basket in ada. This oracle may be implemented using stake pool operators (SPOs) in a decentralized fashion. From the fees received during BEC/DEC issuances, the reserve might award further rewards to all oracle contributors. This will guarantee two things: thousands of contributors from all over the world, and ledger rules that calculate a synthesized exchange rate in a canonical manner. For example, through a weighted median across all price submissions in an epoch. If oracle contributors misuse their contributions, their reputation and performance on-chain can be tracked, and they may be held responsible.

How does the pricing work?

How should transactions be priced, and block producers rewarded? Using the existing approach on Cardano, each transaction will be deterministically converted to a specific value denominated in BECs, using a formula defined by the ledger rules. The formula will consider transaction size as well as processing needs and may include runtime metrics like mean system load. The base fee will be

the result, ensuring that the transaction will be executed by the system. End users will be able to raise the fee by applying a multiplier to the base fee and speed up processing. This will be important during periods of high demand.

When contrasted to the first-price auction model, this strategy has one advantage: the pricing mechanism is continually stabilized to a fair default value. If necessary, users do price discovery in just one direction to speed up processing. Furthermore, transaction issuers may hoard BECs to protect their future transaction-issuing capacity while avoiding ada price volatility.

Stablefees vs Babel fees

The Stablefees mechanism may be seen as an extension of Babel fees — the decentralized reserve's spot conversion of BECs (basket equivalent coin) into ada. Both mechanisms work well together and complement each other. Babel fees may be used in tandem with Stablefees with one caveat: instead of ada, BECs can be used to pay Babel fees. This means that all costs will be paid in ada (via a Babel fee liability convertible in ada on the spot). As a result, the whole process is backwards compatible in that it won't affect casual users who just have ada and don't want to get BECs.

Regarding diversity, while the above scenario describes a single global BEC, the same technique may be used to issue regional BECs pegged to multiple commodity baskets with varied weightings. Such 'regional' BECs will be able to boost system inclusiveness while also allowing SPOs to have more fine-grained transaction inclusion policies.

Stablefees 'lite' alternative

The above approach necessitates the use of a decentralized reserve contract and the contract's issuance of BECs and DECs (decentralized equity coins) to purchasers. A 'lite' version forgoes the reserve contract and instead modifies the fee formula directly using

the price oracle to peg it to the agreed-upon basket of commodities. The mechanism that results denominates transaction costs in BECs and instantly converts them to ada. The amount due varies based on the value of BEC. The process is otherwise comparable, with the multiplier allowing unidirectional price discovery.

The main drawback is that a potential transaction issuer does not have access to a native token that allows for predictable transaction processing; instead, transaction issuers must pay fees in ada. Nonetheless, the fees will adapt and hold steady in relation to the basket due to the pegging mechanism. As a consequence, a transaction issuer will be able to properly structure their off-chain asset portfolio to suit their transaction requirements.

Research-driven approach

The granular aspects of the Stablefees mechanism are being researched by IOG. Charles Hoskinson mentioned in a recent update [\[503\]](#) Babel Fees will be released later in 2022. It's likely Stablefees will follow around that time. The pricing oracle and the global BEC will very certainly find uses other than paying transaction fees, extending the potential of DApps.

Djed algorithmic stablecoin

Cardano's algorithmic stablecoin is named after *Djed*, the symbol of 'stability' in ancient Egypt and the symbolic backbone of the god *Osiris*, the god of the afterlife and resurrection. Djed is the first stablecoin to remove price fluctuation via formal verification. One of the major roadblocks to cryptocurrency adoption is its volatility. Transparency, immutability of data, and proven security of financial transactions are all advantages of blockchain technology. It is, however, more difficult to forecast crypto market fluctuations compared to fiat currencies. This makes it difficult to use cryptocurrency in everyday life.

A stablecoin is a cryptocurrency that is linked to a basket of fiat currencies or a single fiat currency; commodities such as gold or silver; equities; or other cryptocurrencies. Stablecoins have built-in processes that maintain a minimal price variation from their target price, making them suitable for storing or exchanging value since the volatility is removed.

The price stability of certain stablecoins is jeopardized due to a lack of transparency and liquidity in their reserves. To solve these issues, IOG has partnered up with Emurgo (another of Cardano's three founding partners) and the Ergo blockchain, which, like Cardano, employs the UTXO-based accounting model, to develop Djed, a stablecoin contract. Djed has an algorithmic design, meaning it leverages smart contracts to guarantee price stability so a currency will be suitable for decentralized finance (DeFi) activities.

How stablecoins work underneath the hood

Different processes contribute to the coin's value stability and assist to minimize price fluctuations. The economic concepts of supply and demand underlie these systems. A popular technique is to back the stablecoin with a reserve of the pegged currency. If demand for sell or purchase orders exceeds supply, the supply should be raised to minimize price swings.

Stablecoin reserves aren't usually kept in cash. They are usually invested in financial assets that provide interest, such as bonds. The operator raises funds from the returns on these investments. Price stability is maintained as long as the stablecoin is fully backed by reserves in the currency to which it is tied — and the operator can respond rapidly to fluctuations in demand.

Risks

Investments are often connected with stablecoin reserves. Due to the lack of liquidity in these investments, the operator may be unable to respond quickly to demand. In the short term, this weakens

stability. Fiat-backed stablecoins have the disadvantage of requiring faith in the parties holding the reserves. Tether stablecoin (USDT) has already fallen as low as \$0.92 in 2017^[504] due to a lack of reserve transparency and the ‘full-backing’ claim, as well as ineffective stabilizing safeguards.

When the underpinning asset is a cryptocurrency on a public blockchain, there are no transparency concerns. Furthermore, because of its automated and secure processes, the adoption of smart contracts allows the rapid and reliable implementation of stabilizing steps.

What is an algorithmic stablecoin?

Djed is a crypto-backed algorithmic stablecoin contract that functions as an autonomous bank. It works by minting and burning stablecoins and reserve coins, as well as holding a reserve of base coins. The contract uses the reserve to buy and sell stablecoins and charges fees that accrue in the reserve to keep the price of stablecoins pegged to a target price. Holders of reserve coins, who contribute funds to the reserve while accepting the risk of price volatility, are the beneficiaries of this revenue stream.

The Djed stablecoin is intended to be a fiat currency-pegged asset with a governing algorithm. This method ensures a steady flow of funds. Djed isn’t only a dollar-denominated currency. It can function with any currency as long as oracles are available to provide the contract with the appropriate price index.

Formal verification

Djed is the first stablecoin protocol that has been formally verified. Djed’s design and stability features are considerably enhanced by the usage of formal methods^[505] in the programming process. Mathematical theorems are used to prove the properties using formal methods:

- Maintain the upper and lower bounds: the price will not move above or below the given price. Purchases and sales are not restricted in the typical reserve ratio range, and users have no motive to trade stablecoins on the secondary market outside of the peg range
- Peg stability during market crashes: the peg is maintained up to a certain limit, which is set by the reserve ratio, even when the price of the base coin falls drastically
- There is no insolvency since there is no bank involved, there is no bank contract to go bankrupt
- No bank runs because all users are treated equally and honestly, there is no reason for users to scramble to redeem their stablecoins
- Monotonically rising equity per reserve coin: the reserve excess per reserve coin is guaranteed to rise when users engage with the contract under certain circumstances. Reserve coin holders are certain to earn under these circumstances
- No reserve draining: under certain circumstances, it is impossible for a rogue user to carry out a series of acts that would deplete the bank's reserves
- Bounded dilution: there is a limit on reserve coin holders and their profit can be diluted as a result of issuing more reserve coins.

Versions

Djed is available in two versions:

- Minimal Djed: This version aims to be as minimal, intuitive, and simple as possible while maintaining stability

- Extended Djed: this more sophisticated version offers greater stability. The adoption of a continuous pricing model and dynamic fees to further encourage the maintenance of an appropriate reserve ratio are the primary distinctions.

Implementations

IOG, Ergo, and Emurgo have been testing various techniques by implementing the Djed algorithmic stablecoin contract.

SigmaUSD on Ergo was the first Djed stablecoin contract to be deployed. In Q1 2021, it was the first algorithmic stablecoin to be implemented on a UTXO-based ledger. It contained a 1% charge for buying and selling transactions, as well as an hourly exchange rate update from an oracle. An unidentified user with a big quantity of ERGs (Ergo's native currency) launched a reserve draining attack against the first version but the attempt was unsuccessful, and the perpetrator is said to have lost \$100k.

To deter similar attacks, the first version of Minimal Djed was replaced with a version in which the charge was set to 2%, the oracle updated every 12 minutes, and each oracle update could only affect the price by 0.49 % unless the price difference was larger than 50%. This increased resistance to reserve draining attacks.

The IOG team has also implemented Djed in Solidity. One version employs the Ethereum blockchain's native currency ether as a base coin, while the other can use any ERC20-compliant token as a base coin. These implementations have been launched to testnets for Binance Smart Chain, Avalanche Fuji, Polygon Mumbai, Ethereum Kovan, [\[506\]](#) Ethereum Rinkeby, and RSK testnets so far.

Djed: Cardano implementation

Cardano's Alonzo upgrade made Plutus smart contracts possible. Plutus runs on Haskell, which ensures a secure, full-stack development environment.

Stablecoins and reserve coins are native assets in this implementation that are uniquely recognized by the hash of the monetary policy that regulates their minting and burning via the Djed protocol. This approach also expects that oracle data, such as the exchange rate, be delivered to transactions as signed data rather than being posted on the blockchain.

In addition, there is an OpenStar implementation. OpenStar is a Scala-based^[507] framework for private permissioned blockchains. Djed's implementation with OpenStar is based on the concept of off-chain smart contract execution in order to create a stablecoin on Cardano that is not reliant on on-chain smart contracts.

See the Djed paper or Bruno Woltzenlogel Paleo's talk at Ergo summit 2021^[508] for more information about Djed stablecoin.

COTI (currency of the internet)

Charles Hoskinson and COTI chief executive Shahaf Bar-Geffen revealed at the Cardano Summit that the COTI (coti.io) platform will be the official issuer of Djed, a new Cardano stablecoin.

Stablecoins, according to the COTI development team, are a 'killer app' that will be used by a huge number of crypto users to settle payments and cover expenses. The cFund^[509] for Cardano Developments made its first equity investment in COTI.

COTI was to be 'the' stablecoin for Cardano, however, in April 2022 WingRiders launched with their DEX also bringing wrapped stablecoins^[510] (USDC and USDT) and liquidity through the Milkomeda bridge.

COTI have already signed 25 partnerships with DEXs in the build up to the long-awaited Djed launch. The private testnet is live and scalability issues are being addressed. The public testnet was launched in May 2022 and was followed by a full regress audit. Two

security audits will be conducted which is due diligence for such a financial token. June/July is the tentative date for the public mainnet launch. This coincides with COTI's plans to allow native assets to be minted. For the latest, visit the Djed website (djed.xyz).

Terra UST 2022 collapse

Terra's UST stablecoin^[511] lost its peg^[512] to the US dollar in early May 2022. UST plummeted to 9c forcing Terra to dig deep into its Bitcoin reserves (~\$1.3 billion) from its confirmed Bitcoin address^[513] in a desperate attempt to steady the ship. The dramatic collapse was summed up well by the Coin Bureau.^[514]

Tether (USDT), the oldest stablecoin, has previously received criticism for its lack of transparency^[515] and reluctance to be audited. The suddenness of Terra's collapse renewed skepticism on the viability of existing stablecoins and drove many^[516] to re-evaluate their views of Djed, and how it's designed to be more resilient to similar hazards. Shahaf Bar-Geffen confirmed in subsequent update^[517] that Djed survived unscathed from the same tumultuous weekend for the crypto markets.

Arbitrage behavior around Luna and UST

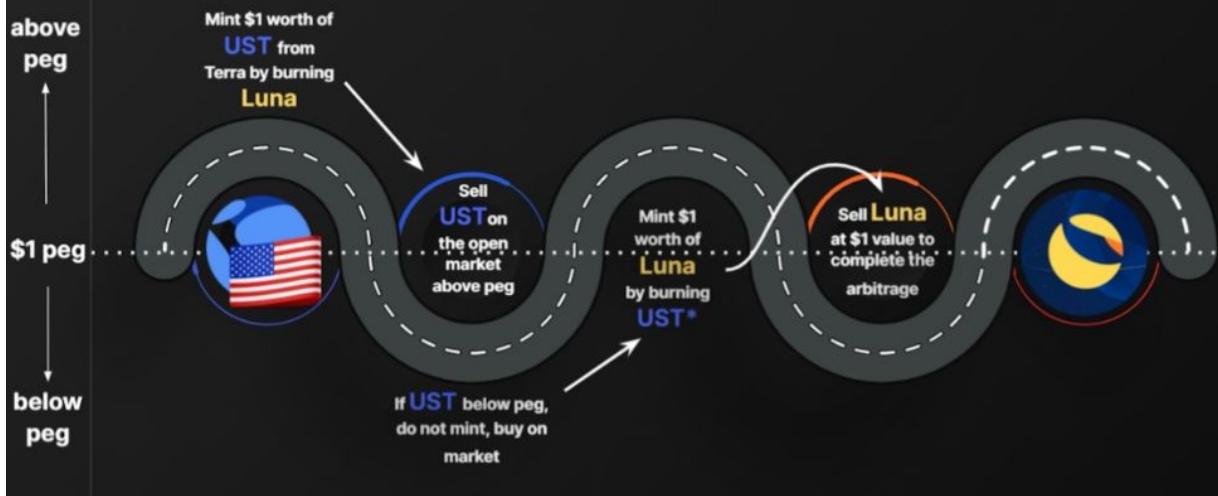


Figure 21. Luna Arbitrage. Image from *Bitcoin Market Journal*^[518]

April 18, 2020. Re: Stablecoins. CH:^[519]

There are really two different classes of stablecoinsso there are asset-backed stablecoins and then there are algorithmic stablecoinsso asset-backed stablecoins those are stablecoins that basically have a promise behind them. For example, Tether, they say, 'okay each of these tethers, they should be backed by a real US dollar somewhere sitting in a bank' ...now the problem with full, or fractional, reserve money is that you are completely at the mercy of the custodian and the person making the promise. Okay so historically every single time this has been tried, it has failed in the long term...

There are no exceptions given enough time. In the 19th century, there were over 200 private currencies issued by banks throughout the United States, every single one of them failed... because there's too much temptation.... there's too many things that can go wrong when you have a backing behind an asset... even the United States, we backed our money by gold with the

Bretton Woods Agreement^[520] and then in the 70s Nixon said, ‘yeah we don’t need to do that anymore’ and we just took the gold awayand we said the US dollar is now not backed by anything.... okay so I’m not a big fan of backing something by an asset to make a lot of sense.... when that asset requires custodian risk, and that asset can be decoupled by a central actor...

So then ALGOcoins ...those are like the MakerDAO^[521] and these things and generally how those work is you have some stable and something that floatsand the thing that floats has an upside and a downside, and somebody takes the upside but they agree to take the downside... and as long as that is somehow bounded and people are able to operate within those bounds... then the other asset doesn’t have an upside but it doesn’t have a downsideso it’s volatility is very low ...but as we’ve seen with liquidations in MakerDAO...that hasn’t worked so well in practice.

I tried to do it too with Dan Larimer, it was the first project I did in the space... it’s called BitShares and we had this thing called the bitUSD... did not work, so algo (algorithmic) stablecoins are super hard, super difficult ...however they can be tremendously valuable if you figure them out...

For example, if we create an algo stablecoin that was backed by ada or some construction involving ada, then it would create gargantuan amounts of trading and demand for ada if the stablecoin was successful, because the only way to generate them would be to have some sort of ada component for its generation ...so if it becomes like Tether and it has billions of dollars of daily turnaround and billions and circulation of value... it would actually push the value of ada up. So it makes a lot of sense to try to create an algo coin where your backer is the underlying asset, but to actually get the monetary policy right ... the economics right...

No one's ever done it, and so we do have a team of people, led by Bruno Paleo, [522] who are just examining these things in general and seeing what we could conceivably do and we have a lot of ideas that have been percolating for the last 7 years ... but it's a very challenging thing, but it's the single most valuable thing we can do in the cryptocurrency space long term, because it's the only way to do lending. It's the only way to do insurance and it's the only way to actually completely decentralize our cryptocurrencies.

There are needs for stable assets.... merchants are not currency speculators.... they need stability if they're going to conduct commerce and furthermore, if you want to onboard people and have them stay in your ecosystem, holding an asset that's not volatile is a very important thing, and it's a very powerful thing. So it's something we think a lot about but it's a lot of work. It's something that will come over time if we can figure it out.

May 14, 2022. Re: Terra UST stablecoin collapse, 'Let's talk Crypto' Twitter space. CH:[523]

...it certainly scares the hell out of certain people, when you have overnight, more than \$30bn just disappears. You know there's no way around this. I mean, I remember growing up...Enron happened and that was around that magnitude. And we passed the Sarbanes-Oxley Act and Bush was talking about it. It was like an international event... and now our industry has that happen, and it's like Tuesday, and we're trying to pretend, like 'well Ok that was shitty but let's move on...'

...no no there are going to be consequences and it's going to take months, to years, for those consequences to be fully realized and unwound. So I think what happened with Luna is that it revealed some inconvenient truths inside the space that the insiders know, and get pretty disgusted about... but the mainstream may not be aware of.

So first, the transitive relationships that the space has, where you have all these VCs (venture capitalists) and these traders, and you have all these very wealthy, powerful insiders and they kind of have a club... and they boost each other's shit and they invest in each other's stuff. So they present these projects, and they say, 'oh, these are the best things ever and there is no risk....and they're incredible and they're growing really fast, and you can't lose and look how smart we are.' And they basically have a two-tiered deal. There's a deal that the mainstream gets, and there's the deal they got, as an insider inside the industry.

So regardless of what price point the retail is getting in at, these insiders, basically, once the momentum starts, make fabulous profits. And they basically do everything in their power to make you believe that these things are long-term. I mean they tattoo themselves with the logo in the most extreme cases. But then they also go on the media, do interviews with 'prominent journalists' who write 'prominent books', and they are all smiles, and they talk about how smart they are, and how great they are. And then all these people who are mainstream people, they watch, and they consume that. And they think, 'oh wow, these guys have it all figured out.'

...but they don't, you know these protocols are very young and they are basically trying to replicate systems that have decades of checks and balances and careful thought, and wherever they couldn't solve something, (they use) human intervention at the end of the rainbow, or regulatory intervention at the rainbow.

So what they're doing is they're taking things they don't have a lot of domain expertise in, and they don't have the decades of experience in, and they're basically trying to say 'not only have built a better version, we built a better version that's totally automated that doesn't require human intervention.' OK, well, they know they can't actually do that, so what they do is they build in secret human intervention.

...also that introduces attack vectors into the protocol, and it also introduces all kinds of potential for insider manipulation, inside the protocol... and basically, they become no better than the central banks. They come no better than the current legacy financial system in this respect. Then, the second part, is that people get fabulous returns in the short term, and they're basically promised that these fabulous returns are going to be somehow permanent ...'oh, you'll get 20% forever per year. No risk.'... It's like OK. What bank do you rob on a regular basis in order to provide this? You could get great returns, but there's a basic fundamental theory in finance that returns are connected to risk. Markets will always price these things accordingly.

Now in the short term, markets may not understand risks as well as they need to, and as a result, they misprice risk and we've seen this happen a lot with financial engineering, but in the long term, markets are very efficient at risk pricing. If you are prepared to take high risk, you get high returns. Now the converse is not necessarily true. That low risk is correlated with low returns. Some cases, low returns mean low risk. There are some cases where low returns can be very risky. OK, but certainly the high risk is required for high returns, there's no way to get around that in the longer term.

...but yet what they've done, in this industry, through these transitive relationships, especially controlling media in the crypto space, is to convince a lot of people that they can basically get great returns with very little risk....just not true in the long term.

The third thing that's happened is that there's no standards about quality, security, protocol engineering, testingno standards about how fast things ought to grow, in order to be able to learn and avoid systemic risk and so forth, because, again, there's a perverse financial incentive to be first to market, not best to market.

There's a perverse financial incentive to basically launch now, not after spending a year or two on the testnet, carefully thinking about things. In fact, our ecosystem, the Cardano ecosystem is one of the most criticized in the entire space by the podcasters and the elite VC^[524] (venture capital) people, who by the way were invested in Luna, for being too slow and taking too long, and doing peer review and doing things the hard way and so forth.

They say, 'Oh well, they'll never get the network effect.' It's like, OK? You're right that it takes a little longer to get TVL (total value locked) and a little longer to get network effect, but on the other hand, we don't lose all of the money and value that we've created as an ecosystem in three days.....and we don't need a bailout, and we don't need centralized intervention and so forth, so maybe that's a priority, I don't know...this is other people's money that we're talking about here, so maybe there's some moral obligation to do things with some basic f\$\$king human decency....But no, they just make fabulous money, and they don't care.

I think that's the meta point that really bothers me the most. I was at a very prominent hedge fund trader's home in California, and I was sitting next to another crypto founder who runs a crypto fund... and you know he's the Golden Boy. All the other investors were saying 'Well, look how much money he's made and all the things he's done'... and this particular person was heavily invested in many of these DeFi protocols which frankly cannot survive in the long term. So they're worshiping a guy that basically found a way to make millions of dollars as a scrap dealer.... and you know they don't care whether it blows up in a retail person's face or not.... taking a step back ...that's the atmosphere and the environment upon which Luna came from, and there are more to come.

So where do we go from here? Well, from the private industry standpoint.... standards, proper protocol design, beta testing for

long periods of time, testNets for long periods of time... and baking in basic consumer protections and guidelines into the service, as well as measuring things properly, especially the degree of decentralization. Having people understand up front, who's in control and who's not for a system.

On the regulatory side, there will be regulation as a result of Luna. It's now just a question of when? and how? and how pervasive? I was less optimistic about regulation passing, but there is now a reasonable percentage chance that regulation will come, at least on the stablecoin side, and it's not going to be friendly to the industry.

Does the industry deserve any better? Honestly ...if we're unable to self-regulate and consumers keep losing money... last year there were \$10.5bn worth of DeFi hacks. ...And now we have a \$30bn stablecoin evaporating into thin air, no checks and balances and consequences.... At some point, the industry has to have an honest moment with itself, and with the leadership, the people actually building protocols, and say, 'are we trying to do better? Or are we just trying to make as much money as possible, as quickly possible? F\$ck everybody else...Lambo forever.'

You see, these are the hard questions and hard truths... and if the protocol designers are unwilling to answer them, or come together as an industry and provide a clear solution for it, the regulator is, and the lawmaker is... that's their bloody job for heaven's sake ...that's what they do for a living, why they exist, and why they were created in the first place ...it's not like we haven't been down this road before.

How EUTXO copes with impermanent loss

Impermanent loss^[525] is a downside to those providing liquidity to a DEX. It can be a confusing term for newcomers.

The automated market maker (AMM) and order book are the most common architectures used to run DEXs (decentralized exchanges). AMMs are straightforward to build, and this architecture has subsequently become the standard for account-based chains. However, there are several drawbacks with this design, ‘impermanent loss’ being one of them.

Cardano employs the EUTXO model, which is deterministic, making it more predictable than the account-based model in terms of impermanent loss. The term ‘impermanent’ is a little deceptive because a drop in token price might only be transitory, and the price could climb again depending on market or trade conditions. Because the price corrected upwards, the loss would be transient (impermanent). All that matters is the dollar price when you withdraw. If it’s lower than the price you bought at, then obviously the ‘loss’ becomes permanent. Ada peaked at \$1.20 in the 2018 bull run.^[526] It plummeted then rose to an all-time high of \$3.10 in Sept 2021. Volatility is to be expected in an immature industry, pricing emerging technology.

With light-touch regulation, it’s arguable that ‘impermanent loss’ is an inevitable risk for liquidity providers^[527] in the ‘wild west’ of crypto trading exchanges. If the loss exceeds the trading fees collected, the liquidity provider bears a loss, which could have been avoided if they had kept their tokens. It’s also common that while liquidity providers may not lose money, their earnings may be lower than if you had simply retained the tokens.

AMM

The Automated Market Maker (AMM) DEX architecture offers smart contract-based automated trading of crypto pairs. With Ethereum being the dominant smart contract platform to date, naturally most pairs are Ethereum token and a stablecoin.

Liquidity pools enable users to pool their assets into smart contracts, which effectively power an AMMs. The more liquidity in the pool, the

more reliable the trading environment for traders on the DEX with which the pool is affiliated, and naturally, the more transaction fees the liquidity providers earn. Liquidity pools provide the liquidity on both sides of a trade. The pool uses an algorithm to determine the price of an asset based on its availability in the pool.

So AMMs are solely dependent on their liquidity providers to provide sufficient pool size to ensure trading is fair and reliable. Liquidity providers are more commonly known as ‘market makers’ in traditional finance.

IOG has several papers [\[528\]](#) on the importance of the right incentives [\[529\]](#) in cryptocurrency space. Incentives are essential to motivate liquidity providers for DEXs to function reliably and fairly. Liquidity providers are incentivized by yield farming [\[530\]](#) in this case.

Order book

The mechanics of order book architecture should be familiar to anyone working in the world of economics. It's a simple model to understand. The order book basically stores all buy/sell (asks/bids) orders and organizes them according to the asset's price when the traders place their orders. The asset can be exchanged if there is sufficient supply and demand.

Order book architecture is much more suited for EUTXO-based ledgers, such as Cardano and Ergo, because its design, together with EUTXO features, mitigates the impacts of impermanent loss.

The number of tokens in a liquidity pool, and the number of liquidity providers contributing to it, are variables when it comes to predicting and avoiding impermanent loss. If there is regular impermanent loss occurring, then pools are not viable and liquidity providers will naturally go to a more profitable rival pool(s). It can be a vicious circle, as it can be too late to salvage once a ‘crypto bank run’ occurs like what happened with the Terra Luna debacle. [\[531\]](#)

To recap from earlier,

- UTXO-based blockchains don't have accounts holding a balance. Users' wallets keep track of a list of unspent outputs

corresponding with all of the user's addresses and determine the user's balance. Remember UTXO transactions are analogous to 'cash in cash out'. The EUTXO model includes a datum, which is contract-specific metadata. This is significant because it allows Cardano to accommodate multi-assets and smart contracts.

- Account-based model holds a coin balance in an account (protected by a private key or a smart contract). Assets are represented as balances inside users' accounts, with the balances being saved as a global state of accounts. Each node maintains its own state, which is updated with each transaction.

There are various major distinctions between the above models, but there is one that stands out. AMMs that operate on Account-based chains are more likely to employ the Constant Formula Market Maker (CFMM) pricing formula, which is one of the most widely used AMM algorithms. There are inefficiencies in this formula, such as it provides users with little to no privacy.^[532]

Also, the Total Value Locked (TVL)^[533] is dispersed throughout the whole price range, implying that an asset's price might be \$1 or \$100,000. CFMM pricing is unreasonable under this premise and does not represent actual market realities. Furthermore, deals with a low token volume tend to have a lot of slippage.^[534] While CFMM is a common feature for AMMs, these inefficiencies may cause liquidity providers' earnings to be impacted. What's more, this liquidity is prone to impermanent loss.

EUTXO and order book DEXs mitigate impermanent loss

The key advantages of EUTXO architecture in terms of security, determinism, parallelism, and scalability were discussed earlier. EUTXO features make Cardano a suitable platform for DEXs that use order book architecture, since it provides greater resistance to impermanent loss. This design has a number of advantages, one of which is the concentration of liquidity allocated within a custom price range. This feature improves liquidity efficiency while reducing impermanent loss.

Global vs Local state

Unlike Account-based blockchains, where each transaction outcome changes the global state, EUTXO-based blockchains verify transaction legitimacy at the transaction level, with the balance equal to the total of remaining UTXOs. EUTXO works at the local level.

This is not the case with account-based blockchains. Smart contracts and other actors constantly interact and impact the global state, resulting in the use of assets and resources, as well as the volatile fluctuation of gas prices. Transaction fees can be very unpredictable as a result of this, even spiking between the time a transaction is submitted and the time it's verified. As a result, the chain may reject such a transaction, but the gas costs are collected nevertheless, potentially resulting in the user's wallet taking a hit. As transaction volumes increase and enterprise customers consider using the platform, this is a critical flaw for the likes of Ethereum.

Extortionate 'gas' fees are not an issue with Cardano's EUTXO model, since transactions are verified and executed at the local state. This is made possible by adding a datum (supplementary contract-specific metadata) to the transaction. The datum is passed to the transaction's validation logic, ensuring that EUTXO remains deterministic. This essentially guarantees that transaction costs are fixed and will not vary in the future. Another advantage of EUTXO and determinism is that bad actors cannot reshuffle transactions, which is a danger with Account-based models.

Another key benefit of transaction validation being local is that it allows for a high degree of parallelism. Transactions can be validated in parallel by a node as long as they don't try to consume the same input. Account-based chains can't do this since transactions must be handled sequentially.

Cardano has met with some criticism for being too conservative by its competitors.^[535] Rather than 'move fast and break things', Cardano has been implemented carefully with scalability and performance addressed only after a secure network and consensus protocols were established. As the enhancements introduced at Vasil take hold, expect to see a raft of DEXs flourish on Cardano such as

ErgoDEX and Maladex among many others.^[536] Genius DEX is another who outlined their strategy in their medium blog and video.^[537]

ERC20 Converter

Cardano's proof-of-stake network can operate Ethereum tokens like SingularityNet AGI^[538] thanks to an ERC20 converter. Connecting blockchain protocols and partnering on applications is critical to realizing the promise of decentralized finance (DeFi) as a viable alternative to conventional banking.

Early in 2021, DeFi Pulse, a monitoring website, claimed that bitcoin worth more than '\$75 billion is now locked up' in DeFi. Later the same year, Cision reported 'DeFi Total Value Locked Hits All-Time High of \$236 Billion'^[539] and reached the existing all time high of \$256 Billion^[540] in Dec 2021. The majority of this wealth is in the form of ERC20 token-based crypto-assets.

The proof-of-work architecture of Ethereum is being tested by ever-increasing fees. IOG predicted this problem, and one of Cardano's basic concepts was to provide a solution. This has now become a reality with unique Cardano wallets growing to over three million^[541] and rising.

Cardano facilitates the transfer of ERC20 tokens to its platform to broaden the range of use cases for application developers and businesses. Plutus smart contracts have arrived as a result of the Alonzo hard fork. Users of supported Ethereum tokens may migrate them from Ethereum's overloaded network to Cardano and benefit from its increased transaction capacity and lower fees, as well as improved security, and interoperability.

Why are ERC20 tokens so popular?

In 2015, Ethereum introduced the blockchain to the notion of smart contracts and 'programmable money.' Because of its value in ordinary business transactions, tokenization and the ERC20 token

have grown in popularity since then. Tokens created by blockchain-based applications may be used for a variety of purposes, including:

- financial payments
- a unit of transaction
- means of access to digital services
- rewards / incentives
- voting rights
- a vehicle for investment

ERC20 tokens that are well-designed may meet a variety of requirements, and the more helpful they become, the more demand for them develops, and their value rises in tandem. That is why these tokens are so popular and supported by so many wallets and exchanges.

Eth v Ada

The ERC20 token standard was created for Ethereum, and there are now over 400,000 contracts (etherscan.io/tokens) based on it, including Binance coin (BNB), Tether (USDT) and Uniswap (UNI) [\[542\]](#) to mention a few.

Ethereum is a well-known and useful blockchain, but it is stagnating and growing more costly. The ‘gas’ fees charged for validating transactions are growing rapidly as more users engage with decentralized apps. A Cointelegraph study featured in *DeFi Adoption 2020* [\[543\]](#) also outlined the issues that Ethereum users are facing. This finding was corroborated by Morgan Stanley’s report in 2022. [\[544\]](#) Ethereum has not yet overcome these obstacles, and it is unlikely to do so soon. Many companies will wish to look at other possibilities.

IOG’s emphasis is on offering a value proposition that exploits Cardano’s advantages over Ethereum by facilitating the transfer of ERC20 tokens to Cardano. Cardano’s boasts greater transaction processing capability and cheaper fees, as opposed to Ethereum’s high cost and often congested traffic.

Powered by Ouroboros

Cardano's Ouroboros proof-of-stake consensus method is the key to solving the issue of network congestion and excessive fees.

Ouroboros uses significantly less energy to execute network transactions than Ethereum's proof-of-work system; it uses power on the size of a modest home rather than a small nation. As a result, Ouroboros is not only environmentally sustainable, but also requires significantly less transaction fees.

Cardano also eliminates the need for smart contract execution fees since the ledger's built-in accounting model allows for native tokens. This means that the ledger, rather than smart contracts, manages the monitoring, transfer, and ownership of various forms of assets. Unlike Ethereum, where the issuance and transfer of ERC20 tokens requires manual modification of the standard contract type, Cardano has built-in logic for this, reducing the chance of mistakes and vulnerabilities.

What does the ERC20 converter do?

Cardano now supports ada and native tokens, both of which have had millions of tokens^[545] issued. IOG introduced the ERC20 converter in late 2021 to secure future compatibility and to build the groundwork for expanded commercial potential.

The ERC20 converter is a utility that will enable ERC20 token issuers and their users to migrate their tokens to Cardano. It's intended for token issuers (organizations that want to migrate their tokens to Cardano) and their users (token holders) when moving their ERC20 tokens to the Cardano network.

Users simply convert their Ethereum tokens in a few clicks, and these tokens will be 'translated' into a native token on Cardano that has the same value and functions similarly to an ERC20 token when transferred over. Additionally, if the user decides to do so at a later

time, they may burn their tokens on Cardano and return them to the source network. Convertibility in both directions is built-in.

SingularityNET (singularitynet.io) were the first to migrate to Cardano. The SingularityNET AGIX token^[546] was launched via the ERC20 converter, and its release represented the first step in the SingularityNET to Cardano migration strategy. The inaugural testnet let users evaluate the migration process while using AGIX tokens on the Cardano and Ethereum Kovan testnets.

Metamask (a Chrome browser plugin) was used to verify an account, and additional functionality followed. Users had to provide their Daedalus testnet address to move their tokens to Cardano and keep track of their balances and transactions.

Users can view SingularityNET coins listed and available for migration in their ERC20 converter account, as well as data such as token balance, by clicking on a token. They only need to choose the token, define the quantity they want to convert, and then migrate them to a Cardano address. When tokens are sent to the address, they may be used for Daedalus wallet payments and transactions. Both Etherscan (etherscan.io) and the Cardano Explorer display all of the actions.

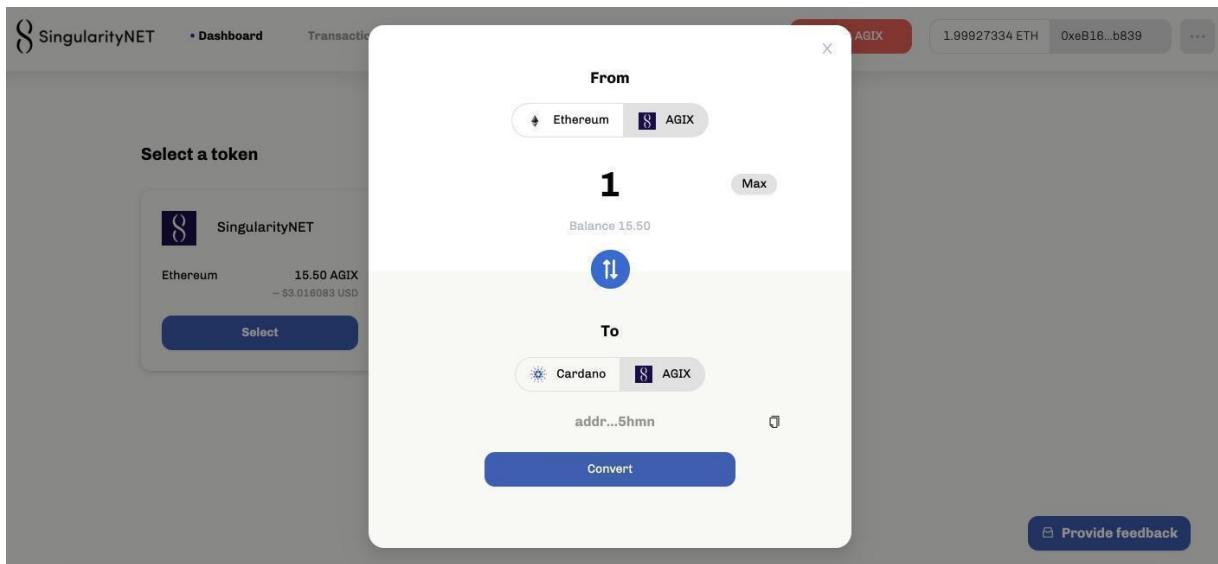


Figure 22. ERC20 Converter

Users will see various tokens on the dashboard as time goes on. Tokens that are eligible for migration will be displayed first, and if tokens are not yet listed, the user may subscribe for notifications on any changes.

The variety of token types supported will expand as the number of ERC20 converter partnerships grows. Previously, partners had to be custodians of their tokens, but with the introduction of Plutus smart contracts on mainnet, there has been greater interoperability.

IOG's purpose is to support a large number of tokens to facilitate commercial transactions. So, in the future, the ERC20 converter will operate as a bridge across blockchains, allowing for successful cross-chain communication with a range of tokens.

AGIX ERC20 Converter

In December 2021, IOG revealed that the AGIX ERC20 converter testnet was online and available for community assessment.

This initiative's first partner was [SingularityNET](#) and the converter was an important step on IOG's budding partnership with the SingularityNET community. Users leveraged a permissioned bridge to transport SingularityNET's AGIX tokens from Ethereum to Cardano and back in the first testnet version. [\[547\]](#) This was a huge step forward in promoting blockchain interoperability in order to create a functioning ecosystem for decentralized finance (DeFi). Users evaluated the testnet's capabilities and tested the transfer of AGIX tokens to take advantage of Cardano's greater transaction capacity, cheaper costs, and proven security advantages.

Bridge to interoperability

Interoperability is critical for growing blockchain adoption and growth across the board. Along with IOG's blanket open-source strategy, making blockchain solutions available to everyone, regardless of

protocol, has always been one of their top goals. IOG is working on making it possible to migrate tokens from other blockchains and sidechains to Cardano in a safe and frictionless manner. Cardano's interoperability goal will be pursued across a variety of permissioned and permissionless blockchains, resulting in a network of linked sidechains with decentralized applications (DApps) built in Solidity, Glow, and other languages. This will broaden the basic ecosystem of Cardano DApps developed in Plutus.

Following their 'security first', 'slow way is the fast way' policy, IOG are addressing the ERC20 converter deployment with the utmost care to protect individual assets at all times. That is why they allowed the community to put it to the test on the testnet, while the code is continually watched and inspected to guarantee that everything is functioning correctly. While the testnet converter's user flow and UI will most likely be comparable to mainnet, the original version was not optimized for performance. As the mainnet launch draws closer, obtaining user data – especially during periods of heavy network saturation – will help solve issues and boost performance.

The AGIX ERC20 converter bridge went live on mainnet on 18 April 2022.

Certified DApps on Cardano

Any new application environment offers an intriguing array of opportunities for discovery. Similarly, at first, an emerging ecosystem confronts two major challenges: discovery and quality assurance. Users must be able to locate the things they wish to interact with while also being assured of a minimum degree of quality.

With the surge of new third-party apps comes the potential of improper or harmful information, as well as content that isn't up to par. As a result, addressing challenges like discovery and quality assurance is critical for early ecosystem development. At the 2021 Cardano Summit, IOG provided a deeper dive^[548] into this crucial

issue by introducing a certification program to examine apps built on top of Cardano. This will be integral to the future DApp Store.

DApp discovery

The DApp Store, a prototype^[549] of which was shown at the Summit, will allow developers to submit their Cardano-based DApps and make them accessible to the rest of the community. Developers will be able to publish their DApps without fear of censorship thanks to the store's trustworthy and democratized environment.

The Plutus DApp Store solves two particular entry barriers:

- There is presently no official DApp discovery mechanism. Almost all new products are discovered organically or by word-of-mouth, or through social media promotions.
- There is no aggregated picture of all DApps accessible in a given ecosystem for end users.

Users will be able to use a web browser to visit the Plutus DApp Store. Consider the Plutus DApp Store a Cardano 'storefront.' The shop showcases the variety of activities available on Cardano. Through automated logic checks, human smart contract audits, and formal verification, a certification program provides consumers with certainty about the behavior of any applications they use.

Any DApp, certified or uncertified, may be found in the store, but IOG will give users clear information regarding a DApp's certification status. The DApp Store's goal is to serve as a platform for transparent user evaluation rather than acting as a gatekeeper or judge.

The importance of certification

The DApp Store is a storefront for DApps. It does not, however, provide any 'built in' guarantee except for community validation. This

is when the second component enters the picture. IOG's certification procedure is responsible for preventing code-level security bugs, achieved by deploying several degrees of 'defense.'

There will be numerous levels to choose from. Automated logic checks, at their most basic level, will help identify some forms of harmful code. These will, for example, be able to determine if the contract has a mechanism for recovering funds that have been locked up. Locked funds must be retrievable under a well-written contract.

Furthermore, manual smart contract audits will assist IOG in verifying the integrity of any DApp. In the end, thorough formal verification will test the mathematical model to establish that a smart contract's behavior matches the formal specification.

Any certification program, of course, is only as good as the people who put it together and operate it. As a result, IOG has partnered with some of the most well-known players in the functional programming field.

Building on granite

This certification attempt is based on a blockchain that already delivers higher levels of assurance than other blockchains such as Bitcoin or Ethereum. Tokens, for example, are incorporated into the Cardano architecture rather than needing to be delivered through contracts like ERC20 on Ethereum. This prevents any complications that could arise from copying and altering an existing contract in order to implement a new token.

The Extended Unspent Transaction Output (EUTXO) accounting model for a blockchain is a fundamentally simpler – and more secure – approach for a blockchain. In Plutus, smart contracts are functional programs, and the simple and verifiable semantics of functional languages drive Cardano's automated testing and formal verification.

IOG aims to create a foundation that is more secure than existing chains. Plutus is a functional programming language.

In addition, by design, Marlowe, IOG's special-purpose language for finance, ensures certain qualities. No Marlowe contract, for example, will keep assets after the contract has ended. That's a built-in feature of Marlowe that doesn't need any further checks. Marlowe's architecture also enables tools to automatically check if contracts have certain attributes by validating every conceivable execution of the contract without having to execute it; this is something that Plutus contracts can't do.

Certification and assurance

IOG demonstrated^[550] automated testing of smart contracts, which are components of DApps rather than whole DApps, during the 2021 Cardano Summit. In the long run, IOG hopes to see user-designed tools, their deployment to the store, and the expansion of the Plutus DApp Store to incorporate additional features like upvoting, reviews, and Atala PRISM integration allowing users to provide feedback on the store's DApps.

IOG has already seen a number of projects begin to build atop Cardano as a result of their work on the Alonzo testnets, the Plutus Pioneer program and Project Catalyst. User discovery and faith in these DApps will be critical when these initiatives begin to hit the market. Because it is an open, decentralized environment, the standard caveat emptor and 'Do Your Own Research' guidelines will still apply. However, assisting in the advancement of better certification and assurance standards will be critical in speeding up the development of a robust Cardano ecosystem and, eventually, the largest potential user base.

When it comes to building and dealing with smart contracts, high assurance is essential. You want to know that the source code is of excellent quality, that the contract is secured and will perform as expected, and that it makes use of good attributes and behaviors.

Certification guarantees that security tests be carried out prior to any deployment, and that smart contracts may be inspected as they evolve. It aids both smart contract developers and end users by assisting with the protection of user assets and reputation from code defects or exploitation.

IOG announced their intentions to offer higher levels of certification for decentralized apps (DApps) at the Cardano Summit 2021. This certification scheme will establish quality standards for DApps and associated smart contacts.

Three certification levels

Professor Simon Thompson, [\[551\]](#) technical project director at IOG, and Shruti Appiah, [\[552\]](#) head of product at IOG, are leading this endeavor. It will assist IOG in adhering to best practices seen in the industry. They're collaborating with companies like Runtime Verification (runtimeverification.com), Tweag (tweag.io), Well Typed (well-typed.com), Certik (certik.io), and others to launch this new certification program, which will be integrated to the new DAppStore. This will be available on IOG's new light wallet, *Lace*, [\[553\]](#) unveiled in Texas at Consensus 2022.[\[554\]](#)

What are the various levels of certification?

In terms of assurance and auditing, there are three levels of certification, each of which is complementary to the others rather than progressive.

LEVELS OF CERTIFICATION		
LEVEL ONE	LEVEL TWO	LEVEL THREE
Automated tooling <p>This level gives continual assurance about a range of properties for smart contracts.</p> <ul style="list-style-type: none"> It covers the discovery of different types of issues or bugs and is characterized as low cost, low effort, accessible to everyone while providing a substantial level of assurance. It can be applied repeatedly and automatically, so each time there is a release or a sub-release of an application, we can test to ensure that the application still has the properties that we expect. 	In-depth audit <p>This level involves looking at the technology and processes that led to it being produced.</p> <ul style="list-style-type: none"> It is characterized by the fact that it involves a manual audit and verification of smart contracts within the DApp itself. The audit is performed at a much more in-depth level and involves more manual effort that can address a DApp in its entirety, even if it is written in a variety of languages. 	Formal verification <p>This level is more specialized.</p> <ul style="list-style-type: none"> We aim to provide full assurance of critical aspects of applications through formal verification of smart contracts. Formal verification involves ensuring that a smart contract serves the specific business or technical requirements defined at the outset.

Figure 23. Levels of Certification

Benefits of assurance

Both application developers and auditors will be able to verify the validity, compliance, and consistency of requirements via certification. It will also ensure that DApps launched on Cardano are free of typical security flaws and offer a degree of resilience, stability, and upkeep. While certification will be heavily encouraged and the DApp Store will be curated, it will not be compulsory or operate as a ‘gatekeeper,’ ensuring a balance between user assurance and decentralized principles.

You can give assurance to the community and ensure that things will operate as planned by auditing the specs, design, and ideation stages. This evidence provides extensive documentation of requirements, which will serve as a future reference point.

Certification and the DApp Store

IOG intends to link this certification with their new DApp Store to produce cryptographically secure non-fungible tokens (NFTs) that serve as proof of the certification levels they will guarantee. The DApp Store will be part of Lace, IOG's new light wallet, and users will be able to access both the light wallet and the DApp Store using a web browser, with users being able to examine the certification status of each DApp as they browse through the categories and individual apps. Users will have more confidence in the quality and safety of DApps if the required certification status is evident throughout the selection process.

IOG presented their DApp Store plans^[555] at the Cardano Summit, Sept 2021.

Oracles on Cardano

Using Plutus and Marlowe (Chapter 7) to develop dependable and transparent financial applications utilizing oracles and smart contracts lies at the core of DeFi and RealFi's promise. IOG announced an innovative strategic relationship with Chainlink^[556] Labs at the 2021 Cardano Summit,^[557] which will assist developers in creating smart contracts for Cardano DeFi apps.

Chainlink's 'decentralized oracle networks' will enable access to real-world databases, allowing 'smart contracts' to execute around data like election outcomes, sports scores, and cryptocurrency prices. Another example where this may be beneficial is the delivery of weather data. Chainlink Labs collaborates with a number of FinTech firms in Sub-Saharan Africa that are attempting to make parametric insurance a reality. Weather data that is secure, reliable, and resilient is a critical input for parametric insurance^[558] contracts.

Across numerous blockchains, Chainlink delivers oracle services to fuel hybrid smart contracts. Smart contracts may connect to any external API via Chainlink oracle networks, allowing them to use safe off-chain calculations for feature-rich applications. Chainlink presently secures tens of billions of dollars across DeFi, insurance,

gaming, and other important sectors, providing a universal gateway to all blockchains to global organizations and prominent data providers.

Developers utilizing the blockchain will be able to inject Chainlink's institutional-grade data into their smart contracts. Support for additional Chainlink decentralized services will come after market price feeds: sports data for betting markets, weather datasets for parametric insurance products, and verifiable randomness for gaming and non-fungible tokens (NFTs). This partnership between IOG and Chainlink Labs will provide access to a plethora of secure data, assisting DeFi in realizing its goal of creating a more cost-effective and equitable global economic system.

IOG state Chainlink is their preferred oracle option for Cardano, however, there are worthy alternatives as listed on Essential Cardano^[559] and third-party sites like CardanoCube.^[560]

One such competitor is Ergo's Oracle Pools^[561] who claim in their blog:

The design of Ergo's oracle pools are more efficient and programmable than using multiple single oracle data points such as in Chainlink's oracle design. We build hierarchies of confidence using oracle pools and pools of oracle pools in Ergo. It's faster, cheaper, and more beneficial to the end user.

Ergo's claims should be taken seriously, having already demonstrated their technical prowess delivering 15k outputs per transaction using EUTXO and rollups.

ZK Rollups (zero knowledge) leverage computation and verification of transactions to be performed on a specialized off-chain network. Rollups are a Layer 2 solution that support greater throughput for DeFi dApps, without jeopardizing Cardano's Layer 1 security guarantees. ZK Rollups boost scalability bundling, or 'roll-up' batches of transactions into a single 'zero knowledge' proof. To

understand more check out ‘Rollups on Cardano Discussion | Cardano Live #48’[\[562\]](#)

IOG have contributed to this space with their paper on Sonic: Zero Knowledge SNARKS.[\[563\]](#)

UTXO alliance

IOG collaborates with other UTXO-based blockchains to develop novel solutions that will improve interoperability, programmability, and scalability. IOG announced a partnership with Ergo (ergoplatform.org), Nervos (nervos.org), and Topl (topl.co) to form the UTXO alliance during the 2021 Cardano Summit.[\[564\]](#) They then invited Komodo (komodoplatform.com), Alephium (alephium.org) and DigiByte (digibyte.org) into the alliance as well.

The UTXO alliance will help cross-ecosystem activities to expand UTXO’s smart contract capability. The joint goal of collaborating with other blockchain sector initiatives is to stimulate and support further research, development, and education throughout the whole area.

The UTXO alliance’s purpose is to keep the UTXO model evolving in terms of interoperability, scalability (sharding, [\[565\]](#) state channels, etc), and smart contract solutions. Improving these solutions and leading major projects to develop bridges across blockchains enables everyone to have access to fair and accessible global finance. This also provides a collaborative effort to promote UTXO-based ledgers in the industry. Bitcoin is obviously the most well-known UTXO blockchain but spin-offs like Bitcoin Cash, Litecoin, and Zcash are among the other projects that use this approach.

Benefits of UTXO

At the heart of financial transactions, the unspent transaction output (UTXO) accounting architecture ensures security, data privacy, and scalability. UTXO models promote scalability by allowing numerous

UTXOs to be processed at the same time, as well as increased security by not aggregating the whole stake into a single account.

UTXO is a safer option than account-based models, such as Ethereum, the most famous exponent of account-based approach. Account-based blockchains, unlike UTXO-based ledgers, keep track of the total balance and utilize the same address for every transaction. Because transactions are executed sequentially rather than in parallel, this makes it prone to hacking and limits scalability.

For instance, Cardano's extended UTXO (EUTXO^[566]) architecture permits multi-assets and smart contracts, as well as arbitrary logic in the form of scripts. These scripts may be spread among many branches, resulting in increased parallelism and scalability. For decades, centralized finance has been at the heart of financial operations. While such a system has performed well in general, it nevertheless suffers from a dependence on a central authority, high transaction fees, and regulatory constraints that cause delays, complexity, and expenses when processing overseas payments. Global financial infrastructure is ripe for disruption.

Building bridges

Instead of depending on expensive middlemen, blockchain technology tackles the difficulties of centralization by allowing trustworthy peer-to-peer transactions based on cryptographic verification. To create a safe and decentralized environment for financial transactions, several blockchain solutions have developed. While these initiatives differ in terms of consensus protocols, accounting models, and smart contract approaches, they all concentrate on similar use cases.

DeFi Growth^[567] has been consistent and shows no signs of slowing. However, fragmented ecosystems, differing governance standards, technology versions, and feature support slow the development of the blockchain environment. Nasdaq's forecast on DeFi Growth is

shared by Romain Pellerin, IOG technology chief:

Mainstream blockchain adoption will pass only through the interconnection of networks, similar to how the Internet was built by the interconnection of intranets and extranets.

With this in mind, it's critical to guarantee that the whole sector is working toward interoperability. Users should be able to interact with one another without being bound by a single ledger, smart contracts should work in a variety of contexts, and decentralized apps (DApps) should be cross-platform compatible. Only in this manner will the blockchain sector be able to realize its full potential, resulting in increased adoption.

'The Island, the Ocean and the Pond'

The UTXO alliance is also interested in blockchain programmability enabling the development of DApps and smart contracts. In reality, new languages must be created to adapt to the UTXO model's particular transaction and data storage management (for example, Ergo's [\[568\]](#) and Cardano's EUTXO). Antara, CKB-VM, ErgoScript, and Plutus are the smart contract languages created by the alliance's founding members. To quickly extend the number of use cases that may be executed on UTXO-based blockchains, alliance members are pooling expertise and cooperating in the development of such technologies.

Furthermore, such languages are constructed as domain-specific languages (DSLs) on top of widely used programming languages such as Scala, Haskell, C, JavaScript, Go, Rust, and others. Those mainstream languages, however, may not always provide the security or convenience of use that smart contract developers seek.

IOG selected Haskell as the programming language for Plutus smart contracts to guarantee increased security and code verifiability. For application development, it is the most extensively used functional programming language. Haskell is a simple, secure, and formally

verified programming language. In terms of acceptance, it is appropriate for a broad variety of financial use cases, providing for quick transfers of payments, accurate outcomes, and scalability. In terms of state distribution and parallelization for increased scalability, this programming approach works well inside the UTXO model.

The sheer scale and scope of Cardano's vision is explained, articulately as ever, by Charles Hoskinson in his video 'The Island, The Ocean and the Pond'. The UTXO alliance will investigate the best-case scenarios for creating a uniform smart contract landscape where a range of programming languages may be built and utilized on various blockchain platforms, taking into account various development initiatives. This will be critical in enabling more blockchain interoperability.

True Scalability

It's also vital to consider a network's scalability potential in terms of transaction processing and throughput as it expands. Because the UTXO model is based on the local state, it differs from the account-based model and hence necessitates a distinct programming paradigm.

These two models have diverse features and provide different trade-offs, different benefits and drawbacks. The account model promotes the creation of use cases that depend on the global state, but the UTXO model assures determinism, predictability, and scalability by managing local states, meaning small sections of the overall graph of transactions. This slows things down as the whole graph of transactions needs to be processed before validation.

As a result, the UTXO architecture has the advantage of ensuring the execution of transactions and contracts prior to their submission to the blockchain, with no fees or validation surprises. Also, since it is easier to shard a graph of transactions by breaking it into a collection of sub-graphs, the UTXO paradigm will enable higher scalability.

It's also simpler to detach a specific transaction or collection of transactions (that transfer data, scripts, and assets) and continue work off-chain before returning to the mainchain with a result, ensuring scalability by off-loading operations off the mainchain. IOG, for example, has created Hydra state channel solutions that boost system performance while allowing several tasks to occur in parallel without sacrificing scalability. Read about concurrency^{[\[569\]](#)} on Cardano and the Hydra^{[\[570\]](#)} solution to learn more about scalability.

Together is better

The UTXO alliance works together to improve the UTXO model and establish a common UTXO standard. Its goal is to provide a variety of options to ada holders, cryptocurrency users, businesses, and the development community that are not tied to a particular standard. For this, the alliance will perform academic research and publish a number of papers that support the creation of safe and scalable smart contracts using the UTXO architecture.

While interoperability is important, blockchain solutions are also necessary for better financial security, transaction processing scalability, and, of course, smart contract capabilities. To allow the use of diverse functionalities in a blockchain-agnostic manner, the alliance is dedicated to tackling such critical concerns as:

- How to transmit data across multiple blockchains in a smooth manner
- What is the appropriate data size for transactions?
- What should the data processing speed be?
- What should the transaction fees be?

As a result, the alliance is concentrating on developing a system that allows for smooth and safe transactions across multiple blockchains

in order to encourage more widespread use of blockchain technology. This will also encourage the creation of reliable DApps and DeFi solutions. This is only the start, as Cardano is looking at partnering with other ecosystems to enhance the UTXO model, examine how the shared knowledge and technological stack may improve scalability features, and contribute to open-source research.

It takes time

Large Scale infrastructure takes time to bed down and mature. Although cloud service providers are not decentralized, they are also global distributed systems^[571] that take years to build and establish. Amazon Web Services began as an internal service within Amazon, was offered to public in 2006 and now has outgrown its parent company amazon.com.^[572] Oracle Cloud Infrastructure was much later to the market in 2016, ceding ‘early mover’ advantage and took years to build out core services into a global footprint of data centers. Coming from relatively nowhere in the market, it recently surpassed Google into third place in a major cloud ranking report.^[573]

It’s no different building out Cardano and releasing new programming languages like Plutus and Marlowe. Customers need to come onboard; feel comfortable with new tools they are working with and gain trust in a new environment. There will be stumbling blocks along the way. It’s possible that early user experiences aren’t flawless. There will be complications with some of the first DApps. Some fantastic development teams and some mediocre development teams are unavoidable. This is inevitable since Cardano is a permissionless, decentralized blockchain. A few DApps may also turn out to be unsafe. Cardano’s secure layer 1 platform provides high confidence and resilience, while Plutus is intended to reduce the risk of exploitation. However, bad coding practices may always put DApp users in danger. Expect bad actors to try to take advantage of the situation via hacks, exploits, and other means.

As the ecosystem grows, everyone must remain watchful as a

community. In fact, IOG feel that certification should be taken more seriously across the board in order for the sector to grow.

DYOR

‘Do Your Own Research’ is sound advice for all involved. Look to fellow members of the community for ‘crowdsourced due diligence,’ and provide your own input. Look for projects that have a history of open and transparent communication, well-maintained social channels, and a solid technological foundation. DApp discovery, along with trust in DApp security and project purpose, will be critical to the Cardano ecosystem’s continued development.

Every project is subjected to some level of toxicity, which seems to be dialed up around key releases. IOG’s blog ‘When it comes to DeFi, Do Your Own Research’^[574] lists some horror stories from other chains. While many competitors are VC backed, Cardano and Silicon Valley’s mutual aversion has been explained several times^[575] by Charles Hoskinson in various media.^[576]

The September 2021 Alonzo update was met with hope but also false expectations. Cardano investors might anticipate a complex ecosystem of consumer ready DApps overnight, but expectations must be managed. Ethereum, which began in July 2015, had to wait more than two years before CryptoKitties^[577] garnered significant user adoption.

As time passes, IOG maintains their fortnightly rhythm of new code releases, routine maintenance updates, and quarterly HFC events. They continue to fine-tune and optimize the platform, as well as analyze and monitor user trends, alter performance, and tweak pricing settings. Only real-world experience will show how to fine-tune Cardano’s adaptable and scalable platform in the months and years ahead. IOG is always looking to the expanding developer community and the Cardano Improvement Proposal (CIP) process to add new features based on the above-mentioned requirements and needs.

Plutus 1.0, the core infrastructure, was launched at the Alonzo HFC event, and it is still evolving and adding features. Cardano's original language is Plutus, but it's merely the start. Plutus 2.0 will come in June with the Vasil hard fork. Anything worthwhile takes time, and rarely runs smoothly.

November 1, 2020. Explain how native assets support on Cardano will be different and better than as we see on Ethereum? CH:[\[578\]](#)

It's a strange thing that Ethereum treats the assets issued on it as second-class citizens ...really these are different things and so Vitalik (Buterin) is a lover of abstraction and I studied mathematics too, I got a little further along than he did, but in both cases, we love the field and one of the first things you learn as a mathematician... is a joy of abstraction. So this concept that everything's a smart contract is kind of cool but there's a price you pay for that because you now have to differentiate the ERC20 tokens from ether itself....and in doing that, it means the things that natively work with ether are intrinsically different than the things that work with the ERC 20 ...and then you also can have multiple token standards and then there's an interoperability problem and so forth.

Given what the ICO (Initial Coin Offering) revolution and soon the STO (Security Token Offering)[\[579\]](#) revolution is doing for the cryptocurrency space ...there's just simply too much value in these tokens and they need to be treated as first class citizens Chainlink is a great example, it's worth like five billion bucks that's worth more than most protocol tokens ... there's only a few exceptions... so probably a good idea to treat that as if it was its own cryptocurrency inside the system.

The minute you do that, then you get uniformity of transaction fees, you get much simpler transaction logic, it's a lot easier to list them on exchanges, it's a lot easier to build wallet

infrastructure for them or get things like Ledger and Trezor to work and then also you can entertain the idea of paying transaction fees with the native asset itself.

...so as part of that commercial conversation, using Voltaire in the future, not today, but in the coming months and years ... eventually we can pitch to the community ..say something like ..hypothetically, Chainlink wants to move over ..but they'll only do it if they can pay their transaction fees in LINK and let the community vote to enable that ...and then the stake pool operators get paid in ada and LINK, every time they process transactions ...and Chainlink is like 'WOW I no longer have to pay ether for transactions ... I own my own blockchain'...and they also get all the other advantages of being inside the system.

So that's one dimension of it ..the other dimension is as I build infrastructure for ada.. all of that infrastructure works natively with your token ..for example, Voltaire we have all these governance tools ...well guess what ? If you issue a token on Cardano ...all those governance tools will work for your token.

...so this is a big problem with DeFi is who's in control and what's happened is that all these DeFi platforms are having to rapidly build their DAOs and decentralized governance infrastructure ...because they're trying to avoid liability and they don't want to get sued, or something, or have to get licenses and it turns out if you run a foundation or something then you're a centralized controller ...and they're like 'whoa that's not good ..so they said well how do we decentralize this?' that's hard to build a decentralized governance layer....

Well we are solving that problem right now for Cardano... and all of those tools are generic and modular ...and so because your assets are treated the same with ada, that infrastructure understands your assets the same way it understands ada ...so you get for free a voting system with your token and you can

build any governance schema you want with the token policy to basically use those voting tools to handle anything from monetary policy, to interventions, rollbacks and these types of things.

And it's the same for all the other infrastructure like when Hydra comes ..we talk about payment channels ..these tokens are treated the same way as ada, so the same way you do a payment system or a state channel system for ada your token will get that as well so you get the low transaction fees and off-chain stuff and blah blah blah ...so that's the power of having native assets. It just makes a lot more sense given the size scope and scale of these things... and then you can offer a lot more to a token issuer than Ethereum is going to in both ethereum 1 and Ethereum 2 and because you can offer a lot more I think it's a more attractive commercial conversation ... and ultimately it's just the right thing to do ... these were always intended to be multi-asset ledgers, Ethereum on up ...in fact the very time we announced Ethereum we put issuing your own token on a t-shirt back in January of 2014. ...so this was always something that was in scope for these types of projects, and no one has really done it the way I think it needs to be done ...and I'm glad that Cardano's around to kind of finish that story.

Chapter 6: Plutus

'There is no honest man! not one, that can resist the attraction of gold!'

- Aristophanes

IOG categorizes smart contracts and financial transactions into two scenarios:

In one scenario, you want to communicate a sense of value transfer from one actor to another. Financial contract(s) must represent that value, as well as the rules and circumstances that control it, as well as a trigger event. Financial contracts are best implemented with a domain-specific language.

In other scenarios, you'd like to write programs, possibly with a view to disrupting an industry, replacing a major corporation, or solving a smaller problem.

These applications normally comprise three things:

- The client which is the part of the program running on your computer
- The server is a computer (or node) that operates on another user's computer (or it can be multiple servers)
- The smart contract is the code that enables a decentralized system to function.

There are two programming languages for Cardano:

- Plutus - the primary platform to code DApps which interact with the Cardano blockchain
- Marlowe - a domain-specific language for building financial contracts, discussed in the next chapter.

What is Plutus?

Plutus, a platform that offers a native smart contract language as well as the supporting infrastructure and tools to implement smart contracts on Cardano, was released with the Alonzo protocol update. Plutus is a framework that allows developers to create decentralized apps (DApps) that integrate with distributed ledgers using scripting.

To comprehend Plutus, one must grasp three concepts:

- The Extended Unspent Transaction Output (EUTXO) model

- The ‘on-chain’ part of Plutus, Plutus Core
- The Plutus Application Framework (PAF) – Plutus contracts are made up of on-chain (code that runs on the blockchain) and off-chain components (code that runs on the user’s device)

Plutus smart contracts are essentially Turing-complete Haskell programs, with both on-chain and off-chain code written in Haskell. You can be sure that your smart contracts will be executed correctly if you follow best practice with Plutus. It is built on Haskell, the foremost purely functional programming language, and builds on recent language research to create a secure, full-stack development environment.

With the inclusion of Plutus scripts into the blockchain, the Alonzo hard fork delivered long-awaited functionality to Cardano. For the first time, these scripts allowed the development of smart contracts on Cardano, opening up a slew of new use cases for decentralized apps (DApps).

If you’re ready to get started, go to the Plutus Playground[\[580\]](#) to learn how to develop Plutus programs and to obtain help from the tutorials. [\[581\]](#) To understand more about the Plutus language, you should read the Plutus explanations. [\[582\]](#) If you want assistance when using Plutus, create an issue in the Plutus repository[\[583\]](#) including as much information as possible.

Smart contracts on Plutus

Plutus smart contracts are made up of on-chain (blockchain code) and off-chain (user-machine code) components. The Plutus Application Framework (PAF) may be used to write off-chain code, which is subsequently compiled by the GHC (Glasgow Haskell Compiler), whilst on-chain code is compiled by the Plutus compiler into Plutus Core.

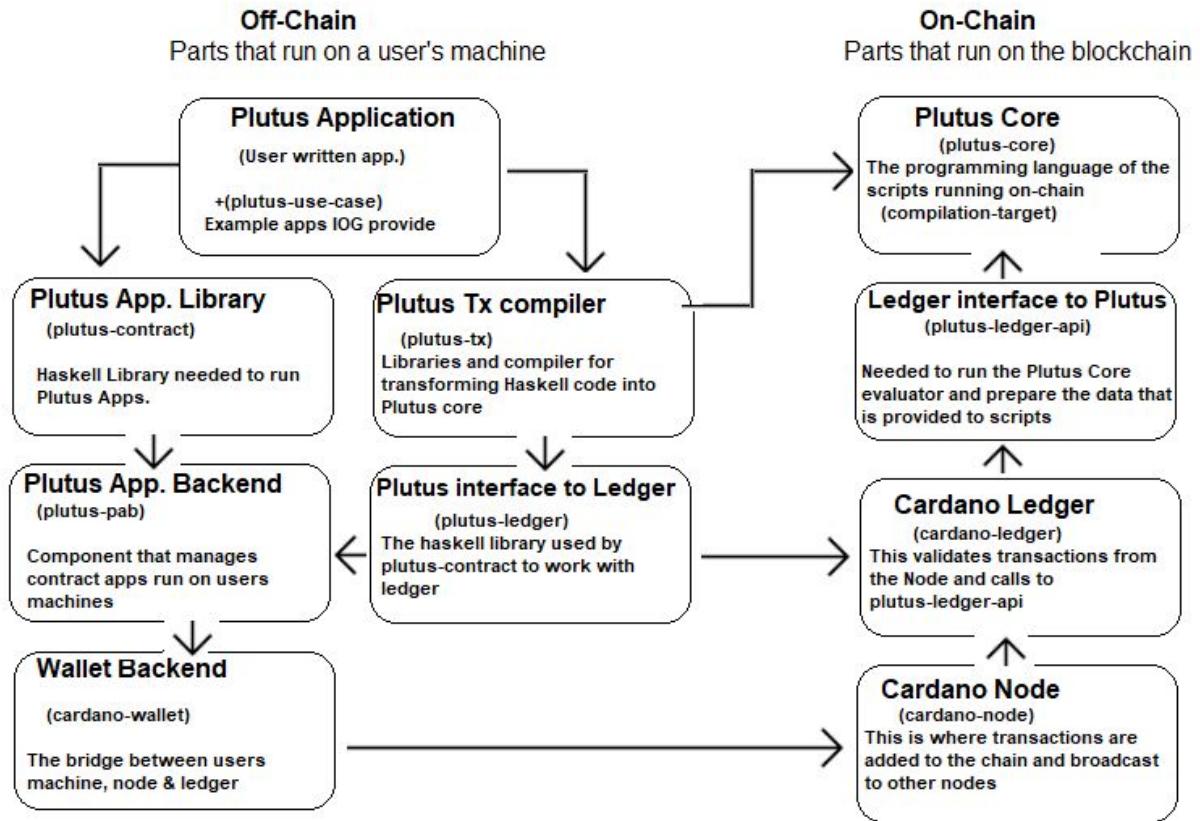


Figure 24. Plutus off-chain and on-chain

Plutus uses extended UTXO (EUTXO)

Cardano employs the extended UTXO accounting model (EUTXO), which extends the UTXO model's unspent (U) transaction (TX) output (O) accounting model (used by Bitcoin). A transaction in the UTXO paradigm contains inputs and outputs, with the inputs being unspent outputs from prior transactions. When an output is used as an input in a transaction, it is considered spent and cannot be reused. An address (a public key or public key hash) and a value are used to specify the output (consisting of an ada amount and optional, additional native token amounts).

EUTXO improves the UTXO architecture by enabling output addresses to include complicated logic that determines which transactions are allowed to unlock them, as well as by adding custom data to all outputs. Compared to other accounting models,

this one has certain distinct benefits. The transaction's success or failure is solely determined by the transaction and its inputs, not by anything else on the blockchain.

As a result, before a transaction is transmitted to the blockchain, it may be validated for legitimacy off-chain. A transaction may still fail if another transaction consumes an input the transaction is expecting at the same time. The transaction, on the other hand, is guaranteed to succeed if all inputs are still present.

Plutus Core

Cardano's programming language, Plutus Core, is utilized to build the EUTXO paradigm. Plutus Core scripts may be written in a concise, functional language comparable to Haskell, and a significant portion of Haskell can be leveraged. You don't create Plutus Core as a smart contract programmer; instead, a Haskell compiler plugin creates all Plutus Core scripts. These scripts will be run 'live' on the chain by nodes during transaction validation. They will either use validator scripts^[584] to lock EUTXOs or minting rules to regulate the minting and burning of native tokens. In practice, you'll create validator scripts in Haskell for smart contracts, which will be automatically compiled into Plutus Core using a GHC (Glasgow Haskell Compiler) plug-in called Plutus Tx.^[585] In a sign of a maturing ecosystem, there is also a third-party alternative to Plutus Tx in Plutarch.^[586]

Why Plutarch?

Plutarch written validators are often significantly more efficient than Plutus Tx written validators. With Plutarch, you have much more fine gained control of the Plutus Core you generate, without giving up any type information.

To put things into perspective, one validator script from a large production contract was rewritten in Plutarch, changed from Plutus Tx. Here's the comparison between the Plutarch script's execution cost compared to the Plutus Tx script's execution cost. These numbers were gathered by simulating the whole contract flow on a testnet:

Version	CPU	Memory	Script Size
PlutusTx (current)	198,505,651	465,358	2013
Plutarch	51,475,605	99,992	489

Figure 25. Snapshot from Plutarch's GitHub

Plutus Application Framework (PAF)

Validator scripts' on-chain status can only be changed by transactions that spend and create script output. When designing a Plutus application, both the on-chain (the Plutus Core scripts) and the off-chain (the transaction building and submission) components must be taken into account.

Unlike Ethereum, where the on-chain code is written in Solidity while the off-chain code is written in JavaScript, the Cardano off-chain code is written in Haskell, exactly like the on-chain code. The business logic^[587] will only have to be written once this way. The validator script and the code that creates the transactions that execute the validator script may then employ this reasoning.

Many applications need to monitor the UTXO set^[588] for changes to certain addresses, so if the contract is written as a state machine,^[589] you need to keep track of the unspent output, which reflects the machine's current state, and update your local state if the on-chain state changes. Many applications need communication with the wallet backend to access the crypto funds they are using for transactions.

The Plutus Application Framework (PAF) makes it simple to access services that are often used by Plutus apps. The Plutus application backend, which offers runtime support for access to the blockchain as well as additional concerns like persistence, logging, and monitoring, may be used to execute applications built using the framework's libraries. Applications built on top of the PAF provide an HTTP and WebSocket^[590] interface that allows users to interact with the app from a web browser.

Plutus Application Backend (PAB)

The Plutus off-chain component is executed by the PAB, which is constantly iterated upon with each release. It handles wallet backend and node application requests, saves application state, and provides an HTTP API for managing application instances.

Native tokens and Plutus

With the Mary hard fork in February 2021, native tokens became accessible on Cardano. Tokens, like ada, may be created by anybody, and they can be transferred and received freely.

Each native token has its own minting policy,[\[591\]](#) which specifies the circumstances under which tokens may be minted and burned. Users are now able to create minting rules in Haskell and compile them to Plutus Core after Plutus was deployed. During the minting or burning process, the Plutus Core policy script will be run in the context of the transaction, and it will have to approve or reject the action. This feature will help to accelerate the development of Cardano's Non-Fungible Tokens (NFTs) by allowing for the establishment of considerably more complicated minting rules and trustless NFT issuance.

Minting policies are made up of a series of basic rules that define signatures and timelocks. For example, a policy may declare that transactions can only mint or burn tokens if they are signed by two of the five potential signatures. A different policy can allow minting only before or after a certain time.

These fundamental building elements, as useful as they are, do not cover every possible application. It is possible to represent non-fungible tokens (NFTs) with such basic principles, although it is impractical. By confining the minting action to a fixed time point, this might be accomplished using a timelock to mint an NFT. If just one token is issued before the deadline, the token is considered non-fungible (unique as there's just one). However, merely looking at the minting policy isn't enough to determine this, you would have to

check the token minting history to be sure it has only been issued once.

Strengths of Plutus

Plutus offers significant security benefits. It provides a simpler, more reliable method of demonstrating that your smart contracts are accurate and will not experience the issues that have plagued prior smart contract language designs.

Plutus allows for a new integrated approach to smart contract and distributed application development that is easier and more secure than prior options. The same language is used for both on-chain and off-chain programming. You employ a common code base, which the Plutus toolchain [\[592\]](#) divides into on-chain and off-chain code and packages for deployment. Plutus also enables user-defined tokens (both fungible and non-fungible) natively, which needs much less code than Ethereum.

The Ledger Model

Cardano, like any other blockchain, is a decentralized ledger or database that keeps track of all transactions and blocks made on the network. This database distributes records with all participants and synchronizes with blockchain activity on a regular basis to deliver transparent and up-to-date data to anybody.

Cardano DB Sync [\[593\]](#) retrieves such blockchain information and lets users run CLI commands to access transaction and block details. You can use the Cardano Explorer – a graphical user interface that exposes information in a straightforward manner – for more easy and user-friendly data analysis.

Before a transaction is submitted to a block, [\[594\]](#) it is validated by a block producer. To avoid double-spending, the sender must have adequate funds, and all nodes across the ledger must establish consensus. Let's look at how this worked in the Shelley ledger, and

how Plutus scripts changed it to enable multi-asset transactions and smart contracts.

Transaction validation before Goguen

The unspent transaction output (UTXO) accounting mechanism is used by Cardano. To monitor financial transfers, ownership, and balances, this approach employs transaction inputs and outputs as records. The funds of users are kept in the form of unspent transaction outputs, each of which has a spendable quantity. Previous transaction outputs that have not yet been spent are referred to as inputs. When an output is used as an input in a transaction, it is considered spent and cannot be reused. The following are the parameters for the output:

- an address which holds a payment credential and an optional stake credential, which may be either a public/verification key hash or a script hash. The stake credential might alternatively be a link to the registration certificate.
- a value: this is the amount of ada that may be spent.

The owner of the private key (also known as the signature key), which corresponds to the payment credential supplied in the address, must sign a transaction. Only ada transactions were supported by Cardano Shelley. The Shelley formal specification introduced the idea of multi-signature (multisig) scripts, [\[595\]](#) which are captured wholly by ledger rules. If a predetermined combination of signatures is given, this multisig approach allows an unspent transaction output to be used as an input to a new transaction. For example, if two people must sign the transaction at the same time, two out of three keys must be given, and so on.

Multisig is a very simple language that enables you to interact with `RequireSignature`, `RequireAllOf`, `RequireAnyOf`, and `RequireMOf`, among other constructors. Scripts should be designed to allow more phrases for expressing a variety of different conditions as the ledger's functionality grows.

Multisig upgrade to Plutus Core

With the introduction of multi-asset support and smart contracts on Cardano, upgrading the fundamental multisig scripting language with more complex options was required. As part of the Alonzo upgrade, IOG implemented the required tools and infrastructure, as well as support for a new programming language called Plutus Core.

The Alonzo ledger employs the extended unspent transaction output (EUTXO) accounting model accounting paradigm to upgrade multisig to Plutus Core, and Plutus Core to give strong scripting features.

EUTXO improves the UTXO architecture by enabling complicated logic to determine which transactions may be used to unlock output addresses, as well as adding custom data to all outputs. Scripts need a clear, well-defined scripting language to do this, and data should be tied to outputs that will be supplied to the script during execution. Plutus Core allows nodes to run complicated scripts during transaction validation while ‘live’ on the blockchain.

They’ll either use validator scripts to lock UTXOs or minting policies to govern the minting and burning of native tokens. The data of the Redeemer is then provided as a simple (algebraic) data type that is easy to construct in Haskell. In reality, a smart contract developer will create validator scripts in Haskell, which will be compiled into Plutus Core automatically.

By providing core data types for the examination of transactions during validation, the relevant Haskell libraries make implementing such validation logic easier. These also provide a plethora of utility functions and higher-level abstractions, enabling contract writers to focus on business logic rather than low-level minutiae.

Alonzo made the following adjustments to the ledger data:

1. Plutus scripts have the ability to lock UTXOs.
2. Script state-like functionality is enabled via a new component added to the contents of the output pieces of UTXOs. A UTXO locked by Plutus scripts includes a datum in addition to assets and an address. A datum is a piece of information that represents an interpretation of the script state.
3. A number of new protocol parameters have been added to enforce extra transaction validation requirements. These include upper restrictions on how much processing power scripts may use.

Transactions were updated to support Plutus scripts as follows:

1. The transaction now has a redeemer, which is a user-specified parameter for each of its activities. A redeemer may fulfill a variety of functions depending on the script. It may, for example, serve as the user's decision to 'hit' or 'stand' in a game of blackjack or a 'like' or 'share' in some utopian decentralized social media app.
2. The transaction defines each script's computational execution budgets.
3. Alonzo leverages collateral to verify that a transaction can pay its execution cost
4. Transactions include an integrity hash, which is used to confirm that it hasn't been tampered with, isn't expired, and so on.

The node runs new Alonzo-specific tests to guarantee that the transaction is built successfully. It must not, for example, exceed the maximum execution resource budget. It also runs the scripts by using Plutus script interpreter.

Ethereum's non-deterministic 'gas' model has the potential to charge consumers extortionately high costs. This form of indeterminism is addressed in Cardano scripts by requiring that both the resource budget and the fee necessary to cover it be included in the transaction. When designing a transaction in Alonzo, a user may forecast both locally. Script execution will always return one of two

values: True or False, and it will not loop endlessly. This is because every action a script does requires a non-zero amount of resources, which the interpreter keeps track of. If the transaction's budget is exceeded, the script is terminated and False is returned.

The following critical features help to forecast the results of script and transaction validation:

- When applied with the same parameters, the script interpreter will always terminate and deliver the same validation result
- During validation, a transaction should correct all variables provided to the script interpreter
- A transaction enumerates all of the operations it performs that need script validation
- a transaction's mandatory signatures guarantee that it can't be tampered with by an attacker in a manner that causes scripts to fail.

In the EUTXO ledger paradigm, implementing a transaction is deterministic.

Typical Plutus Use Cases

Plutus implementations are often used for the following high-level use cases, among others:

- Oracles — fully operational oracles that interact with and feed smart contracts by bringing off-chain data onto the chain. Oracles also provides Plutus applications with a centralized and trusted off-chain data feed (for example, to interact with price feeds from various centralized exchanges)
- DEX token swaps — building a decentralized exchange system that lets users swap supported tokens. Users may form liquidity pools (or contribute funds to existing ones), which will provide coins for trading. They may earn fees for any transactions that utilize their funds in exchange for this. Users may also donate to liquidity pools for any supported token and earn commissions in the form of exchange fees in return for their efforts. When a user

provides liquidity to a pool, the user is given a liquidity token that represents the deposit. Fees should be calculated by the contract and then distributed to liquidity providers based on each provider's portion in the liquidity pool

- Lending and borrowing - developing a lending protocol that allows users to lend and borrow cryptocurrencies of their choosing in a safe and secure manner, with variable and stable interest rates. Users may take part as either depositors or borrowers. Lenders must deposit funds into liquidity pools in order to transact, and borrowers must borrow from these liquidity pools. Depositors are rewarded with interest-bearing tokens. To protect against volatility, each pool has a reserve pool
- NFTs; minting, sending, and receiving NFTs into a wallet — developing core functionality for minting, sending, and receiving NFTs into a wallet, as well as additional use cases
- Decentralized finance (DeFi) tools — building multifunctional dashboards (web-based or mobile) that interface with smart contracts to provide value to native token traders. These solutions may have numerous functional dashboards that display token and liquidity pool balances, among other things. They may also combine many services into a single transaction, such as swaps and providing liquidity, making DeFi adoption simpler
- Crypto-backed stable coins — leveraging Cardano's Atala PRISM decentralized ID system to create a new stable coin implementation based on-chain collateral. Transfer restrictions, asset freezes, and other measures may be implemented.

Plutus Tools

The Alonzo hard fork enabled the architecture and tools for functional smart contract creation using Plutus, bringing fundamental

smart contract capabilities to the Cardano ledger. Users, developers, and organizations may now construct decentralized apps (DApps) using smart contract technologies in a secure manner. Developers may leverage a variety of tools to assess and implement smart contracts on Cardano.

Plutus Playground

The Plutus Playground is a place where smart contracts may be written and tested before being put on the Cardano blockchain. It's a web-based platform for Plutus development with modest resource consumption. The Plutus Playground offers a web-based simulator for building and executing smart contracts, as well as access to popular smart contracts that have already been developed. To assist you with getting started, the Plutus Playground includes 'how to' guides and tutorials.

There is no need to install anything to use the Plutus Playground, which can be accessed from a web browser. The user interface is divided into three parts:

- editor
- simulation
- transactions

The simulator displays how a contract will function on Cardano. One of the key parts of this is that it can be used as a teaching tool for beginners. The wallets that interact with a contract, as well as the actions that affect the result, may be defined and updated by users. The outcomes may then be analyzed to determine what occurs on the blockchain and how transactions take place. Visit the Plutus git repository or watch the Plutus application compiling and testing tutorial [\[596\]](#) for further details.

Plutus Application Backend

The Plutus Application Framework (PAF) includes the Plutus Application Backend (PAB), which is the off-chain infrastructure in the UTXO paradigm that produces the transactions that power the DApps. Because it has to look at the ledger state, take some information from the ledger, and put it all together to produce a transaction with the proper bits of data in the right location, this off-chain architecture is somewhat complex. The PAB is a Haskell library that simplifies the development of both off-chain infrastructure and on-chain scripts.

The PAB assists in the construction of UTXO transactions in two ways:

- The read path entails retrieving data from the blockchain and responding to events that occur there
- The write path - This is where the transactions that execute the Plutus scripts are built.

Plutus Application Backend (PAB) offers the components and environment that allow developers to interface with smart contracts and design and test DApps before deploying them to a live production environment. It's a sandbox environment, similar to the Plutus Playground and the Marlowe Playground, [\[597\]](#) where developers may test DApp features before committing to a full Cardano deployment.

The PAB eliminates the need for developers to build their own infrastructure from the ground up (including chain indexes, [\[598\]](#) etc.), cutting down on development time and resources. It enables developers to model how an application would operate on-chain for testing and error reduction before launch, ensuring a smooth transition.

It's an off-chain backend service that manages and handles the application instance's demands throughout its lifespan. This involves interacting with third-party clients (such as wallet frontends) and serving as a link between Plutus apps, the node, the wallet backend,

and end users. PAB commands and dummy components enable easy simulations and integration of DApps, allowing for this kind of interaction.

It assists in the construction of UTXO transactions for both the read and write routes by obtaining information from the chain, responding to events, and generating the transactions that execute the Plutus scripts.

The PAB's main goal is to:

- provide a standard environment for Plutus apps to run in
- offer disciplined state management
- provide external clients with discoverable interfaces
- keep track of on-chain data for smart contract applications
- make it possible for developers to operate in either an emulated or non-emulated environment
- handle requests like starting contract instances, passing user input to these instances, and informing these instances of ledger state changes.

The PAB can effortlessly transition between emulated and non-emulated (real network) contexts. This makes writing various types of tests — unit tests, integration tests, property-based tests, and so on — much simpler. Because the PAB's backend can receive and send messages, DApps can easily interface with it. As a result, the DApp may make standard requests to endpoints provided by the PAB, which correspond to actions and operations that each smart contract can handle.

The PAB, which offers runtime support for access to the blockchain to further conduct smart contract activities triggering transactions based on the EUTXO paradigm, can run applications built using the framework's libraries. PAB also includes capabilities such as persistence, logging, and monitoring. The architecture of the PAB is seen in the figure below:

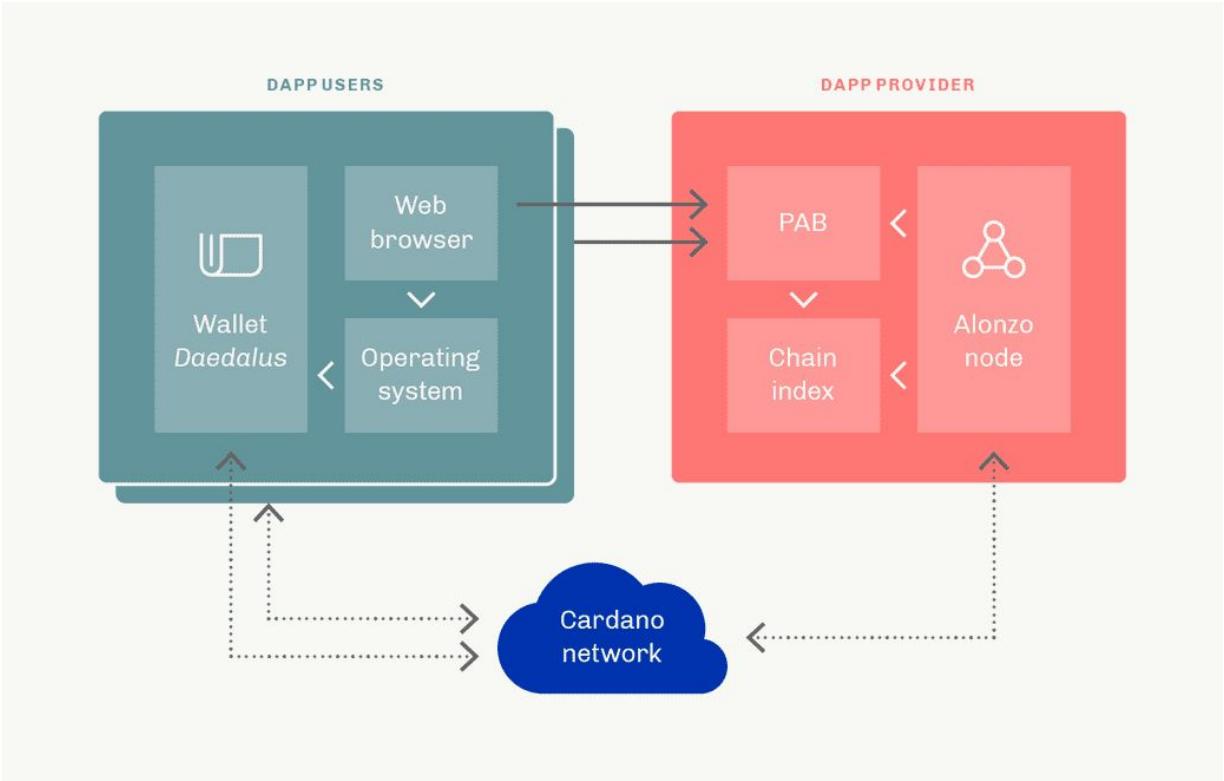


Figure 26. Plutus Application Backend (PAB)

Once the PAB was ready, it was deployed in one of two ways:

- hosted - this option was available in the PAB's first version. The DApp provider / developer hosts an instance of the PAB, as well as the chain index and an Alonzo node. The Plutus app's off-chain code is executed on the DApp provider's infrastructure
- in-browser - available after the first release.

The following components must be present in addition to the PAB:

- Chain index: a database of information obtained from Cardano transactions. It must be co-located with a Cardano node and utilizes the Cardano node's chain sync protocol. The PAB's chain index is a read-only component. As a result, a single instance of the chain index may be shared by several instances of the PAB. A HTTP API is used to serve all chain index requests

- Alonzo node: the PAB leverages a socket protocol to subscribe to ledger changes from the node.

While not mandatory for DApp creation or implementation – the community are developing their own tools, and API-based alternatives^[599] – the PAB is another useful Cardano tool that makes developing DApps easier, safer, and more cost-effective. It relieves developers of numerous mundane duties by giving information from relevant sources in an accessible style.

'The slow way is the fast way'

IOG launched the first in a series of color-coded testnets to bring core Plutus smart contract technology to Cardano earlier in 2021. The Alonzo hard fork was used to bring this to mainnet. Initially, smart contract functionality was only available through a command line interface (CLI). While smart contracts were implemented on mainnet for the first time in September 2021, this was always just the first step on the path to DApp deployment on mainnet.

In the meantime, developers were working locally on their DApps (many through the PAB) while testing any key smart contract features on the testnet. These components had to come together before a DApp could go live on the mainnet, and this took time. Developers were able to move their DApps into a state of readiness and deploy them to the Cardano testnet prior to mainnet launch after the PAB was connected with the node and other fundamental components like the wallet back end (WBE) connector.

These early locally developed apps were then able to communicate with the mainnet as planned. Because of the mockchain^[600] approach to development, DApp had a seamless transfer from testnet to mainnet. To start the PAB, all that is required is a modification in the configuration files; no changes to the real code or Haskell code were required. IOG wanted to make sure this integration work was done appropriately since it was a sophisticated and important aspect

of the Cardano architecture. IOG worked on the last integrations until late 2021, when the integration was delivered.

The Plutus ecosystem will evolve iteratively. IOG invite the developer community to install their own tools and generate off-chain code for their DApps running on Cardano as the Plutus platform matures. IOG will be gradually improving the platform and adding additional features and functionality as they test with their engineers/QA and the developer community.

Plutus fee estimator

IOG performance specialists created the Plutus fee calculator as an in-house tool for pricing benchmarking and comparison. It predicts the fees that will be charged for a transaction using data from real-world Plutus transactions. The estimator may be used to estimate costs for individual script transactions or whole DApps before or during development, as well as to compute fees for existing transactions (e.g., to assess the fees that will be charged if network parameters change).

The Cardano ledger's design principles enable great performance while maintaining stringent security standards. Cardano employs an Extended Unspent Transaction Output (EUTXO) accounting model, which adds significantly to the deterministic nature of its architecture. The predictability of outcomes is referred to as determinism. This means that Cardano transactions and scripts may be checked locally (off-chain), allowing users to see whether a transaction is legitimate before executing it on-chain and incurring fees. Furthermore, transaction fees are fixed with no surprises. For comparison, the cost of executing a smart contract on Ethereum varies based on network traffic, ranging from \$5 to hundreds^[601] of dollars. Even unsuccessful Ethereum transactions may incur fees, adding to the price unpredictability.

Users on Cardano, on the other hand, may assess the prospective transaction processing fees in advance. There is no need to pay for

a transaction that may fail since the user knows whether the transaction is legitimate or not in advance. This prevents money from being wasted and eliminates on-chain failures. Cardano's ada execution fee is always consistent because it is based on predetermined network protocol parameters rather than, for example, varying network congestion variables.

Cardano's pricing strategy is based mostly on market demand rather than real supply. With Cardano's smart contract functionality, many types of demand are now vying for the same supply. As a result, both relative and absolute price^[602] must be considered. One means of doing this is by examining the implications of smart contract pricing, non-fungible token (NFT) activities, and other factors with regard to a common value — in this example, the use of Cardano's processing power.

Smart contract pricing in Cardano is based on a fixed cost, which is determined by the price of used resources (UTXO size or computation/memory consumed while executing). Stake pool operators' (SPO) labor and resources that verify network transactions must be adequately compensated with fees. Furthermore, ensuring that any method of adopting Cardano is not significantly less expensive than another helps to prevent a wide range of adversarial attacks (e.g. a DDoS attack).

Flexibility is also a significant characteristic of the Cardano protocol, since it allows users to adjust their settings and respond to price swings. If the value of ada rises dramatically, protocol settings may be modified if necessary to avoid the user from overspending for smart contract execution.

IOG created the Plutus fee estimator tool for pricing benchmarking and comparison. It was released on their public testnet in January 2022. To anticipate the costs that will be paid for a transaction, the estimator leverages data from real-world Plutus transactions. The estimator may be used to estimate costs for individual script transactions or whole DApps before or during development, as well

as to predict fees for existing transactions. It might also be used to see how script updates or optimizations affect costs.

The fee calculation formula used by the estimator is the same as that used by the Cardano node. It can provide an accurate estimate of the required fee if the inputs are sufficiently correct. A user may simply forecast how much a DApp will cost by summing the charges from many transactions. Developers, business analysts, and others will benefit from this. The estimator contains a number of real-world examples that have been cross-checked against actual fees.

Three pieces of information are needed to calculate fees:

- The size of on-chain transactions in bytes: a basic transaction is roughly 300 bytes, a transaction containing metadata is around 650 bytes, and Plutus scripts are generally 4,000-8,000 bytes (ongoing optimizations will improve these)
- The number of computational (CPU) steps used by the script: each step on a benchmark system equals 1 picosecond of execution time. Scripts should use less than 1,000,000,000 CPU units (1 millisecond) on average
- The number of memory units used by the script: this is the number of bytes allocated by the script. Scripts should use fewer than 1,000,000 memory units in most cases (1MB of memory allocation).

A user just has to enter in relative information to utilize an estimator, which may be retrieved from the Plutus compiler after generating a script in it. There is also no need to run a node for this, which makes the procedure much easier for non-techies.

Plutus script execution on the Cardano mainnet was enabled by the Alonzo HFC event. IOG is now focusing on optimization and scalability^[603] as the number of smart contract projects begin to grow.

This involves a continuous evaluation of actual smart contract use in the real world.

IOG must strike a balance between user requirements and what is beneficial for the network, speed against accuracy, and – as always – security, scalability, and decentralization. The Cardano fees model will be refined over time when future code/script optimizations and system efficiency improvements are made. IOG will monitor the expansion of smart contracts, improve the Cardano node and Plutus interpreter implementations, and make various modifications with their developer and stake pool operator communities to best serve Cardano's user base in terms of equitable and consistent transaction fees.

Test Drive the Plutus fee estimator on testnets.cardano.org and see how easy it is to estimate the processing fee without saying goodbye to your funds if a transaction fails.

Cooked Validators

With the ‘cookedValidators’ library, you can write off-chain code and obtain property-based testing for free. A Haskell and formal methods engineer should be devoted to using tools and procedures to ensure the safety and soundness of decentralized applications (DApps). Writing and deploying a DApp is inadequate; all on-chain code and Plutus scripts should be carefully tested against a variety of bad actors. *Tweag* responded by introducing *cookedValidators*, [\[604\]](#) a collection of ready-to-use tools for working with Plutus validator scripts. This library aids in the implementation of the innermost layer of off-chain code, which is responsible for transaction generation and submission. You receive property-based testing at the transaction level for free by using this library.

You may verify various safety and correctness aspects of your on-chain code by utilizing cookedValidators to create your off-chain code, which can considerably boost your trust in the code’s correctness. During an audit, this may save time and money. The

first step in a Tweag audit is to leverage cooked Validators to write transaction-generating code, allowing them to interact with their client's infrastructure.

Writing Plutus transactions

Writing a Plutus transaction is accomplished in the following order:

1. Write your Plutus on-chain code.
2. Convert your Plutus code to text envelope format (this is the format expected by the cardano-cli .ie. command line interface).
3. Using the Plutus script(s) available, create your transaction.
4. Execute Plutus script by submitting the transaction.

The workings of a Plutus transaction

A transaction is a piece of data that has both inputs and outputs, and they may now incorporate Plutus scripts since the Alonzo upgrade. The unspent outputs from prior transactions (UTXO) are referred to as inputs. A UTXO gets spent as soon as it is used as an input in a transaction and cannot be used again. An address (a public key or public key hash) and a value are used to specify the output (consisting of an ada amount and optional additional native token amounts). This flow diagram provides a better understanding of the technical components of a transaction:

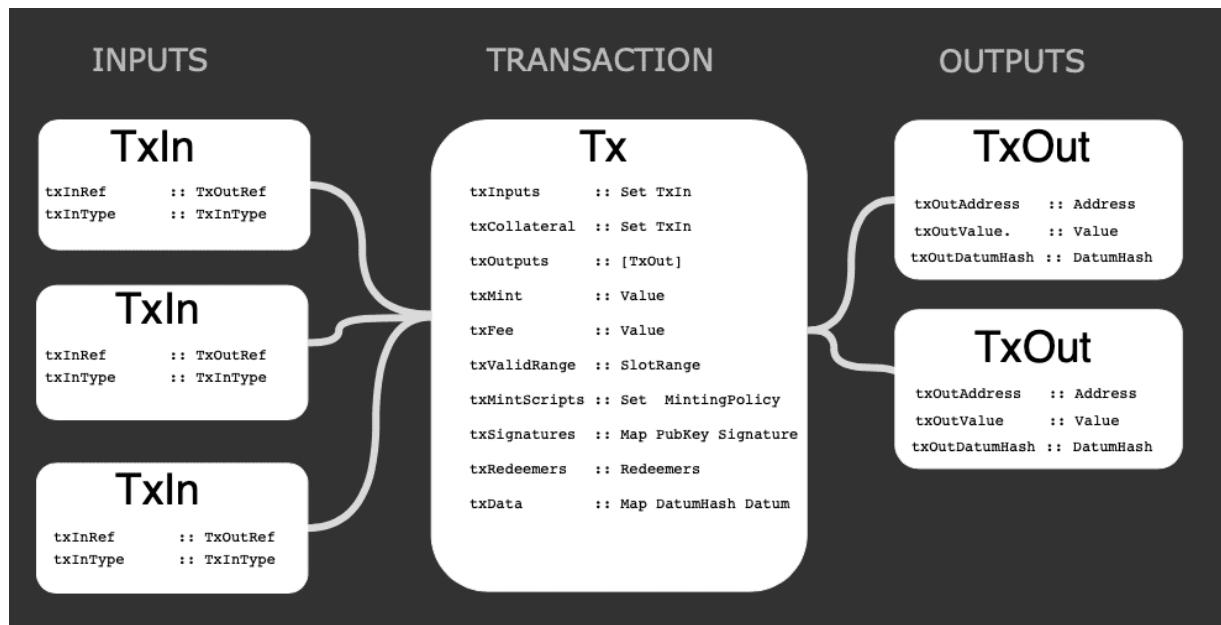


Figure 27. Transaction inputs and outputs

In a nutshell, inputs are references to UTXOs introduced by earlier transactions, and outputs are the new UTXOs produced by this transaction. In addition, since new data may be stored in the generated outputs, this enables the status of a smart contract to be modified.

It's also crucial to clarify what Plutus Tx is. Plutus Tx refers to delimited parts of a Haskell program that are used to compile a contract application's on-chain component into Plutus Core (this compiled code is then used for validating a transaction, hence the 'Tx'). The Plutus Core expression that results may be included in transaction data or saved in the ledger. Plutus script refers to certain chunks of code that need specific processing on the blockchain. You can manage the flow of execution of a Plutus script by utilizing transactions. As a result, a transaction can be thought of as a series of messages sent to the smart contract. To appreciate the development of smart contracts, one must first understand transactions.

While assessing the off-chain code, the wallet should initiate a transaction. For the time being, cardano-cli can be used to build the

transaction and add the compiled Plutus script inside. However, in the future, the user's wallet software will automate this process. Once the transaction is submitted, it will be verified, and a validator node will analyze the Plutus code. The transaction will be deemed legitimate if the script evaluates correctly. The transaction will be denied otherwise.

To master Plutus, one must first grasp three concepts:

- The Extended UTXO (EUTXO) model
- Plutus Core – the ‘on-chain’ component
- The Plutus Application Framework (PAF) – the ‘off-chain’ component that facilitates interaction with smart contracts.

Plutus contracts are made up of on-chain (code that runs on the blockchain) and off-chain (code that runs on the user's computer) components. Plutus smart contracts are basically Haskell programs, with both on-chain and off-chain code written in Haskell. PAF may be used to write off-chain code, which is then compiled by the GHC (Glasgow Haskell Compiler), while the Plutus compiler compiles on-chain code (written in Plutus Core).

It's critical to grasp the link between these Plutus principles and native tokens functionality to realize how the latter becomes a more powerful feature as a result of their interaction.

Ignore the ‘concurrency’ FUD

Concurrency may increase or hurt a system's performance, throughput, and responsiveness. The number of simultaneous operations that may be executed is limited by the degree of concurrency. [\[605\]](#)

Processors in a UTXO-based blockchain should be able to do many actions at the same time to achieve real efficiency. The maximum parallelism possible increases as the amount of concurrency increases. As a result of this strategy, performance and throughput

increase. It also has several benefits over account-based systems (like Ethereum).

Deploying DApps on UTXO ledgers is different

To recap from earlier, remember Cardano's approach to DApp deployment is different. It requires scaling a steep learning curve and employing a careful strategy.

Concurrency optimization is a discipline that must be studied: developers must create code in such a manner that contention is limited (e.g., by avoiding shared states and accidental dependencies). This concurrency must then be translated into parallelism by the system. A number of developers have previously found successful approaches, while others are currently working on them. It is not possible to simply transfer skills learnt on one blockchain to another; although there is a learning curve, the benefits outweigh the effort.

In any case, it's vital to remember that a developer can't simply utilize an adapted Ethereum contract to build a scalable DApp on Cardano. Cardano is built on the UTXO paradigm rather than the account-based approach; hence a single on-chain state will not satisfy Cardano's concurrency condition. DApps should instead distribute their on-chain state across several UTXOs. As a result, their application's concurrency will increase, allowing for faster throughput. Read how to design a scalable Plutus application [\[606\]](#) to learn more about scalability, and the order book pattern [\[607\]](#) to learn more about how to organize DApps on Cardano using patterns.

The Cardano ledger was built with high certainty, security, and formal verification in mind. In line with this philosophy, it's also critical to make sure transaction processing is deterministic, which means a user can anticipate the effect and result of a transaction before it happens.

With the addition of smart contract capabilities, the ability to guarantee the cost of transaction execution and how the transaction acts on the ledger before it is submitted becomes even more important. The deterministic design of Cardano and Plutus scripts^[608] ensures this possibility.

In Alonzo, the minimum ada value to perform a transaction is calculated differently than it was in Mary. The minUTxOValue^[609] protocol parameter has been deprecated in Alonzo. However, in Alonzo, the requirement that each UTXO include an amount of ada that is proportional to the size of the entry is still in place. The min-ada-value is the size-dependent minimum ada amount in a UTXO, and it is currently derived using the Alonzo parameter coinsPerUTxOWord. Read the details of the Alonzo min-ada-value calculation^[610] to understand more.

Cardano Docs^[611] goes through a worked example (beyond the scope of this book) which covers:

- Setting up the Environment
- Running the Cardano Node
- Writing and serializing your Plutus on-chain code
- Create your transaction with accompanying Plutus Script(s)
- Transaction to lock funds
- Submit transaction to execute Plutus script.

Datums and Redeemers

Datums and redeemers are two crucial features in Plutus; it's important to know what they are and how to use them when submitting transactions. The datum is a piece of data that may be connected with a UTXO and is used to hold script state information like the script's owner or timing metadata (which can define when the UTXO can be spent). It's typically used in conjunction with a redeemer, which is arbitrary data provided in a transaction that's used as a script input.

Transaction validation over two phases

The unspent outputs from prior transactions are referred to as inputs. The datum hash and a value (consisting of an ada amount and optional, extra native tokens) are kept in a UTXO at an address (public key or public key hash). The script decides whether to ‘unlock’ the funds when a UTXO at a script address is an input to a valid transaction. This may be implemented if the script’s requirements are met (an arbitrary combination of factors including datum, redeemer, and script context). A transaction must be signed by the holder of the private key associated with the address during the first validation step.

From the perspective of a redeemer transaction, it’s critical to grasp the following concepts:

1. Script address: the Cardano address that stores funds guarded by a Plutus script that can be further unlocked. It is a hash of the Plutus script.
2. Datum hash: the datum hash must be linked to a UTXO at a script address in Cardano. This is done to save memory and allow for quick access when verifying transactions.
3. Plutus script is a ledger-based executable application that performs further (phase two) transaction validation.
4. Datum value: you need to supply the datum value that matches the datum hash supplied in the locking transaction when sending a transaction to redeem funds.
5. Redeemer value: the same arbitrary data format as datum is used. The redeemer value is utilized by the script to verify the transaction and is tied to the input transaction to release funds from the script.
6. Script context: a synopsis of the transaction that is also required by the Plutus script in order to verify it.

The process of working with datums and redeemers is beyond the scope of this book, but you can study worked examples in the Plutus

Pioneer Program, [\[612\]](#) currently in its third iteration and Cardano Docs. [\[613\]](#)

Plutus Scripts

Cardano validates operations via scripts. Pure functions with True or False outputs are implemented in these scripts. The process of invoking the script interpreter to run a script with relevant arguments is known as script validation. A script is code that determines if the transaction spending the output is approved. This kind of script is known as a validator script since it checks if the transaction is permitted. A simple validator script would verify whether the spending transaction was signed by a certain key, just as basic pay-to-pubkey outputs do. Scripts may be used to express meaningful logic on the chain. Metadata and scripts are bundled together in a single transaction for greater throughput.

The EUTXO paradigm operates by passing three parameters to validator scripts:

- Datum: This is a piece of data that is linked with the output and is locked by the script (just the hash is present). This is usually used to carry state.
- Redeemer: a piece of info associated with the spending input. This is usually used to provide the spender's input to the script
- Context: this is the metadata concerning a spending transaction. This is used to make assertions about how the output is sent (for example, 'John signed this one').

Plutus Core

The words script and data must be properly defined in order to apply the EUTXO paradigm. Scripts need the employment of a specific, well-defined scripting language, as well as the definition of the kind of data that is connected to outputs and used as redeemers. Plutus Core comes into play here. Cardano uses the Plutus Core scripting

language. Plutus Core scripts, which may be written in a basic functional language comparable to Haskell, and a large chunk of Haskell, can be utilized. You don't code any Plutus Core when creating a contract. A Haskell compiler plugin produces all Plutus Core applications.

These scripts will be run 'live' on the chain by nodes during transaction validation. They will either use validator scripts to lock UTXOs or minting policies to govern the minting and burning of native tokens.

Another reason Haskell is an excellent choice for creating Plutus Core scripts is because redeemer data is a basic (algebraic) data type that can be specified simply. A smart contract developer will create validator scripts in Haskell, which will be compiled into Plutus Core automatically. Appropriate Haskell libraries make writing such validation logic easier by providing core data types for transaction inspection during validation, as well as a plethora of helper functions and higher-level abstractions which allow contract programmers to focus on the business logic rather than the low-level details.

Simple example

A customer 'John' wants to buy 'Cardano for the MÄsses' which costs ⠈10. There must be confirmation they have enough ⠈ in their wallet before they can buy it.

```
if EnoughADA(book=CardanoForTheMasses, customer=john):
    buyBook()

def EnoughADA (book,customer):
    return customer["balance"] >= book["bookPrice"]

def buyBook():
    print ("You have enough ADA to buy the book")
```

```
CardanoForTheMasses = {"bookPrice":10}
john = {"balance":11}
```

In the above example:

- The datum is the information about this transaction:
john.balance
- The context is the state of the world, at that point meaning:
CardanoForTheMasses.bookPrice
- The redeemer, is the action to perform: *buyBook()*

The validator script is the function that uses all that information, in this example, *EnoughADA*

IOG's GitHub contains examples of validator scripts on every smart contract:

- Plutus transaction tutorial[\[614\]](#)
- Plutus Hello World[\[615\]](#)
- Plutus pioneers English Auction[\[616\]](#)

Cost model parameters

A number of parameters in the cost model for Plutus Core scripts are also included in the Cardano protocol parameters. Individual settings may be tweaked by developers.

See the following for more details:

- A list of cost model parameters and their brief description[\[617\]](#)
- Sources to find out more about the meaning of parameters[\[618\]](#)

March 12, 2019. How is a simple transaction different from running a smart contract? CH:[\[619\]](#)

So the goal of Plutus is to actually turn all transactions into a

smart contract in some way. So basically if you look at the difference between what Ethereum does and what a UTXO system like Cardano does... they're different data structures. So one is kind of a mutable ledger and you send messages to it to wake it up, and then you're going to have all the state management that you have to contend with ...and it's really difficult especially as the system grows and especially as you want to shard the system to keep track of everything ...so you have to add a lot of complexity into your model.

When you look at UTXO system it's what's called a data flow graph ...and basically it's just saying alright you have all these threads... and you have outputs and all you have to do to wake one of them up is just claim that you have the right to spend it ...and then if you have the proof that it validates, it spends...

... so what we've done is we've taken that model and we've extended it to include some state information and include the value and include some data ...and we call this the Extended UTXO model... so you keep the same semantics of Redeemer validator^[620] (btc scripts) that Bitcoin introduced over 10 years ago... but now you've added a capability of having enough information in it, that you actually can have code running, this is what Plutus is basically all about...

Now the advantage of this type of a system is that now all transactions can be either as simple as push value from Alice to Bob ..or they can be as complicated as a smart contract that you would see like creating a currency or something like that... so there's a whole spectrum of complexity there ...and you can chain these things together.. and you can also more easily interact with that on-chain transaction with off-chain code ... because when you actually look at these smart contracts generally what they are they're wrapped in complexity from things living outside of the system... so you'll have some JavaScript code and some web3 action going on and that's running on a server or a client ...and then that's talking to

something living on-chain ...that's the Ethereum model

...with Cardano it'll just be Plutus... template Haskell... Haskell and then that runs and it runs as a single unit ...and you can write all the code together and it's very easy to validate that the off-chain and on-chain code is actually working correctly together ...and we're actually working with GHCJS (project to build a to Javascript backend for the Glasgow Haskell Compiler) and with webassembly ...and you'll be able to port that code off-chain code to run on.... anywhere javascript can run ...so can run as a node package or you can run it the browser via web assembly...

So we have a nice framework there and you can do a lot of property-based testing and a lot of cool validations... and say things are working correctly ...because it's running this data flow model that's immutable ...what's really nice about it is that it is much easier to shard these types of transactions... So basically the answer to your question, succinctly, is that all transactions are technically smart contracts in this Redeemer validator model... it's just their complexity is up to the user and how they run these types of things ...there are a lot of really interesting use cases that do require further extensions, especially if we're thinking about things like pub sub (publisher subscriber) and contingent settlement.

Collateral mechanism

Alonzo brought the dawn of smart contracts. The collateral mechanism is a crucial component that guarantees smart contracts are run successfully.

Cardano uses a two-phase validation mechanism, relying on the assurances offered by the Alonzo ledger's deterministic architecture. The primary goal of implementing two-phase validation is to reduce the amount of uncompensated validation effort performed by nodes. Each phase has a specific role to play in reaching this goal:

- The first step verifies that the transaction has been accurately structured and that the processing fee can be paid
- The transaction's scripts are executed in the second phase.

Phase-2 scripts are executed if the transaction is phase-1 compliant. If phase 1 fails, no scripts are executed, and the transaction is rejected right away. In the event that phase-2 verification fails, collateral is utilized to ensure that nodes are rewarded for their efforts. As a result, collateral is given when a user gives a monetary guarantee that the contract has been properly constructed and rigorously tested. The amount of collateral input is set and included when the transaction is created. The transaction's collateral amount is the entire balance in the UTXOs corresponding to these specifically tagged inputs. The collateral is secured if the user meets the guarantee's requirements, and a contract is implemented.

The problem

If a smart contract fails without collateral, the user is not penalized. However, by the time the transaction fails, the network has already paid for the transaction to be initiated and validated. A hostile adversary might spam the network with dummy transactions, thus depriving other users of service for very little expense.

How collateral solves this

When a user starts a transaction, they commit enough ada to satisfy the transaction's cost of execution. Transactions that employ non-native smart contracts (also known as phase-2 contracts) in Alonzo need adequate collateral to cover the expenses of any transaction failures. This sum may seem insignificant, but it is enough to make a denial of service (DoS) attack prohibitive. Only if a transaction fails validation are collateral costs collected. The transaction costs are paid if the contract passes validation, but the collateral is not. The collateral of an honest user is never in danger of being lost.

Transaction costs on the Cardano blockchain are predictable since they are solely influenced by local values and state. A user may predict the transaction's execution cost (in ada) before initiating it. Other blockchains, like as Ethereum, whose design lets other network activities impact the gas cost. The amount of collateral needed is solely determined by the execution cost.

The Cardano testnet^[621] offers a secure environment with free 'test' ada, allowing DApp developers to extensively stress test their smart contracts before publishing them to the mainnet. If transactions go well on the testnet, the developer may be certain that all of the scripts will run smoothly as well.

If the on-chain circumstances have changed after the transaction was created, the transaction will be completely rejected with no fees collected. No collateral would be charged if a signature was absent, for example.

In practice

The total ada included in the UTXOs referenced by collateral inputs is referred to as collateral. If a phase-2 script fails, a transaction uses collateral inputs to pay its fees.

The idea of 'multi-signature' scripts was introduced by the Shelley formal specification. The ledger rules completely capture Phase-1 scripts like these. Execution costs may therefore be readily estimated prior to the implementation's running, and any fees can be determined directly inside the ledger rule implementation depending on the size of the transaction that contains the script.

Phase-2 scripts, on the other hand, may do any Turing-complete computation, in theory. We want a budget in terms of a number of abstract ExUnits for transactions that leverage phase-2 scripts. This budget establishes a quantitative limit on resource consumption in terms of a variety of measures, such as memory utilization or

abstract execution steps. The budget is then utilized to calculate the transaction fee.

From the Plutus Technical Report,[\[622\]](#)

Resources are tracked in terms of two abstract units: abstract time, and abstract (peak) memory. Together we refer to these as **exunits**. Why are the units here ‘abstract’? They must be, because we need to be able to keep things deterministic, and so we cannot use real time or memory usage. Rather we have to define some abstract measures which we try to align with real resource usage.

For more info, read the Cardano ledger specification for Plutus Core.
[\[623\]](#)

Learning Plutus

The best place to start is to study the original Plutus Tutorial[\[624\]](#) from the documentation.

There is plenty of help from the community also. Chris Moreton (@PoolChess[\[625\]](#)) has transcribed the Plutus Pioneer Program lecture notes. Visit his ‘readthedocs’ site[\[626\]](#) where you can also download a pdf or epub version.

The IOG education team wrote an introductory Plutus ebook, available on Amazon[\[627\]](#) and LeanPub. The ebook is aimed at beginner-level Haskell developers focusing on the fundamentals of the Plutus smart contract language with real-world examples.

You can also engage the community directly about Plutus on the Cardano Forum[\[628\]](#) or on the IOG Technical Discord.[\[629\]](#)

Get started with Haskell

IOG recommends the popular book or website Learn You a Haskell for Great Good[\[630\]](#) by Miran Lipovača. ‘Learn You a Haskell’ is an

engaging, reader-friendly illustrated guide that is many peoples' introduction to Haskell.

The Plutus Pioneer program is not for beginners, so it's perhaps best to first study the online course Haskell and Crypto Mongolia Sept 2020^[631] available on YouTube, delivered by Andres Löh, co-founder of the Well-Typed consultancy and Dr. Lars Brünjes, Education Director at IOHK.

You should now be ready to apply^[632] to the next cohort of the rigorous Plutus Pioneer Program.

Plutus Pioneer Programs & educational partnerships

IOG created the Plutus Pioneer Program in anticipation of Alonzo. This initiative gathered a wide range^[633] of software developers to take on smart contract programming challenges, such as the ones mentioned above. The program's purpose is to allow smart contract implementations that serve as informative examples for incoming external DApp developers utilizing the Plutus language. These could also be used as foundational examples for the Cardano community at large.

April 2021 was the first in a series of IOG's Plutus pioneer training programs where participants learn the fundamentals of Plutus and help to test the code. This innovative program aimed to recruit and train developers within the ecosystem so that they are fully prepared when Plutus was deployed to the Cardano mainnet later in 2021.

Since IOG announced this new course in March 2021's Cardano360 show,^[634] they have had a lot of interest from the developer community, both from developers who want to create decentralized applications (DApps), and smart contract programmers who want to work with Cardano's principal development language.

Course syllabus

The course, always evolving, will teach you the fundamentals of Haskell and Plutus programming. The course modules will cover the fundamentals of Haskell and Plutus, such as functions and data types, type classes, monads, template Haskell, the Plutus Playground, the Extended UTXO model, working with Plutus on and off the chain, minting policies, state machines, the Plutus application framework, and some case studies and practical exercises.

The course is modular and highly interactive, with new instructional videos from IOG's director of education, Lars Brünjes, released each week, as well as a series of practical assignments to do throughout the week as part of each module. There are also frequent Q&A sessions, and pioneers get access to a dedicated Discord community channel designed to help you interact with other course participants as you study.

Because Plutus is partly based on Haskell, previous expertise with Haskell (or similar functional programming language) is very beneficial. You should have some programming expertise, as well as a mathematical and technical mentality, at the very least, as the program is not a beginner's course in coding. While formal methods expertise is not required, programming skills and a general aptitude for logical and mathematical reasoning are. Template Haskell, type-level programming, [\[635\]](#) and effect systems will all be covered in this course. It's recommended pioneers read Learn You a Haskell guide (learnyouahaskell.com) before beginning the course if you need a refresher or an introduction to Haskell.

New Pioneer Programs

Plutus Pioneer and Atala Pioneer programs from IOG were launched in 2021. Thousands of individuals have finished these interactive training courses, which were designed to expand the reach of IOG's educational content.

The response on the courses, delivery, and support has been positive. As a result, IOG is preparing several additional programs in

other fields for 2022, as well as further courses on Plutus smart contract programming and Atala digital id software. Decentralized finance, or DeFi, intends to enable direct peer-to-peer financial transactions between people and businesses without the need of central authority.

The Marlowe Pioneer Program^[636] was announced at the April Cardano 360 episode. You can find out more from IOG's blog.^[637]

With new Plutus enhancements (see chapter 9) to be introduced by the Vasil hard fork in July 2022, expect to see a new iteration of the Pioneer Programs soon as well fresh content delivered at hackathons. See the dedicated 'IOG Workshops' site^[638] for the latest details.

Partnerships

In September of 2021, a partnership with the European Business University of Luxembourg (EBU)^[639] was launched. EBU is a well-known educational institution and a non-profit committed to higher education and certificate programs.

The IOG education team funded this initiative, which strives to make education more accessible throughout Africa. It provides free educational materials to a large number of pupils while also supporting the IOG strategy in the area. In 2021, EBU offered its first Plutus and Haskell course.

The Marlowe team has also attended IOG planning sessions. In May 2022, Niamh Ahern (IOG Education Manager) announced the inaugural Marlowe Pioneer program. The Cardano Foundation are also building out partnerships such as their recent announcement^[640] to work with the University of Zurich on Academic Blockchain Research.

IOG also plans to release many new books in 2022, including an upgraded edition of the Plutus ebook.^[641]

What is programmability?

Programmability generally refers to program logic (business rules). While IOG selected Haskell as the foundation for achieving strong assurances on the functional correctness of fundamental system components, no single language or technology can produce a rock-solid blockchain platform.

With so many diverse programming contexts to choose from, IOG's mission is to guarantee that both internal developers and the larger developer community have a uniform and unified experience when working with Cardano. As a result, IOG is pushing the boundaries of development while working with various programming languages and development tools in the infrastructure. This entails improving coding principles and broadening the scope of diverse systems and approaches.

Internal procedures must be the starting point for every endeavor to expand functionality and utilization. As a result, IOG designed a new internal structure that promotes development agility to offer a flexible and uniform environment for everyone developing and deploying on Cardano.

DevX

IOG established a new Developer Experience department (DevX), directed by Moritz Angermann, [\[642\]](#) to ensure that developers at IOG aren't hampered by the tools they use on a daily basis. The department works closely with all engineering teams and is in charge of maximizing team synergies and simplifying development processes. As a logical extension of the 'tools' team that is now part of DevX, another priority of DevX is developing Haskell tooling.

Dev tooling

While Cardano is a multi-functional smart contract creation platform, it is still in its infancy, with the ledger and network being enhanced iteratively. Cardano is built to service millions of users all around the world, therefore IOG are adjusting it to be more adaptable as demand grows. When the network grows, IOG continuously alter protocol settings^[643] to accommodate the increased scalability and throughput.

The DevX team is working on developing technology that will allow for continual ledger updates and improvements. This toolset caters to the demands of developers and provides for more efficient use of diverse building libraries. The following are some of the things that can be done to make the Haskell development experience more efficient:

- Significant enhancements to cross-compilation capabilities
- Improved plugin support
- Interoperability with the Rust programming language and other languages.

These enhancements allow developers to not only use Haskell libraries written in other languages, but also to leverage Haskell libraries written in other languages. In addition, the department focuses on improving the workflow associated with the use of Nix,^[644] the Glasgow Haskell Compiler (GHC), and GHCJS (Haskell to Javascript compiler).

IOG anticipate that when Cardano evolves into a completely open infrastructure model in 2022, these enhancements will empower the larger developer community with improved capabilities for working on various projects and deploying them on Cardano. Charles Hoskinson has outlined^[645] his wish for Cardano to mirror other OSS (open source systems) such as Hyperledger to Linux.^[646] In June 2022, The Cardano Foundation joined The Linux Foundation as a Gold member, becoming the only nonprofit active at this level.

Cardano Stack Exchange

Cardano developers access a dedicated community hub for support with the (CSE) Cardano Stack Exchange. The establishment of a decentralized, functioning ecosystem with a broad user base requires a thriving, knowledgeable community. As Cardano matures, everyone may benefit from its decentralized financial solutions while offering best-in-class blockchain technology, in keeping with the open-source strategy.

To achieve shared objectives, it is critical that everyone participates in the development process and has access to the information, advice, and support they need at all times.

IOG encourages developers from all around the world to join in one location — Cardano Stack Exchange^[647] — to help this cause. This developer hub is a great location to exchange ideas, ask and answer questions regarding all aspects of Cardano development and operations, and pool resources. This site, which is run by Cardano community members, is one of the tools for learning how to create DApps and smart contracts or if you just want to know ‘What is Layer 0?’^[648]

Origins

Cardano Stack Exchange originated from Stack Overflow.^[649] One of the most recent is for Cardano developers. It’s a community-moderated question-and-answer site where all Cardano developers, including Plutus pioneers, may obtain professional answers to a wide range of questions, from installation questions to configuration and implementation specifics. Stack Overflow’s community-driven, decentralized mentality meshes especially well with Cardano’s open-source, decentralized philosophy.

How does the Cardano Stack Exchange work?

It functions more like a question-and-answer forum than a debate forum like the Cardano Forum.^[650] This structure allows you to quickly locate the questions you’re searching for without getting

bogged down in lengthy discussion threads. Once you've signed up, you'll be able to search through all of the prior questions and recommended answers.

The community elects the moderators^[651] and shows their gratitude by upvoting questions and answers. As you use the site, you earn reputation points^[652] by asking questions, upvoting questions and replies, and answering other developers' inquiries. Reputation points help you improve your total score and get access to additional features on the site. Many individuals believe that discussing something with another developer is one of the most effective methods of learning. Teaching is, as they say, the best way to learn.

CSE's graduation from its trial stage, with the 'Beta' designation removed, demonstrates that it has attained a critical mass of usable, decentralized information. The group behind Stack Exchange helps and judges the creation of new communities, which is a difficult procedure. Discussion, Proposal, Community Commitment, Private Beta, Public Beta, and Graduation are the six stages that a Stack Exchange project must go through before it can properly get up and running.

Stack Exchange is a federation of learning communities driven by merit-based editing powers and moderator elections, as well as a framework for Q&A-focused content curation. The value of this platform may be shown (particularly in the context of open source projects) by looking at the most well-known example: Stack Overflow (stackoverflow.com) has long been an important developer community center, setting the path for the development and acceptance of all of today's most popular programming languages.

Leveraging a self-governing, self-sustaining community is a useful approach and Cardano is already blessed with the world's largest DAO^[653] in Project Catalyst. Similar to how Stack Overflow empowered programming communities such as Python and Javascript, CSE has the capacity to strengthen Plutus and Marlowe development.

Plutus FAQ

Q: What is Plutus Core?

A: Cardano's programming language, Plutus Core, is used to deploy the EUTXO paradigm. Plutus Core scripts are written in a basic, functional language comparable to Haskell, and a significant portion of Haskell can be reused.

Q: What tools are included in the Plutus platform?

A: The Plutus Playground, the Plutus Fee Estimator, and the Plutus Application Backend (PAB) are all part of the Plutus platform.

Q: What is the Plutus Application Backend (PAB)?

A: The Plutus off-chain component is executed by the PAB, which was initially released late 2021 and is constantly improved with each iteration. It handles wallet backend and node application requests, holds the application state, and provides an HTTP API for managing application instances. The PAB is a command-line interface (CLI) wrapper.^[654]

Q: When I build my Haskell code in the Plutus Playground, what occurs behind the scenes?

A: The Plutus Playground passes Haskell code to the server, and the server compiles the Haskell code.

Q: Where can I find documentation on Plutus?

A: Here are some useful links:

- Learn about Plutus section^[655]
- Tutorials^[656]
- Explainers^[657]

Q: How do I set up an Alonzo testnet?

A: To test the submission of transactions including (basic) Plutus scripts, you can develop on the Alonzo testnet. To do so, start an Alonzo cluster in Byron mode and then transition to Alonzo gradually, or start it in the selected era right away. See instructions and sample Plutus script^[658]

Q: What are the cost model parameters for Plutus?

A: Plutus scripts include a number of cost model parameters that may be modified separately.

Q: What is the difference between wallets and UTXOs?

A: A wallet may hold zero or more UTXOs and spend value from those UTXOs, while a UTXO holds value in ada or native tokens and is recorded in the blockchain.

Q: What is the difference between off-chain and on-chain code?

A: Off-chain code evaluates and modifies values outside of the blockchain, while on-chain code verifies transactions and changes the state of the blockchain and ledger.

Q: Are there best practices outlined anywhere for writing smart contracts?

A: Yes, there is a section in the Cardano Docs.[\[659\]](#)

What the Vasil Hard Fork meant for Plutus

Named after a Bulgarian mathematician Vasil Dabov, who was also a Cardano community member, the Vasil hard fork in July 2022 brought major enhancements[\[660\]](#) to Plutus. John Woods, the then head of Cardano architecture at IOG, provided an update back in April.[\[661\]](#)

IOG increased the block size to 88 kilobytes, a 10% increase in throughput on Layer 1. Memory units rose from 10m to 14m. Block level limits were boosted from 50 to 62m. Cardano didn't actually need it at the time, as the load was being serviced efficiently. The goal all along, however, has been not to wait and for the network to scale as demand grows.

As is par for Cardano, IOG were 'code complete' for the Vasil hard fork event back in April. This allowed for a thorough QA (quality

assurance) to run in to ensure everything was robust and secure. This is the sensible approach when making significant changes to the ledger. Aside from the hard fork features, IOG are also brought several new features, fixes and enhancements that make apps performant on Cardano and a smooth developer experience.

Also introduced with Vasil was pipelining, IOG's enhancement to block diffusion. Pipelining enables Cardano to scale even further, boosting performance right up to the point where input endorsers will be introduced later in 2022. Input endorsers are a next generation 'end game' strategy. More about these features later in the Basho chapter (scalability).

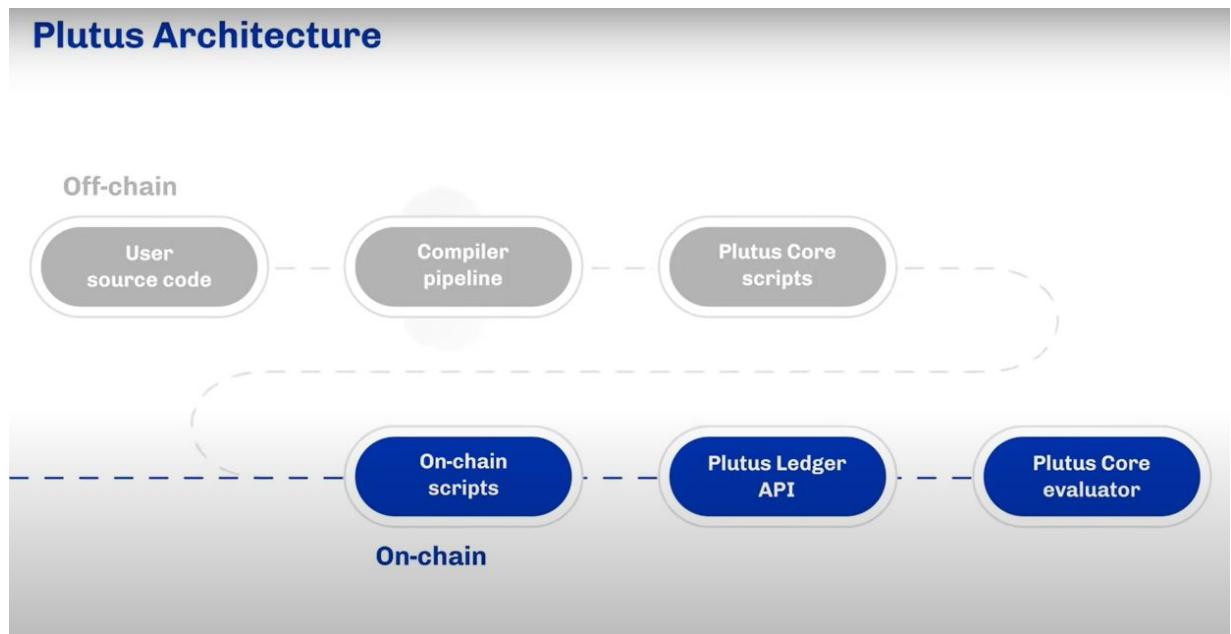


Figure 28. Plutus Architecture, following Graphics are from Cardano 360 episode

Plutus architecture

The above graphic displays the process of going from code to on-chain DApp. It starts with developers writing the source code to the DApp, and all of the Plutus contracts are currently written in Haskell. Other languages will be introduced in the future and DSLs (domain

specific languages) will make things easier for certain use cases, but right now, it's done in the functional programming language Haskell.

How does a developer start with user code and end up with an on-chain script?

It starts with the compiler pipeline. The Haskell code that's written by the developer is turned into what's called Plutus IR.^[662] Plutus IR is an intermediate representation,^[663] a concept inherited from LLVM work. When you write code, it goes through a pipeline in all contexts, whether that's a smart contract code that's destined for a blockchain, or Mac os or Linux app.

The intermediate representation provides an opportunity to mold and boost efficiency. The source code that was written by the developer, the application is represented in machine language that's going to be executed at runtime. By taking the Haskell source code, and by driving it through several optimization stages, whilst it's in this intermediate representation, it yields really fast performing apps.

From that intermediate representation, it then goes to type Plutus core. Type Plutus core is just before the raw ones and zeros that get executed on-chain. It's a convenient item for developers. Type Plutus core is really low level, but it still has some extra information that developers can use to debug. Finally then there is untyped Plutus core, which is a lambda calculus variant.

It's basically a logical way to express the app. Untyped Plutus core gets executed on-chain. So how does that untyped Plutus core or compiled app get on-chain?

After all those optimization stages, scripts get on-chain with toolkits and other Plutus apps. There is a whole suite of applications that help developers take the compiled application and inject it on-chain. Even when the on-chain code is written and has been compiled and is ready to go on-chain, an off-chain component is still needed.

The off-chain component is the application that will correctly form transactions to interact with that on-chain app. The on-chain app can be great, but there is still a need for something that helps build and form correct transactions that provide the inputs to that app. Inputs like the redeemer and the datum.

So you start with user source code, move through the compiler pipeline to make it as efficient as possible, taking that human code and bringing it down to the raw ones and zeros. The result is Plutus core scripts. Tools are used to inject that in a transaction on-chain, where that on-chain script will be processed by the ledger API and ultimately executed and run by the Plutus core evaluator in a decentralized way.

The off-chain or contract monad^[664] is a way to interact with this on-chain component by forming the right transactions.

How do you ‘interact’ with a Plutus contract?

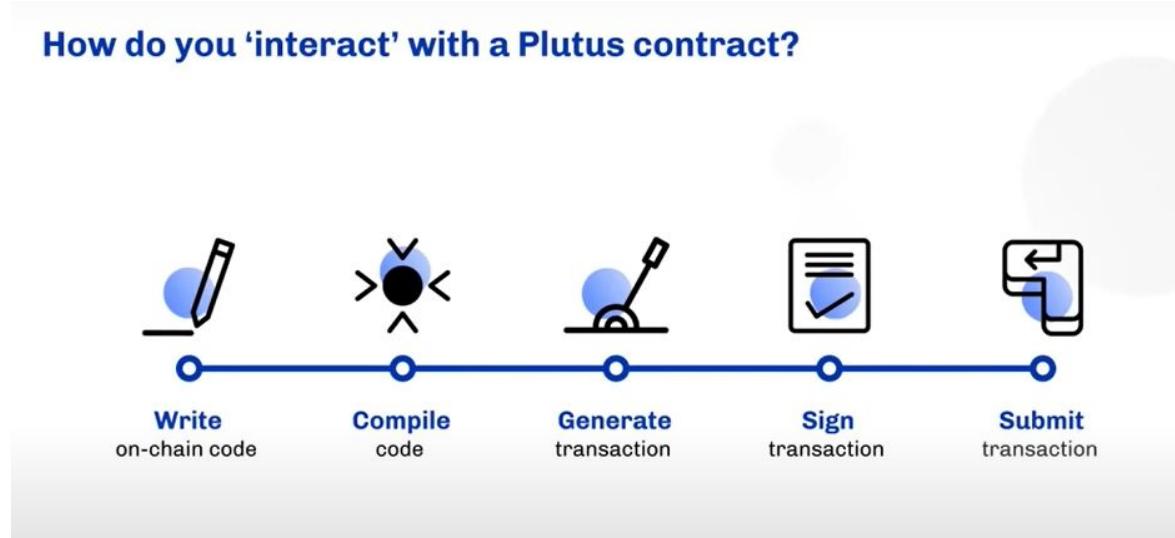


Figure 29. Interacting with a Plutus contract

What happens when using one of these scripts and a user wants to interact with a DEX, or another DeFi DApp? How does a user interact with a Plutus contract? It differs from how it works on Ethereum and it changed with IOG’s enhancements that came as part of the Vasil hard fork combinator (HFC) event.

Previously, you had to interact with a Plutus contract in the following way. You wrote the code, compiled the code, generated the transaction. You then used edwards25519, which is an elliptic curve signature^[665] algorithm, to sign the transaction with your private key. That transaction was then submitted onto the chain and executed by the ledger API.

Plutus DApps or Plutus scripts didn't go onto the chain until you were interacting with them. Before Vasil, the developer needed to include the Plutus script in the transaction that they are submitting to the chain, each time they want to interact with it, but this changed with Vasil. The following CIPs (Cardano improvement proposals) were implemented with Vasil in July 2022.

CIP31 ^[666] **defined reference inputs.** Reference inputs are a major enhancement to how developers interact with UTXOs. A reference input is a transaction input associated with a specific transaction output, however, rather than spending the output, it just references it.

A datum can be thought of as the data for your script, bits of data attached to outputs, where you might store data like a user handle, or avatar etc. Before Vasil, if you wanted to read your handle, or score of a soccer match etc., in your DApp, you had to consume the UTXO and then recreate it after you had read the datum.

Reference inputs allow you to read the datum, or the data that's stored at a UTXO, without consuming it and recreating it. This means that multiple DApps can read from the same datum simultaneously. This boosts concurrency and throughput dramatically.

CIP 32 defined inline datums. Before Vasil, this high score, or other data from the datum wasn't stored on-chain. The hash (fingerprint) of it was stored on-chain and it was up to the developer to include it when they were interacting with the script. Since Vasil, the data can be stored on-chain, eliminating the need for hashes and moving closer to a truly decentralized architecture.

CIP 33 is about reference scripts. On Ethereum, the contracts live on-chain, and you talk to them by a reference. On Cardano, developers previously had to include the script in the transaction every time they are interacting with it. CIP33 changed that. Developers are now able to push a script onto the chain, or contract onto the chain, and then interact with it via a reference. This is a very lightweight way to interact with a smart contract. Rather than having all of the app logic in your transaction, you now just have a small address, like an email address, that you include in the transaction, and it points to the script that already exists on-chain. These reference scripts can also be referred to at transaction validation, without requiring a spending transaction to do so.

More about these CIP enhancements in Chapter 9.

Additional Cryptographic Primitives

Bitcoin, and other chains, use different elliptic curves to Cardano. Edwards25519 is used on Cardano, similar to other cryptocurrencies like Monero. Bitcoin, Ethereum and others use secp256k1.^[667] Initially, Vasil was to add built-in support for secp256k1 on Cardano, enabling developers to interact with signatures from those other blockchains. However, after extensive testing, it was decided to omit this enhancement from Vasil. This can still be done manually by developers.

On the postponement of introducing this feature, CH^[668]:

ECDSA primitives are not where they need to be, and so that feature has to be put aside.. but all of the remaining features, CIP 31, 32, 33, 40, and other such things are pretty good

Pairing-based cryptography^[669] was another sophisticated cryptographic enhancement introduced with Vasil. This opens up whole new classes of app, with pairing based crypto, developers are

now able to use homomorphically^[670] additive signatures for more advanced use cases.

Making Plutus faster.

The core interpreter, which executes the untyped Plutus core, or the ones and zeros, was made faster and more performant. This helps ensure that validation of blocks is quick and efficient. It also ensures that the overall block propagation times are low, and DApps get executed quickly.

The script size, or the lambda representation is now 20% smaller since the update. The interpreter is 40% faster and non-evaluation processing is 80% faster. The non-evaluation process is not related to running the code, but to other things like data-munching and cost modeling.

CIP 40 Collateral Outputs

One of the things developers encountered early on with Plutus was collateral outputs. Whenever interacting with a Plutus script, some collateral is needed as part of the transaction to cover the unlikely event that the script fails in phase 2 validation. Phase 2 validation is when you have a Plutus script, there is a check before it's submitted to the chain that it can definitely run to completion correctly.

This is determinism and it's one of the virtues of Plutus over other contract platforms like Ethereum. But what happens if a malicious actor creates a transaction that they know will fail phase one validation and submit it to the chain? This had already occurred with some poor implementations in certain wallets and certain hardware wallets. In such a scenario, nothing too bad would happen, but ultimately the collateral got taken, so users lost collateral. It's similar to overcharging a fee.

IOG wanted to improve the user experience, so they found a way to submit a transaction including collateral, where the collateral included is just enough to cover. If you include an extra '0' by accidental fat finger or whatever, like a million ada, you get back

everything that's not required. A welcome correction. This is all part of a journey in getting Plutus to be a great user experience. Even if people make mistakes, they don't get harshly penalized.

Vasil postponement

IOG decided to postpone^[67] the Vasil update for a month to allow for more testing and due diligence. Given the current market conditions and recurring bad press for the industry, this cautious approach seems more and more prudent.



Ran NeuNer @cryptomanran · Jul 21

Last 90 days in Crypto:

1. LUNA collapse (\$80bn).
2. LUNA dump \$3bn in BTC over 48 hrs.
3. TESLA dump \$1bn BTC.
4. Blockfi dump \$900mn.
5. Celsius Bankrupt. \$1,5bn
6. Voyager Bankrupt. \$1,5bn
7. 3AC Bankrupt \$3bn.
8. Blockfi Bail out.
9. Miners Capitulate \$300m.
10. stETH depeg

724

1,696

5,904

Following the tried and trusted practice proven with prior hard forks, IOG had a testnet to help developers and exchanges understand what they need to prepare for. These major enhancements to Plutus don't automatically boost DApps. Developers need to take advantage of them actively, they are not a passive feature. DApps running prior to Vasil won't avail of these features automatically. Developers need to design and update their code to use reference scripts, making their DApp lighter. If you want to use reference inputs to do more reading of UTXO values and datums concurrently, you similarly need to update your DApp's code.

With the Vasil update now behind us, expect new content and a fresh iteration of the Plutus Pioneer Program to arm developers with the steps required. CardanoDocs (docs.cardano.org) is long overdue for an update and will likely be refreshed accounting for the new enhancements and updates to the Cardano Architecture (see Appendix). For more advanced users developing DApps with Plutus, Sebastian Guillemot provided a technical update^[672] on dcSparks's YouTube channel.

Determinism, parallelism and concurrency.

These features are differentiators for Plutus. There's a structure called a directed acyclic graph mentioned previously, which can be thought of sometimes like a spider web of little nodes, little circles and they have lines to the next one and lines to the next one as a web grows, especially if it goes in one way.

The Cardano ledger forms a graph of transactions, and graphs are great for parallel processing. Cardano enables, by definition, parallel processing with the way UTXOs work. This means that because Plutus core is deterministic, and because scripts only have access to local information, it's possible to parallel process many things during both validation of the Plutus script and validation of the ledger.

Regarding contention and application concurrency, it's important to remember UTXOs can only be spent once. With DApps, if multiple entities or actors try to spend the same UTXO simultaneously, they'll ultimately be blocked. When you're building on Cardano, better concurrency can be achieved by using multiple UTXOs and exploiting the parallelism and you can build with this style a scaling architecture that's massively parallel and allows you to service all of your users at the same time. The Vasil HFC is covered later in the Basho chapter.

Looking further out to sea, there is a lot more functionality on the horizon. IOG is already looking at privacy requirements for smart contracts. Kachina-Foundations of Private Smart Contracts^[673] is a

paper Charles Hoskinson ranks as ‘one of our most forward-thinking publications’.^[674]

January 29, 2021, Re: Cardano smart contracts model. CH:

We had to write new programming languages and new accounting models from scratch. Whenever you redo any programming language, it takes a few years. We also did a lot of foundational PL (programming language) research because we really wanted to understand what a smart contract programming language is. So it wasn’t just hey let’s go do something, release something …we started from first principles, and we hired people who actually write programming languages for a living. Like the leader of the Plutus project is Phil Wadler, along with Manuel Chakravarty.^[675] Remember that Wadler was the creator of the Haskell programming language and worked on probably a dozen programming languages throughout his career and made meaningful contributions everywhere from Go to Java.

So we brought some really serious, high-caliber people in and we said, ‘do it right’. So we don’t want it just a language, let’s take a step back and really understand what problems are you trying to solve with smart contracts and what problems aren’t you trying to solve. So you can get the right balance between off-chain and on-chain.

The other thing is we really wanted to think about the accounting model because at some point you’ve got to shard. At some point you need to move transactions off-chain and it turns out that the model that bitcoin uses is almost right. You just need to extend it. The accounts model is not. In fact, the model that Ethereum uses, Tezos uses, and these other systems use really is hard to shard. So the longer you live with that, the harder it’s going to be to go parallel. UTXO is super easy to shard and you don’t need a global state, you just have a local state for what your area of concern is. It’s just you have to extend it to do more. So it was really hard for us to figure out

how much extension was required for UTXO so we had to invent an entirely new accounting model from scratch.

Then we were really curious. Is that accounting model equivalent to the accounts model that Ethereum uses? In other words, can you move value back and forth between these systems? Or will something be lost? So we had to come up with a paper called Chimeric Ledgers^[676] that proved that they were. So there was a lot of infrastructure and background work that needed to be done. That took years. We did it in a very rigorous way that's recognizable to any professional programming language. So we actually wrote formal semantics, we proved some things in Agda^[677]. We had to redesign the language. I think Plutus was redesigned about 18 times... 19 times so there were a lot of iterations there, but that's great because we were saving the developers a lot of heartache and pain.

If you look at Solidity, it came out quickly, but it's already gone through an enormous amount of versions and they had to save their developers a lot of heartache and pain through iterating gradually. Meanwhile you have the DAO hack and meanwhile you have all these other things and there were a lot of do-overs that I think they would like to have. Unfortunately, you have to live with the sins of your language after you've released it.

JavaScript is the greatest example in history of that. They wrote it too quickly, less than 54 days, I think, and we spent 15 years, as an industry, 15 years cleaning up JavaScript to a point where it's actually a useful programming language. It was so bad for a while that people were creating like meta languages ... supersets like TypeScript and Dart and CoffeeScript to try to get away from JavaScript because it just could not be used for enterprise-grade applications.

Eventually they got their act together and put in classes and big arrows^[678] and you know these types of things to get JavaScript to a point where you could write maintainable code. We didn't

want to inflict, because billions of dollars are at stake, those sins into our community. We said instead ‘let’s do it right the first time’ and then all the iteration can be about better libraries, better tooling, some more syntactic sugar and you know things that developers want, perhaps better specification languages and these things... instead of ‘how do you fix the core language?’ We’d like the core language to be used again and again and the advantage we had is that we kind of started from a very good place.

Haskell was created in 1985 by a committee and they’ve spent more than 30 years carefully thinking about... ‘well how do we improve it?’ We had the hindsight of all these old language designers, who are now their 60s who had to live with all the sins they’ve committed in programming language design ...and they say, ‘okay we’re not going to do that again, that was a horrible mistake... and let’s not go through that pain’, and that’s just beautiful, we just saved our community so much by going down that road.

So what does it mean? It means for you, the developer, now that that’s almost there, you’re going to have much more concise code. You’ll have a better testing experience, and ultimately, you’ll be able to write more productive DApps with a better life cycle with those applications. Okay so that means it’s easier to maintain, your development team is smaller, you have higher developer productivity, and these are all things that developers really care about, and executives really care about, because they have to release software with predictable timelines and costs. They have to use this thing called ‘agile’, [679], they have ‘story points’ and ‘burndown charts’ and these things so you’d like to know that the platform is working with you instead of against you.

So we took a very ‘first principles’ approach to that. The other thing is that we had to be interoperable with the incumbents. The problem was that the incumbents made almost no effort to

formalize anything. So one of the first things that we did is we actually paid to have the Ethereum virtual machine formalized. We had this IELP paper, but nobody actually wrote down formal semantics. So we funded the KEVM project, and we actually wrote the first set with runtime verification. They did the work; we paid the money to formalize the Ethereum virtual Machine. Then after we did that, we knew where all the bodies were buried like what was the good, the bad and the ugly of this virtual machine and that execution model and then from that, they built IELP which is (was, put on hold) the execution model for ‘the ocean’, for all of the programming languages.

So there’s a vastness to the smart contract strategy of Cardano that is absent with all of these other projects. Usually what they do is they say, ‘let’s start with webassembly and then okay we’ll just figure it out from there.’ Then you have to build a resource model and a memory model and all this stuff. Then as you’re adding it in, you make mistakes and then you spend 5 - 6 years in the market fixing those and your gas fees are never right, and these other things are never right meanwhile who suffers?

The DeFi space suffers, your customers suffer. The problem is the financial incentives are all perverse. You get paid up front and then you get to sell at the top. So you’re not really paid in a traditional sense for quality or for whether it works or not. And so that’s why we see the mistakes we’ve seen in the industry, but we said, ‘that’s immoral, that’s wrong take a step back, do it right’ and look, when it comes, developers are going to flood in and we’ll be able to catch up for whatever lost ground in 12 to 24 months and we’ll just surpass all of it.

It’s kind of like when Apple did their do-over, they did objective-C. They weren’t super happy with it and then they moved over to Swift and they’re like, ‘okay this is the way, we’re very happy with this now and we think this ecosystem is good and the IOS development ecosystem is great as a consequence.

April 10, 2020. Do you regret going with Haskell? CH:[\[680\]](#)

We probably could have gotten away with F# or Scala over Haskell and gotten a lot of the Haskell benefit. I didn't realize that Haskell was going to require as much as it did ...and I wasn't prepared for it, we didn't set up the organizational structure that we needed at the beginning for that and had I been better prepared in the beginning, we probably could have avoided some of our growing pains that we had. On the other hand, we were able to attract some of the brightest minds in the world and work with those minds to solve problems in completely original creative ways and so Cardano was ultimately a better product for it but our time to market suffered. Whether that was the right decision or not... Who knows?!

Because we have to look at the project in 2022 and 2023 and if we're the size, scope and scale of Ethereum and we have a resilient robust ecosystem then it was the right decision ... if we're not there, it was the wrong decision... but we just won't know. We did actually look aggressively at Scala; in fact we wrote a product in Scala... and we wrote Mantis[\[681\]](#) which is an Ethereum Classic client in Scala. It was a great experience, I loved it... I had so much fun we had no delays, it was easy to get out, it was like paint-by-numbers... so I like Scala a lot, it's one of my favorite languages and I think there's a huge amount of advantages in that ecosystem. The sharp edges have been mostly muted.

That said, because of work we did with Haskell and the improvements we've made especially with GHCJS[\[682\]](#) and the improvements[\[683\]](#) we've made on Windows and the library level improvements we've made... if somebody chose Haskell today for a project, with the things that we've done, and the ecosystem has done, I think it would be a lot easier to build a product in Haskell. We've left a template to do that and future projects won't have the growing pains that we had.

At one point, I actually considered writing Cardano in JavaScript... I really thought about it, I said we have formal semantics through the JSCert program, out of Imperial College London, [\[684\]](#) and there are some functional things we can do... and we could do formal verification of some of the JavaScript code ...so here's a crazy thought ...why don't we actually get some Haskell hard core programmers and then force them to actually write JavaScript? ...and build a whole ecosystem around it, write up a whole bunch of beautiful JavaScript tooling for QuickCheck [\[685\]](#) and for all this other stuff and actually create a TLA [\[686\]](#) port ...so we can do TLA+ and connect it with JavaScript code.

Chapter 7: Marlowe

'Hell is just a frame of mind'

— Christopher Marlowe, Dr. Faustus

What is Marlowe?

Marlowe is a simple programming language for writing financial smart contracts for Cardano. It is named after the Elizabethan poet, dramatist and spy, Christopher Marlowe. Marlowe is limited to financial applications and is not Turing-complete. It is for people who are experts in finance rather than having programming knowledge.

Marlowe is based on peer-reviewed research carried out by a team led by Prof Simon Thompson, first at the University of Kent with the help of an IOG research grant, and then as an internal IOG team in collaboration with the University of Wyoming Advanced Blockchain R&D Laboratory. The research has resulted in several published papers.[\[687\]](#)

Context for Marlowe

'Machine code' was used to program the first computers. Each system had its own code, which was low-level and inexpressive: programs were long sequences of extremely simple instructions that were incomprehensible to anybody who hadn't created them. Higher-level languages such as C, Java, and Haskell may now be used to program systems. The structure of the programs mirrors what they perform, and the same languages may be used on a variety of devices. Languages like Plutus, Solidity, and Simplicity are blockchain counterparts. These higher-level languages are general-purpose in that they may be used to address a wide range of problems; yet, the solutions they represent are still programs, and using them successfully demands programming expertise.

Marlowe, on the other hand, provides blockchain financial contracts that anybody can write. It's a domain-specific language (DSL) for creating and executing financial contracts that lets users utilize their domain knowledge to quickly create and manage contracts without

the steep learning curve that comes with software development, blockchain, and smart contracts.

Marlowe is a user-friendly programming language that may be used to mimic financial products. It's a decentralized finance (DeFi) platform that allows for direct peer-to-peer lending, contracts for difference (CFDs),^[688] and other related products. Marlowe contracts are tailored for financial transactions, development platforms, and a fast track for financial service providers to establish competence in smart contracts and blockchain technology.

Marlowe contracts are simpler to read, write, and comprehend because they are written in a special-purpose language. It's also safer: certain faults are impossible to create, and IOG can fully analyze contract behavior without running a contract. Marlowe has several advantages over a Turing-complete language. It's more secure, predictable and addresses the halting problem^[689] by guaranteeing termination.

Marlowe's design features:

- No recursion^[690] or loops as contracts are finite
- There are timeouts on all actions, guaranteeing termination
- Commitments and timeouts are central to how Marlowe works in a blockchain context
- All contracts have a defined lifetime
- No assets are retained on close
- Value is conserved.

Who is Marlowe's target audience?

Because Marlowe enables you to write contracts graphically as well as in more conventional code, it may be used by someone who is an expert in the subject of financial contracts or business but lacks programming abilities and expertise. It may be used by financial institutions to create and deploy unique instruments for their customers and clients.

The Marlowe language is embedded in both JavaScript and Haskell, giving you a variety of editors to choose from, depending on your preferences and skill level. You can write contracts in these languages and then convert ('compile') them to Marlowe in the Marlowe Playground. Haskell is a functional programming language with its own established ecosystem and robust testing environment, but JavaScript provides flexibility and speed of usage with a vibrant community.

Marlowe may interact with real-world data, such as oracles, and contract participants can choose what occurs on and off-chain, such as in a wallet, by making decisions inside the contract flow. Marlowe is blockchain-agnostic, allowing smart contacts to be expressed on top of account-based models like Ethereum as well as Cardano's extended unspent transaction output (EUTXO) model. Marlowe is an industry-scale solution that incorporates examples from the ACTUS^[691] (actusfrf.org) taxonomy and financial contract standard.

Marlowe language structure

Marlowe is based on special-purpose financial contract languages adopted by academics and companies like LexiFi (lexifi.com), which produces financial contract software. IOG customized these languages to function on blockchain while creating Marlowe. Marlowe is a simple language with a few distinct structures that define behavior with a fixed, limited number of roles for each contract. These responsibilities are carried out by the contract parties.

Contracts may be constructed by combining a limited number of these constructs, which can be used to describe and represent a wide range of financial contracts. A running contract that can make a payment to a role or a public key, a contract that can wait for an action by one of the roles, such as a currency deposit, or a decision from a set of options are just a few examples. Importantly, a contract cannot wait forever for an action to be taken: if no action is taken by a certain period (the timeout), the contract will proceed on a different

path, such as taking a corrective action such as refunding any funds in the contract.

A contract may choose between two different future courses of action, each of which is a contract, depending on its present condition. The contract will terminate when no more activities are necessary, and any leftover money in the contract will be reimbursed. When a contract is executed, the duties it entails are completed by participants (blockchain identities). Each position on the blockchain is represented by a token, and roles may be exchanged during contract execution, thereby allowing them to be traded.

Marlowe as a domain-specific language for DeFi

There are many benefits to being domain-specific rather than general-purpose. Contracts are written in a finance-oriented language rather than a blockchain-specific language. As a result, certain types of mistakes are impossible to write, and some types of improper contracts are totally eliminated. Every Marlowe contract, for example, will have a fixed lifespan after which it will stop performing acts and any monies attached to the contract will be returned to the participants, meaning funds in a contract can never be locked up eternally.

Without needing to execute a contract, it is possible to analyze how it will react in all scenarios automatically. For example, you can assess whether a contract may fail to make a payment in certain circumstances or if it is guaranteed to make full payments in all circumstances.

Contract behavior may be replicated in a browser, allowing users to test out various scenarios before committing cash and executing the contract for real. Users may construct DeFi contracts in a variety of methods, including writing them in text or using visual programming to create smart contracts by connecting blocks that represent the various components. Users may also choose and select from a

variety of templates, which they can then customize as required.

Marlowe differentiators

The way Marlowe ensures that the contract is followed is where it distinguishes from non-blockchain alternatives. This assumes not just that the contract's directions are followed, but also that the participants commit and do not leave money locked up in the contract indefinitely. Timeouts are used to accomplish this.

A contract can request a person to make a deposit of a certain amount, but it cannot compel that person to do so. Instead, the contract can wait for them to commit to the contract for a set amount of time, after which it will proceed to follow some alternate instructions. This prohibits a party from canceling a contract by refusing to participate, ensuring that there's not a stalemate.

Timeouts safeguard all of Marlowe's constructs that need user input, such as user deposits and user selections. As a result, it's straightforward to observe that an user's commitment to a contract is finite: Marlowe can foresee when the contract will be completed - when it may be closed. Any unspent assets in the contract are repaid to participants at this time, and the contract comes to an end. As a result, any assets deposited into the contract by a participant cannot be locked up indefinitely: the commitment essentially terminates at this moment.

Furthermore, it is simple for us to read from the contract when it will end, which Marlowe refers to as the contract's lifespan: all parties will be able to determine this lifetime prior to entering into any contract.

A running contract in Marlowe cannot demand a deposit or a choice; it may only seek a deposit or a selection from a user. It can't 'push' these actions, but it may 'pull' them. However, it may make payments automatically, thus some features of a Marlowe contract might 'push' for certain events to occur, such as guaranteeing that a payment is sent to a participant by generating an appropriate transaction output.

Because Marlowe is a DSL, it can predict how Marlowe contracts will function without having to execute them: meaning you can leverage static analysis^[692] to deliver important diagnostics to users before they sign a contract. Marlowe can also leverage logic tools to explicitly establish Marlowe contract properties, providing users with the maximum level of certainty that their contracts will perform as intended.

Marlowe roadmap

IOG will complete the implementation of Marlowe on Cardano as part of the Goguen deployment, allowing individuals and organizations to execute DeFi contracts that they have written themselves or received from a contract repository, transferring crypto assets according to the contract conditions. Marlowe will operate on the Cardano blockchain initially, but it is ultimately blockchain-agnostic and might work on other blockchains in the future.

Through oracles, Cardano smart contracts will be able to retrieve external data values like the exchange rate between ada and Bitcoin. In some respects, an oracle is similar to a participant who makes a decision, and as part of the implementation, IOG wants to provide oracle values, enabling contracts to obtain values straight from a stock market ‘ticker’ or a data feed like CoinMarketCap.

Depending on their programming ability, finance professionals and developers may now start writing financial smart contracts directly in Haskell or pure Marlowe, or graphically using the Marlowe Playground. Later into the Goguen era, you can simulate and analyze the contracts you build in the Playground to ensure that they perform correctly and are ready to be released into the world of decentralized money. As IOG prepares to finish Marlowe’s implementation on Cardano and introduce financial smart contracts to the blockchain itself, the IOG Marlowe team will continue to implement examples from the Actus standard.

Marlowe Language Structure

Haskell types

The different components of the contract, such as accounts, values, observations, and actions, are represented using Haskell types.

These Marlowe components are used to manage how a running contract evolves by supplying external information and inputs. Basic portions of Marlowe are modelled using a mix of Haskell data types, which develop new types, and type synonyms, which give an existing type a new name.

You can use one of the following visual programming environments in addition to developing contracts in the textual version of Marlowe:

Using Blockly[\[693\]](#)

Using JavaScript[\[694\]](#)

Using Haskell[\[695\]](#)

Marlowe contracts

In Marlowe, a contract is made up of a small set of building blocks that may be used to express a variety of financial transactions, such as making a payment, making an observation, waiting until a specific condition becomes true, and so on. After that, the contract is executed on a blockchain, such as Cardano, and it interacts with the outside world.

Marlowe is written in Haskell, and it is represented as a set of algebraic data types, with contracts specified by the Contract type:

```
data Contract = Close
  | Pay Party Payee Token Value Contract
  | If Observation Contract Contract
  | When [Case] Timeout Contract
  | Let Valueld Value Contract
```

| Assert Observation Contract

Marlowe offers six different means of constructing contracts. Five of these methods – Pay, Let, If, When, and Assert – combine smaller contracts to create a more complicated contract, while the sixth method, Close, is a basic contract. Effects – payments – and warnings may be created at each phase of execution, in addition to producing a new state and continuation contract.

Pay

A contract of payment **Pay a p t v cont** will transfer the value **v** of the token **t** from account **a** to payee **p**, which will be one of the contract participants or another account in the contract. If the value **v** is not positive, or if the account balance is insufficient to cover the payment in full, a warning will be produced (even if there are positive balances of other tokens in the account). A partial payment (of all available funds) is made in the latter situation. The continuation contract, **cont**, is given in the contract.

Close

The contract **Close** denotes the closure (or termination) of a contract. Its only function is to provide refunds to account owners who have positive balances. This is done one account at a time, however all accounts get refunded at the same time.

We must first define values, observations, and actions before going on to additional contract types:

- Values - consist of quantities that vary over time, such as ‘the current slot interval,’ ‘the current balance of some token in an account,’ and any previous decisions. These are ‘volatile values’. Values may also be conditional on an observation and merged using addition, subtraction, and negation
- Observations - are boolean values that may be joined using typical boolean operators and are obtained by comparing values. It’s also possible to see whether any decisions have been taken

(for a particular identified choice). Observations will be useful at every stage of execution

- Actions - occur at certain moments throughout execution, such as:
 - depositing funds
 - selecting from a variety of options, including an oracle value
 - alerting the contract of an observation that turned out to be true
- Oracles - Oracles such as Chainlink and Ergo Pools are being built for the Cardano blockchain and will be usable in Marlowe on Cardano. Until that time comes, there is an oracle prototype in the Marlowe Playground. Oracles are represented as decisions made by a participant with the dedicated Oracle role.

If

The predicate **if obs cont1 cont2** will result in **cont1** or **cont2**, based on observation **obs** ‘s boolean value each time this construct is executed.

When

With the form **When cases timeout cont** , this is the most complicated contract constructor. It’s a contract that’s triggered by events that may or may not occur at any specific slot: the contract’s cases define what occurs when certain events occur.

In the contract **When cases timeout cont** , the list **cases** holds a collection of cases. Each case has the form **Case ac co** where **ac** is an action and **co** a continuation (another contract). When a certain action occurs, for example, **ac** , the state is updated and the contract will resume as the corresponding continuation **co** .

In order to ensure the contract ultimately completes, the contract **When cases timeout cont** will continue as **cont** once the **timeout** , a slot number, is reached.

Let

A let contract **Let id val cont** allows a contract to record a value, in a specific point in time, and name it using an identifier. In this example, the expression **val** is evaluated, and stored with the name **id**. The contract then resumes as **cont**.

This approach not only allows us to leverage abbreviations, but it also allows us to capture and preserve volatile data that may change over time, such as the current price of gas or the current slot number, at a specific moment in the contract execution, to be used later in the contract execution.

Assert

An assert contract **Assert obs cont** does not impact the state of the contract, it resumes straight away as **cont**, but it gives a warning when the Observation **obs** returns false. It can be used to guarantee that a property holds at any stage of the contract, since static analysis^[696] will fail if any execution forces an **Assert** to result as false.

There is a Sample Escrow contract^[697] in Cardano Docs.

Escrow in Marlowe

Extra constructs are included in Marlowe contracts to guarantee that they progress appropriately. When we observe a **When**, we must also supply two extra details:

- A timeout value after which the contract will continue
- The continuation contract to which it advances

Marlowe accounts and token usage

A Marlowe Account may store a variety of currencies as well as fungible and non-fungible tokens. A set amount is indexed by

a **Token**, which is a pair of **CurrencySymbol** and **TokenName**. Consider an Account to be a Map Token Integer, where:

```
data Token = Token CurrencySymbol TokenName
```

Cardano's ada token is denoted as **Token adaSymbol adaToken**

Marlowe Playground

Users would ideally like to understand how contracts will perform once deployed to the blockchain, but without the risk of actually deploying. Marlowe can help here as it replicates the contracts behavior off-chain in the Marlowe Playground.

The Marlowe Playground is an online sandbox environment where you may build, model, simulate and test the process of developing smart contracts, without having to install anything. Its goal is to empower all sorts of developers to create financial products on Cardano, even if they have no previous Haskell or JavaScript knowledge. There are a number of tutorials^[698] available that detail sample contracts as well as general information about Marlowe and how contracts should be modeled.

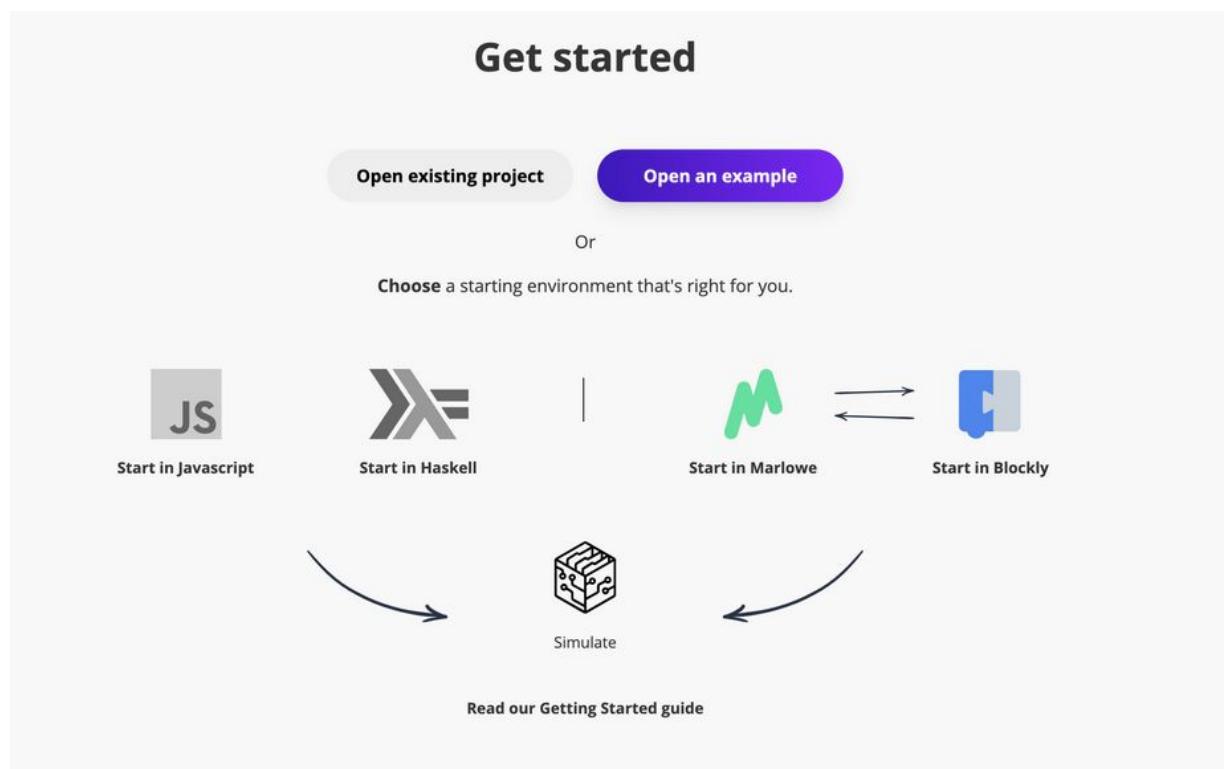
The Marlowe Playground is a platform for creating end-to-end financial smart contracts. Developers may use it to not only build smart contract code, but also to undertake early iterative design using simulations, formally validate smart contracts, and test them. These characteristics, together with a dedicated DSL (domain specific language) for finance, guarantee that contracts are simple to create, secure, verifiable, and well tested.

Marlowe written in the Playground may be saved as a github gist.^[699] At a later time, projects can be reloaded or cloned. The project is stored across sessions even if you don't use GitHub, however, be careful as clearing your browser cache may delete your work.

Getting started

When utilizing the Marlowe Playground, you have three choices to select from. You may write in Marlowe text directly, but you can also utilize the visual. Blockly is a visual programming tool that allows you to design contracts by connecting blocks that represent the various components.

You may also use the inbuilt Haskell or JavaScript editors to help you write more readable and concise Marlowe contracts. Once a contract is created, you may examine its behavior, such as determining if any of the contract's payments might possibly fail. You may also simulate the activities of the parties to see how a contract would function.



[Figure 30: Marlowe getting started](#)

Using Blockly with Marlowe

You can use the Blockly visual interface to link together the pieces of the contract or write Marlowe code directly as Marlowe text. This is a great tool for people who don't have a lot of familiarity with programming editors and prefer to write contracts graphically. Blockly

is used by hundreds of other projects such as MIT App Inventor^[700] which I used myself, many moons ago, to create these exam primer apps.^[701] It was a seamless user experience to make these with Blockly.

With just a few clicks, it was easy to create a contract in Blockly using a ‘Zero Coupon Bond’ demo file. The contract ‘Loan to buy John’s book’ took about 10 mins to create. I just needed to update a few placeholders before I could then view the contract as blocks or as Marlowe code. The Blockly editor also gives you access to the metadata editor and static analysis.

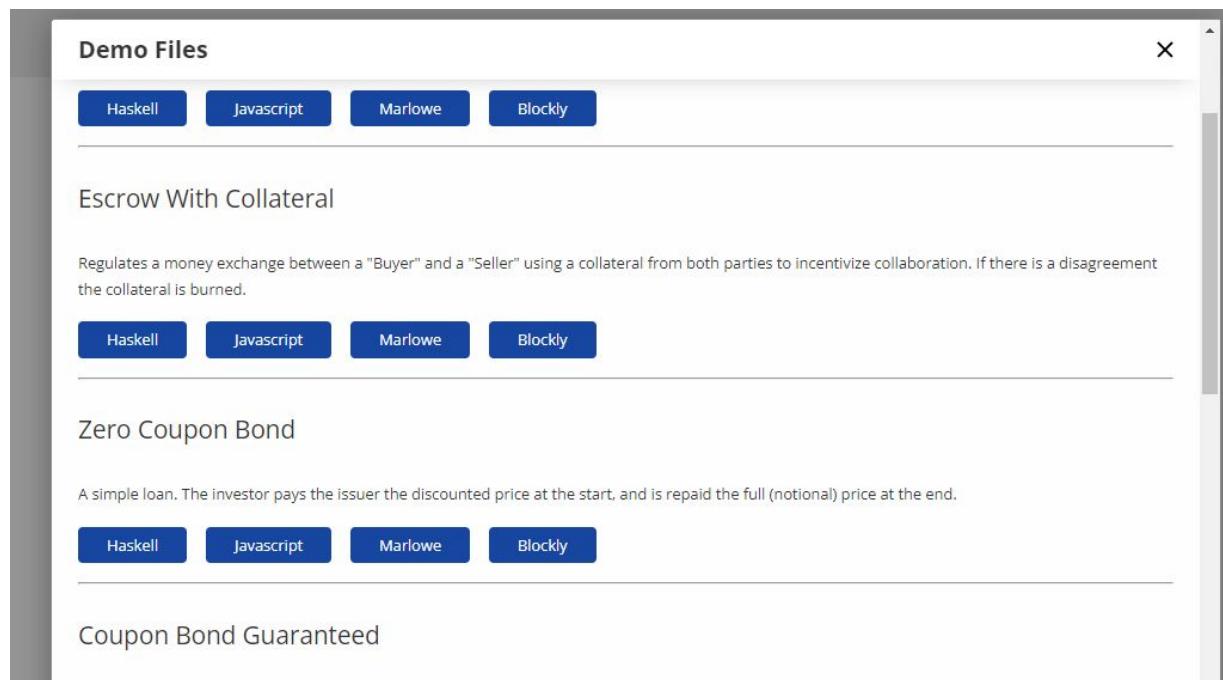


Figure 31. Blockly Demo Files

Contracts are built by dragging and dropping components to the holes in the blocks. Blocks are selected by just clicking on them, the current active block you are using will have a yellow outline.

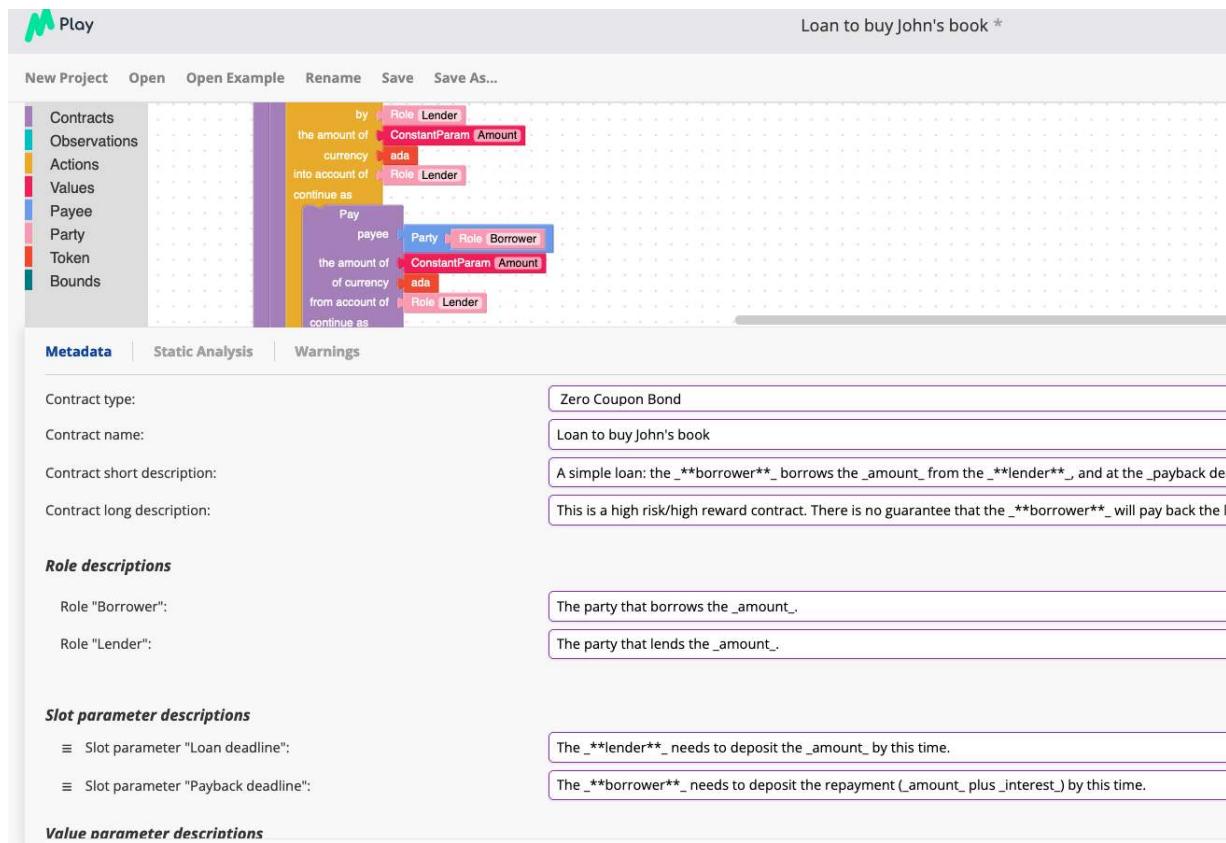


Figure 32. Blockly Tabs

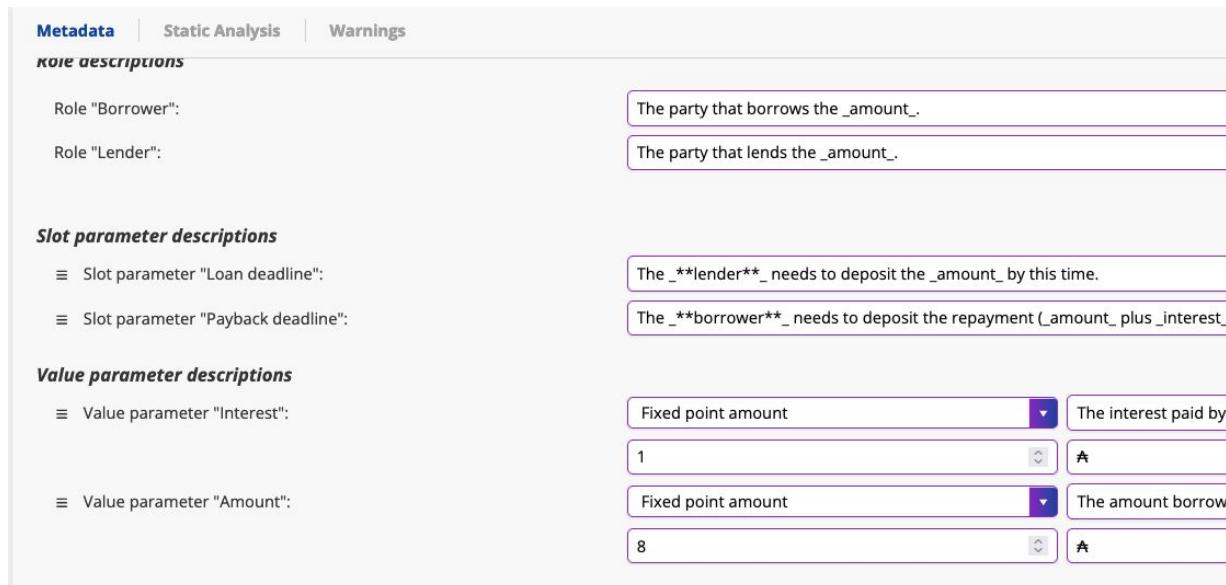


Figure 33. Blockly Metadata

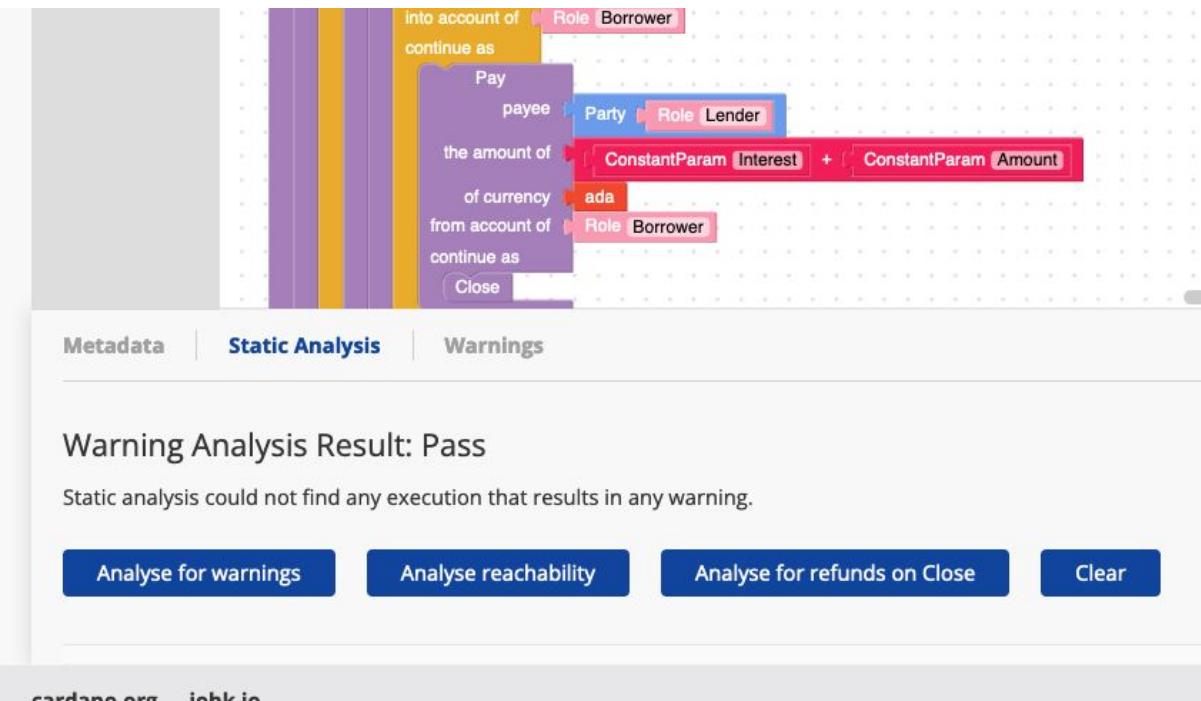


Figure 34. Blockly warning

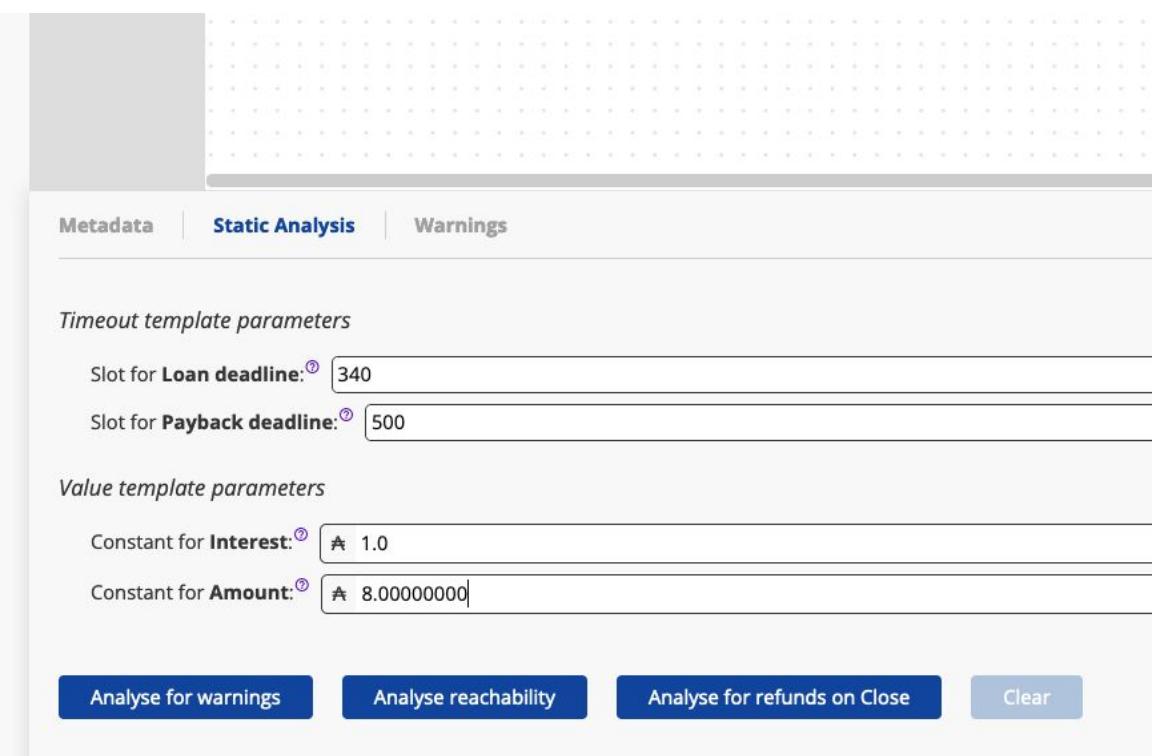


Figure 35. Blockly static analysis

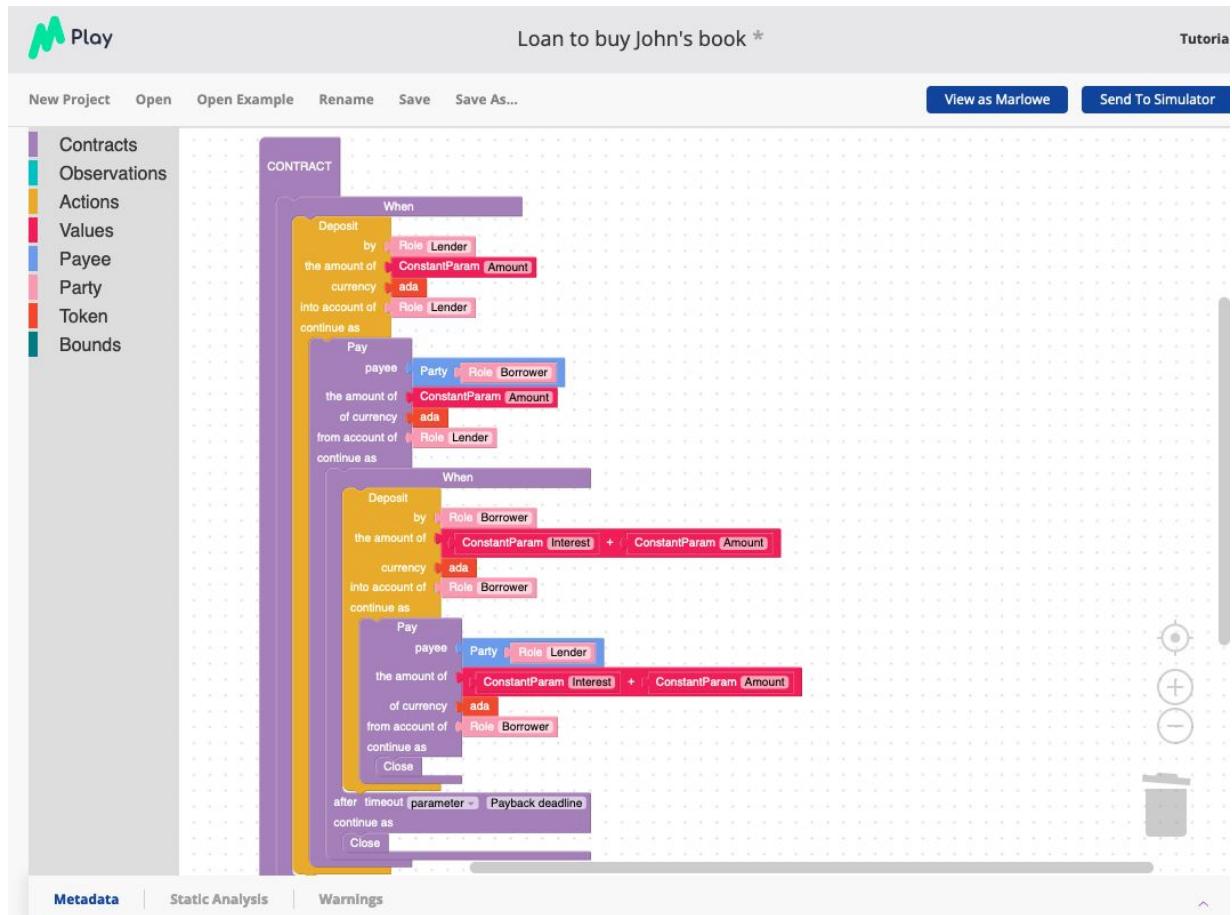


Figure 36. Block example

```

1 When
2   [Case
3     (Deposit
4       (Role "Lender")
5       (Role "Lender")
6       (Token "" "")
7       (ConstantParam "Amount"))
8   )
9   (Pay
10    (Role "Lender")
11    (Party (Role "Borrower"))
12    (Token "" "")
13    (ConstantParam "Amount"))
14    (When
15      [Case
16        (Deposit
17          (Role "Borrower")
18          (Role "Borrower")
19          (Token "" "")
20          (AddValue
21            (ConstantParam "Interest")
22            (ConstantParam "Amount"))
23        )
24      )
25      (Pay
26        (Role "Borrower")
27        (Party (Role "Lender"))
28        (Token "" "")
29        (AddValue
30          (ConstantParam "Interest")
31          (ConstantParam "Amount"))
32      )
33      Close
34    ])
35    (TimeParam "Payback deadline")
36  Close
--
```

Metadata | Static Analysis | Warnings | Errors

Figure 37. Marlowe Haskell

Using the Editor for Haskell or JavaScript

You can use the Haskell editor to produce Marlowe code if you're a seasoned Haskell developer. Because Marlowe is built as a Haskell data type, creating Marlowe smart contracts using Haskell is easy. Just select 'Haskell' in the sample 'Demo files'. You can use Haskell to make contract definitions more readable by using Haskell definitions for sub-components, abbreviations, and simple template functions. The editor will assist you with auto-complete, error checking during editing, and binding tips on mouse over..

Zero Coupon Bond

A simple loan. The investor pays the issuer the discounted price at the start, and is repaid the full (notional) price at the end.

Haskell

Javascript

Marlowe

Blockly

Figure 38. Zero Coupon Bond

The screenshot shows the Marlowe Play interface. At the top, there's a navigation bar with 'Play' and a project title 'Loan *'. Below the navigation is a toolbar with 'New Project', 'Open', 'Open Example', 'Rename', 'Save', and 'Save As...'. The main area contains the Marlowe code for a zero-coupon bond:

```
1 {-# LANGUAGE OverloadedStrings #-}
2 module ZeroCouponBond where
3
4 import Language.Marlowe.Extended
5
6 main :: IO ()
7 main = print . pretty $ contract
8
9 discountedPrice, notionalPrice :: Value
10 discountedPrice = ConstantParam "Amount"
11 notionalPrice = AddValue (ConstantParam "Interest") discountedPrice
12
13 investor, issuer :: Party
14 investor = Role "Lender"
15 issuer = Role "Borrower"
16
17 initialExchange, maturityExchangeTimeout :: Timeout
18 initialExchange = TimeParam "Loan deadline"
19 maturityExchangeTimeout = TimeParam "Payback deadline"
20
21 transfer :: Timeout -> Party -> Party -> Value -> Contract -> Contract
22 transfer timeout from to amount continuation =
23 | ...
```

At the bottom, there are tabs for 'Metadata', 'Generated code', 'Static Analysis', and 'Errors'.

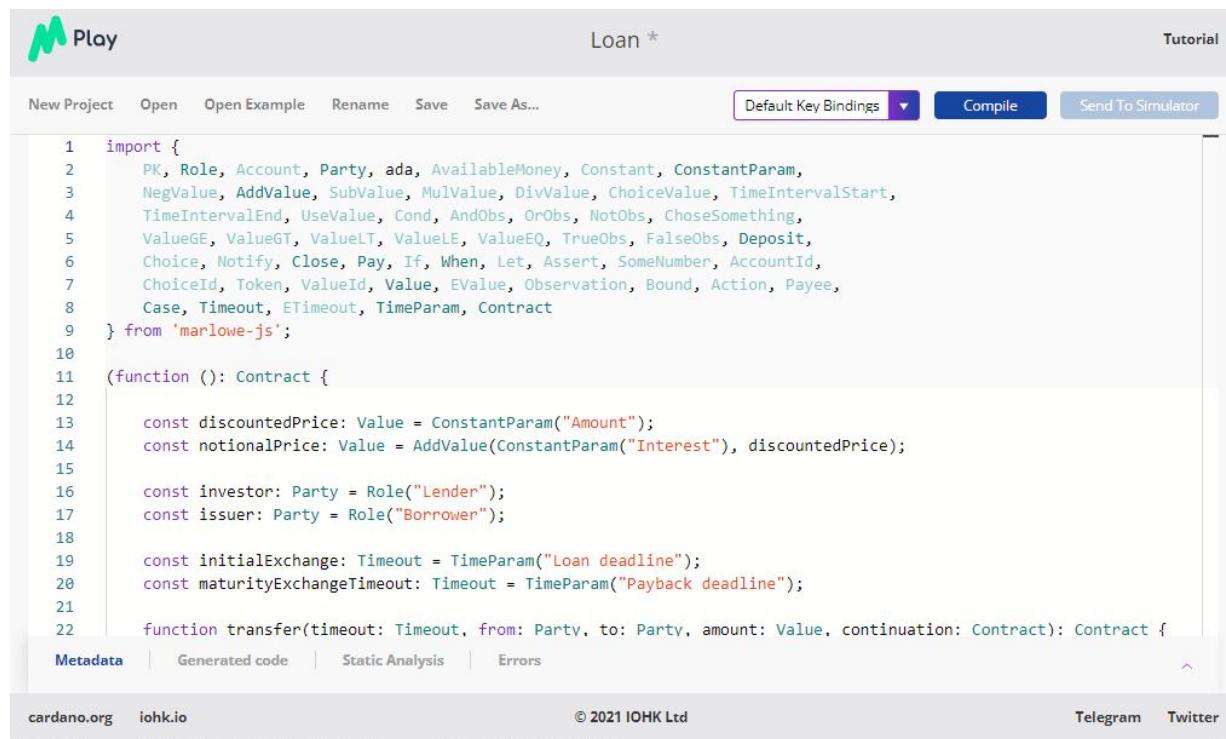
Figure 39. Marlowe JavaScript

Once you get a successful compilation, you can send the result to the simulator or to Blockly. Just click on the 'Send to Simulator' and 'Send to Blockly' buttons in the top right-hand corner.

Because Marlowe is coded as a Haskell data type, describing Marlowe smart contracts in Haskell is simple. However, because

Marlowe contracts are just data, you can express them in other languages like TypeScript (a superset of JavaScript), as outlined in the documentation. [\[702\]](#)

Marlowe code may be written using the integrated JavaScript editor. You can code JavaScript to make contract definitions more readable by using JS definitions for sub-components, abbreviations, and simple template functions. The editor is user-friendly with auto-complete, error checking during editing, and mouse over tips on bindings. The Compile option in the top right will execute the code in the editor, and the JSON object returned by the function is parsed into a real Marlowe contract; you can then hit ‘Send to simulator’ to commence contract simulation. If the compilation was successful, the generated code may be viewed by choosing ‘Generated code’ in the page’s footer; it can also be minimized.



The screenshot shows the Marlowe code editor interface. At the top, there's a navigation bar with 'Play' (highlighted in green), 'Loan *' (the current project name), and 'Tutorial'. Below the navigation bar are buttons for 'New Project', 'Open', 'Open Example', 'Rename', 'Save', 'Save As...', 'Default Key Bindings', 'Compile' (which is blue), and 'Send To Simulator'. The main area contains a code editor with the following TypeScript code:

```
1 import {
2     PK, Role, Account, Party, ada, AvailableMoney, Constant, ConstantParam,
3     NegValue, AddValue, SubValue, MulValue, DivValue, ChoiceValue, TimeIntervalStart,
4     TimeIntervalEnd, UseValue, Cond, AndObs, OrObs, NotObs, ChooseSomething,
5     ValueGE, ValueGT, ValueLT, ValueLE, ValueEQ, TrueObs, FalseObs, Deposit,
6     Choice, Notify, Close, Pay, If, When, Let, Assert, SomeNumber, AccountId,
7     ChoiceId, Token, ValueId, Value, EValue, Observation, Bound, Action, Payee,
8     Case, Timeout, ETimeout, TimeParam, Contract
9 } from 'marlowe-js';
10
11 (function (): Contract {
12
13     const discountedPrice: Value = ConstantParam("Amount");
14     const notionalPrice: Value = AddValue(ConstantParam("Interest"), discountedPrice);
15
16     const investor: Party = Role("Lender");
17     const issuer: Party = Role("Borrower");
18
19     const initialExchange: Timeout = TimeParam("Loan deadline");
20     const maturityExchangeTimeout: Timeout = TimeParam("Payback deadline");
21
22     function transfer(timeout: Timeout, from: Party, to: Party, amount: Value, continuation: Contract): Contract {

```

At the bottom of the code editor, there are tabs for 'Metadata', 'Generated code', 'Static Analysis', and 'Errors'. The footer of the page includes links to 'cardano.org' and 'iohk.io', copyright information '© 2021 IOHK Ltd', and social media links for 'Telegram' and 'Twitter'.

Figure 40. Marlowe code editor

You can expand the footer section and review the different tabs where you can examine and edit the contract Metadata and review the results of Static analysis, etc.

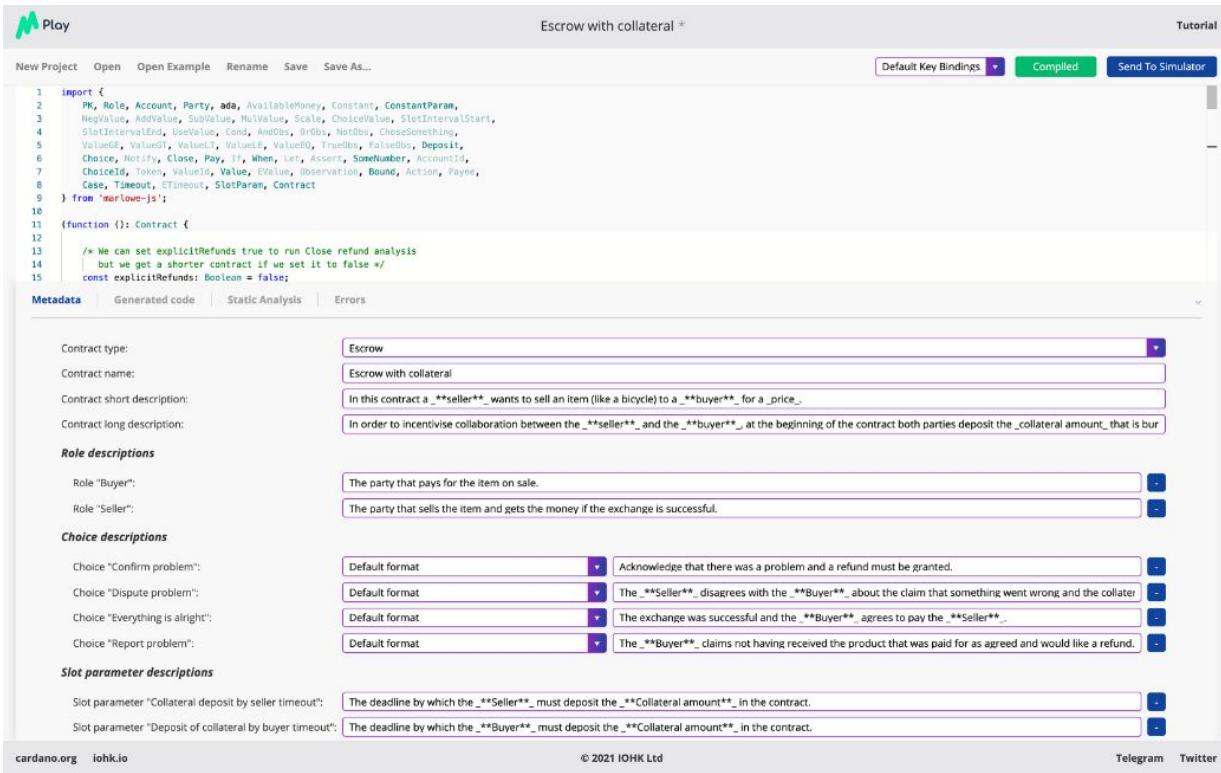


Figure 41. Marlowe Play

Marlowe Run

Marlowe Run^[703] is an end-user client for downloading and running Marlowe contracts on the Cardano blockchain. In only a few minutes, you can have your smart contracts up and running. For you to conduct financial agreements with your friends, coworkers, or customers on the blockchain, Marlowe Run offers an easy, clear, and smooth interface. It provides you with access to carefully prepared, secure smart contract templates for every sort of agreement.

Marlowe Run is a simple and quick method to utilize and run Cardano contracts. You'll uncover a variety of financial contract templates to help you choose the best smart contract for your needs. After you've chosen a template, all you have to do now is fill up the roles and conditions, and then run your contract.

UTXO and Marlowe Run

The UTXOs, which are secured cryptographically by a private key controlled by the owner, are the source of value on the blockchain. These keys can be used to redeem the output and therefore as inputs to subsequent transactions, thereby spending the value in the inputs. In a cryptographically secure wallet, users keep track of their private keys and the values associated with them.

Users will need to leverage the Marlowe Run client application to engage with a blockchain contract. Since deposits are made from users' wallets and payments are received by them, Marlowe Run interacts with the wallets to validate transactions that spend crypto-assets. Note that these are off-chain activities that must be initiated by code running off-chain, which is usually found in the Marlowe Run application: they cannot be kicked off by the contract running on-chain.

Note: The following screenshots are from a demo version of Marlowe Run which uses dummy funds and test contracts.

Marlowe Run Demo

To access and view the dashboard, follow these steps:

1. Go to Marlowe website[\[704\]](#) and click **Marlowe Run** on the main menu.
2. Click **Try demo**.
3. The Marlowe Run demo launches:

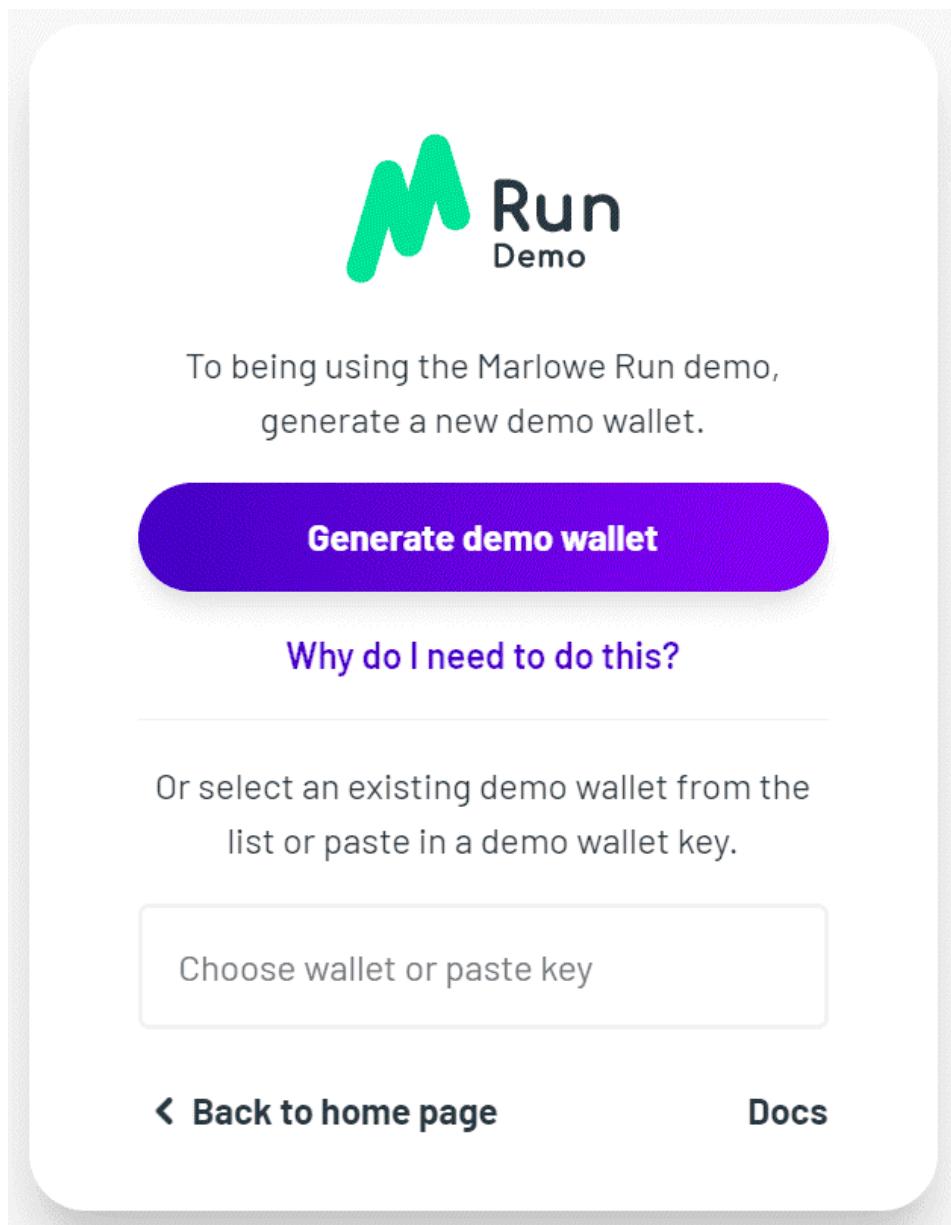


Figure 42. Marlowe Run

For this demo version, you generate a test wallet so that you can try it out. You can use any wallet on Marlowe Run using the 'demo wallet ID'. This will become the integration point with a real wallet in the full release version of Marlowe Run.

4. Click **Generate demo wallet** to use a demo wallet.
5. Enter a nickname such as 'testwallet'.

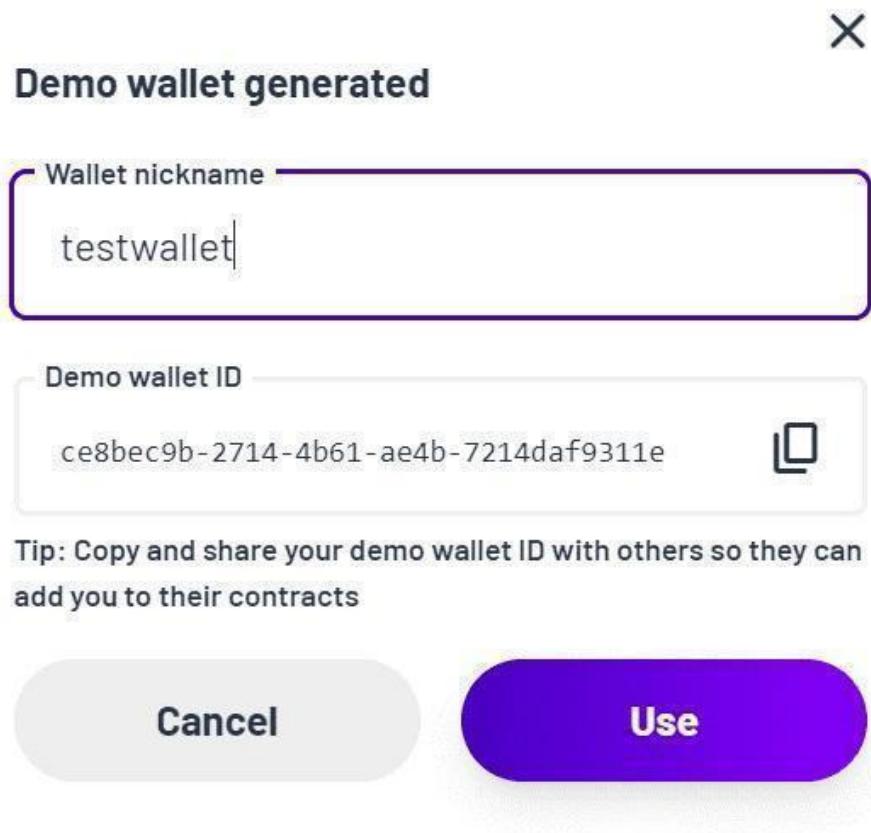


Figure 43. Marlowe demo wallet

6. Click **Use**.

After you have selected your wallet, the following screen is displayed:

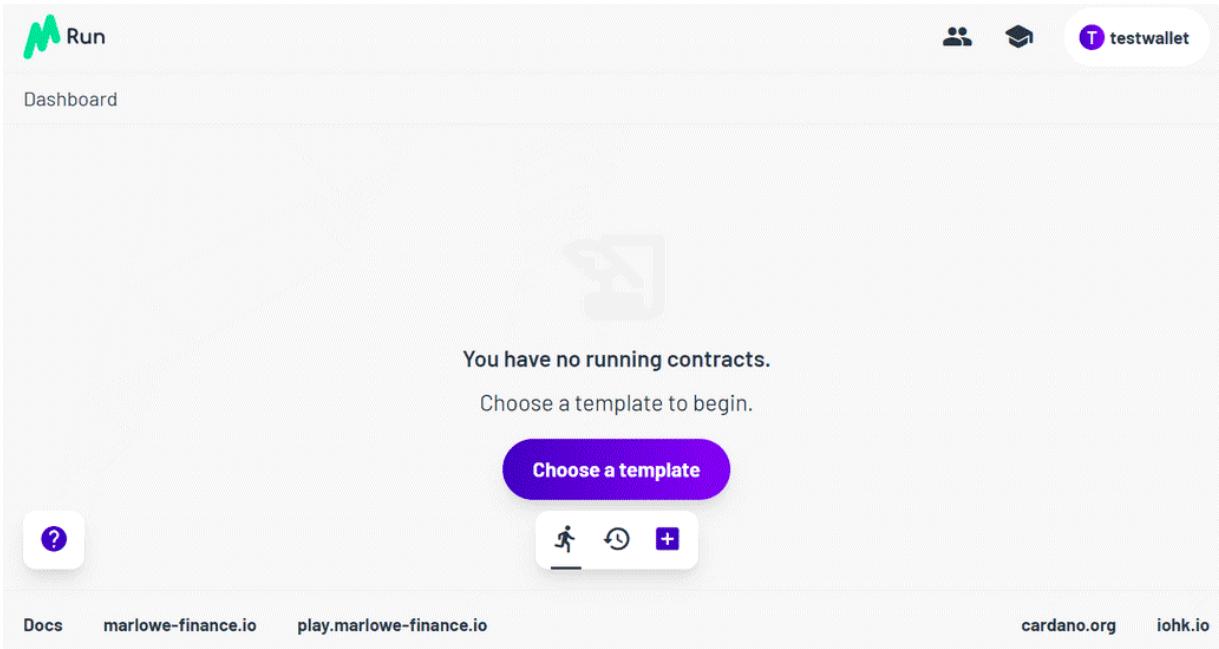


Figure 44. Marlowe template

7. Click **Choose a template** to create your contract.

The Contract templates selection card is displayed with three options:

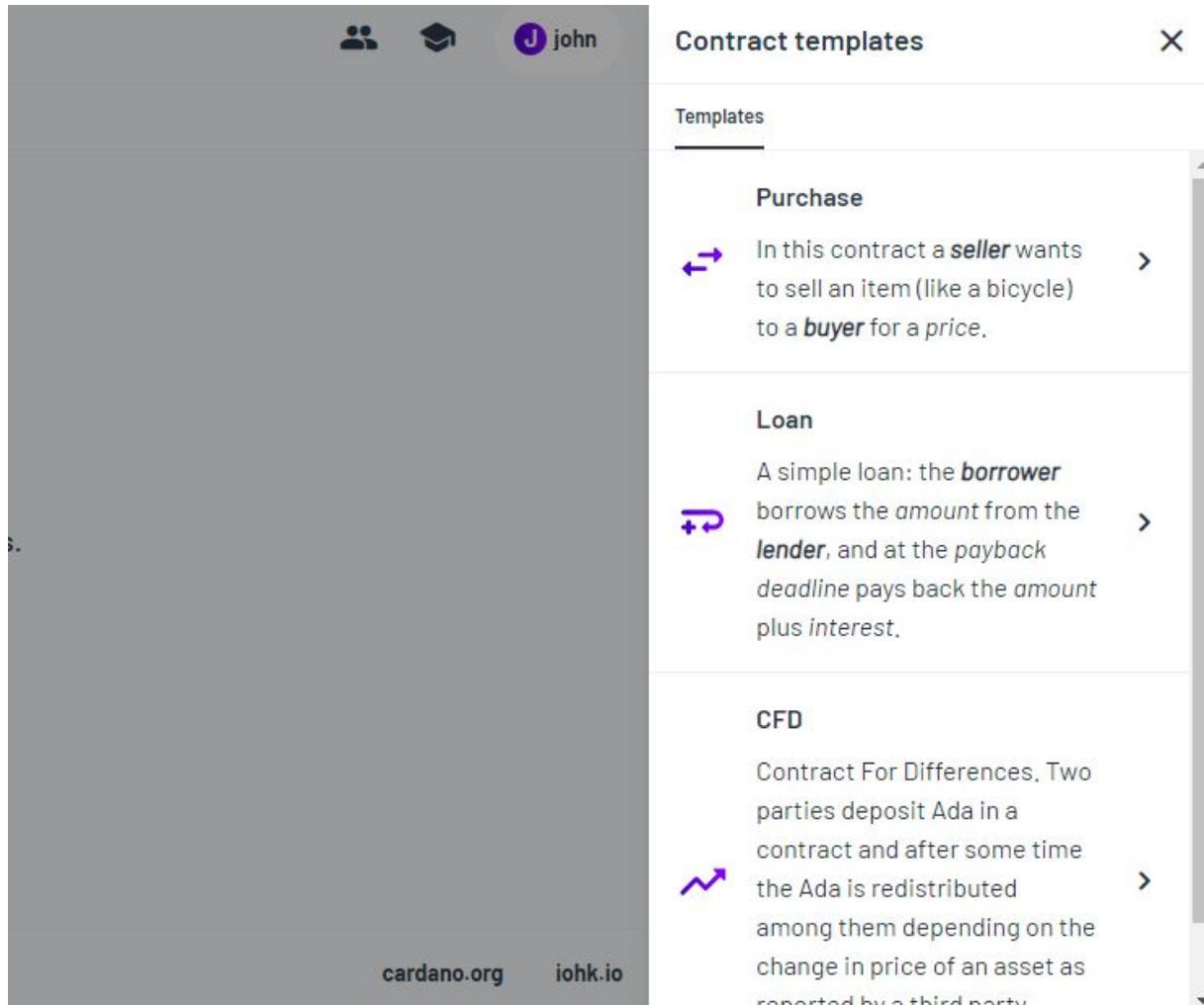


Figure 45. Marlowe contract templates

8. Click the contract template you want to use, for this example, Loan.

An dialogue wizard guides you through the self-explanatory steps, as follows:

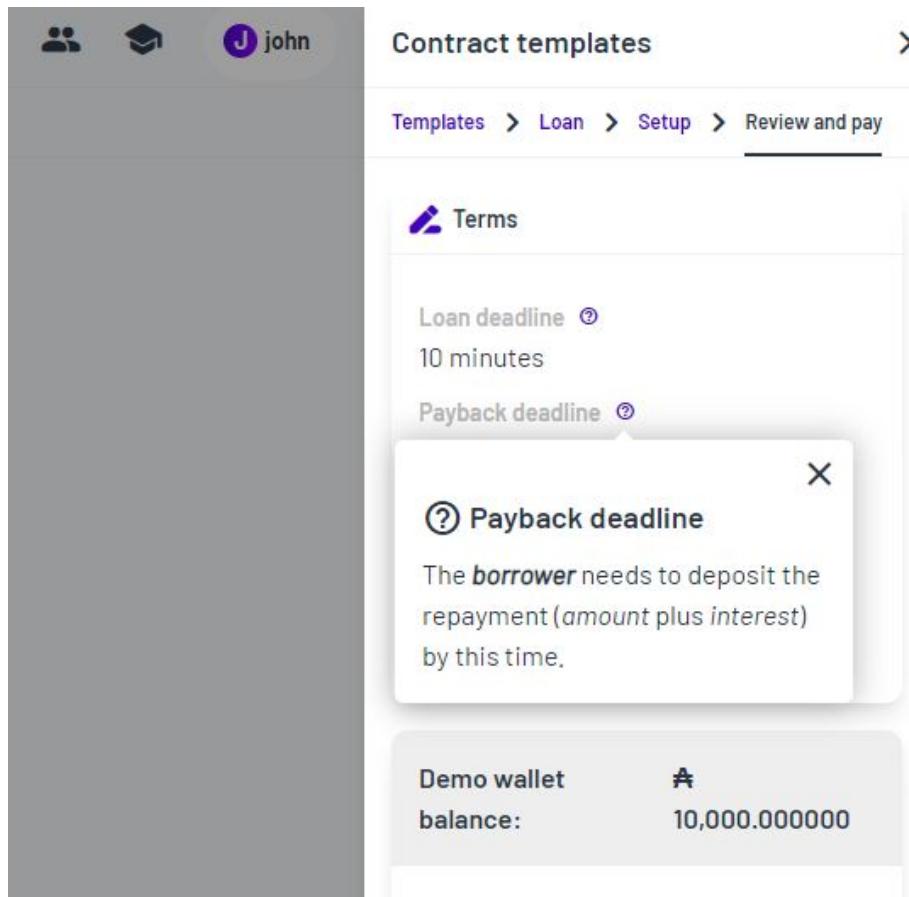


Figure 46. Marlowe UI

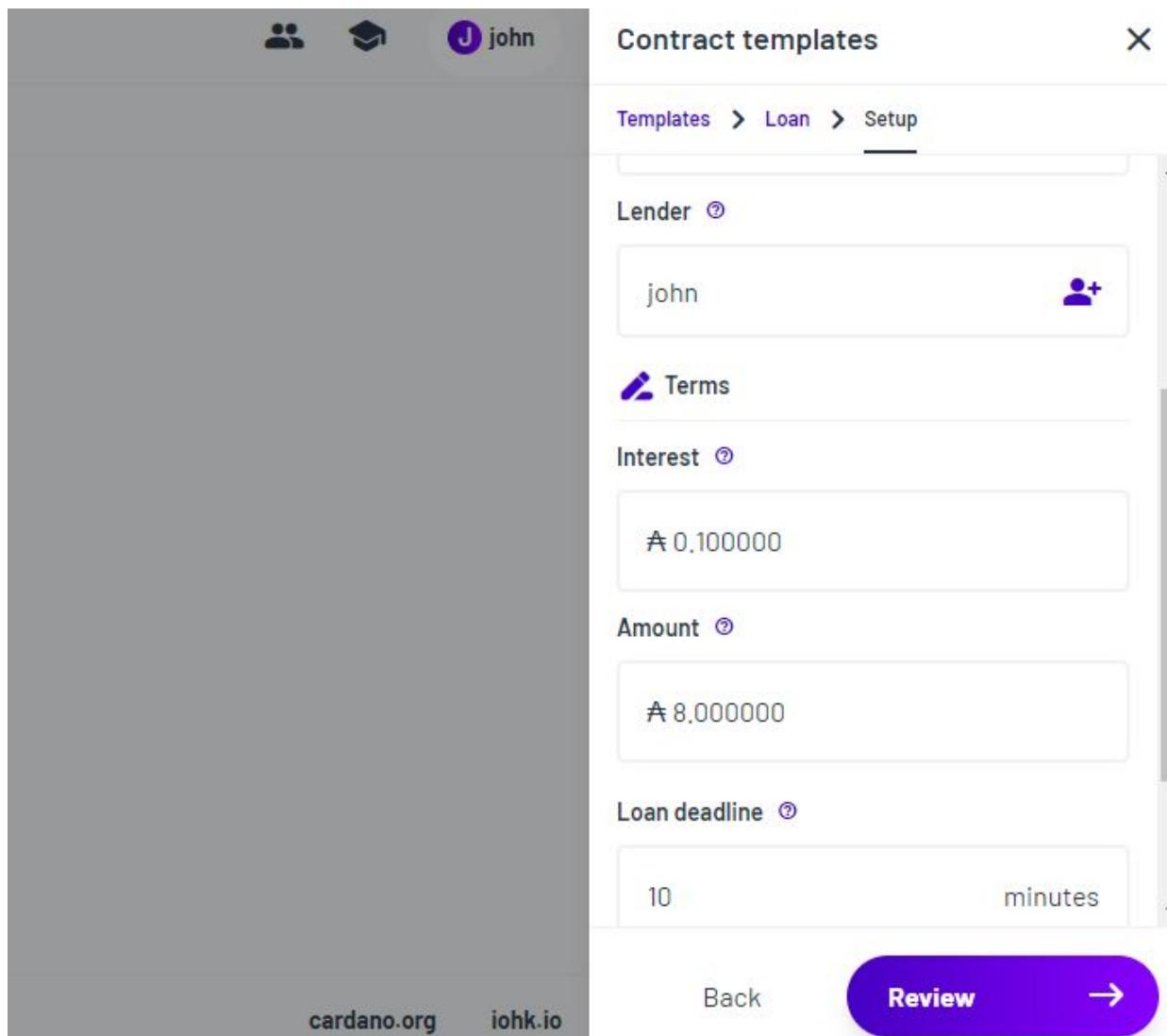


Figure 47. Marlowe Contract template dialogue box.

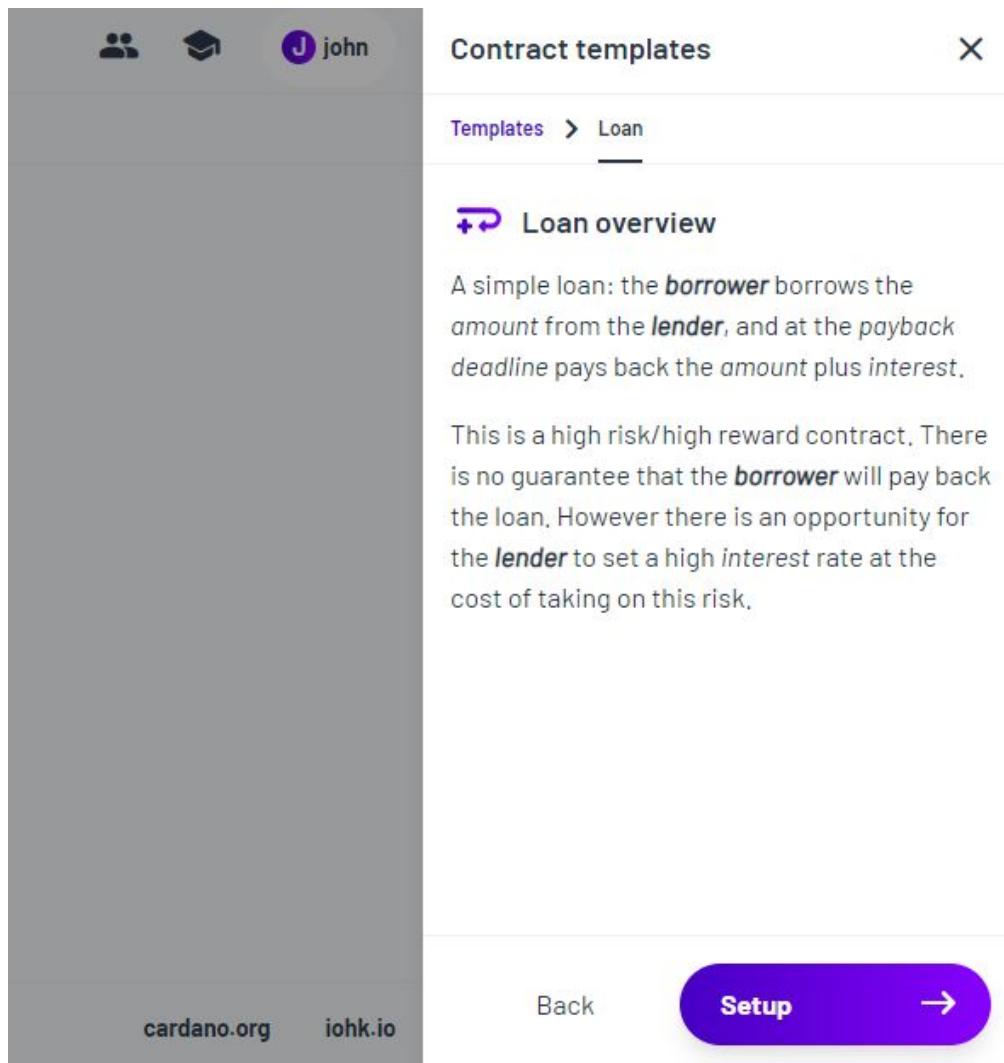


Figure 48. Contract template UI flow.

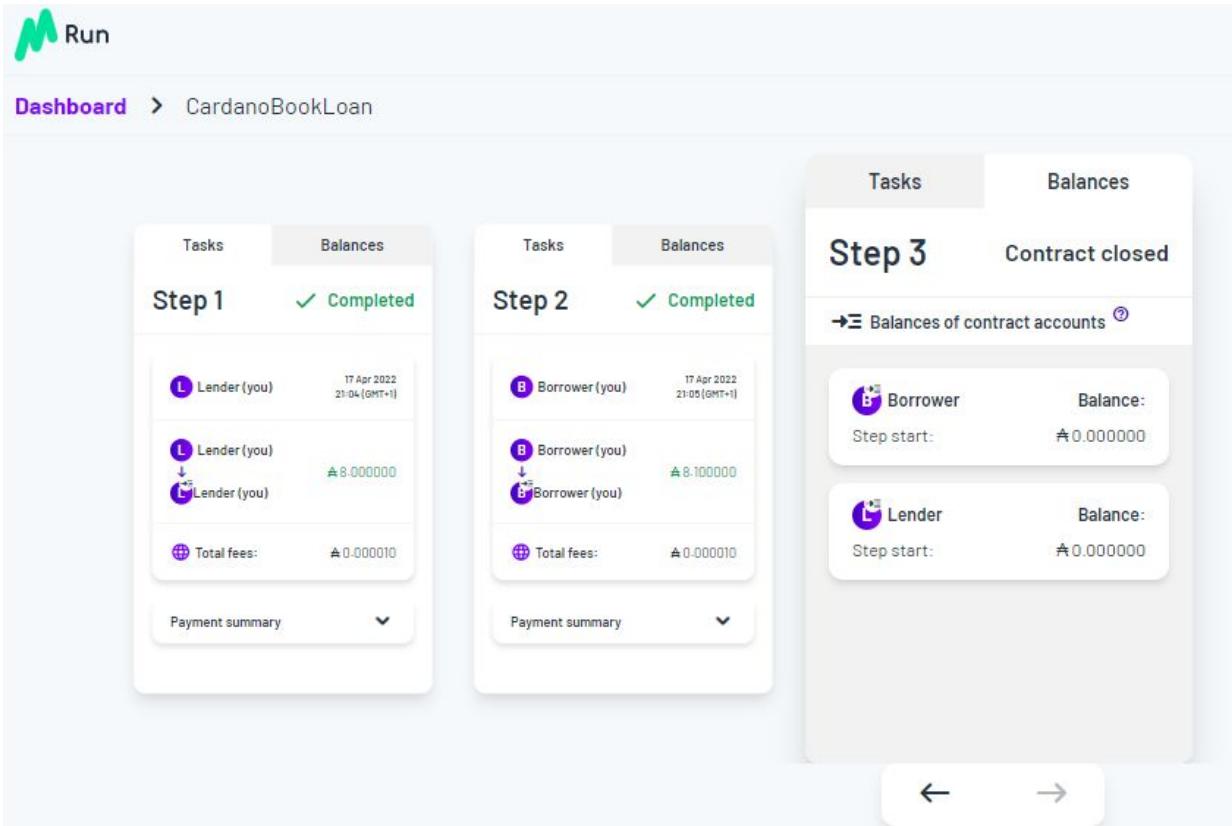


Figure 49. Marlowe CardanoBookLoan

Simulation

The Marlowe Playground supports an *omniscient* contract simulation, where the user can perform any action for any role, and thereby review the execution from the perspective of all the users simultaneously.

Marlowe Run differs in that each participant can only review the contract from their own point of view. Participants are only able to interact with a running contract which is awaiting their input. If that's not the case, then they will see that the contract execution is waiting for someone else's input.

Actus Smart Contracts

IOG is developing Marlowe, a domain-specific language for safe financial smart contracts, leveraging the Cardano blockchain's Goguen capabilities. As the world moves into the era of decentralized

finance, it's worth reviewing the nuances of the language and the many methods of building Marlowe smart contracts. The Algorithmic Contract Types Unified Standard (Actus) for financial contracts was implemented by IOG in Marlowe with their approach to oracles, which import 'real world' information into a running contract.

IOG purposefully kept the language as minimal as possible so that it would be easy to implement on Cardano and in the Marlowe Playground. Marlowe specifies the movement of cryptocurrency between participants, and to do so on the Cardano blockchain, code must be performed both on-chain and off-chain; however, just one Marlowe contract covers both sections.

The on-chain section accepts and verifies transactions that meet the smart contract's requirements: this part is built as a single Plutus script for all Marlowe contracts, with each Marlowe contract having a datum that is provided via the transactions. Off-chain, the Marlowe contract will be accessible via the user interface and wallet, allowing users to make deposits and decisions, as well as receive bitcoin payouts.

A contract's behavior can be mimicked in the Playground, allowing prospective users to walk through various contract scenarios based on different activities done by the parties. Users have an omniscient point of view in the primary simulation, and may execute activities by any participant, with the possibility to reverse the acts performed at any moment and subsequently choose an alternative course. The wallet simulation enables users to experience activity through the eyes of a single participant, modeling how that person would interact with the running contract after it has been published on the blockchain.

This simplicity also allows you to represent Marlowe contracts in an SMT solver,^[705] a logic engine that checks the characteristics of systems automatically. IOG can examine whether or not a contract will fail to fulfill a payment using this model, which they call static

analysis, and if it will, they can collect proof of how it will fail, allowing the author to alter the contract if they desire.

IOG may use a proof assistant to create a formal model of their implementation, from which they can generate machine-checked proofs of how the language works. While the SMT solver works on individual contracts, the proof assistant may prove characteristics of contract templates and the system as a whole: for example, IOG can demonstrate that the accounts referenced in any running contract can never be in debit. Simulation, static analysis, and proof are three layers of assurance for a contract to which users would commit assets to guarantee that it acts as it should.

Oracles

One of the most common questions with Marlowe is about financial oracles, or how to get a contract to account for external data values like the exchange rate between ada and bitcoin. Because an oracle is essentially the same as a participant who makes a decision, Marlowe's semantics can already deal with external values. However, as part of the implementation, the aim is to provide oracle values, which would allow contracts to obtain values directly from a stock market ticker, or a data feed like Coinbase or Binance.

Simultaneously, the Plutus team is investigating the best method to deal with oracles in general, and there will be support for it in the future.

Why Actus?

The blockchain guarantees that the contract is fulfilled, therefore Marlowe has the potential to let individuals establish financial promises and exchanges without the need for a third party to facilitate them. IOG is developing a Marlowe implementation of disintermediated contracts for end users who wish to conduct peer-to-peer financial transactions without the involvement of a third party. Financial contracts are classified by the Actus Financial Research

Foundation using a taxonomy^[706] that is outlined in a technical specification.^[707]

Financial contracts are legal agreements between two (or more) counterparties on the exchange of future cash flows, according to Actus. Such legal agreements have always been expressed in natural language, resulting in ambiguity. As a result, Actus uses a set of contractual words and deterministic functions to translate these terms to future payment obligations to construct contracts. As a result, most financial instruments may be described using 31 contract types or modular templates.

What does Actus look like in Marlowe?

Products in the Actus taxonomy, such as the principal at maturity contract, may be presented in Marlowe in a variety of ways, depending on how willing they are to accept modifications in their terms throughout the course of the contract's existence.

In the most basic scenario, all cash flows are established, or frozen, at contract start, ensuring that the contract's operation is completely predictable, given that all participants continue to participate with it throughout its existence. Actus-F contracts are such a contract (F for fixed or frozen).

Dynamism, or change in the course of a contract's development, may take two forms. Participants may make unplanned payments, which will necessitate a recalculation of the remaining cash flows, as well as modify the cash flows by factoring in external risk variables. Actus-M models the whole range of contracts that accomplish both (M for Marlowe).

Intermediate stages are also available: Actus-FS (fixed schedules) contracts have set schedules, enabling risk factors to be considered but no unexpected payments; Actus-FR contracts, on the other hand, enable payments to be made at any time but do not take into account risk factors.

Finally, Actus-H (H for Haskell) models contracts directly as Plutus or Haskell programs, with Marlowe used to validate each transaction over the contract lifespan by producing Plutus code from the Marlowe description of the contract logic.

Why are there so many distinct Actus contract models?

The reason for this is because there's a trade-off between the dynamic nature of contracts and the certainty IOG can provide customers about how they'll function before they're executed.

- Actus-F (fixed or frozen) contracts have a completely established payment schedule that can be reviewed directly by the parties, making it easy to determine, for example, that all payments from such a contract will be successful
- Contracts in the Actus-FS and -FR series have greater dynamism, yet they are readable and simple to examine. Furthermore, they are subject to static analysis to ensure that all payments, for example, will be successful
- Because Actus-M (M for Marlowe) contracts are written in Marlowe, they can be analyzed. However, due to the unpredictability of the activities that the contract will take at any given moment in time, analysis takes much longer. It's worth noting that assurance may be provided for scaled-down contracts that have the same computational content but grow over a shorter period of time, resulting in fewer interactions
- Because Actus-H (H for Haskell) contracts are written in a blend of Plutus and Marlowe, they are not as easy to static check as the others. This platform, on the other hand, provides complete extension and customization of the Actus standard implementation for corporate customers.

Users may build Actus-F (fixed or frozen) and -FS contracts from the terms of the contract using a visual presentation of the data necessary in IOG's implementation of Actus, which was accessible as a pre-release version under the Labs tab of the Playground.

Marlowe is a DSL (domain specific language) that solely defines financial contracts, not smart contracts in general. It varies from general-purpose blockchain languages like Solidity and Bitcoin Script^[708] because of this.

Marlowe is a large-scale project. IOG created Marlowe contracts using examples from the Algorithmic Contract Types Unified Standards (Actus) framework, which is one of the most popular projects for financial smart contracts. These and more examples are available in the Marlowe Playground.

Marlowe for P2P Finance

If you ever tried to sell your Bitcoin or ada and withdraw funds from Binance in a hurry, you could very well be blocked from doing so. Binance often suspends withdrawals due to a backlog^[709] or you may be forced to withdraw via an expensive option instead of a relatively cheap bank transfer.^[710] Are centralized exchange fees^[711] any less extortionate than legacy banking fees? Most people would have thought that in the crypto space, they would always be able to access their assets, make trades and withdraw without third parties blocking you or charging hefty ‘processing fees’.

Is it ever true that you can have complete control over our finances? Most people have no choice but to entrust the management of their money to a third party, leaving it up to them to determine if and when those monies may be accessed, utilized, or even seen. The primary point of control is something that all of these third-party banks and brokers have in common. An external self-interested actor may influence, attack, or manipulate the primary point of control, making it the opposite of democratized finance.

 Adrian Weckler ✅
@adrianweckler

Bank Of Ireland, 2022

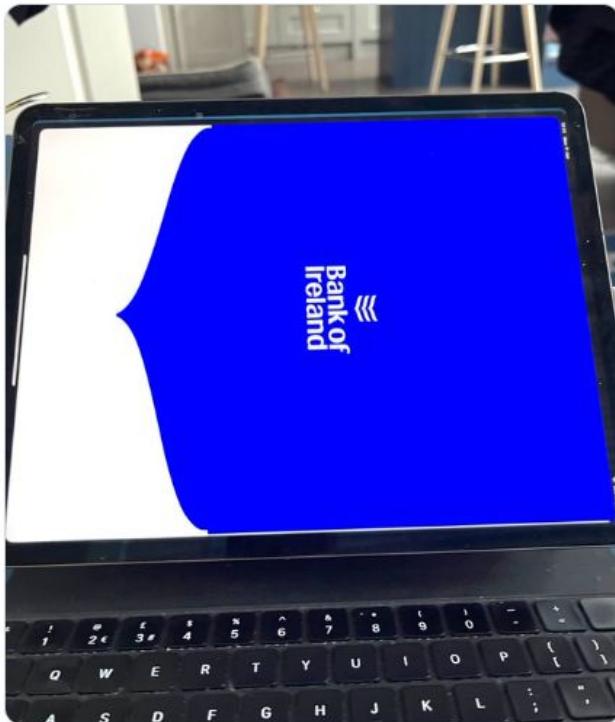


Figure 50. Online Banking in 2022

This is the driving force behind decentralized finance, often known as DeFi. Lending, escrows, derivatives, swaps, and securities are among the financial instruments provided by DeFi, which are comparable to those supplied by Wall Street. DeFi platforms distinguish themselves by being able to provide various financial products without the need of central market makers, banks, or brokers. Each financial arrangement is recorded on the blockchain as a smart contract that is settled algorithmically. Because of their decentralized character, they are significantly more resistant to market manipulation and centralized system failure.

IOG is working on a set of Marlowe products to help democratize money and make financial agreements more accessible. This includes Marlowe Run, a tool that will allow users to securely and independently execute off-the-shelf financial agreements with friends or businesses. This peer-to-peer system will be cost-effective and,

more significantly, democratizing, with increased automation capabilities and no need for third-parties.

Marlowe suite

IOG wants to democratize finance with Marlowe by allowing peer-to-peer agreements to operate on a blockchain. They aim to provide individuals the ability to build their own financial instruments and make agreements with whomever they choose to deal with. Marlowe will provide a number of distinct products, each of which will cater to a particular set of consumers and functions. Marlowe's product strategy is divided into three categories: Marlowe for developers, Marlowe for end users, and Marlowe for enterprise.

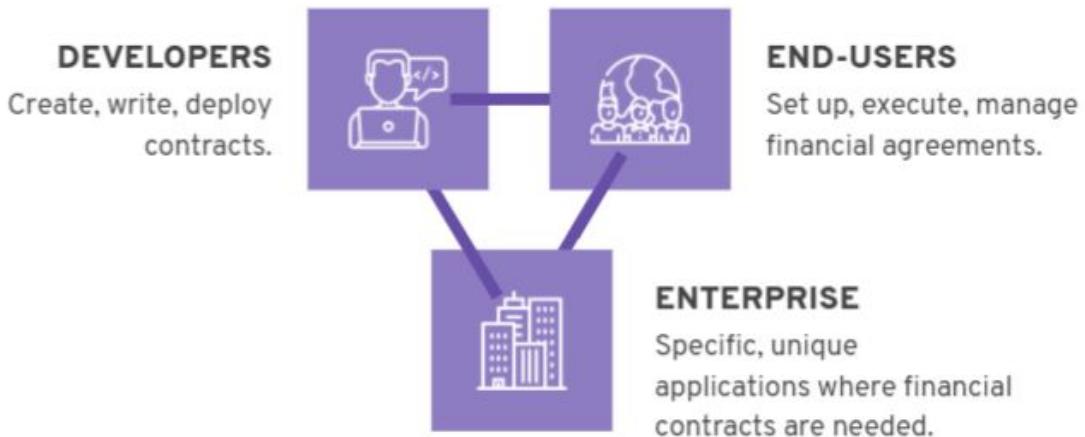


Figure 51. Marlowe user groups

Developers

Developers may use Marlowe Build and Marlowe Play (also known as the Marlowe Playground), and also the input to the Marlowe Library. The combination of Marlowe Build and Marlowe Play allows for end-to-end financial smart contract creation.

Marlowe Build allows developers to write smart contract code. They may then use simulations to undertake basic iterative design and formally verify and test smart contracts on Marlowe Play. These characteristics, when combined with a finance-specific domain-specific language (DSL), guarantee that contracts are simple to

create, as well as secure, verifiable, and well tested. Developers may donate their smart contract templates to the Marlowe Library, an open-source smart contract template library, after they've been developed and tested.

End users

Marlowe for end users will provide a simple, intuitive, and seamless interface for users to sign financial agreements on the blockchain with their friends, colleagues, or customers. This contains Marlowe Run and offers you access to the Marlowe Library's financial instrument templates. These products were designed with the user in mind by IOG. The user does not need to be a blockchain expert or know how to develop smart contracts to form financial agreements on the Marlowe Run.

Every step of the contract is explained in layman's terms, and each action is carried out only with the user's express permission. IOG has designed a set of carefully tested and confirmed financial mechanisms like escrows, debt securities, and swaps that may be utilized on the Marlowe Run. The Marlowe Library makes these, and many more validated open-source contracts, accessible.

Enterprise

Marlowe for Enterprise seeks to take DeFi beyond individual users, allowing businesses to reap the advantages of smart contracts in a practical way. This will feature a customized, configurable set of capabilities and financial agreements geared to a specific business use case, as well as smart contract templates based on the Algorithmic Contract Types Unified Standards (Actus) for financial contracts.

Marlowe on Cardano

IOG released the Marlowe Playground Alpha^[712] in 2020. This allowed contracts to be written in JavaScript in addition to Haskell or directly

in Marlowe. Proof-of-concept oracles were also added, with the ability to retrieve external data such as price straight from a stock market ‘ticker’ or, in the future, data feeds like Kraken.^[713] IOG created guides to help developers with the rollout, then expanded on this effort by improving the user experience and developing, testing, and verifying a growing bank of smart contract templates.

IOG is finishing the implementation of Marlowe on Cardano as part of the Goguen era deployment, allowing individuals and organizations to execute DeFi contracts that they have authored themselves or obtained from a contract repository. Marlowe will initially operate on the Cardano blockchain, but it is blockchain agnostic and might run on other blockchains in the future to reach a wider audience.

Marlowe will be made available to end users in phases. The first was the Marlowe Run prototype, which allows users to showcase and test their own financial agreements. Users could modify a set of financial smart contract templates to meet their specific requirements. This prototype enabled users to experiment with forming decentralized financial agreements in a peer-to-peer setting without the need for a value-extracting third party. Users didn’t need actual tokens to use the Marlowe Run prototype, so they could check it out before committing.

IOG’s developers created a set of template financial instruments for this deployment. On Marlowe Run, these templates can be used to run test agreements. IOG shared several demos of Marlowe Run such as this one^[714] on their ‘IOHK’ YouTube channel. Check out marlowe-finance.io/ for details on webinars, events, etc.

Marlowe Playground evolves

You can make your own templates out of Marlowe contracts and utilize unique metadata to provide users suggestions. The sandbox setting of the Marlowe Playground is where you may experiment drafting financial contracts. This playground lets you work directly in a variety of languages, including Marlowe, JavaScript, Haskell,^[715] or Blockly, depending on your preferences. New tools for creating and

modifying templates and customizing information, as well as a new JSON download option for the contracts themselves, were introduced to the Marlowe Playground.

Template support

With the release of Marlowe Run, IOG expanded the Marlowe Playground to include template support. An enhanced version of Marlowe (aka Extended Marlowe, available in the Marlowe Playground) is used to create these templates. Users will be able to easily reuse and repurpose contracts using these new templates for a variety of scenarios and contexts.

Extended Marlowe is more versatile than ordinary Marlowe (or Core Marlowe). Contracts are quite specific, and timeouts are specified in absolute values, first through slot numbers, and subsequently using standardized POSIX^[716] timestamps.

Marlowe Values are usually hardcoded in Marlowe, with the exception of those supplied as Inputs. For example, you may use a **Choice in a When** construct to create a loan for ⠈ 100 or one that asks the user how much to lend, but before you couldn't have a reusable Marlowe contract that could be deployed at any moment and with any provided parameters. The ability to incorporate contract parameters in Extended Marlowe resolves these constraints. Currently, extended Marlowe is almost the same to plain Marlowe, with the exception of two additional constructors that represent template parameters:

- **SlotParam** — In a When construct, it may be used instead of a timeout.
- **ConstantParam** — a type of **Value** construct
- Both constructors accept a single parameter, which is a string that acts as a parameter identifier, such as:
- **SlotParam “Payment deadline”**
- **ConstantParam “Price”**

Even if they exist in separate locations, two parameters of the same

type (**SlotParam** or **ConstantParam**) and with the same identifier are considered the same parameter. If a contract has parameters (if it is a template), the user will be prompted to provide values for those parameters before beginning a simulation or deploying the contract in Marlowe Run.

It's worth noting that the value template parameter input field isn't merely an integer field. Rather, it expects a decimal number with a currency sign on the label to indicate that the predicted value reflects an amount of ada. Also, quantities of ada do not have to be represented by choices, they may be used to indicate anything, such as a ratio. Each parameter has its own set of clues, which may be accessed by clicking the purple question mark beside each box. The suggestions text ('tool tip') is unique to the contract template.

The screenshot shows a code editor with Marlowe code and a static analysis tool. The code is:

```

1  {-# LANGUAGE OverloadedStrings #-}
2  module ZeroCouponBond where
3
4  import Language.Marlowe.Extended
5
6  main :: IO ()
7  main = print . pretty $ contract
8
9  discountedPrice :> optionalPrice :> Value

```

The static analysis tab is selected. A tooltip is open over the 'Payback deadline' parameter, which is highlighted in blue. The tooltip text is:

② Payback deadline
The **borrower** needs to deposit the repayment (*amount* plus *interest*) by this time.

Figure 52. Marlowe static analysis

Metadata customization

Metadata may be used to alter elements in user-defined contracts. Each of the editors in the Marlowe Playground has a Metadata tab at the bottom. Users may change the metadata to suit their needs. Every contract is required to provide some fundamental metadata, such as contract type, contract name and descriptions. The metadata tab also allows you to format the choices and value parameters.

In the Metadata tab, each new role, choice, slot, or value parameter added to a contract will be highlighted in red. It may be required to compile the code successfully first in the case of the Haskell and JavaScript editors.

By pressing the red '+' button, a new metadata entry for the selected object will be created. Similarly, if a role, choice, slot, or value parameter is no longer used in the contract, the existing metadata will be highlighted in red and the user must remove the metadata item from the contract by using the '-' button.

Ordering of metadata

The sequence in which the parameters are set is critical. The end user can choose from a number of slot parameters so it would make sense to present those parameters in order of their occurrence. The user can now drag items into the appropriate order to organize metadata, for example:

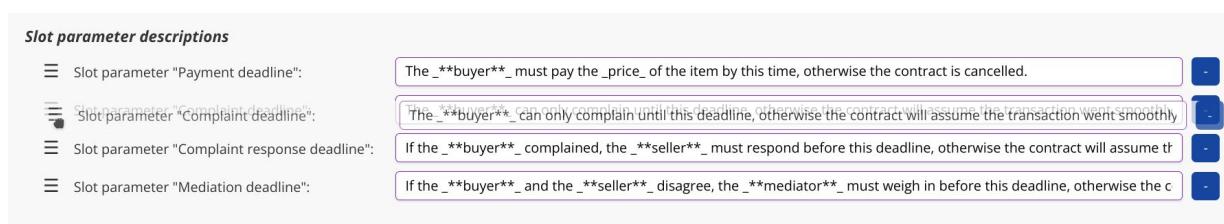


Figure 53. Marlowe drag and drop

The order of the parameters in the metadata will be utilized to generate the form that will be shown at the start of the simulation or

contract execution.

In April 2022, IOG introduced the Marlowe CLI (command line interface) tool.^[717] For users who wish to manage contracts from the command line, this new tool provides a simple approach. It allows you to concentrate on the Marlowe contract while the tool handles the specifics of the contract's input and state. It also automates several parts of Plutus, as well as interactions with the Cardano node itself, to relieve users of some of the heavy lifting.

This new CLI tool will be beneficial for teaching users how to get up to speed with Marlowe. It will be used heavily in the inaugural Marlowe Pioneer Program

Marlowe FAQs

Q: What is Marlowe?

A: Marlowe is a language created by IOG for authoring and executing blockchain-based financial contracts. It's a financial-industry-specific domain-specific language (DSL). To learn more, read IOG's Marlowe explainer^[718] and try out the Marlowe tutorials.^[719]

Q: Where can I learn more about Marlowe?

A: This chapter was just an overview of Marlowe. To learn more, subscribe to Prof Simon Thompson's YouTube channel^[720] and review his videos. The first cohort of Marlowe Pioneers Graduated in July 2022, all the lectures are available on the 'IOGAcademy' YouTube channel.^[721] Read the recently updated docs^[722] and register to be in the next cohort of the Marlowe Pioneer Program.^[723]

Q: Are there any new additional smart contracts on Marlowe Run?

A: You have the option of utilizing Marlowe Build to create your own contract. IOG are generating new contract templates for users to test, which will be uploaded to the contract catalogue soon.

Q: Can I edit a contract after it's created?

A: You may make modifications to your contract before it starts

operating. You may simply modify the Roles and Terms fields. All conditions are established once it begins to run, exactly as they are with a typical legal contract.

Q: Are you using real funds with Marlowe Run?

A: No, when you utilize Marlowe Run, you are running and executing your contracts using test funds.

Q: Is there a hard limit to the number of contracts I can run in parallel?

A: IOG are not putting any hard user-specific limitations on the prototype but may do so in Marlowe Run. Keep in mind that IOG servers have a limit on the number of contracts and transactions they can process at any one moment, although this is not user-specific at this time.

Q: Can I create a contract with a user from a different blockchain, ie. not Cardano?

A: Because all financial agreements initially were established between Cardano wallet addresses, all agreements should be made with someone who possesses a Cardano wallet. IOG may allow agreements on other chains in future editions, since Marlowe is fundamentally blockchain-agnostic.

Q: Can I create new smart contracts on Marlowe Run?

A: You may create financial agreements right now utilizing a variety of templates from Marlowe Market, a smart contract template library. You may even create your own financial contracts on the Marlowe Playground if you wish to. After that, you can submit them to Marlowe Market and run them via Marlowe Run.

Q: Where does Marlowe Run begin and Marlowe Playground end?

A: Marlowe Run is a product aimed towards a bigger audience of non-developer end users. The Marlowe Playground is designed for technical developers, and contracts may be created there and then utilized on Marlowe Run.

Q: Where can I get help with Marlowe Run?

A: If you have any problems, use the ‘Submit Feedback’ email form on the Marlowe website’s Feedback page, Sign up for the Marlowe Pioneer Program to collaborate with IOG and help IOG stress test Marlowe even further.

Q: What are Marlowe’s use cases?

A: Marlowe contracts may be leveraged in a variety of ways, such as automating the functioning of a financial contract that transacts cryptocurrency on a blockchain using Marlowe software. It might also be used for auditing reasons to track user compliance with a contract that is being implemented in the real world.

Marlowe is simply one example of a DSL operating on a blockchain. It serves as an example of how new DSLs may be constructed to cover supply-chain management, law, insurance, accounting, and other areas.

Q: When should I not use Marlowe?

A: Although IOG emphasized that Marlowe is a financial DSL, what if you need to build other types of contracts? Cardano uses Plutus, a blockchain-based general-purpose language, to create them. Plutus contracts can manage a wide range of crypto assets and lack the limitations of Marlowe contracts, such as the length of time they can be active and the number of individuals they may include. Every Marlowe contract is managed by the Marlowe interpreter, a single Plutus application.

Q: This all sounds too easy, is it really just a matter of dragging and dropping blocks around?

A: No, you should study the content and become a Marlowe Pioneer before developing DApps that use other peoples’ funds. Start by reviewing the best practices, ‘bad smells’ and ‘Potential problems with contracts’ in the docs.[\[724\]](#)

Chapter 8: Voltaire

*'I may disagree with what you have to say, but I
shall defend,
to the death, your right to say it'* [\[725\]](#)

Money is social

With a few noteworthy exceptions most cryptocurrencies have made no provision for future upgrades. The capacity to effectively drive a soft or hard fork is critical to a cryptocurrency's long-term viability. As a result, financiers are unlikely to invest millions of dollars on protocols whose roadmap and participants are fleeting, petty, or extremist. There must be an efficient procedure for forming agreement on a vision for the underlying protocol's evolution. Fragmentation might split the group apart if this process is difficult.

Cryptocurrencies are an excellent illustration of money's social component. When comparing Bitcoin and Litecoin merely on the basis of technology, there is little difference between the two, and even less between Ethereum and Ethereum Classic. Despite this, both Litecoin and Ethereum Classic have huge market capitalizations, active communities, and their own social agendas.

It might be claimed that a significant portion of a cryptocurrency's worth is generated from its community, how it utilizes the funds, and how involved it is in the currency's progress. Adding to the idea, other currencies, such as Dash^[726] or Tezos,^[727] have built methods directly into the protocol to allow its users to vote on what should be prioritized for development and funding.

The huge variety of cryptocurrencies also demonstrates their social aspects. Fragmentation and forks result from disagreements over philosophy, monetary policy, or even petty squabbling amongst the core developers. Unlike their digital cousins, however, fiat currencies tend to weather political upheavals and local disputes without a currency crisis.

As a result, it seems that certain aspects of legacy systems are absent from the crypto sector. IOG (Input Output Global) believes that protocol users need incentives to understand the social contract that underpins their system and the opportunity to suggest

modifications in a constructive manner. This independence applies to every facet of a value exchange system, from market regulation to project funding. However, it cannot be mediated by centralized actors, nor does it need any particular credential that may be co-opted by a wealthy few.

Funding invariably dries up, regardless of the success of a crowdsale^[728] to bootstrap development. As a result, Cardano contains a decentralized trust that reduces inflation and transaction fees over time.

Through a ballot mechanism, any user should be able to seek funds from the trust, and stakeholders should vote on who becomes a beneficiary. By creating a discussion about who should and should not be financed, the process produces a positive feedback loop similar to that found in other cryptocurrencies with treasury/trust systems, such as Dash.

The relationship between long- and short-term objectives, the cryptocurrency's social contract, priorities, and the belief in value creation with specific ideas is forced during funding conversations. This dialogue ensures that the community is always assessing and arguing its views in light of potential roadmaps.

Cardano will have a formal, blockchain-based method for proposing and voting on both soft and hard forks in the future. Long running and, in many instances, unresolved disagreements about the technical and moral direction of the codebase have plagued Bitcoin with its block size debate, Ethereum with the DAO split, and a slew of other cryptocurrencies. Many of these conflicts, as well as the splitting of the community that occurs when action is taken, can be attributed to a lack of established methods for discussing change.

Looking to lessons from the past, Bitcoin's adoption of (SegWit) Segregated Witness^[729] could have been handled a lot better.^[730] Did the DAO attack^[731] really have to result in the hard fork on Ethereum?

Could it have been managed better so there was not such a dramatic community breakdown?^[732]

In the worst-case scenario, moral authority to act might simply devolve to whomever has the developers, infrastructure links, and money, rather than the majority of the community's best interests. It's difficult to gauge if actions are valid if a major segment of the community is unavailable, or disengaged owing to poor incentives.

^[733]

Some cryptocurrencies like Tezos have a model where the cryptocurrency protocol is handled as a constitution, with three parts (Transaction, Consensus, and Network) and a set of explicit rules and procedures for updating the constitution. However, there is still a lot of work to be done on incentives and how to represent and update a crypto protocol using a formal language.

Formal methods, machine comprehensible specifications, and combining a treasury with this process for financial incentives are just some of the solutions IOG pursued. Even if more elegant solutions cannot be created, the ability to propose a protocol change in a transparent, censorship-free manner via blockchain-based voting is pivotal to Cardano's long-term viability.

Cardano Improvement Proposals (CIPs)

Anyone who has ideas for Cardano improvements may present their ideas in the form of CIPs (Cardano improvement proposals). CIPs are a means of formally proposing enhancements in a consensus-based manner. They are an essential component of Cardano governance, even though they are not binding nor a requirement for treasury or protocol modifications. Before a vote can be taken, someone must submit a proposal for others to consider.

A CIP follows a standard format: the proposal structure is templated to make debate and evaluation easier. This allows other members of

the community to weigh in on particular improvement recommendations, or issues in a proposal. CIPs are kept as text files in a versioned Github repo, [\[734\]](#) and their revision history provides the proposal's historical record. For those who aren't on GitHub, cips.cardano.org is being developed as an auto-generated sister site.

There are three different types of CIP:

1. A **Standards Track CIP** is a modification that impacts Cardano implementations. Examples: a network protocol update, or basically any other change that affects the compatibility of Cardano applications. CIPs on the Standards Track have two parts: a design doc and a reference implementation.
2. A **Process CIP** outlines a Cardano-related process or suggests a modification to one. Process CIPs are similar to Standards Track CIPs, however they are used for topics other than the Cardano protocol. They usually need community approval; thus, unlike Informational CIPs, they are more than suggestions that users are not free to disregard.
3. An **Informational CIP** discusses a Cardano design issue or gives broad Cardano community standards or information, but it does not propose anything new. Users and implementers are entitled to disregard Informational CIPs, or follow their advice because they do not necessarily reflect a Cardano community consensus or suggestion.

Every CIP has the following format: Preamble, Abstract, Motivation, Specification, Rationale, Backwards compatibility, Path to Archive, Copyright.

The concept is developed as a properly written proposal and submitted as a pull request[\[735\]](#) to the CIP repository after initial discussion and feedback. The updated Draft CIP is then publicly processed in the following manner:

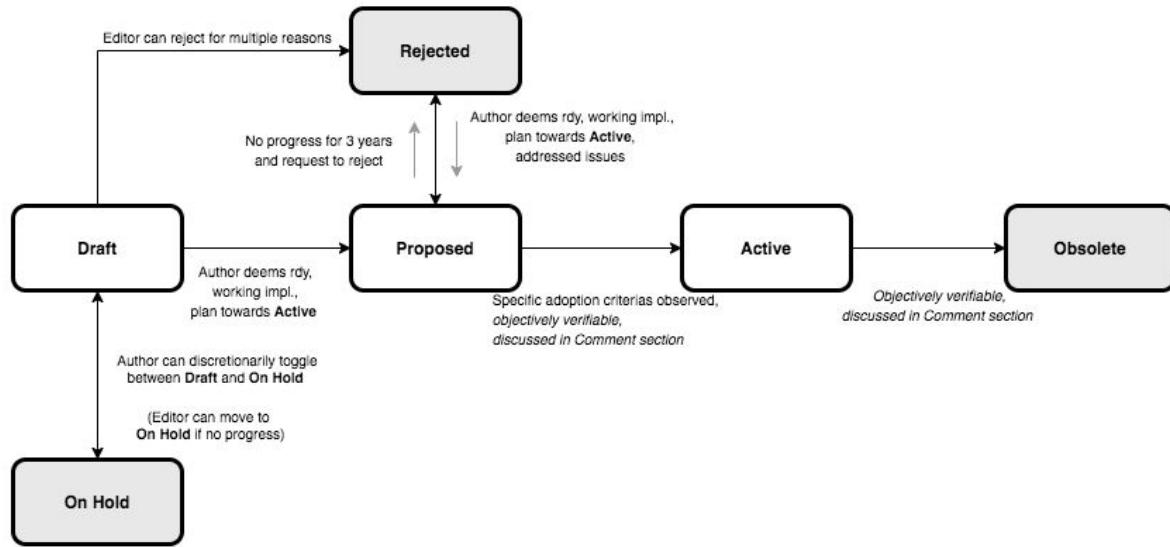


Figure 54. CIP process diagram from Cardano Developer Portal

CIPs are processed in a semi-formal manner: Editors of CIP proposals (IOG / Cardano Foundation / Emurgo / Community) meet on a regular basis to discuss and assess ideas. Meeting minutes are available to the public,^[736] and meetings are held every two weeks. Authors are encouraged to contribute and offer comments, and discussions often take place simultaneously in the Cardano forum CIPs section^[737] and/or in the GitHub pull requests.

Consider the CIP repository to be a collection of useful tools - some may play well together, while others will not. You have complete control over which CIPs your implementation adheres to. The community will lean toward some more than others, new ones should be submitted as Cardano grows.

Notable CIPs:

- CIP 1 - CIP process

'A Cardano improvement proposal (CIP) is a formalized design document for the Cardano community, providing information or describing a new feature for the Cardano network, its

processes, or environment in a concise and technically efficient manner.;

- CIP 9 - Protocol Parameters

'This CIP is an informational CIP that describes the initial protocol parameter settings for the Shelley era of the Cardano blockchain, plus the changes that have been made. It is intended to serve as a historic record, allowing protocol parameter changes to be tracked back to the original settings.'

- CIP 25 - NFT Metadata Standard

This proposal defines an NFT Metadata Standard for Native Tokens.

- CIP 27 - CNFT Community Royalties Standard

A community standard for royalties' functionality, that does not require smart contracts to implement.

- CIP 31 - Reference Inputs

'We introduce a new kind of input, a reference input, which allows looking at an output without spending it. This will facilitate access to information stored on the blockchain without the churn associated with spending and recreating UTXOs.'

- CIP 32 - Inline datums

'We propose to allow datums themselves to be attached to outputs instead of datum hashes. This will allow much simpler communication of datum values between users.'

- CIP 33 - Reference scripts

'We propose to allow scripts ("reference scripts") to be attached to outputs, and to allow reference scripts to be used to satisfy script requirements during validation, rather than requiring the spending transaction to do so. This will allow transactions using common scripts to be much smaller.'

- CIP 50 - Liesenfelt Shelleys Voltaire Decentralization Update
(Under review)

'Improving decentralization is absolutely necessary for the long-term health and growth of the Cardano ecosystem. The current reward formula has resulted in a stable but stagnant level of decentralization. With the benefit of hindsight over the last year the intent of (a_0, k) has not resulted in the desired decentralization outcome. This CIP provides the justification, methods, metrics, and implementation schedule for an improvement program to increase decentralization of the Cardano network.'

Ambassadors program

The Cardano community is not short of committed members who are willing to be part of the Cardano Foundation's Ambassadors Program, [\[738\]](#) established in 2018.

The program's goals are to:

- Boost adoption of Cardano
- Drive awareness
- Educate the community

To apply to become an ambassador, send the Cardano Foundation an email: community@cardanofoundation.org

What is Project Catalyst?

Project Catalyst is a prototype treasury system that combines proposal and voting processes. Establishing a long-term future for Cardano growth began with a treasury and democratic voting in the Catalyst project. It is hosted on IdeaScale^[739] for now as the Voltaire era unfolds.

When creating a proof-of-stake blockchain, it's critical to make sure the system is self-sustaining. It will be able to generate development and maturity in a genuinely decentralized and organic manner as a result of this. Voltaire^[740] is IOG's approach to create this capacity, enabling the Cardano community to maintain the blockchain while also suggesting and implementing system enhancements. This places decision-making authority in the hands of ada holders.



Figure 55: The opening screen for each Catalyst Town Hall meeting, (crowdcast.io/ohk)

The foundation of a robust blockchain is a non-trivial, broad area of study and debate. A talk^[741] on the necessity of funding for Cardano's development was given during the Shelley conference in July 2021. This was based on research conducted by Lancaster University and IOG on the concept of a treasury system^[742] and a viable, democratic method to long-term development financing for Cardano. Project Catalyst, which combines research, social experimentation, and community consent to develop an open, democratic culture within

the Cardano community, uses IOG's treasury mechanism capabilities.

Built on democracy

The advancement of blockchain technology has resulted in the establishment of platforms across a wide range of businesses. Long-term blockchain sustainability and development need technological advancement and maturity. That is why growth and system improvements must be supported and funded by someone. Because it allows for collaborative, sustainable choices without depending on a single governing institution, a democratic approach is an important aspect of the blockchain ecosystem. As a result, governance and decision-making must be done collectively. Users should be able to see how improvements are made, who makes decisions, and where the money comes from to make these judgments.

Sustainability

There are various options for raising funds for development. The most frequent methods include donations, venture capital investment, and initial coin offerings (ICOs). While such models may be effective for generating initial cash, they seldom guarantee long-term financing or estimate the amount of capital required for development and upkeep. Furthermore, these models suffer from centralized control, making it difficult to reach a consensus that meets everyone's demands and aspirations.

Some cryptocurrency projects use taxes to generate a long-term financing source for blockchain development, collecting a proportion of fees or incentives and depositing them in a separate pool called a treasury. The funds in the Treasury may then be utilized for system development and maintenance. In addition, as the value of cryptocurrencies rises, so does the value of government reserves. This opens up a new potential source of revenue.

When it comes to making judgments on how to guide development, however, finance systems are often in danger of centralization. Only a few people within the organization or firm are authorized to make choices about how to spend available cash in these systems. Because the decentralized nature of blockchain renders centralized management of funds problematic, disagreements among organization members can occur, leading to conflicts.

Cardano's Treasury

To solve the issues, a variety of treasury systems have emerged. These systems might include iterative treasury periods when project funding requests are presented, debated, and voted on. Poor voter privacy and ballot submission security are two typical downsides. Furthermore, if master nodes are coerced, the validity of funding choices may be jeopardized, and a lack of expert input may promote undesired contributions.

Cardano was established as a third-generation cryptocurrency platform to address the issues that previous platforms had. Cardano wants to make the process more democratic by giving everyone influence and guaranteeing that choices are made fairly. It is critical to have transparent voting and financing mechanisms to achieve this. This is where Voltaire enters the picture.

The whitepaper on treasury systems for cryptocurrencies [\[743\]](#) proposes a community-controlled, decentralized, collaborative decision-making method for long-term blockchain development and maintenance financing. This kind of collaborative intelligence is based on liquid democracy, [\[744\]](#) which is a combination of direct and representative democracy that combines the advantages of both.

This method allows the Treasury System to use expert knowledge in the voting process while also guaranteeing that all ada holders are given a chance to vote. As a result, for each project, a voter may vote personally or delegate their voting authority to a community member who is knowledgeable about the subject.

To maintain long-term viability, the community controls the treasury system, which is regularly replenished from prospective sources such as:

- a share of stake pool rewards and transaction costs
- contributions or charities
- newly minted coins held back as financing.

It will be able to finance initiatives and pay for improvement suggestions since ada is always being amassed. As a result, the financing process may be split into ‘treasury periods,’ each of which is divided into the following phases:

- pre-voting
- voting
- post-voting.

Project ideas may be presented at any time throughout the term, debated by experts and voters, and then voted on to finance the most critical initiatives. Despite the fact that anybody may submit a proposal, only a select few will be funded, based on their value and attractiveness for network expansion.

Decision making process

Scientists (even nuclear ones^[745]), developers, executive types, investors, and the general public are among the ada holders who vote in the treasury. With such a diverse field of participants, with different agendas and motives, there must be proper mechanisms in place to preserve inclusivity, and ensure fair reviews and voting takes place.

A person’s voting power is proportional to the quantity of ada they hold; the more ada they own, the more power they have over choices. Along with direct yes/no voting, a person might transfer their voting authority to an expert they trust as part of the liquid

democracy concept. In this instance, the expert will be able to vote directly on the idea that they believe is the most significant.

Following the voting, project ideas may be assessed and ranked depending on the number of yes/no votes; the poorest project proposals will be eliminated. The top-ranked ideas will be financed in turn until the treasury money is depleted, after which the shortlisted proposals will be ranked according to their score. Breaking down the decision-making process into phases ensures each proposal is rigorously and fairly critiqued.

IOG's research team leveraged ZK proofs to safeguard voter privacy. Zero-knowledge (ZK) approaches are mathematical methods for verifying information without exposing any underlying facts. The zero-knowledge proof in this situation indicates that someone may vote without providing any personal information other than their eligibility to vote. Any prospect of voter coercion is eliminated as a result of this.

IOG has built Treasury prototypes for benchmarking. Implementing the study as the foundation for Voltaire will aid in the delivery of trustworthy and secure treasury voting and decision-making methods. Project Catalyst is a treasury system that combines proposals, and voting processes, with the goal of fostering a democratic culture in the Cardano community.

Cardano's treasury will initially be replenished by a proportion of stake pool payouts, assuring a long-term treasury supply. Other blockchains have treasury systems, but IOG's combines perfect anonymity thanks to zero-knowledge proofs, liquid democracy thanks to expert engagement and vote delegation, and participation for everyone. Participation, incentivization, and decentralization should all be encouraged in order to make fair and transparent judgments.

It's also worth noting that this treasury system technique may be used on a number of blockchains other than Cardano. It has

previously been suggested that it be implemented for Ethereum Classic^[746] and we'll see later how COTI availed of the Catalyst Natives feature. Treasury systems may aid in this process by allowing everyone to see how a network will evolve.

Following a successful limited user group trial, Project Catalyst became accessible to the public. Although Cardano on-chain governance is still in its infancy, all metrics and indicators point to a bright future with the community leading the way.

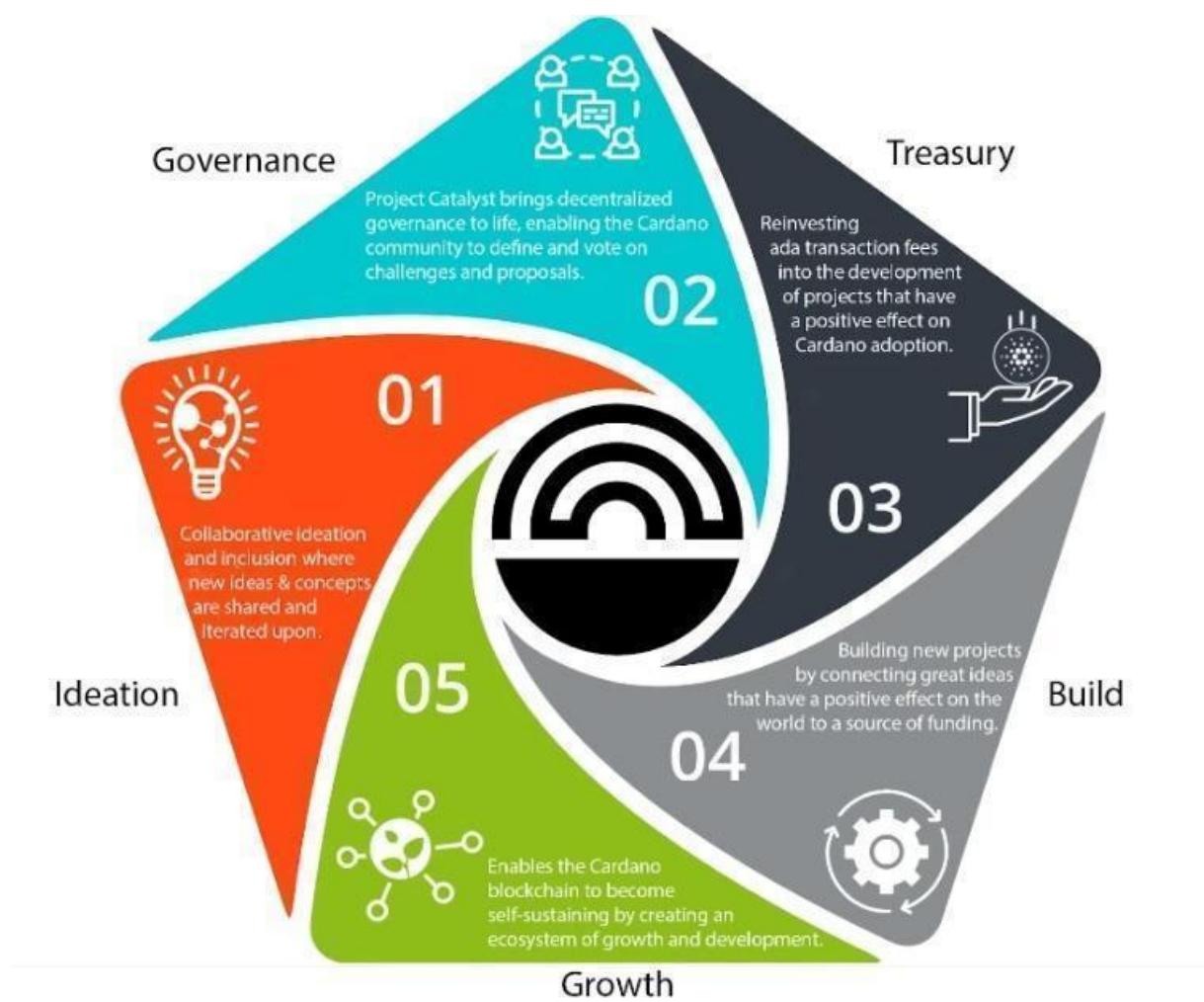


Figure 56: Catalyst overview

There are a lot of moving parts to Catalyst. This graphic from IOG's blog post 'Project Catalyst - A virtuous cycle of Cardano ecosystem development'^[747] is a good summary of the steps involved and end

goals. Former Catalyst Product Manager, Dr Dor Garbash, goes into greater detail in this presentation. [\[748\]](#)

Catalyst's first fund

In Sept 2020, IOG announced the establishment of Project Catalyst's first public fund, a milestone for Cardano in terms of on-chain governance, treasury, and community innovation.

The public fund was launched after five months of intensive activity across two earlier pilot 'funds'. The first experiment, dubbed 'Fund 0,' was conducted with the help of an IOG focus group. 'Fund 1' was the first time the concept was shared with the Cardano community, enlisting the aid of over 50 people to help IOG construct the platform and procedures. While this voting round did not provide 'real' financing, it was a significant opportunity for the IOG team and the Cardano community to test and enhance the new process.

There was a long way to go. However, with the help of the community, IOG sustained a steady rate of advancement. Fund 1 was the dress rehearsal if Fund 0 was the technical run through. Fund 2, which was announced in September 2020, was the opening night when the community's top performers fought for financing to bring their concept to fruition.

Funding great proposals

Since the start of the private part of the program in August 2020, IOG learnt a lot. Their pioneer group of 50 community members assisted them in identifying areas for improvement so that they could build and enhance the process before making it more broadly available. IOG discovered that giving clear documentation and standards encourages community members to participate more and concentrate on the ideas.

They also discovered that they may create other forums for community members to debate proposals. This improves the

Catalyst and Voltaire processes while allowing participants to concentrate on developing compelling ideas. Furthermore, IOG felt that it was critical for them to provide assistance to people submitting proposals to guarantee that their views were adequately reflected.

Cardano will prosper when the global Cardano community's creative potential is unlocked. The voting system will be only as good as the ideas that feed it. To that end, IOG worked on a guide to assist anybody in creating their best proposal possible for Fund 2 and beyond.

The community could access up to \$250k worth of ada in the first public fund. Anyone can come up with a concept and make a proposal. The 'winning' concepts began their development process after a public vote.

IOG started small, asking the community to respond to a challenge statement: 'How can we encourage developers and entrepreneurs to create DApps and businesses on top of Cardano in the next six months?' Funding proposals could address this with a broad range of concepts, including marketing campaigns and infrastructure development, as well as business planning and content production.

The first step was to 'examine the problem,' which included asking members of the community for their input. Then, through a special Telegram chat channel,^[749] IOG urged everyone to submit their ideas to the innovation platform, where they could collaborate and debate.

The public votes

IOG put things to a vote after the phases of brainstorming, cooperation, and proposal. Proposals are evaluated on the innovation platform or via a mobile voting application. When it came time to vote, everyone registered to vote using the voting app. Each participant's 'right' to vote is connected to their ada holdings, and voting will earn them further ada rewards. Ada holders will be able to delegate their ada and receive incentives as usual if they participate

in this initial financing round. Voting works similarly to a ‘transaction,’ enabling all participants to cast a vote to say ‘yes’ or ‘no.’

Today, Catalyst is implemented as a mix of on-chain and off-chain components. There is the voting center in the Daedalus wallet, the android and iphone voting apps and a dependence on the re-purposed Jormungandr^[750] node (previously used for the Incentivized Testnet). As the Voltaire era unfolds, the voting experience will move into IOG’s new light wallet *Lace* (lace.io).

How it works

Voltaire is a critical component of the Cardano ecosystem since it enables every ada holder to participate in choices about the platform’s future development and contribute to the ecosystem’s growth. Project Catalyst is a critical first step in achieving such capacity. The Cardano community’s enthusiasm and dedication to developing this further was exhibited in the early phases of this project. With the implementation of an on-chain voting and treasury system, network users will be able to utilize their stake and voting rights to drive Cardano toward achieving common objectives in a democratic and self-sustaining manner.

The inaugural Catalyst-funded entrepreneurship programme, dubbed ‘BoostCamps’,^[751] used the Entrepenerdy (entrepenerdy.com) platform to allow enterprises to participate in sessions aimed at developing their company strategy.



Figure 57: Catalyst 'here's how it works'

Initial Funds

In September 2020, Catalyst sprang into action for the first time with Fund2. [\[752\]](#) IOG observed a pioneering example of decentralized cooperation. Thousands of individuals joined together to produce, refine, and prioritize financing for ideas to move Cardano forward — pitching teams, community advisors, and ada-holding voters.

Fund3

Meanwhile, IOG proceeded with even more purpose by leveraging the community energy that's so important to Catalyst. Fund3 went live in January 2021, and with each fund, IOG wanted to grow the Catalyst community by encouraging more individuals to participate.

Every investment cycle starts with a set of objectives. Each challenge symbolizes the Cardano community's 'intention,' a common objective to accomplish. IOG likes to speak about 'return on intention' as a means of monitoring project success. Each challenge is intended to be wide enough to elicit both technical and general ideas while remaining focused. IOG will evaluate any suggestion that tackles a problem and makes a compelling argument for achieving the desired result. As a result, IOG embraces all ideas, from marketing campaigns to infrastructure development, to content creation and product improvement.

Project Catalyst focuses on the creativity of a worldwide network of participants; thus all ideas are welcomed and may reappear in future funds if they don't satisfy the current challenge requirements.

Fund2 had a \$250,000 ada pool, while Fund3 doubled that, awarding \$500,000 in ada to proposers, voters, and community advisors.

Fund3 had three challenges:

- Developer ecosystem challenge: 'What can we do in the next six months to encourage developers to build on Cardano?'
- DApp development challenge: 'In the next six months, what decentralized apps (DApps) should be sponsored to increase user adoption?'
- 'Community choice' challenge: In this new category, IOG encouraged the community to create one or more challenges, each of which subsequently had its own financing round in Fund5. An extra \$500,000 pool was available to support whatever objective the community set, whether it was completing the community roadmap, sponsoring content or podcasts, promoting non-profit activity, or anything else.

So, how exactly do you become involved with Project Catalyst?

Insights & ideas

To begin, everyone interested in participating in the project, whether as a proposer, advisor, or just a voter, should register on IOG's collaboration platform, IdeaScale (cardano.ideascale.com). To suggest an idea or participate in the debate phase, you do not need to be an ada holder.

Before proposals were presented, Fund3 started with an insight-sharing phase in which individuals shared their ideas on the topic. Consider this phase to be a community brainstorming session to help proposers come up with new ideas. Participants with ideas

publicly submitted a first draft once the challenge has been discussed.

IdeaScale funnel

Members of the community are encouraged to provide constructive criticism, recommendations, positive affirmations in the form of ‘kudos,’ and even propose to build partnerships and collaborations with the proposing teams. The purpose is to pool community knowledge and skills, and Catalyst members are a broad group of people with a wealth of personal and professional experience to contribute.

Proposers are given the option to alter and complete their ideas after receiving community input. Once the plans are complete, a panel of professional reviewers who have been recruited as community advisors will assign each one a score based on how effectively it meets the problem. Following that, ada holders may register and vote. The votes are then tabulated and requested funds are awarded to the winning proposals, which are weighted according to the amount of each voter’s holding.

Fund4, the first million-dollar fund

The breadth, amount of money, and community participation have all increased with each funding cycle. On the IdeaScale innovation platform in Feb 2021, there were 7,000 members and 1,800 active voters. Adoption was increasing by 10% per week.

Fund4 was the most accessible and ambitious round yet, as well as the first million-dollar round — the ada pot used to finance Cardano development initiatives. The funding was used by proposal teams to create tools, construct DApps, establish developer education and training efforts, and much more. Every new input boosted the ecosystem’s worth and, since the community is at the heart of Catalyst, 20% of treasury funds were set aside to reward and motivate community advisors, referrers, and voting participants.

IOG continued to make the project more available to the Cardano community during 2021 to promote participation. Voter registration increased considerably in Fund3. Within a redesigned registration center, registration was now completely connected with the Daedalus wallet.

Yoroi lite wallet users could easily register via a browser plugin. After that, voters could finish the process using a specific mobile voting app, which can be downloaded on iOS or Android. Users can also register and vote from their wallets in Daedalus.

Project Catalyst had risen to become the world's biggest decentralized autonomous organization in less than six months (DAO). It serves as a fulcrum for future growth and sustainable innovation, led by and for the Cardano community.

Catalyst Circle

Since its inception, Project Catalyst has grown at an astounding pace, almost tripling in virtually every dimension from fund to fund. Catalyst is proving to be a crucial fulcrum for Cardano's future development on every measure — whether it's the amount of votes cast, financing available, or simply participation in itself. Fund4 came to an end in July 2021, but Project Catalyst had already shown to be a successful teamwork and decentralized innovation endeavor.

This rapid expansion has brought with it new obstacles. Project Catalyst is gaining a number of contributions from increasingly different functional groups who are helping to bring the collective intelligence forward. Specifically, community advisors, funded-proposers, stake pool operators (SPOs), and toolmakers & maintainers, who all contribute to Project Catalyst's success and expansion, as well as Cardano's success.

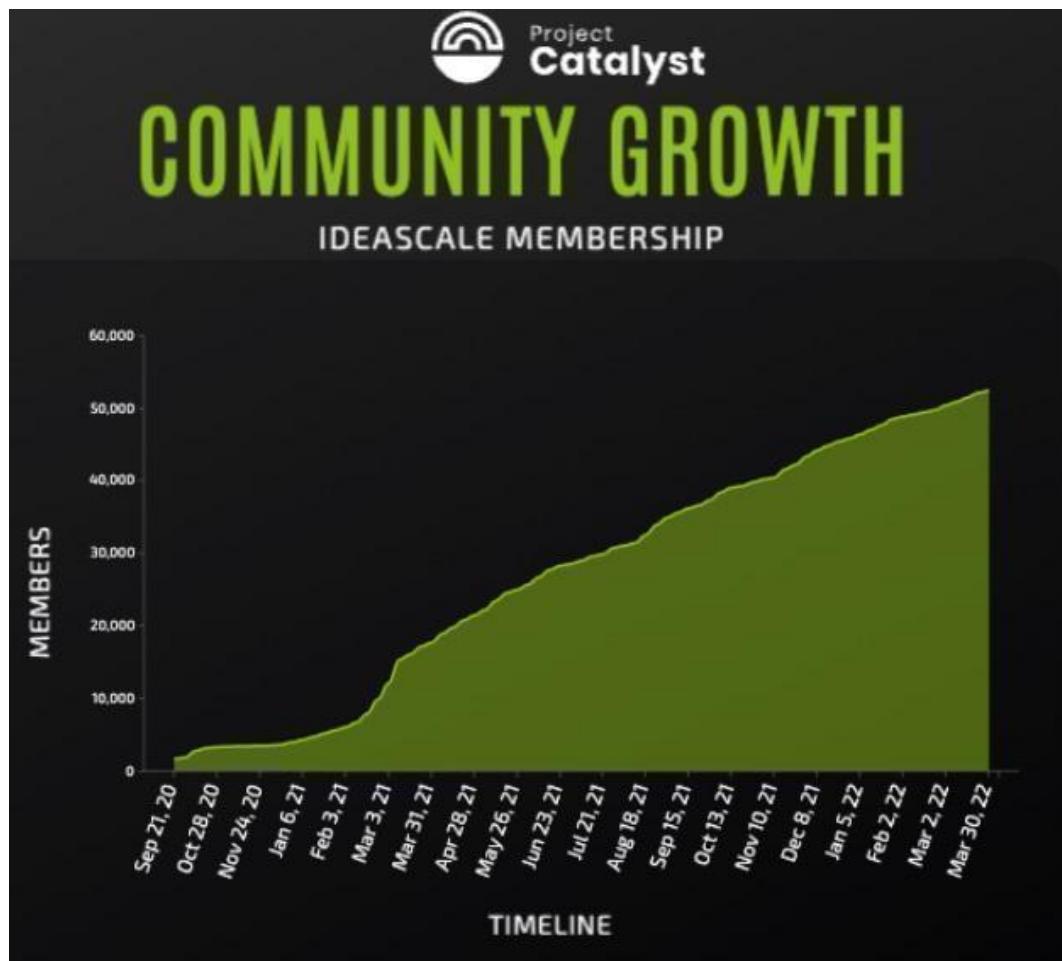


Figure 58: Catalyst growth

Project Catalyst gains benefit from this expanded variety since it allows for the formation of even more ideas and proposals. It also makes communication between all of these groups more difficult. Every cohort wants to be heard, and their thoughts and concerns need to be aired at the project level.

It's clear these groups need representation and trustworthy leadership to advocate for them. Project Catalyst's influence would be severely reduced if such representation was inadequate or non-existent. This is why the Catalyst Circle was created.

'Human sensor array'

IOG describes the Catalyst Circle as a ‘human sensor array’ that serves as a representative body for all of the Project Catalyst participants. The Circle that keeps track of Catalyst’s present state and future intentions for governance. Within the Catalyst ecosystem, it identifies and discusses issues, objections, and possibilities. For example, the Circle might debate the amounts distributed to challenge Fund after Fund, tweaks or conditions to incentive parameters, the Catalyst API, and so on.

This activity will give an insight into the hopes, desires, needs, and worries of the community inside Project Catalyst by documenting meetings and collecting activities in a backlog available to everyone. The Circle is also in charge of choosing its own future form and designing the Circle v2 election procedures.

The Circle exists to achieve four main objectives:

- To make it easier for various functional groupings to communicate with one another.
- To give people notice when lines are crossed
- Make suggestions for enhancements to Project Catalyst’s plans and procedures
- Define the Circle V2 election process.

Elected members

The Circle, like Project Catalyst, will grow and change over time. Initially, elected members will serve three-month terms, with further elections to improve and iterate the process. These basic tasks and obligations have been specified for elected members.

Each Circle member should do the following:

- Represent the people who chose them
- Use their best judgment when it comes to topics that come before the Circle

- Educate other members about their communities' initiatives, activities, goals, dreams, and concerns
- Take advantage of opportunities to incorporate policy recommendations into the Circle's agenda for discussion on a regular basis
- Inform their communities about the Circle's efforts.

Each team member is expected to:

- Attend regular meetings every fortnight
- Keep an agile backlog to keep track of concerns in between sessions
- Review and comment on items on the agenda ahead of time
- Remain informed of their community's interests and concerns
- Distribute the Circle's outputs in a clear and accessible manner
- Study and practice good meeting processes
- Create a protocol paper for the next elections
- Participate in training seminars on inclusive and lean startup leadership
- Provide comments on the Circle's efficacy.

Inaugural election

To include community members who couldn't attend the usual weekly (Wed 5pm Irish time) Town Hall, IOG organized the first election in July 2021 for Catalyst Circle members globally. Members will be able to establish the agenda for each meeting and submit policy recommendations to the Catalyst Circle for consideration on a regular basis. The bootstrapping version is the 'minimal functional group,' which is based on conversations with Catalyst community leaders and Governance Alive (governancealive.com), an expert group in the area of new governance structures.

The Circle may expand and split as best practices are established. In the end, it will be up to members to help IOG achieve their aim of legitimizing decentralized government, opening the road for a viable

alternative to the status quo, and breaking new ground in the development of blockchain governance.

The Cardano cFund

The cFund, which was first unveiled at the 2020 Shelley summit, is an early-stage investment fund that focuses on creative firms on Cardano. Wave Financial, in collaboration with IOG, manages the cFund, a crypto-native hedge fund. The fund uses an early-stage venture approach to invest in creative technological firms that are building Cardano-based apps, services, and products, as well as other R&D projects that IOG is working on.

The ‘c’ in cFund

The letter ‘c’ in the name relates to the mathematics word ‘coefficient,’ which refers to a variable’s multiplier. cFund is positioned to provide a multiplier effect in terms of growth and reach for its portfolio firms by using both IOG’s and Wave Financial’s subject knowledge and industry relationships.

The cFund’s role

IOG is concentrating on achieving two goals. One is making it possible for developers to create blockchain-based systems that are scalable, interoperable, and long-lasting. The other is to promote financial inclusion for the world’s neglected communities. By building a community of DApps and protocols deployed on Cardano and other blockchains, IOG hopes to establish a new financial infrastructure for emerging economies.

IOG collaborated with Wave Financial, a digital asset manager with \$500m in assets under management across several strategies and products, to build the cFund to work together to make this dream a reality. While the cFund, IOG, and Cardano Foundation all operate separately, they are always looking for ways to work together. cFund,

in particular, assesses and advises its portfolio firms interested in deploying on the Cardano blockchain.

The cFund's investment strategy

Third-party, high-net-worth individuals and institutional investors finance the cFund (including IOG). cFund seeks to engage with and invest in top early-stage initiatives and companies that are largely focused on the Cardano ecosystem and related technologies. The fund is already investing and forming relationships within the Cardano ecosystem.

When assessing investment possibilities, cFund employs a rigorous strategy that takes into account a variety of elements. To begin, the fund assesses if there is a clear market demand for the service a firm offers and whether other rivals can outperform it. This is referred to as 'timing the market' in investing parlance. The fund then assesses the founders' history to see whether they have the expertise, skills, resources, and capacity to expand their firm or project. Exit possibilities are also taken into account by the fund.

One of the most essential elements cFund evaluates during its due diligence process is whether or not the entity can be a value-add to the Cardano ecosystem, since one of its key aims is to assist Cardano in forming relationships throughout the blockchain world.

Decentralized Finance (DeFi), or more generally, what is known as Open Finance, is one market in which cFund has invested. COTI, a decentralized and scalable payments network for the e-commerce sector, was cFund's first investment in this area. COTI (currency of the internet) is a value-add since it intends to act as a bridge between DeFi apps and the Cardano blockchain. COTI offers a solution called ADA Pay (adapay.finance), a payment gateway that allows retailers to accept ada payments with near-instant settlement. The business is also working on a stablecoin based on Cardano called Djed.^[753]

Another example is Occam.Fi, a suite of DeFi solutions optimized for Cardano, also backed by cFund. Their initial product is a decentralized financing platform. The next generation of DeFi apps will be able to raise funding utilizing the Cardano blockchain thanks to this launchpad.

Services offered

To its portfolio firms and the greater Cardano ecosystem, cFund serves as a funding provider, adviser, and partner. cFund delivers unrivaled access and direction to its portfolio by using IOG and Wave Financial resources, reputation, knowledge, and network. cFund is a great believer in adding value to its investments. cFund strives to be the first port of call for management teams.

In addition to being an important part of the Cardano ecosystem, cFund intends to be the top early-stage venture fund that invests solely in Cardano blockchain-based innovations. According to IOG's foundational philosophy of 'cascading disruption,'^[754] most of the structures that make up global financial, governance, and social systems are inherently unstable, and slight disturbances may generate a ripple effect that radically reconfigures the system. The purpose of cFund is to find and fund solutions that bring these disparities together in a fair and transparent way for all participants. While other cryptocurrencies^[755] have strong ties to Silicon Valley, Cardano is innovating with Catalyst acting as its own 'built in' VC Fund.

October 16, 2020. There are a lot of different funds so could you explain to us what is DC fund? cFund and the Cardano Foundation fund? CH:^[756]

So the DC fund is what we've termed the funds that are coming out of Catalyst... and those are grant models ... Cardano doesn't have agency, so we can't own land, it can't have intellectual property... it can't have equity, these types of things ...so when it gives out funding... It's like when the National

science foundation (NSF) gives out funding, or DARPA^[757] gives out funding ...where it's funding the development of something because we, as a society, have determined that that is a good idea.

So for example when NSF gives research for theoretical physics ...it says we, as a society, would like our brilliant physicist to be well funded so that they can figure out how time works and gravity works and so forth ...but there's no money that comes out of that ...or these things but there's a social benefit, that potentially could be leveraged over time to make the country better... Perhaps we invent anti-gravity at some point but it's not the primary goal.

So we look at DC fund like that where we say it's a 'return on intention'. Grants are coming through, and the goal is to make Cardano better.... but it's not to make Bob a millionaire or something like that...

cFund is a venture capital arm of my company and Waves^[758] ... we're working together and setting all of that up and basically that's going to be where you run a project and you come to Charles and the others who are involved with that... you say, 'I would like you to invest in my company... and give me the resources I need to get it to the next level.... and then we would look at you like any venture capitalist would look at you.... ask you the same questions Andreessen Horowitz (a16z.com) will ask you, or Kleiner Perkins (kleinerperkins.com) will ask you and so forth ...and if we determine it's a good investment, I'll open up the checkbook and cut a check and send your way and we get equity back for that, because that's a private investment.

Then the Cardano Foundation they have something called the CCCI, Commercially Critical Cardano Infrastructure... and that's saying there needs to be some product validation and bootstrapping, that Cardano really is competitive, or capable of

doing the things that Ethereum and EOS and Tezos and Algorand do.

So we're going to give out some very specific very targeted grants to help get the ecosystem along ...okay the DC Fund, the community is in charge of that ... the grants from the (Cardano) Foundation, the Foundation's in charge of that and they're very directed towards catching us up and getting us where we need to go to compete with Ethereum and the rest of the gang ...and the cFund is a good old-fashioned investment for things that I think we ought to have on our ecosystem.

Catalyst Natives

I dipped my toe in the water with my own proposal in Fund6: ‘DID as a bridge to Microsoft’^[759] which met with a lukewarm response. I hadn’t really thought it out properly but wanted to see how the system worked, as a participant. It was kind of reassuring to see my idea scrutinized, dissected, and rejected as it was not worthy of funding ahead of the likes of dcSpark.

As part of Project Catalyst,^[760] the first Catalyst Natives pilot, was launched in late 2021. Catalyst Natives allows any project to tap into the collective intelligence of the community to solve business challenges and outsource solution execution. This initiative expands the potential of blockchain technology to include new use cases for both big and small enterprises.

IOG started a series of pilots, the first of which was in collaboration with COTI, an enterprise-grade fintech firm that helps businesses construct their own payment systems. COTI has created a highly user-friendly and scalable ada payment system for the community in collaboration with Cardano. As a consequence, by incorporating adaPay into their site, online merchants of various sizes, from a tiny hotel^[761] in Europe to a large e-commerce website in Asia, may effortlessly accept hundreds or thousands of ada transactions.

Project Catalyst has risen to become the world's biggest decentralized innovation fund in less than a year. It is a hub for long-term growth and innovation led by the Cardano community and for the Cardano community. IOG opened the gates to companies outside of the Cardano ecosystem to leverage the potential of the Project Catalyst innovation engine in its inaugural test of Catalyst Natives.

Project Catalyst has set various challenges for the community to cooperate on and produce answers throughout each fundraising cycle. In November 2021 Fund7, a total of \$8m in ada was available, with 80% of it put aside for project financing and 20% for rewards for voters and community advisors. Fund7 had 24 challenges, 21 of which were suggested and voted on by the community, two of which were proposed by IOG, and the Catalyst natives prototype, which was developed in partnership with COTI. The Catalyst community voted on the ideas provided, and the winners got funding to finish their projects.

COTI, the first Catalyst Native

Catalyst Natives expands access to Project Catalyst features such as the Cardano native tokens feature, which increases the number of tokens available on the Cardano blockchain. Organizations outside of the Cardano/Catalyst ecosystem could now present challenges and give incentives and rewards to individuals who successfully satisfy the challenge with their suggested innovations, thanks to the launch of Catalyst Natives.

COTI presents the community with a novel technological challenge in this pilot. By adding a plug-in to their site, any small and medium businesses using platforms like Shopify and WooCommerce will be able to take advantage of new and innovative methods to accept ada payments with seamless integration.

Following the pilot, IOG will allow Catalyst Natives to accept more challenges from other entities; however, these challenges will be

selected by IOG, in the first phase, to ensure they provide value to the Cardano ecosystem. Organizations proposing challenges via Natives will finance those ideas, thus Catalyst Natives will not utilize Cardano Treasury funds to pay for the initiatives that have been successfully voted on. COTI distributed \$100k in COTI tokens plus fees in Fund7, which was in addition to the \$8m ada fund.

Catalyst Natives is an opportunity for businesses of all sizes to have access to a vault of ideas and the people who can help them come to life. Catalyst Natives is now aiming to assist Cardano ecosystem partners, and native asset token projects, handle particular pain points for which they either do not have the resources or simply do not have a solution and outsource them as Catalyst challenges for proposers to solve.

Organizations must adapt to continuously changing market circumstances as the future unfolds, and technologies like Catalyst can open the door for disruption in how individuals communicate and make choices outside of the Cardano community. Emerging markets make planning very difficult. Because of this ambiguity, the flexibility to call on a think tank as required and outsource execution is quite useful.

IOG ‘OG’ and Ergo strategic advisor Dan Friedman[\[762\]](#) announced on a recent Ergo update[\[763\]](#) that Ergo is planning to be the next Catalyst ‘Native’. Anyone interested in Catalyst Natives can apply here.[\[764\]](#)

Catalyst Fund8

Every three months, a new Project Catalyst innovation fund campaign launches, offering the chance to obtain resources from the Cardano Treasury paid in ada. Resources that may be used to construct, produce, and contribute to the realization of excellent ideas that are worthy of support.

What began as an experiment in collaboration, competition, and human potential had grown into the world’s largest decentralized

innovation fund in just over a year. Fund8 offered \$16m funding in ada.

To propose, assess, and finally determine which proposal submissions should be financed, a worldwide community joins together. Proposals included innovative decentralized finance (DeFi) apps aimed at reducing financial inequity and RealFi, which establishes an ecosystem of goods that removes frictions from real-world economic operations and provides people with cheaper credit/financial products. For example, the collective manufacturing project (wayacollective.com) run by African entrepreneurs and employees.

Milestones

Every Catalyst fund cycle has provided new, remarkable accomplishments. Fund7 was no different.

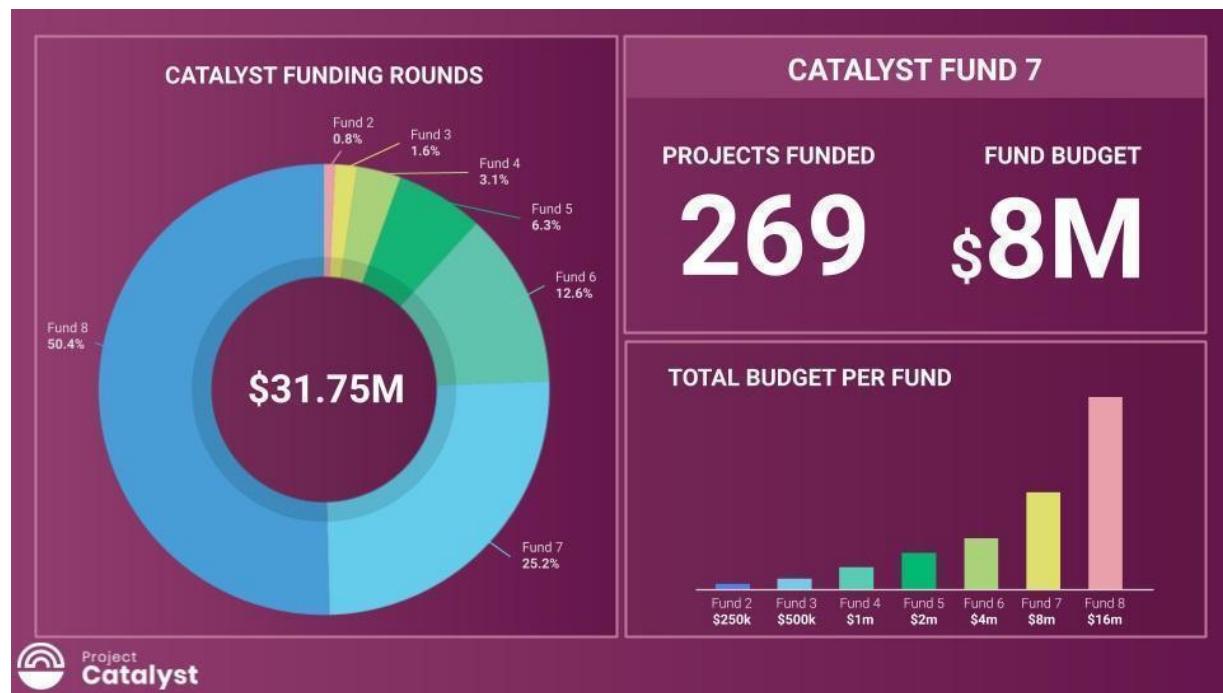


Figure 59: Fund7 stats

After the votes were tabulated and counted in Fund7, 269 additional initiatives^[765] were selected to get ada. Given that each of these

projects was created in response to 24 real-world problems provided by the Cardano community, as well as one additional task issued by COTI, Cardano's first Catalyst Native pioneer, these were impressive numbers. Catalyst Natives gives decentralized innovation fund management to partners aiming to develop their ecosystem by incentivizing innovators to assist in finding solutions to problems.

This time around, over 52,500 wallets registered to vote, and community advisers reviewed over 900 proposals to assist voters make informed judgements. The number of ideas financed by the Cardano Treasury had almost quadrupled in a short period of time, reaching 575 projects. Importantly, nearly a million votes had been cast since the initial Project Catalyst community vote in Fund2.

The Cardano Treasury now contained roughly 800m ada in order to maintain and build the ecosystem. Many of the projects that were funded in previous rounds have now been completed and their end products are being showcased. [\[766\]](#)

The Catalyst community established and agreed on each and every task in Fund8. What were the goals? Within Cardano's open-source architecture, to speed up the developer and DApp ecosystem. Cardano Ecosystem Foundations & Development, Community Development, Outreach & Adoption, Identity & Interoperability, and Project Catalyst Improvements are among the 23 challenges.

The 'stat attack' about Fund8 reported in the recent Cardano360 episode indicate Catalyst is not slowing down anytime soon:

- \$25k up to \$16m in funding
- 3.5k catalyst proposals
- a million voted
- 52k members in 91 countries

Catalyst is also partnering with the Financial Times and Seedstars (seedstars.com) to launch the 'FT x Cardano Blockchain Challenge' where selected startups will participate in a 3-day Bootcamp and

connect to Seedstars' network of mentors. 'The global winner will get a short-track to Seedstars' International Ventures Fund. Additionally, 24 startups will be selected to participate in a 3-month Acceleration Program.' Apply on Seedstar's website.^[767]

Participating in Catalyst

There are several ways to participate in Project Catalyst. As a creator, voter, commentator, proposal reviewer, or mentor. Making an account on the collaboration platform is the first step. Another option is to join the Project Catalyst community at TownHall every Wednesday, which is live broadcast on IOG's YouTube Channel.^[768] Join the Project Catalyst Community if you have an idea or simply want to learn more about what's going on with Cardano. Fund8 results^[769] confirmed the momentum just keeps growing as voting turnout increased and a diverse range of projects were funded. One of the smallest amounts requested, and funded, was also one of the most significant. Sebastien Guillemot's successful proposal^[770] means he is the first CIP editor to be paid for his time.

You can track each fund and check in on proposals that were previously approved here.^[771]

April 21, 2019... Who pays? Who decides? CH:^[772]

This is why it's so incredibly important that you have a treasury system ...and voting systems because right now here's how the cryptocurrency space works and this is why things get so toxicyou have a very small group of people who are developers, investors, big people who are actually building stuff in the space, the entrepreneurial class, developer class the infrastructure class... then you have the speculators which are everybody else ...and they hold the currency, they're fans of it, maybe even philosophically aligned with it ...but they don't have a voice, they can't do anything ...they're just sitting there just hoping for things to materialize.

....and then a subset of them maybe move into the other class when they have smart contracts or whatever... but the vast majority of them are there yet they have opinions about where things should go...what they should do ...and so the key is to give them tools to organize... tools to vote... tools to discuss the philosophy and direction ...to have teeth, not just 'here's my opinion', but also when my opinion is let manifest and gets a Democratic consent behind it ...then that opinion will turn into money ...that then can be used by the other class.

All of a sudden everybody has power and actually has a voice ..and an opinion and you're not just talking about when is this coming out or what is that coming out...you're actually talking about where do we want to go and how are we going to get there and the things we need to do to get there... who's the best leader to get there... you can't fork that.... you can fork the code and have another Treasury system.

...but it's like saying well that big meetup group over there... I'm going to host my own meetup group and I'm going to copy everything... the same banners and the same catering and the same everything... it doesn't mean other people are going to show up ... the other thing is that it gives people the freedom to compete with you in ways that make you better ...anything any of our competitors make ...we can take,... it's fair game and if they hire a brilliant person, I'm happy because I know that brilliant person is going to write papers and code...and everyone can review it.

Can you stop the banks coming in and owning critical infrastructure? CH:[\[773\]](#)

So a lot of the design of Cardano was built with future proofing, like heterogeneity by design. So stake pool operators, as they strengthen and grow and become their own consortia. They can become infrastructure providers. Multi resource consensus, at the consensus level, can also incentivize network and

bandwidth and compute power decentralization, so you can decentralize the hosting and the server components of it. That's why we wrote the Minotaur Paper.[\[774\]](#)

For decentralized governance and funding, you don't need to go to JP Morgan and ask them for money. You can get money from Catalyst. Having the ability to work in a large global ecosystem and also protocols that tend to get more decentralized overtime, and also protocols that emphasize local state which makes them work very well with payment and state channels and roll ups. The ability to use sidechain infrastructure very well.

All of those things contribute to a system that gets faster, more decentralized and more resilient over time. We spent 6 years trying to figure this out and I think the recipe is there. We're told by the podcasters and the YouTube elite and the crypto media that unless we somehow win the next 15 minutes, the battle is lost. Network effect is set in and we're doomed to this centralized dystopia. I don't believe that. I don't believe it for a moment. I think this is a long war of attrition and ultimately principles do matter, if they're built correctly and they have the right incentives behind it.

The recipe of Cardano, what we've put together, I firmly believe it's going to stand the test of time. It's inculcated a community that values these things and they're not going anywhere. And even if it takes a little bit more time to prime that pump and get it where it needs to go, never forget that we're at over three million people now. Never forget that our TVL (total value locked) is growing radically and our new wallets are growing radically. Never forget 74% of ada is staked. Never forget that we have 900 plus DApps being built on the ecosystem and we had none just 9 months ago. Never forget 4,000,000 assets have been issued on Cardano and this is the beginning.

So that gives me every indication that if we continue this growth rate we will wake up with millions of users and those people

don't need legacy money. We're creating our own. So I think we'll win in the end.

dReps

IOG introduced the notion of delegating your voting rights to a Delegate Representatives (dReps), and urged people interested to register during a Fund8 Project Catalyst Town Hall.[\[75\]](#)

This ongoing growth of the Cardano ecosystem is great news for the whole Cardano community. Exponential expansion, on the other hand, offers a problem. The community's obligation to examine and vote on ideas grows as the quantity of proposals grows. A new approach is needed to guarantee that all ideas get the attention they deserve, as well as to support further development.

Ada holders may give their votes to one or more dReps through delegation. This provides the more passive voter a chance to have their voice heard, but now across a larger number of proposals than they could read and evaluate personally.

These dReps will vote on the vast majority of Project Catalyst proposals, improving the quality of decision-making within each Fund. dReps will collaborate to develop policy, gather and evaluate data, consult with experts, and ultimately vote on a variety of initiatives and issues proposed by the community.

As the community continues to learn and expand, the introduction of dReps is another exciting step ahead. As IOG rolls out delegation into additional Project Catalyst grants, there will be more to share and explore in the months ahead. IOG is soliciting interest in joining the first dRep cohort to promote inclusion and diversity. If you'd like to get involved, you can join the dRep pioneers here.[\[76\]](#)

Project Catalyst FAQ[\[77\]](#)

Twitter space 'Sunday Chat with Charles'. **What's the main feature**

that will make ada more interesting than multi chain networks?

CH:[\[778\]](#)

Well, I think it's probably governance because that's something that's very difficult to replicate. And then second, it's something that seems to be an area we spent a lot of time talking about doing things with, but the space as a whole undervalues, maybe because Vitalik (Buterin) hasn't quite embraced it yet, or whatever who knows, you know. But don't worry, in two years everybody will be doing it, then they'll claim they invented it, and that we're a shit coin. That's usually how it goes.

You know, because at the end of the day, when you look at these features and functionality like tiered pricing or Babel fees, extended UTXO, that is pretty novel and hard to copy, but it can be (copied). Same with sidechains. These are all from Cardano's side, well integrated together and well balanced and carefully thought about, so they tend to work well and it's really hard to get that delicate recipe right. But in general somebody probably could copy it. Polkadot, for example, is using part of our consensus on their ideas.

People have copied a lot of our concepts, that's fine, but governance is really hard to replicate because even if you have identical governance tools, you cannot replicate the set of people who are involved in governance. The dReps (delegate representatives), the people who actually go every day to IdeaScale, the people submitting ballots, the people reading ballots saying yes, no or maybe.

That's a very difficult practice to replicate. And I think it's something that's already tens of thousands of people that are already involved in that and that sets growing very rapidly on the voting center and dReps. We're probably going to close out the year with not only tens of thousands, potentially hundreds of thousands of people directly and indirectly participating in that.

And every year that set is going to grow. And so as that grows, your capabilities grow. With it, you make better decisions. You can fund more things in parallel. You can audit more proposals. CIP 50 (Liesenfels Shelleys Voltaire Decentralization Update) is an enormous amount of work that has been put in by a nuclear engineer on the economics of Cardano. Contrast that with some of the earlier community CIP (Cardano improvement proposals) which were very well intended, but they didn't have that rigor or depth behind it. So times that by 10, times that by 20 ...you can start seeing how quickly you evolve, and you can start seeing how quickly the ecosystem as a whole becomes self-reinforcing and it's just so hard to replicate, copy that, especially when there's financial incentives for people to participate.

April 2022. Re: Privacy on Cardano, should be decided by the governed '4/20 Hangout with Charles' CH:[\[779\]](#)

As for Cardano having privacy features. That's a decision of the community. What I could do is get you guys to a point where you can take that as a vote, and I have a great menu of options you could use, but you have to walk into that with both eyes open. If you increase the level of privacy beyond what bitcoin provides, you lose liquidity, you start seeing exchanges delist you, start seeing governments fight you and it's above my pay grade to make that decision for all of you guys.

I can build you a beautiful, scalable system. Whether the system goes at one TPS or a million TPS, that's not controversial. The system's properties of privacy...that's a philosophical question, and that requires the consent of the governed, to make that philosophical question. So you guys have to make that decision and we have to build a governance system that can give you the right to do that.

November 24, 2020. Re: Why is Cardano different? CH:[\[780\]](#)

So it's coming together, just to build this infrastructure in a scalable, decentralized way, so you can have billions of users is super-hard. That's what we spent 5 years researching and thinking about. Meanwhile Vitalik is trying to go to proof of stake... and you hear... 'but you guys don't have smart contracts yet!'... guys, take a chill pill, we're not only going to have smart contracts, we're going to do the pond and the ocean.

We'll have resource determinism and much lower operating costs...and Ethereum doesn't have that...anything they can do; we can do, and we'll do a lot of other stuff better. Proof of stake is far harder (than proof of work), that's why Vitalik (Buterin) has spent 5 years on it,^[781] and he's not there yet. Not only did we get there before him, we got there with a protocol that doesn't require bonding and slashing^[782] ..and we got there with a protocol that has much better security, much better path to scalability and is built on a peer-reviewed theoretical foundation with 12 papers behind it, 3,000 citations at major conferences. We just keep accelerating, we've already decoupled the clock, we understand how to recover from spikes of dishonest majority, we have a much better way of generating random numbers...all kinds of stuff with Ouroboros that is innately better than Casper.^[783]

They can't even get Casper^[784] off the ground. It'll take 2-3 years. It's like we have it, but we don't have it.... I said Shelley is launched, I said the d parameter is going to decrement, went from D = 1 to less than 0.5 in a few months. It will be zero (fully decentralized) by March 2021, we have a 1,000 registered SPOs (stake pool operators), we'll have 1,000 sustainable pools by March, a network fully run by the community. We did a hard fork, nothing happened, just a beautiful transition point for the end users.

It was hell for the exchanges, as they had to migrate but now that they're migrated it's a very easy upgrade path. Every time we do an update, we have a hard fork combinator event (HFC).

It's just a flip of a switch to do upgrades and turn stuff on, no disruption to service. Meanwhile, Ethereum can't even figure out how to transition the network... it's so fragmented they're probably going to have two Etereums running at the same time, the miners aren't going to go along with it....it's very hard, under the hood, to do this stuff from a theoretical foundation, and people just don't get that.

When people say PoS (Proof of stake) is easy, I say prove it! Name one PoS system that's working at scale in the top 10. There's only us and Polkadot. Polkadot's stuff is based on our stuff, nominated PoS was a derivative of Ouroboros. We did the hard stuff first with the accounting model, with the network stack, with the consensus model, with the programming languages....and now that that's all done, we get to enjoy the fun stuff, which is building real cool stuff at scale for millions of people.

If we do one deal in Africa, it's probably five million people.... then we can scale that easily to a dozen deals suddenly you wake up and you have 100 million users. We ask ourselves, are we really ready for that? We're the only game in town that actually thought about how you actually get there, and get there with regulation, get there with identity, get with off-chain, with permissioned ledgers and all these other things.

The latest flavor of the month is usually a fork of someone else's code. We wrote all the code from scratch. Here's the reality, when the price of ada goes up, we get more decentralized, the K parameter increases so you get more stake pools, you get more participation, so you end up getting more resilient as a system. We get more decentralized, we run more Hydra nodes once Hydra turns on. Every Hydra node that runs is a thousand TPS (transaction per second)thousand stake pools times a thousand TPS...your throughput is a million TPS with a system like that. We have a beautiful path to get there, and it doesn't

even require a hard fork combinator (HFC) event. It's a gradual process but predictable.

Bitcoin is the opposite. When the price of Bitcoin goes up, you get more vertical integration with mining towards ASICs and subsidized power and the pools go from public to private. You end up getting small groups of people you could feed with 2 pizzas...that's not decentralized. Your power consumption skyrockets, our power consumption stays flat. The entire Cardano network can be run on 20 kilowatts of power. I'm installing a 250 kW solar system for my farm, I could run the entire Cardano network and still have enough power to heat my driveway and grow my mushrooms,.etc.

You can't do that with Bitcoin, it uses more power than the country of Switzerland and if it goes to a trillion dollars it'll use more electricity than Canada....and it's constrained to single figure TPS (transactions per second). Our system, as we get more decentralized, we scale easier, we have more off-chain capabilities. The base layer alone, we can go from what we're currently at... about 150 TPS (based on current simulations) to 1,000 TPS just with the current design pre-sharding.

You tell me if I have 1,000 TPS at the base layer, state channels which can run all the bloat, the micro-transactions off-chain, low economic value transactions off-chain...then at what point do I need to exceed that? Maybe in 10 years....at that point, look at where sharding technology is at, every day we have new sharding capabilities. I have 5 years, or more, just to think about sharding from an architecture perspective and do it right before I actually need it, before the network actually needs it.

This is the problem with Eth2 (Ethereum 2.0)...they did something that was replicated and not scalable with Ethereum 1... then they said ...'Oh God...we're victims of our own success, it's so expensive to run this system....what the f\$ck do we do?!'. So then they try to do everything all at once. They try

to do game theory, sharding, proof-of-stake move from proof-of-work, try to figure out the transition mechanism. It's too much complexity and you see this all the time with young graduate students. They want to solve these big, super-complicated problems.

A real researcher breaks down the problems into bytesize parts. Even if we want to solve the Riemann Hypothesis, the road to Riemann is going to be a million little steps...a million little papers you write. So what did we do? Let's just ask what is a blockchain? And the security definition for that.....2015, the GKL Paper, Eurocrypt^[785] ... we asked, can proof of stake (PoS) even work? We don't even know. So let's create a toy, theoretical proof of stake, but not a real one, just to prove that under realistic conditions, can PoS match Bitcoin. That was the original Ouroboros paper. Then we said we need to actually make this work at scale in a real operating environment.

We went from synchronous to partial synchrony, we went from not scalable random number generation to high-throughput random number generation, we went from static to adaptive security....and that was Ouroboros Praos. Praos appeared at Crypto.^[786] Then we said we want to be able to bootstrap from Genesis, like Bitcoin does...and that was Ouroboros Genesis. Genesis appeared at CCS. Every step of the way, we have peer-reviewed paper after peer-reviewed paper. We have Ouroboros Chronos to resolve the clock issue. To recover from dishonest majority...Consensus Redux: Distributed Ledgers in the Face of Adversarial Supremacy We want to have state channels, so we have Ouroboros Hydra.

Every time we did this, it built on top of the foundations that we laid so never had a regression. Furthermore, we have thousands of citations. The GKL Paper had 800 plus citations from Harvard, MIT, Oxford, Stanford, Peking University, University of Tokyo...etc...all across the whole world. What

does it mean? They've read our stuff; they think our stuff is novel...and they're building stuff on top of our stuff.

Look at the first paper Ethereum published on Casper^[787] ... within a few months of publishing it, there was already an attack discovered by a Professor at Stanford.^[788] We're so far ahead of these guys on the theory side and engineering side. We rolled out the ITN (Incentivized Testnet), we spent 6 months building a stake pool population, learning the mechanics of staking, getting the parameters right...before we did the Shelley hard fork. Then we did the Shelley hard fork, we have the hybrid era where we gradually move from OBFT to Praos. We've had no disruption, the network has never stalled, have we ever shut it down....no... it's always been up 24/7, always had great checks and balances, tons of transparency.

That's how you do it in a professional, adult way. We talk to the government and Fortune 500 companies...and we say you should run your elections on this system, you should run your bank backend on this system, your healthcare system... What are you going to do to prove yourself otherwise!?'oh here's me at an event dancing in a unicorn costume...but we have to shut the whole network down because of a clock issue or something like that.' They're just going to say no, we can't do that, we don't trust the system.

As for on-chain governance, we have such a lead there... Ethereum is not even doing it, Ethereum 2, Vitalik says oh you can't do blockchain governance^[789]...but then I ask what do you do when you have 100 million users? How do you avoid another Ethereum Classic or a Bitcoin Cash? How do you upgrade the system? Bitcoin can't upgrade...they all know smart contracts are necessary, they all have to get higher throughput and the Lightning Network^[790] is a good idea.... despite everyone knowing this in the Bitcoin community, they can't hard fork. It takes so long, and look at their population size, it's only a few million users today.

So what the hell happens when there's half a billion users in that system? They will never upgrade again! Whereas we have a governance system. We have the hard fork combinator, we have the Voltaire framework, there's on-chain voting, we have the CIP (Cardano improvement proposal) process. So at the end of 2021 it's just going to be buttery smooth for Cardano. Even if we have half a billion users, there will be an upgrade path.

So what does a corporation know? I'm never going to have a Cardano Classic or a Cardano Cash. It's going to be one network, it's stable and I'm building on granite. The code works, the formal methods work, the science works, and the community works. It's just that simple, I'm so tired of these elitist people in the Ethereum ecosystem who pretend their shit doesn't smell, everything they do is just going to work out...and when it blows up and hurts people, then it's all an experiment! It's all just a beta-test. No, sorry when you're dealing in DeFi and your valuation is in billions of dollars, you have retail investors, and you got paid up front, so you don't give a crap... and then you blame the very people who were there. No accountability again and again. They adopt this 'move fast and break things' attitude...that works when you're a social network, when you control the entire server and you can roll things back and the worst thing that can happen is Bobby loses his pictures.

That doesn't work when a person's property, identity and savings... What if your voting system is blockchain-based and it collapses? You won't know who the president is, you'll lose your audit log, etc. How can you ask for mission critical systems to be put on your system? ... when you say ...'well it's an experiment, it's a beta-test, it's an experiment, move fast and break things, code isn't law...who cares....no peer-review is necessary, it slows us down too much.' It's an insane viewpoint and it's just immature, irrational and it's ultimately very damaging because you're handing the bill to somebody else.

No matter how good your product is, life changes, technology improves.... there's always an upgrade required. We invited Vint Cerf, the creator of the internet, to the Shelley summit. The topic was... ‘now that you’ve had 40 years to think about it, what would you do differently?’ When he created the internet, there were 30 computers, so they weren’t predicting billions of computers, and they’re mobile with people carrying them in their pockets. Nobody would have believed that. That’s why the internet has issues today, so you’re going to need an upgrade system. No matter how good your system, there’s going to be surprises, every 5 years you’re going to have to pull something out of the closet and upgrade things. What’s so patronizing about Bitcoin maximalism, or lack of on-chain governance, is that there’s no disaster recovery plan...you’re just stuck. Oh well, just got to live with it! It’s like herpes, we’re going to have it forever, there you go!

Fund9

Catalyst’s relentless, Borg-like momentum continued with Fund9 opening in June 2022. It will roll through until voting commences in August. There is typically something new and innovative with the arrival of each fund, and this time Cardashift^[791] joined the Catalyst Natives program.^[792] Their challenge was based on value creation through positive impact-oriented projects. Cardashift list Cardano’s ‘green’ credentials, it’s focus on Africa and its deterministic nature among their reasons for partnering with Catalyst in their medium blog post.^[793]

As with every quarterly fund, the rewards for successful proposals increased. The Fund9 launch guide^[794] outlines how the 16m ada will be allocated.

Chapter 9: Basho (Scalability)

'The journey itself is my home'

— Matsuo Basho

Scaling in 2022

Unlike many blockchains who adopt a ‘move fast and break things’ approach, Cardano has always stuck to a deliberate, careful and methodical strategy focusing on security, network stability, formal programming for smart contracts before obsessing about the coveted ‘one million TPS (Transaction per second)’ claim. Despite this relative conservatism, Cardano was the most developed crypto project on GitHub in 2021.^[795]

The holy grail of the blockchain world is resolving the scalability issue. This is a big focus for Cardano in 2022. The time has come to develop and create blockchain scaling solutions using a principled, evidence-based methodology. Cardano’s Basho era focuses on performance improvement and scalability now that the fundamental smart contract functionality has been implemented with the Alonzo (Sept 2021) and Vasil (summer 2022) HFC events.

Cardano has always been focused on solving the basic blockchain trilemma of scalability, security, and decentralization. IOG have always followed a set, clearly structured path to deliver on Cardano’s capacity and meet its long-term promise as the company entrusted with constructing the core platform.

IOG developed a strong, secure platform suited for the future using formal methods and Haskell code — with deep roots in a peer-reviewed academic philosophy — built for correctness. Byron was the name given to this era. IOG’s efforts have sparked an awesome community, and Cardano now boasts one of the most decentralized proof-of-stake networks in the world, thanks to a community of over 3,000 stake pool operators. Shelley was the era of decentralization and stake pools.

Goguen (which includes the Alonzo and Vasil HFC events) introduced essential smart contract functionality, which opened the door for DeFi and DApps. With the first Plutus capabilities in place, IOG is working with a growing community of developers to improve the expressiveness of the Plutus language and the entire offering.

IOG detailed their systematic strategy to prepare Cardano for its anticipated expansion this year in a blog post.^[796] As more decentralized apps migrate to Cardano, and as the decentralized finance (DeFi) and ‘RealFi’ ecosystems develop and adapt, the blockchain must be able to keep up.

Cardano is now in the Basho era, which will concentrate on optimization, scalability, and network expansion. IOG expect a large increase in transactional traffic and this chapter outlines their plan to accommodate it.

IOG will be implementing their research throughout 2022. Adjustments to parameters, changes, enhancements, and other innovations will all contribute to Cardano’s capacity and throughput continually improving this year. While keeping the careful, cautious approach that has served Cardano well in the past, IOG anticipates periods of increased demand and, at times, network congestion. It will be an interesting adventure with usage rocketing. While users may get restless at times, the approach remains the same. Here’s how IOG intends to optimize and expand as the number of users rises.

On-chain solutions encompass block size increases, pipelining, input endorsers, parameter adjustments, Plutus script enhancements, node enhancements and on-disk storage improvements. Off-chain solutions include sidechains, Hydra, off-chain computing and Mithril.

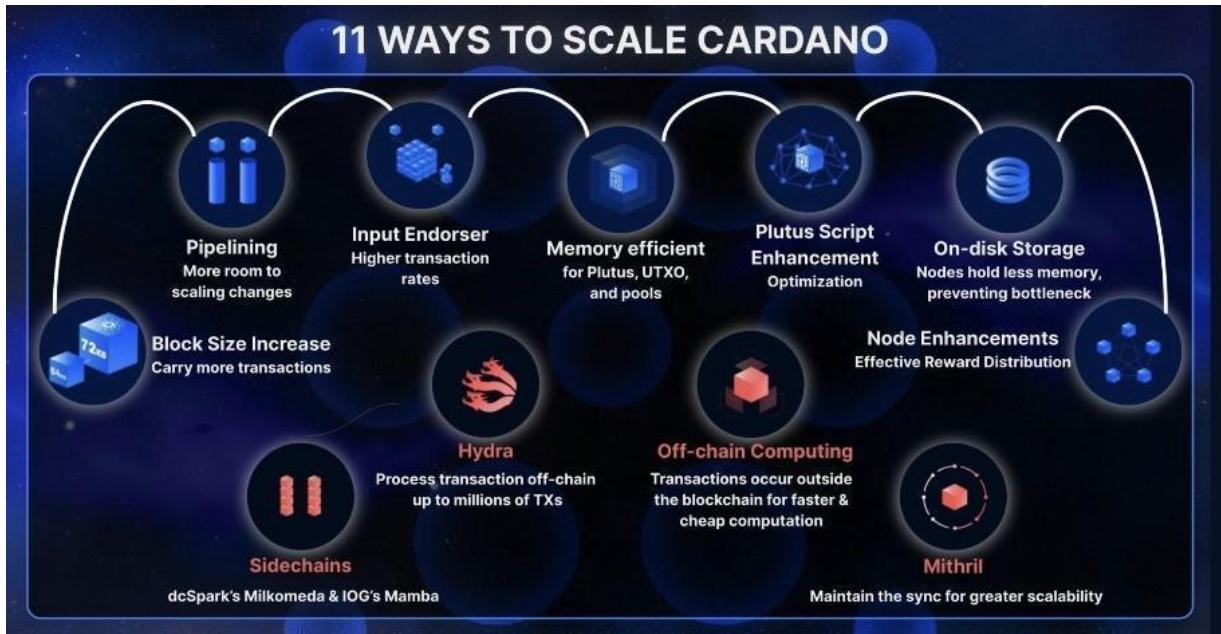


Figure 60: 11 Ways to scale Cardano

April 20, 2022, '4/20 Hangout with Charles' Twitter space, Re: The slow way is fast way^[797]

...there needs to be patience because sometimes things take a little while to solve. We made certain design decisions. For example, the throughput on Cardano....now in the long term, those decisions, I think everybody is going to be so happy with because we get everything the other guys got, but we don't have to kick the network every 15 minutes to reboot it, we don't have to take the video game out of the Nintendo, blow on it to get the damn thing to work, Ok, but those design decisions take time and effort to implement... starting with pipelining and then input endorsers, and then the broader sidechain roll out and state channel ecosystem that comes...

At the end of the rainbow, you're happy, but in the interim, it takes time...Now right now, because people are in the thick of it, it's a vector of attack for people outside the ecosystem. They're being very destructive, they're just running around... just diarrhea flowing out of their mouths, talking about how slow Cardono is.

Ok great, I'm fully aware that Cardano is not the fastest cryptocurrency in the world, but don't you understand that we actually have all the protocols prewritten?... and we know how to get that to the next level, and when we do, it's safe and secure and has all the properties that you've come to know and love, but at the same time it's now faster than everybody else. They say, 'yeah, well, you know that's six months or whatever it takes to get there. You will lose all this network effect...and everybody is going to go away'...I'm like dude, people are tattooing the logo on their body, I don't think they're going anywhere...come on.

...but these are tradeoffs, right? And so just because you have an issue come up, sometimes the solution does take some time and patience to work the way through. Like, for example, we need to get a voting center into our wallets. I've been the biggest proponent of that.... God I have yelled at my people more than I think I've ever yelled about anything else, about the voting center... and I even outsourced a big chunk of work to speed up getting a voting center in.... because it's important to get people voting.

Oh my God though, the headache that's going to be once that actually happens. When you see, for the first time ever...huge amounts of people, tens of thousands, hundreds of thousands flooding in voting on things they know nothing about, and there's going to be a huge education curve. Lots of discussions, lots of stuff on Reddit and Telegram.

It's going to be so frustrating, but it's a necessary growing pain, because on the other side of it, you'll eventually have a highly engaged group of people where we have the largest voting set of any cryptocurrency, by percentage, but we have to pay to get there, and that payment is in patience, and that payment is in education, and that payment is in the fact that everybody's not going to do things right the first time and so forth. ...and being

able to kind of work our way through all of that. And that's just how it ought to be done.

Bitcoin was not built in a day. Great things are not built in a day. Any great thing you see, it has something in common... It took a damn long time to get there, but if you build it right, it stands the test of time.

Block size increases

Two major changes were made to the network to increase throughput. The first was an increase to the block size from 64 kilobytes to 72kb, to 80kb and all the way up to 88 kilobytes in April 2022. That was a significant increase immediately enabling more transactions to be fitted in a block. IOG planned on increasing that block size again and to lead to a place where you could have more than 4 scripts in a block. So the goal was to be able to eventually support up to 5 or 6 scripts on the block.

The second change was an increase to the amount of memory units (abstract memory units) available to each script in the block. Scripts express various kinds of logic in order to spend UTXOs. IOG allowed these scripts to basically make use of more memory than they had previously, an increase of 12.5% and they intend to do that again, another 12.5% increase soon after. IOG has given 40% more memory resources, so it used to be 10 million units, and now 14 million units.

Throughout 2022, IOG is going to introduce some significant changes in relation to layer one throughput. So features like pipelining, which is the concept that IOG established as a new secure way to propagate blocks through the Cardano network prior to validation. This will allow them to have a significant increase of layer one throughput.

There were more than two million Cardano wallets in circulation in December 2021, heading towards four million as of March 2022, [\[798\]](#)

and traffic had increased by more than 20 times in a year (from fewer than 10k transactions per day in November 2020 to 200k+ transactions per day in November 2021). The block size was becoming a critical factor due to the expected increase in traffic as developers rolled out new DApps. Larger block sizes allow more transactions to fit within a single block, giving users additional capacity. Cardano is processing more transactions per second, or - a more meaningful statistic^[799] – more data throughput since it can fit more transactions into a block.

Previous updates meant you could then fit more in a block, and it meant that you can effectively write a Plutus script which was more sophisticated, with basic transactions being roughly 300 bytes on average. These limits have been carefully adjusted to guarantee optimal network use while reducing transaction latency. Users will experience longer block adoption times if the number of blocks is raised dramatically all at once. That's because throughput and timeliness are at odds: boosting throughput means greater network performance, but it might come at the expense of delays when the system is overburdened.

At a transaction level, where there are limits around how much resources exist for a Plutus transaction, a smart contract can use memory and CPU, and there are also block level limits. It's important that block level limits are scaled up so that the transaction-level increases are already provided. IOG wanted to make sure that they expanded the block level limits too. So they've already taken them from 50 million memory units for the block to 56 and subsequently up to 62 million.

IOG didn't want to make changes that introduced any kind of risk of affecting the security of the network, which was and is one of the primary concerns. So how did they make sure that this didn't cause any issues? Making these changes in mainnet, they were made in reasonably moderate sizes. 12.5% is reasonably big, but it's not too big... and so IOG's philosophy is to make slow and steady changes by increasing these limits until maximum throughput is hit.

IOG has a number of tools for monitoring to make sure that they don't blow through the 5 second budget. So they not only have their own metrics built into the node, but also metrics from the SPOs and also third-party metrics that they watch meticulously to ensure that there are no issues on the network.

This was the first change on the network and the first of many coming into a period where some major decentralized exchanges were going to be launching on the platform. There are more and more community-built projects that are going to be launching tokens, coins, NFTs, etc.

Parameter Adjustments

Cardano is, in a sense, a living organism that evolves and increases with each evolutionary step. While its roots are built on granite core research, flexibility, including the ability to modify whole protocols through the hard fork combinator (HFC), has been built in from the start.

Updating parameters is key for a flexible infrastructure that can bend, but not break, as conditions change. While there will always be some who wish to 'move fast and break things', IOG's emphasis will be on a gradual, safe progression as Cardano's scope and usage expands.

The way the system operates as a whole while processing, validating, and signing transactions determines network performance. If you want a system that will last for a long time, doing this right from the beginning of the design process is critical. However, since network bandwidth is a precious resource, it is critical that compute, memory, storage, and network resources be used efficiently for the best performance metrics.

Cardano is designed to be adaptable. It is meant to enhance throughput while allowing for increased demand responsiveness. As

the network expands, IOG are fine-tuning protocol parameters to account for price swings, boosting scalability, and throughput requirements. So let's look at how IOG plan to improve network performance over time.

Congestion

Efficient systems, from networks to highways, are designed to reduce congestion while allowing for efficient management in the event that it does occur. Congestion on the blockchain means that the network is overburdened and has difficulty processing huge numbers of transactions and signing corresponding blocks. In late 2021, Cardano blocks used around 25% of capacity throughout a given epoch, indicating that the network was not overburdened and that there was sufficient spare capacity to execute even more transactions.

Cardano is built to be fair and robust, even in the face of heavy demand. The following metrics are used to calculate current performance metrics:

- Throughput: the amount of data transmitted. The block size was set at 64 KB. Plutus script transactions were restricted to 16 KB, with basic transactions being roughly 300 bytes on average. These limits have been carefully adjusted to guarantee optimal network use while reducing transaction latency. Users will experience longer block adoption times if the number of blocks is raised dramatically all at once. That's because throughput and timeliness are at odds: boosting throughput means greater network performance, but it might come at the expense of delays when the system is overburdened.
- Timeliness: the time it takes to adopt a block. The entire 'budget' for block adoption is set at 5 seconds for a block to spread through 95% of the network, with Plutus scripts having a budget of around 50 milliseconds. This is done to avoid monopolization

by allowing the block to contain both scripts and simple transactions.

Users have reported [800] longer transaction processing times as a result of huge NFT (non-fungible token) drops. The reason for this oversaturation is because a large number of NFTs were launched at the same time, resulting in the following:

- A significant number of NFT transactions occurring at the same time
- Several users attempting to buy the same NFT at the same time, resulting in multiple transactions being processed at the same time
- Reimbursed transactions for users who were unable to acquire the NFT at that same time.

This situation resulted in network scarcity for NFT sales, resulting in a massive demand for the service. However, it's also worth mentioning that the 'congestion' only lasted less than an hour.

This is a rapidly expanding business, and NFT creators are already adapting their methods to reduce the effect of such drops on the customer experience. It's still early, and the industry is evolving at a rapid pace. It's worth noting that the process of minting NFTs can be run in parallel, which means there's no theoretical limit on how many NFTs can be minted. Once minted, NFTs storing the programmable swap code and assets needed to transact are ready to participate in the market.

However, in the short to medium term, it is more important to develop more efficient traffic systems rather than expanding roadways. Some developers are already developing such solutions expressly for NFT drops, which should lower costs and network loads.

IOG alleviated NFT drop congestion by spreading the stake distribution and reward distribution computation more widely. As a

result, they are able to raise block size, remove delays and congestion at epoch bounds, and reduce computational spikes (which cause block propagation to slow down).

Decentralized exchanges (DEXs) on Cardano

DEXs, or Decentralized Exchanges, are among the first DApps established on Cardano. Furthermore, with certain apps, consumers were encountering delays. Because their DApp architecture requires that the whole state be stored in one UTXO (rather than being split over numerous UTXOs), a future transaction becomes reliant on a prior transaction's output. The 'problem' of concurrency has been extensively discussed by 'experts' on crypto twitter. Coding DApps with Plutus does have a learning curve, but it's simply a new method of doing things. Sure enough, if a developer does not adjust to this new approach, they will run into issues. It isn't always more difficult; it just requires a different approach.

When creating DeFi applications, Cardano's EUTXO paradigm removes whole classes of challenges. The deterministic aspect of EUTXO, in addition to its native ability to execute transactions in parallel, guarantees that developers and users avoid wasting 'gas' on extortionate transaction fees. The EUTXO paradigm, however, is not the same as the account-based approach. A poor application design will arise from lifting and transferring application architecture built for account-based systems to an EUTXO-based system. The optimal user experience will be provided by applications created expressly for Cardano's EUTXO paradigm.

DApps developed on Cardano should move away from single-threaded state machines and instead create a solution that utilizes concurrent edges in the EUTXO graph by going down a level of abstraction to the EUTXO directly. It is critical to employ various sets of UTXOs to enforce parallelism, which will increase system throughput while maintaining individual operation speed.

Any developer familiar to Ethereum's methodology will have to change their approach. UTXO-based models, on the other hand, are more secure than account-based models since putting all state in a single account makes it more susceptible to attacks. Users will benefit from higher throughput and scalability if parallelism is employed effectively. Off-chain alternatives are also well suited to UTXO ledgers.

January 10, 2021: Will decentralized exchanges kill centralized exchanges? CH:[\[801\]](#)

I think in the next 10 or 20 years, it's definitely a possibility.... it's a better business model, it's more aligned with how crypto assets work. You don't need a trusted third-party custodian. The problem is there's just front-running, efficiency, fees, market depth and liquidity ...so a lot of problems there and so it's really hard to get at a decentralized exchange working in tandem with centralized exchange...but to be honest, decentralized exchanges have made enormous progress in the last 5 years. When I started it was a pipe dream, but now it feels like an inevitability.

Incremental optimization in 2022

Prior to optimizing, IOG's emphasis at launch was always on providing fundamental capabilities and accuracy. This has been their declared objective from the beginning while keeping an eye on performance and make modifications as needed. IOG adjust parameters to keep up with network demand as the network expands and Cardano runs at a greater capacity. These are incremental enhancements that will be phased in over months to ensure that modifications fulfill network needs while not jeopardizing other properties.

IOG conducted a thorough investigation and began to implement node metrics that correctly measure data diffusion time. The process of disseminating transactions and blocks among nodes that validate

the blockchain is known as data diffusion. It is critical to deliver the necessary information to nodes so that the consensus algorithm can make judgments.

IOG will probably implement an average wait time between transaction submission and adoption. In addition, they're looking into and evaluating situations that can improve network performance in the short and long term, such as:

- **Increased block size** - a larger block size equals more transactions per block. During instances of network saturation, there will be reduced waiting time for transactions to be accepted by a block, which is a positive. There is, however, a cost. It takes longer for larger blocks to propagate throughout the network. Nodes will also need additional time to validate transactions as a result of this. Although increasing the block size might improve network speed, such adjustments should be done with care. IOG progressively alter settings and monitor the outcomes during high saturation times to guarantee that the increase does not impact block adoption time. There isn't a one-time update, but rather an iterative process that will provide clear findings and enable efficient changes
- **Mempool size:** The size of the mempool was initially set to 128 KB, which is twice the size of the block at the time. When adding transactions to a block, the mempool acts as a network buffer and may cause a little delay. However, increasing the size of the mempool will not boost network throughput since transaction queues would remain the same. The mempool enables for a fair adoption of new transactions that arrive at random
- **Script compression** — with the initial transaction size of 16 KB (subsequently increased), IOG implemented compression, which enabled the protocol to transparently ‘zip’ the code. Because of the smaller size of script transactions, one block could contain more. Developers were able to submit more

complicated code compressed to 16 KB or less, leaving more room for other transactions. This initial tactic was subsequently discarded.

IOG were looking at script compression as a technique to squeeze more scripts into blocks. This was before there were bigger blocks and more memory units available to scripts in general. Script compression simply became obsolete. If script compression was still performed, it would be an extra step in the process, it would be something that would require having to change the structure of the chain because scripts from certain eras would be uncompressed, and in later eras compressed, so it just wasn't an optimal solution and IOG decided to drop the idea because features like pipelining and input endorsers basically make it redundant.

Gradual, deliberate iterations

As Cardano keeps growing and iterating, there is a lot of work going on behind the scenes. It is still early stages, so IOG keep an eye on network performance and tweak settings as needed. Cardano is a permissionless decentralized blockchain that is available to anybody who wishes to use, or develop, on it. Many new users have joined the Cardano ecosystem as a result of recent hard forks (which included native tokens and smart contract functionality), and there's been a significant increase (and spikes) in transaction volumes and network traffic.

IOG expected considerable rise in network activity when fundamental components, such as wallet connections and the Plutus Application Backend (PAB), were completed and fully deployed onto mainnet. A slew of Cardano-based projects (see Essential Cardano, essentialcardano.io) began to roll out, first on the testnet and later on the mainnet.

There will always be a lot of traffic surrounding the debut of new decentralized apps (DApps). IOG began making a series of network

parameter changes to handle this continued increase and guarantee that Cardano maintains its durability and stability. Cardano's usability and experience will continue to improve as a result of these parameter modifications throughout its entire user base.

Built for growth

Ouroboros is built to manage massive amounts of data, as well as transactions and scripts of various sizes and complexity. The Cardano network initially only used around 25% of its capacity on average, based on current specifications. This is inefficient since the most efficient case is for Cardano to operate at or near 100% capacity (the network being 'saturated').

While many networking systems would suffer in such circumstances, Ouroboros and the Cardano network stack have been built to be fair and very durable, even in the face of extreme saturation.

Congestion is minimized by efficient systems, which also leads to efficient management when it does occur. Cardano's network utilizes 'backpressure' to control overall system stress. While certain individual users may report higher transaction wait times during a big NFT drop, this does not indicate that the network is 'struggling.' It really signifies that the network is working properly. It's known as graceful degradation, [\[802\]](#) and you can learn more about it in the network design paper. [\[803\]](#)

IOG is also considering a queueing mechanism to boost performance. Ethereum already has a one queue system where on-chain transactions rely on fees paid. The more you pay, the greater chance of skipping the queue and being served. This has been infuriating for many users, as extortionate fees became the norm. IOG are considering three queues with no fee 'auctions'. Instead, it will be based on admission control, with new transactions served and posted on-chain on a first-come, first-served (FIFO) basis.

Tweaking parameters

Apart from the original architectural design and extensive benchmarking across a variety of simulated scenarios, IOG can only fully evaluate demand and the efficacy of any adjustments in actual real-world usage. IOG started to make gradual adjustments on mainnet December 1, 2021, based on extensive benchmarking and developer feedback, and submitted two initial changes.

IOG increased the block size and intends to proceed with subsequent block size modifications in a ‘slow and steady’ manner to make the underlying network capacity accessible to end users while guaranteeing that they can continue to function effectively as a global decentralized blockchain.

The latest version of Ouroboros (Praos) has precise criteria that must be fulfilled to achieve its security objectives, with block propagation time being one of the most significant characteristics. Block propagation time refers to how long it takes for a newly minted block to be propagated through 95% of the staked ada nodes on the network. In order for Praos to remain secure, new blocks must be propagated every 5 seconds.

This 5s limit is seen by IOG as a ‘budget’ that they may use to increase the block size, for example. Increased block size would automatically lengthen the time it takes to propagate blocks; thus they must carefully monitor any modifications they make to improve speed without jeopardizing the network’s security. This budget will be expanded in future Ouroboros iterations. Meanwhile, IOG will concentrate on preserving security while extending the network to meet increased demand.

Plutus requires resources and both computational (CPU) units and memory units in order to do useful things with a Plutus script. They started off with 10 million units on Plutus, then moved to 11.25 million and 12.5 million and eventually to 14 million.

This was a significant update that DApp developers welcomed.

Plutus memory limitations were extended, allowing them to create more complex Plutus scripts or allowing current scripts to handle more data items, enhance concurrency, or otherwise extend their capabilities. This was the first in a series of adjustments to the memory unit parameters that would significantly improve Plutus scripts' real-world capabilities. IOG implemented the modifications gradually but slowly, exactly as they did with block sizes, to let the network and SPOs to cope with the elevated demand.

Many DApp developers requested the adjustments outlined (increased block size and Plutus script memory units per transaction). Both of these adjustments are intertwined. It isn't merely a matter of writing more complicated scripts. It's also about pushing more information through the system.

Steady, as she goes

Every update to the Cardano platform will be carefully examined as it progresses, and once implemented, it will be closely watched to see how it affects performance. All adjustments will be based on network-derived empirical data and real-world, long-term user demand. It is critical not to make choices having a long-term effect in response to short-term spikes in network traffic. IOG will not make modifications prematurely or at a rate that jeopardizes Cardano's long-term security.

The development of Cardano is based on both fundamental and continuing research. Further network upgrades in the midterm will result in significant capacity increases as well as network optimization to provide the greatest overall experience.

This is about constructing new and competent blockchain infrastructure based on cutting-edge decentralized technology. IOG will first concentrate on a variety of performance enhancements that will allow them to take advantage of the protocol's limits. They'll next concentrate on minimizing the size of Plutus scripts as well as improving the efficiency of the Plutus interpreter and Cardano node

implementations. They will be able to process more interesting work while staying within the same protocol parameters.

Decentralization Parameters

Another area of intense discussion amongst the SPO community has been around the decentralization parameters and former IOG Director of Architecture, John Woods, has had calls with over 250 SPOs to understand the concerns in the community about certain decentralization parameters. Since the d parameter had been '0' for over a year, it will be completely removed from the protocol as part of the Vasil hard fork. It was another milestone on the road to complete decentralization, with the community now permanently responsible for block production.

Measure twice, cut once

IOG are very deliberate and cautious with these changes but ultimately, they are hitting an average of a change every three weeks. For a network as nuanced and sophisticated as Cardano, which has a global uptime approaching 100%, this is a relatively aggressive cadence.

IOG are also looking at how big a transaction is allowed to be, how many CPU units are available to Plutus, and other economic parameters that they've discussed with the SPOs. IOG is scaling the platform so that it has the bandwidth to contend with the demand that's placed upon it. So the changes and hard forks allow it to grow out scalability aggressively and also, when IOG adds things like pipelining and input endorsers on top, it enables even more scope to make further enhancements.

Pipelining

Before Vasil, a block was minted by an SPO, that's a new block in the blockchain that had to be validated and sent onto a peer. The problem was that peers also had to validate it and then send it onto

their peer and that's how the blocks diffused across the network.

By combining validation with propagation, the time it takes for a block to propagate is reduced. By minimizing the 'dead time' between blocks, the objective is for blocks to be propagated to at least 95% of peers within 5 seconds (block propagation overhead). This allows flexibility to make more drastic scaling adjustments, such as raising block size, or other Plutus parameter limits.

Pipelining is a natural progression of Cardano's 'plumbing.' It's an important part of the scaling strategy for 2022, and one of a series of stages outlining IOG's logical approach to ramping up Cardano's capacity as the ecosystem expands. IOG need to make sure that the underlying protocol, Ouroboros Praos, is fast enough to support the myriad of DApps that are now being developed, or in the works for Cardano.

Throughout this process, it will be critical to keep a careful eye on real-world network performance and, more crucially, the cumulative effect of parameter changes. IOG carefully monitors and reviews each update for at least one epoch (5 days) before proceeding with subsequent changes. A decentralized network architecture must be scaled depending on real-world usage, notwithstanding the substantial research and technical effort that has gone into creating and installing the system.

Diffusion pipelining

Pipelining, or more specifically, diffusion pipelining, is a consensus layer innovation that allows for speedier block propagation. It allows for more headroom, allowing Cardano's performance and competitiveness to improve even more. It's important to understand system behavior of how blocks propagate, to see how this strategy accomplishes its purpose.

As it passes around the chain, a block goes through 6 stages:

1. Block header^[804] transmission
2. Block header validation
3. Block body request and transmission
4. Block body validation and local chain extension
5. Block header transmission to downstream nodes
6. Block body transmission to downstream nodes

The path of a block is highly sequential. At each node, all steps occur in the same order every time. Block transmission takes a long time due to the large number of nodes and the ever-increasing quantity of blocks. Diffusion pipelining layers some of the above stages on top of one another, allowing them to happen simultaneously. This takes less time and boosts throughput.

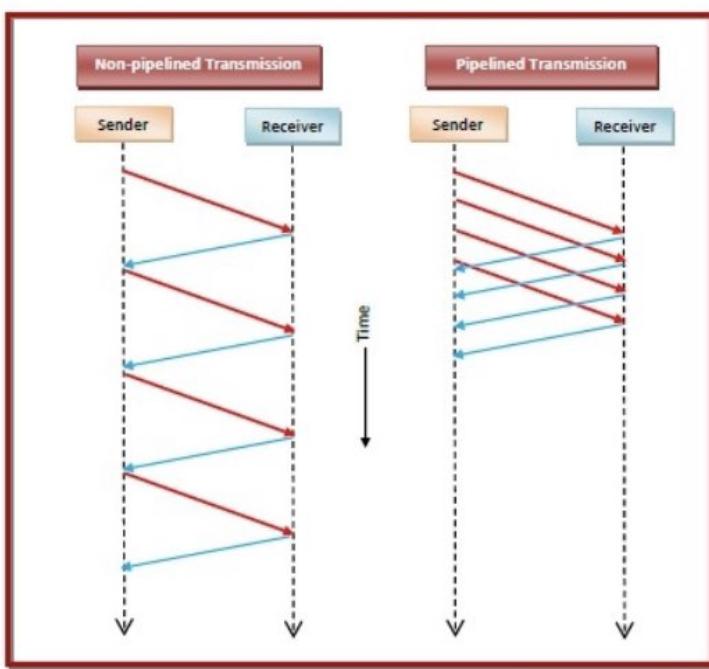


Figure 61. Pipelining (courtesy of @jJosjuaThreatt tweet)

The time savings provided by this technique will allow Cardano to expand even further, including adjustments to:

- Block size – the larger the block, the more transactions and scripts it can accommodate
- Plutus memory limitations - the maximum amount of memory that a Plutus script may use

- Plutus CPU limits - a script may be given extra computing resources to execute more effectively.

From theory to practice

Diffusion pipelining was created with the goal of achieving quicker block propagation while avoiding ‘destructive’ alterations to the chain. Because nodes depend on these current approaches, IOG did not want to eliminate any of the protocols, primitives, or interactions currently in use in Cardano. Instead of modifying how things operate now, they’re establishing a new mini protocol whose purpose is to pre-notify subscribing entities when a new desired block is detected, prior to full validation. Implementing Pipelining doesn’t require a hard fork and can be rolled out with a standard node release. It was scheduled to coincide with the Vasil hard fork.

The ability to pre-notify peers and provide them a block before it is verified, allowing the downstream peer to pre-fetch the new block body, is the most significant feature brought by pipelining. This saves a lot of time since the time it takes to verify a block over several hops is reduced significantly.

On-disk storage

IOG are acutely aware that the Cardano node needs RAM^[805] when it’s running. They want to start moving things out of RAM, out of that expensive volatile memory into on-disk storage. This is a common practice in computer science. On-disk storage will improve the user experience for developers on Cardano.

By storing elements of the protocol state on disk, nodes will use less memory, allowing RAM-starved systems to operate nodes as long as they have enough storage, and memory will no longer be a scaling restriction. The blockchain state will be able to increase significantly as a result of this.

Plutus script enhancements

IOG wants Plutus to be a great developer experience when building DApps on Cardano. They want to eliminate friction for developers. They don't want to have a situation where developers have to do more work than is necessary. So IOG listens to developers, they spend time with the community at large and with the open-source space, investigating what obstacles have been causing the most friction. As a result, there were three CIPs implemented with the Vasil hard fork to enhance the way Plutus operates, to make things easier for developers. All three dovetail together and complement each other.



Sebastien Guillemot
@SebastienGilmot

...

Pretty cool: 50% of the Cardano ledger changes for the upcoming Vasil upgrade were CIPs (Cardano Improvement Proposals)

Smart contract optimization allows for even more efficient use of the advanced EUTXO model, including reference inputs, inline datums and reference scripts.

Reference inputs (CIP-0031) [806]

Plutus scripts may view transaction inputs without spending them. This means that inspecting the information held by an input does not require the creation of UTXOs.

Oracles are built as DApps, and an oracle might typically provide something like the price of the euro versus US dollar. The way the oracles worked previously was that they stored that value as part of a datum on a UTXO. A UTXO held the value of the dollar in a little piece of data, or 'state'. If a developer was building a DApp on-chain, and they wanted to use that piece of information that's on the chain, they had to take that UTXO, include it in their transaction and use it and then on the output, they had to recreate the UTXO for someone else to use with the same value. This worked but was suboptimal.

It makes more sense if you can read the value sitting at a UTXO, like an oracle value or some other piece of data, without having to spend the UTXO itself. Reference inputs enable this feature. It allows users to reference the state at a UTXO without having to spend and then recreate it. This improves concurrency because you can then have many users reference an input without waiting for the output from the previous user. This enhancement dovetails well with reference scripts.

Ergo, pioneers in the UTXO space, already introduced a similar concept called ‘data inputs’^[807] in 2020.

Inline Datums (CIP-0032)^[808]

Instead of using datum hashes, Datums may be connected directly to outputs. This makes it easier to utilize datums since the user can now see the actual datum instead of needing to provide the datum that matches the supplied hash.

A datum is a little piece of state such as a ‘save player profile’ or a leader scoreboard in a game. It lives in a UTXO as a little bit of data, and that is used by DApp developers in different ways. It could be to store a public key so their app can verify who’s allowed to do something with the app. Prior to Vasil, the datum wasn’t actually stored on-chain. Instead, a hash of the datum was stored, and it was the responsibility of the user who was interacting with the contract, in their transaction, to include the script and the datum.

This was doable, but again, a bit of a pain. Since Vasil, developers can store the datum physically on the chain, not just its hash, but the actual datum itself.

Reference scripts (CIP-0033)^[809]

Plutus script references can be linked to transaction outputs, allowing them to be stored on-chain and reused later. It means you

are no longer required to provide a copy of the script with each transaction, thereby reducing developer friction. Using the same script in several transactions decreases transaction sizes, boosts throughput and lowers script execution costs.

Before Vasil, developers had to share the scripts offline so that they could be included in transactions. The likes of SundaeSwap and WingRiders (both cFunded) had the resources to build websites with UIs to handle the user experience nicely. However, it was harder for smaller developers and tricky to share those scripts with different people so that they could interact with their DApp.

Reference scripts allow developers to put Plutus scripts on-chain and then, rather than include them in a transaction, they can instead include a pointer in the transaction that just references that script on the existing chain. That means that a user doesn't need to have a copy of this script to interact with it. You just need to let people know the address it's at, and then users anywhere can use the same script and point to it.

This enables a use case where a developer can put reference scripts on-chain and allow others to use them as a library. There could be a number of libraries considered to be core to Plutus, and IOG will put them where anyone can use them and then publish the address. This allows anyone in the ecosystem to take libraries and make them available to the wider public, a powerful enhancement.

Looking at all three CIPs holistically, these enhancements push Plutus forward and make developers' lives easier. IOG is putting more on-chain, freeing developers from the need to monitor scripts and share scripts. This frees developers from the need to monitor and share datums and increases concurrency by allowing users to interact with UTXOs.

Node enhancements

Improvements allow for a more uniform distribution of stake and reward calculations over epochs, allowing for larger block sizes. Memory use is also more efficient overall. Memory compression minimizes RSS^[810] footprint, while memory sharing reduces the amount of data that needs to be instantiated. From January 2022, node version 1.33.0 minimized demand at crucial points, such as the epoch boundary.

Nodes on the network

The node is the heart of the Cardano network. As Cardano expands in 2022, nodes will play a key role. Improvements to the core node are part of this, and node v1.33.0 was jam-packed with features and enhancements to old components, increasing Cardano's expressiveness and chain's capacity to accomplish more.

Why nodes matter

Node v1.33.0, which was released in January 2022, was created with simplicity and efficiency in mind. The ongoing enhancements are intended to minimize block propagation time, allowing IOG to make the necessary adjustments to enable DApps, decentralized exchanges (DEXs), DeFi environments, and other technologies.

Blocks have been propagating faster since, providing IOG with more time to execute further improvements. RAM utilization optimization and efficiency optimizations are among the technical changes incorporated in node v1.33.0. Check the release notes^[811] for the very latest.

RAM usage

The new node allowed for a large reduction in memory usage due to two features: memory compression and more efficient memory sharing. Rather than having multiple instances of the same object, multiple flows within the system could now use the same object. Unspent Transaction Output (UTXO) management, stake

distribution, live stake^[812] distribution and pools, and hash representation all benefit from memory optimizations.

These enhancements involved:

- UTXO handling. Node v1.33.0 needed less for transaction inputs
- Stake distribution snapshots take up 35% of total live data. Release v1.33.0 achieved a reduction by a factor of eight by sharing and changing representation
- Live stake distribution makes up 22% of total live data within the system. Node v1.33.0 saved on memory in two ways: Combining multiple maps that are keyed on stake addresses (11 less words per stake address for each map combined) and sharing of stake pool IDs (5 words)
- Hash representation. This release used 5 words instead of 6. This may seem like a benign update, but hashes are widely used throughout the system, so this resulted in big savings.

RAM optimization factors

Due to compaction and sharing, the new node allowed for significant live data reductions. Node v1.33.0 features modifications to the methods that Cardano employs to compute rewards and stake distribution, in addition to making memory consumption significantly more efficient than prior versions.

These adjustments were made to alleviate the unequal network performance that occurred while computing rewards, which resulted in network load spikes. Because of the updated reward calculation mechanism, these spikes will no longer occur. The reward calculation method has been updated from ‘column-major’^[813] over 4,000 pools to ‘row-major’ over a million stake addresses. This enables the calculations to be stretched out across three days rather

than one. The stake distribution formula has also been tweaked to make it more efficient.

Nodes' role in Pipelining

IOG will make ongoing major enhancements to the node later in 2022. A node works hard to process a block, then waits for another block to arrive, and so on. The node is less busy in the interim. Certain strategies may be used to decrease block propagation overhead (that is, the time period when the node is relatively inactive, referred to as 'dead space') and make better use of that otherwise 'dead' time. This is when pipelining enters the picture.

The validation and propagation of blocks are combined in this approach. Instead of obtaining a header, verifying it, then getting its corresponding block, verifying it, and then sending it to peer, now a header is received, verified, and sent to the peer without validating the block. This simplification will allow the network to make even more improvements.

By minimizing block propagation overhead ('dead time'), pipelining will considerably extend the scope/headroom allowing for additional network enhancements.

Incremental updates

The Cardano project has always been committed to building out a secure, resilient and highly decentralized network that can meet the needs of the next decade and beyond. And taking a methodical, responsible long-term approach is central to this. As the old axiom goes, 'the slow way is the fast way.'

Sidechains

A sidechain is a blockchain that is linked to a main blockchain (the 'main' chain, also known as parent chain) through a two-way mechanism (the 'bridge') that allows tokens and other digital assets

from one chain to be utilized in another and the results to be returned to the original chain. As required, assets may be transferred across chains. Multiple interoperable sidechains may be joined to a single parent chain, each of which can function in a different fashion.

Sidechains have many different use cases. Some examples are stablecoins, all the way to things like potentially having a sidechain that can execute smart contracts from other platforms. Sidechains will let IOG take load off layer 1 on mainnet and put it onto a sidechain, all the while enjoying the veracity that's provided by that mainnet layer one. IOG is also looking at off-chain computing which is a potential way to do faster and cheaper transactions via a trust model.

Milkomeda^[814] from dcSpark and *Mamba*^[815] from IOG (released publicly as *Alpha*^[816]) are just two main EVM sidechains on Cardano. Community stalwart 'Big Pey' spoke about it^[817] on his YouTube channel.

In April 2022, Wanchain^[818] launched new bi-directional decentralized, non-custodial cross-chain bridges linking Cardano to other tier 1 blockchains. Wanchain is a decentralized interoperability solution as well as a layer 1 proof-of-stake (PoS) blockchain. Wanchain's layer 1 PoS blockchain is an Ethereum-like ecosystem that supports industry-standard Ethereum tools, DApps, and protocols. It has certain similarities to Cardano. Wanchain employs the Galaxy Consensus PoS consensus method, which employs a number of cryptographic approaches such as distributed secret sharing and threshold signatures to enhance random number generation and block creation processes. Galaxy Consensus is a continuation of Cardano's own Ouroboros protocol, built by world-class researchers and academics.

In the April 2022 Cardano 360, ^[819] IOG outlined their plans to roll out upcoming sidechain(s). As expected, it will be deliberate and iterative...

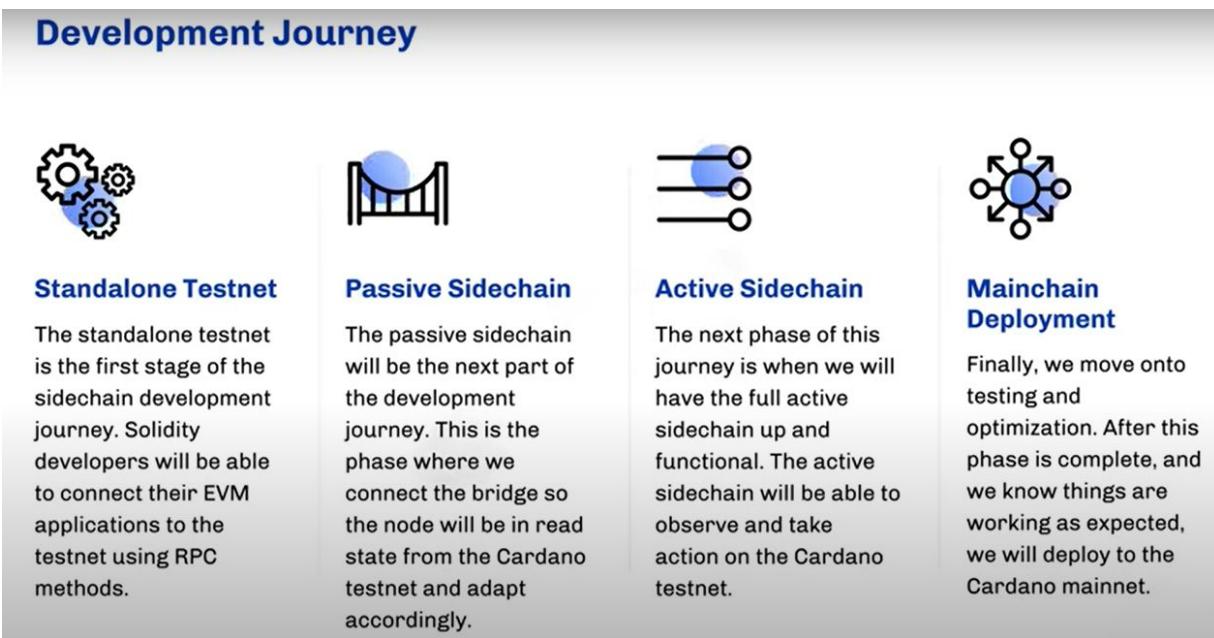


Figure 62: IOG Sidechain rollout journey.

On June's Carano360^[820], Kathryn Stacy, Product Manager for Sidechains, explained how IOG plans to enable more programmability by making it easy for developers to contribute. IOG is granting access to the EVM source code so developers can use the code as a framework to create their own EVM sidechains. The vision is to create an 'ecosystem of ecosystems'.

Hydra

Hydra introduces isomorphic^[821] state channels to increase throughput, decrease latency, save money and reduce storage needs. The most difficult aspect of blockchain adoption is scalability. IOG developed Hydra as a solution for Cardano and related networks using a principled, evidence-based methodology. Hydra is the result of substantial research and a critical step toward allowing decentralized networks to grow securely to meet global demands. Hydra makes it easier to perform transactions off-chain while still utilizing the main-chain ledger for secure settlement. Find out more on the appropriately named website <http://hydra.family>

Considering absolute numbers in terms of certain measures, while analyzing a particular algorithmic design, can be misrepresentative. The reason for this is because absolute values must relate to a certain underlying hardware and network setup, which might muddle the benefits and drawbacks of specific methods. Even if a protocol is badly conceived, it may still operate well enough when used with better technology and networking.

Hydra overview

Hydra is a distributed ledger scaling solution that meets all three of the aforementioned scalability challenges: high transaction throughput, low latency, and minimum storage per node. While Hydra is being developed in collaboration with the Ouroboros protocol and the Cardano ledger, it may also be used with other systems that have the same key properties as Cardano.

Hydra is a system made up of many subprotocols that work together to solve a single problem: scalability. Cardano's ecosystem is diverse, with numerous organizations with varied technological capabilities: the system supports block producers with stake pools, high-throughput wallets like those used by exchanges, and end-users with a variety of computing performance and availability characteristics. It's unreasonable to expect a single-protocol, one-size-fits-all method to provide overall scalability for such a diverse group of network actors.

The Hydra scalability architecture can be divided into four components: the head protocol, the tail protocol, the cross-head-and-tail communication protocol, as well as a set of supporting protocols for routing, reconfiguration, and virtualization.

The centerpiece is the 'head' protocol, which enables a set of high-performance and high-availability participants (such as stake pools) to very quickly process large numbers of transactions with minimal storage requirements by way of a multiparty state channel – a concept that generalizes two-party payment channels as

implemented in the context of the Lightning network. It is complemented by the ‘tail’ protocol, which enables those high-performance participants to provide scalability for large numbers of end-users who may use the system from low-power devices, such as mobile phones, and who may be offline for extended periods of time.

While heads and tails can already communicate via the Cardano mainchain, the cross-head-and-tail communication protocol provides an efficient off-chain variant of this functionality. All this is tied together by routing and configuration management, while virtualization facilitates faster communication integrating head and tail communication.

Hydra head

The Hydra head protocol was the first part of the Hydra architecture to be released. In the optimistic situation when all head participants agree to the protocol, it enables a group of participants to build an off-chain state channel (called a head) where they may execute smart contracts (or process simpler transactions) among themselves without interacting with the underlying blockchain. The state channel provides ‘lightning’ quick settlement and transaction throughput, as well as requiring very little storage since the off-chain transaction history may be destroyed as soon as its resultant state has been secured by an off-chain ‘snapshot’ operation.

Even in the most pessimistic scenario, when a large proportion of users disobey, complete safety is ensured. Any member may begin the head’s ‘closure’ at any moment, transferring the head’s state back to the (less efficient) blockchain. IOG wants to underline that any smart contract’s execution may be smoothly continued on-chain. Off-chain funds cannot be created, and no single, responsive head participant may lose any funds.

Hydra’s state channels are isomorphic in that they use the same transaction structure and contract code as the underlying blockchain, allowing contracts to be transferred directly between channels and

the blockchain. As a result, state channels produce parallel, off-chain ledger siblings. The ledger, in effect, becomes multi-headed.

An asynchronous off-chain certification procedure leveraging multi-signatures achieves transaction confirmation in the head in full concurrency. As discussed in previous chapters, the extended UTXO (EUTXO) model allows for this high degree of parallelism. The EUTXO architecture makes transaction dependencies clear, allowing for state changes without the need for excessive sequentialization of transactions that are unrelated.

Evaluating the Hydra head protocol

A simulation was created by IOG as a first step toward empirically evaluating the Hydra head protocol's performance. The simulation was parameterized by the time necessary for particular activities (validating transactions, verifying signatures, and so on), and it simulates a cluster of dispersed nodes creating a head in a realistic and timing-correct manner. As a consequence, transaction confirmation time and throughput estimations were more realistic.

Simulations showed that a single Hydra head can reach up to 1,000 TPS (Transactions per second), so if 1,000 heads are run in parallel (one for each stake pool in the Shelley release, for example), so it should be able to get a million TPS. That's impressive, and it puts Cardano far ahead of the competition, but it can be pushed further. Two million TPS from 2,000 heads is possible, and if you need a billion, then run a million heads. Furthermore, different implementation enhancements may increase the 1,000 TPS single head measurement, boosting the protocol's possible performance even further.

So, is Hydra able to call whatever TPS number it wants? In principle, the answer is a resounding yes, which highlights a flaw in the prevalent^[822] use of TPS as a system comparison measure. While it's easy to simplify the complexity of evaluating protocol performance to a single number, this leads to oversimplification in reality. A TPS

number is almost worthless without further information.

Clearly, a higher standard is required. Is the Hydra head protocol a good one to use? Will it hit the network's actual constraints, not just a TPS figure? To guarantee that the data IOG present is credible, they adopted the following technique:

- IOG explicitly describes all of the variables that affect the simulation: transaction size, time to verify a single transaction, time required for cryptographic procedures, allotted bandwidth per node, cluster size and geographical distribution, and transaction parallelism limitations. It would be difficult to replicate these numbers without this controlled setting
- IOG evaluated the protocol's performance on baselines that define the underlying network and hardware infrastructure's exact and absolute bounds. How effectively IOG approaches such boundaries indicates how much space for progress there is. This follows the methods outlined above using an encryption algorithm as an example.

For Hydra, IOG utilizes two baselines. The first, Full Trust, is a generic term that refers to any protocol that distributes transactions across nodes and requires each node to verify transactions one by one – even if consensus is not guaranteed. Simply combining the message delivery and validation times produces a TPS limit. Without depending on comparisons with other protocols, how well IOG approaches this limit informs them what price they are paying for consensus.

The second baseline, Hydra Unlimited, offers the optimal latency and storage for any protocol while also yielding a TPS limit for the head protocol. IOG do so by assuming that they can transmit enough transactions in parallel to fully amortize network round-trip delays and that all operations can be completed when required, with no resource congestion. The baseline allows IOG to determine what can be accomplished under ideal conditions with Hydra's general

architecture (for a particular set of input parameter values) as well as compare confirmation latency and storage cost versus any protocol. IOG's paper^[823] (Section 7: Simulations) has further information and graphics.

Comparing scalability ideas to well-defined benchmarks may be a useful tool in the development of protocols. It offers strong proof for the correctness of design decisions, leading to the development of effective and performant distributed ledger protocols that give the greatest available absolute metrics for use cases of interest. While the Hydra head protocol is being created and tested, the rest of the Hydra components will be released in future using the same principles.

What is isomorphism?

Hydra maintains security assurances while being loosely tied to the mainchain by enabling more efficient ways of processing transactions off-chain for a group of users while utilizing the main-chain ledger as the secure settlement layer. It can fit a wide variety of applications since it does not necessitate global consensus. Hydra, for example, permits Tx costs and minimum UTXO Value to be set as low as 1 or 2 lovelaces, which is crucial for microtransactions and the applications they enable.

Notably, Hydra introduces the idea of isomorphic state channels, which entails leveraging the same ledger representation to produce uniform, off-chain ledger siblings, which are referred to as Heads (hence ‘Hydra’, in deference to the mythological, multi-headed creature). Each Hydra Head comprises native assets, NFTs and Plutus scripts. Isomorphism enables a natural expansion of the system.

Hydra will directly benefit many of the applications (and their transactions) running on the main chain today since it recognizes the same transaction formats and signatures. Existing (and new) users can leverage Cardano’s proven infrastructure to

develop wallets and apps that communicate with the layer 2 system, drastically reducing the learning curve for Hydra. A Hydra Head may also be formed without the need for any initial funds from the receiving party, ensuring a seamless user experience.

Hydra in practice

As a proof-of-concept hydra-node, IOG has already developed the main Hydra Head protocol. This was presented at the 2021 Cardano Summit.^[824] Developers can host one or more hydra-nodes online, opening a Hydra Head with a restricted number of participants, and send transactions to it. Users can view a functioning prototype on a dedicated testnet, as well as the latest benchmarking data and documentation on GitHub^[825] and <http://hydra.family>

Hydra's evolution

Other significant features being developed by IOG include support for multiple heads per node, persistence, and Head protocol enhancements.

The findings of research and experimentation, as well as input from the developer community, will be critical to progress. IOG is looking at ways to link numerous Hydra Heads to extend the ‘reach,’ as well as experimenting with new approaches to make Hydra simpler to integrate and use. The creation of ‘Virtual Heads’ by implementing the Hydra Head protocol within Hydra Heads, exploiting isomorphism of the Layer 2 solution, is one of the most promising plans.

Hydra’s overall aim is to provide a cutting-edge layer 2 scaling solution for Cardano. Hydra will save expenses while boosting throughput and ensuring security. Hydra replicates the main chain’s functionality while minimizing friction for users, but still allows the flexibility of having a different fee structure and timing constraints on the layer 2. Any successful ecosystem balances the needs of all users. IOG wants the ecosystem to serve the needs of individual

consumers, enterprises, professionals, and the growing list of DApps and their developers.

Hydra is a collection of layer-2 technologies aimed at improving network security and scalability. Although it was developed as part of the Ouroboros research agenda, it has taken its own route after the initial paper's release. The Hydra Head protocol began to take shape in 2020, and IOG's understanding has evolved since then, especially during this early implementation and proof of concept^[826] stage. The Hydra Head protocol evolved from that first notion into a proof of concept, and it has continued with a more detailed implementation for the testnet MVP (minimum viable product).

IOG has seen a lot of enthusiasm as well as a lot of misunderstandings. The majority of these issues have emerged as a result of the Hydra theoretical proposal versus the practical implementation. However, the Hydra Head protocol isn't only about SPO implementation; it's also about the hypothetical 'one million TPS,' which has become an obsession on Crypto Twitter.^[827]

Hydra Head example

A channel is a communication link between two or more peers. To be a part of a Head, you must be one of the peers. Channels establish isolated networks that may develop independently of the main network. Participants on these alternate networks use a different, simpler consensus algorithm: everyone must agree on all transactions that pass through. As a result, as a participant, I am unable to lose money that I have not specifically decided to lose. Why? Because every binding transaction needs my express permission.

Participants may make financial commitments to a Head while creating it. This entails transferring funds off-chain to a script address that binds them to a set of rules. The script ensures that the protocol is executed safely on-chain, and that participants cannot defraud one another. Any participant, however, may choose to leave

the Head at any moment by closing it. In this situation, everyone gets the most recent state they consented to off-chain, on their parallel network.

Consider Heads as a ‘private poker table’ where players bring their own chips to play with. The game may be played for as long as the participants like. If no one participates, the game will not advance. Participants are, however, able to leave with their chips. The game will terminate with the existing pot distributed if they do so.

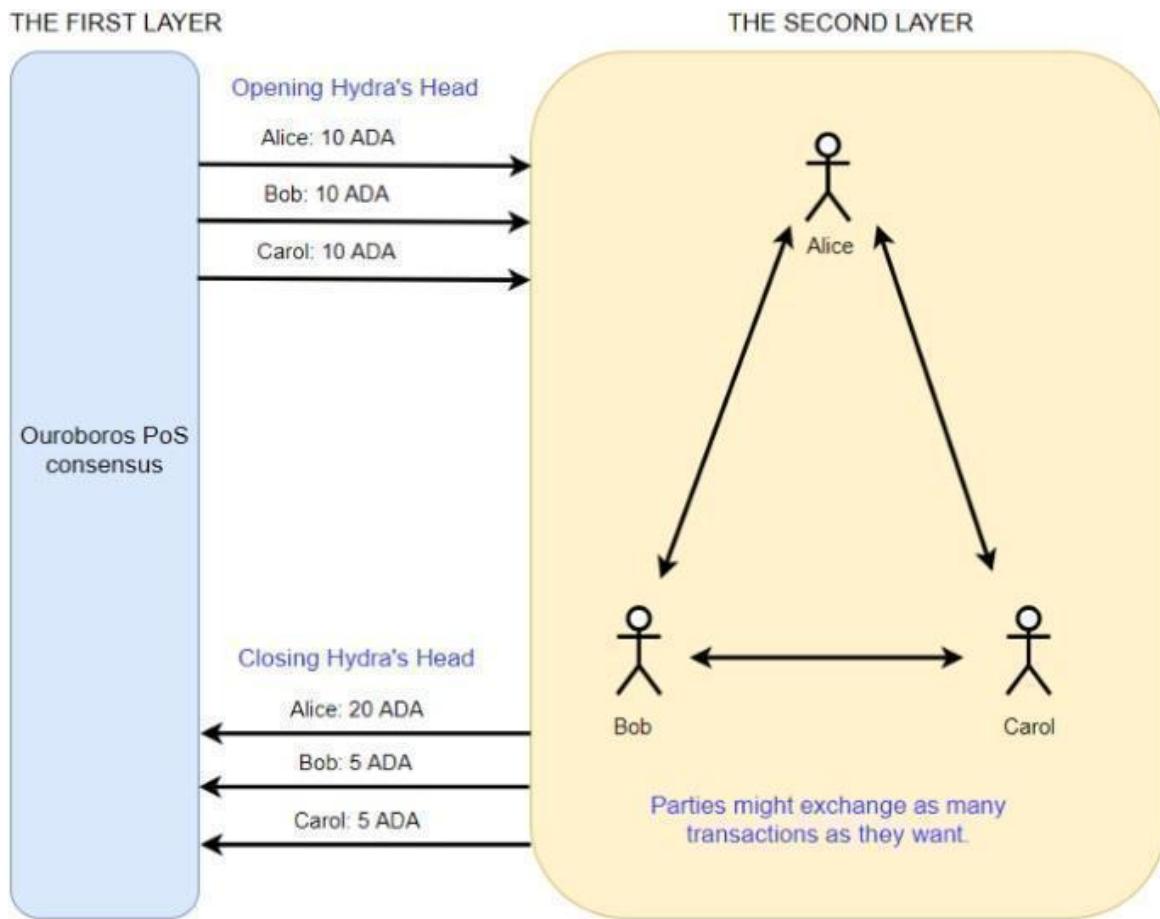


Figure 63. Courtesy of Cardanians's medium post 'Hydra: Cardano Scalability Solution' [\[828\]](#)

The on-chain script’s dealer at the table guarantees that everyone follows the rules and doesn’t cheat. In conclusion, there are the same number of chips out as there were before the game began, although they may have been rearranged throughout the game. While the ultimate outcome is known outside of the table, the players

are the only ones who know the history of all acts taken throughout the game.

This protocol is part of a larger group of protocols known collectively as ‘Hydra.’ In early 2022, the technical work was focused on implementing the Hydra Head protocol, as described in Chakravarty and co ‘[Hydra: Fast Isomorphic State-Channels](#)’.

In 2021, there was a paper released from Tokyo Institute of Technology titled ‘[Interhead Hydra: Two Heads are Better than One](#).’^[829] It is an iteration on top of Hydra Head proposing a mechanism for linking two Hydra Heads together, allowing the formation of a network of linked Hydra Heads in the long term. Other protocols, such as the ‘[Hydra Tail](#),’ have previously been mentioned. These, as well as new concepts arising from recent work on the Hydra Head protocol, are currently being investigated.

Hydra misnomers

IOG has recently noticed a lot of discussion promoting Hydra as the ‘ultimate’ be-all and end-all Cardano scalability strategy. Hydra Heads, without a doubt, provide a solid basis on which to develop Cardano’s scalability layer. They are a critical building piece that allows more complicated solutions to be built on top of the Extended Unspent Transaction Output (EUTXO) architecture. They are an important part of the scaling journey, but they are not the end goal.

TPS considerations

TPS (transactions per second) is perhaps the crudest measure to use as a comparison tool out of all those available. Transactions occur in a variety of sizes and formats. While this is true for Cardano, it is much more important when comparing two systems that are so significantly different.

A transaction involving hundreds of native assets and outputs is definitely different from a single ada payment between two actors.

It's useful to use TPS as a statistic if two things share the same context. For example, to compare two Cardano node versions. It's not a good idea to use it to compare blockchains.

With this in mind, it's better to consider scalability measures such as:

- Throughput: the quantity of data that a system can process in a given length of time
- **Finality**: the amount of time it takes for an action's consequence to become immutable and true for everyone in the system
- Concurrency: the amount of work that various actors can do without interfering with one another.

Hydra Heads are known for their ability to achieve near-instant finality inside a Head. Setting up and closing a Head might take a few blocks, but once it's up and running, transactions can flow quickly among collaborators. Hydra Heads can process non-conflicting transactions simultaneously because they employ the EUTXO paradigm, which, when combined with strong networking, provides for the most efficient use of available resources. The Hydra Head protocol's early simulations, back in 2020, predicted a highly promising '1000 TPS'. IOG is benchmarking the real-world implementation in terms of performance and finality.

One point to bear in mind: a Hydra Head is a very small-scale creation created by a small number of people. Because these groups will be autonomous at first, looking at the total of their separate metrics is deceptive. Because groups are self-contained and can be formed at whim, adding them together yields any number: ten, a thousand, one million, one billion, and so on.

As a result, although the Hydra Head protocol's initial iteration will enable small groups of participants to scale up their traffic at a reasonable cost, it will not provide a solution for worldwide consumer-to-consumer (micro) payments or NFT sales right away.

Why? Because the consensus inside a Head necessitates each participant's response to each transaction. And, without some extra technical work, a single head doesn't grow endlessly with the number of participants. The connectivity of Hydra Heads, for example, allows bigger networks of individuals to emerge, thereby converting local Heads into a worldwide network. IOG is looking at a few different ways to expand the Hydra Head protocol's capabilities.

Use cases

So, when do Heads prove useful? Hydra Heads are convenient when a small group of users have to handle numerous interactions in a short space of time. Consider a pay-per-use API, a bank-to-bank private network, or a high-speed auction between a vendor and a limited set of bidders. The use cases are many and come in a variety of shapes and sizes. Some of these may be Heads running for months, while others could be considerably shorter and simply last a few hours.

The role of SPOs for Hydra

Stake pool operators (SPOs) were identified as possible candidates for operating Hydra Heads in an earlier Hydra study in 2020.[\[830\]](#) However, since the Hydra Head protocol was studied and implemented as a proof of concept, IOG can confidently declare that claiming that only SPOs need operate a Hydra Head to assure ledger scalability is a misconception. In reality, without a cause to transact, SPOs have no intrinsic motivation in opening Heads with one another. When it comes to the Hydra Head protocol, SPOs are similar to any other actor. They, like everyone else, may be a participant and open up Heads with their peers.

SPOs are typically adept at running infrastructure and may be among the first users to deploy Hydra Head instances. However, this only enables participating SPOs to transact with one another, limiting end-user applications. Only complex layer 2 system designs, such as the Interhead Hydra protocol, need the involvement of

intermediaries to manage infrastructure for end users. In fact, IOG believes that one of the most common Hydra Heads setups will be to provide consumers managed Hydra Heads as a service (HaaS). This can be done without giving up custody of funds by managing infrastructure on behalf of end users, who, in most cases, lack both the inclination and technical expertise to do so.

This is quite similar to the existing operating paradigm of light wallets and light wallet providers, who are far more likely to be running Hydra Heads over time. Consider a network composed of the Cardano ecosystem's top light wallet providers. As a result, such providers may permit quick and low-cost payments between their clients.

Services for developers and DApp providers are also plausible candidates for running Hydra Heads. DApp developers do, in fact, need access to on-chain data. Developers may depend on internet services for this, which often charge monthly usage fees and offer interfaces. With pay-per-use API calls between service providers and DApp developers, Hydra Heads may enhance this process and enable a more decentralized business model.

Hydra iterations

It is critical that IOG communicate often with Cardano ecosystem developers as a collection of protocols that will be deployed over time will include more sophisticated layer 2 system designs on top of the Hydra Head protocol. This isn't a one-time release, but rather a series of incremental releases. IOG must comprehend developer issues, ensuring that their demands are satisfied, and ultimately, guarantee that IOG are doing something worthwhile.

This is why, beginning with an early proof of concept in 2021, IOG created Hydra Head as an open-source GitHub project.^[831] IOG launched their first developer preview (0.1.0) in September 2021, followed by a second iteration (0.2.0) before Christmas, aiming for a regular and frequent release cadence. In February 2022, the next

increase (0.3.0) was made. They use semantic versioning, and each of those pre-releases (0.x.0) adds new features that partners, and early adopters will be able to try out on the private and public Cardano testnets.

You can see the Hydra roadmap on GitHub^[832] also. Visitors will discover feature problems, milestones, and project boards on the Hydra Head repository as a way to communicate with the developer community and to be open about the progress of development initiatives.

While IOG's priority is to provide significant and feature-rich releases as they go to testnet, and then mainnet maturity with version 1.0.0, the roadmap also contains estimated release dates. These projections are based on both the work completed to date and IOG's estimations of the work to come. To maintain the roadmap as accurately as possible, they'll reflect on the content and the dates regularly.

Community buy-in is key

IOG will gauge their progress by the amount of traffic that passes via Hydra Heads versus the Cardano mainnet. This means they won't be able to achieve their aim without the help of the community, and Hydra will only succeed if it is valuable to present and future Cardano users.

April 13, 2022. **What is the importance of Hydra for Cardano to scale on a global level?** CH:^[833]

So what's ended up happening is a lot of people in the Cardano community, and outside of the Cardano community, are looking at hydra as this panacea. It's like when Jesus was born, it's like b.c. and a.d., before Christ after Christ. No it's not like that, we have pipelining and input endorsers and a lot of optimizations. That plus improvements in the way that applications are developed, will massively scale Cardano, at a scale of 100x or

something like that from where we're at today. So that's good enough for the load that we're looking at on the network. Then you have sidechains come and that means a lot of traffic gets pushed into other domains, other computation layers.

By the way, Cardano can be a computation layer of itself, so that's one way that we can shard and scale. So that is great and there's all kinds of things that can be done to improve throughput, and constrain it, not as a consensus problem, but a network problem. When you look at hydra or roll-ups. That's saying for particular patterns of use, micro payments or things that can be batched and bundled together, NFT airdrops whatever it is... some DEX logic, you can do those things with a different network, a layer 2 technique. The advantage there is that only a small representation of all of that traffic ends up on mainnet. So instead of trying to improve your overall throughput, you now have a situation where you get additional throughput through a different network. That potentially has a chance to scale near infinitely for those classes of transactions. Tipping, microtransactions, airdrops... these types of things.

So Hydra is churning away and we're in the theory stage, and applied cryptography and applied research stage. We're coming up with all kinds of interesting questions and we're chipping at those questions, quickly updating, modernizing Cardano to make it a better fit and integrate Hydra. So hydra is a great 2023 technology which is going to substantially chip away at certain use cases and make them a lot easier for our network to handle. Rollups will do the same, sidechains will do the same. In the meantime, 2022 this year as part of the Basho agenda, we have pipelining and we have input endorsers and that is where you're going to see the most significant gains and throughput. Really, it's going to take us to a point where the network will be able to handle what's added, regardless of how many DApps people throw on.

Off-chain computing

Offloading part of the computing, such as via Asynchronous Contract Execution^[834] (ACE), may improve the efficiency of the core network. Transactions take place outside of the blockchain, yet a trust model allows for quick and inexpensive transactions. This concept is still in research mode and will likely be implemented in a future update.

Mithril

Mithril proposes a stake-based threshold signature technique that may be used as a protocol in blockchain applications to handle chain synchronization, state bootstrapping, and trust concerns.

Paraphrasing the then IOG Architecture Director John Woods on the January 2022 update:^[835]:

Ultimately what Mithril does is enable a computer, or a device, that doesn't have a large computational capability, such as a phone or a raspberry pi, to be able to validate the entire chain. Of course they can't validate the entire Cardano layer one chain, block by block, because that would be too computationally expensive, so what Mithril does is it effectively checkpoints the chain. It puts a stake in the ground and says, 'hey it's good up to here ...and then go maybe forward another 400 blocks... another stake hey it's good up to here.' What IOG can do using some cryptographic magic, is that they can have one of these light devices take all of the stakes out of the ground, check them quickly, and then they know that the chain is valid without having to do that work themselves.

Stake-based signature aggregation

To appreciate Mithril's advantages for Cardano, it's important to understand some context.

Because Cardano is a proof-of-stake blockchain, the consensus algorithm chooses block producers at random based on their stake. It is critical that a specific number of stakeholders submit their

cryptographic signatures for certain activities. The consensus protocol dictates how nodes evaluate the present state of the ledger. The protocol has three primary roles:

- Conduct a leader check to determine if a block should be generated
- Manage chain selection
- Validate produced blocks^[836]

To achieve true scalability, it is vital to address the intricacies of key processes that rely logarithmically on the number of participants. The more participants there are, the harder it is to effectively aggregate their signatures. To assume a signature that represents the majority of stakeholders in a base scenario, each stakeholder must sign the relevant individual message. This is doable, but in terms of scalability and performance, it is impractical.

Given the time it takes to verify a message and the amount of resources used during chain synchronization, it's essential to offer a solution that enables multi-signature aggregation quick and easy without sacrificing security.

Mithril design

Mithril is a protocol that aims to do the following:

- Increase efficiency by leveraging stake
- Ensure that the setup is transparent while avoiding the need for increased trust settings
- Take advantage of trade-offs between size and efficiency, which the modular component design ensures.

Mithril is used in a public setting where signers do not need to communicate with one other to create a valid signature. The aggregator merges all of the signatures into one, and this process is logarithmic^[837] in terms of the number of signatures, resulting in Mithril aggregation's performance being sublinear. Mithril, for

example, may speed up full node data synchronization and reduce resource usage when used with full node clients like Daedalus.

Mithril employs the stake-based threshold setting to represent a large portion of the overall stake. This is in contrast to the usual configuration, in which a certain number of participants are necessary to verify a certain message. The protocol needs a portion of the overall stake to verify a message and generate a signature under the stake-based threshold setting.

In a trustless environment, Mithril also verifies consensus. This means it doesn't make any further assumptions about trust. Consensus certification is achievable without adding any new assumptions to proof of stake. It may, for example, be used in wallet-as-a-service, with the mobile client relying on a Mithril node's certificate. A technique like this might be more efficient than SPO blockchain verification if advanced security parameters are used.

Finally, the signature scheme enables various stakeholders to verify only a given checkpoint of the chain to guarantee fast chain state bootstrapping. Stakeholders don't need to go through the whole transaction history of a particular state; instead, they just need to go over the checkpoints to ensure that the final stake is valid. This is useful for light client applications and wallets that need to function quickly without synchronizing the whole chain. Mithril signatures may also be used for tally verification and cryptocurrency governance decision-making.

How does Mithril work?

Mithril allows for multi-party signatures by storing a number of separate lotteries (M) and deeming a message genuine if it has been signed by a number of different winners (K) over those lotteries. As a result, each user tries to sign the message and then passes their signature via a lottery mechanism. Individual users may use this method to see whether their signatures are lottery-eligible and then print the results without having to wait. This is not like a standard

arrangement, when slot leaders must wait until their slot is active before they may engage. Once you have case signatures from several lotteries, they can be combined into a single Mithril signature.

The design of Mithril involves three phases:

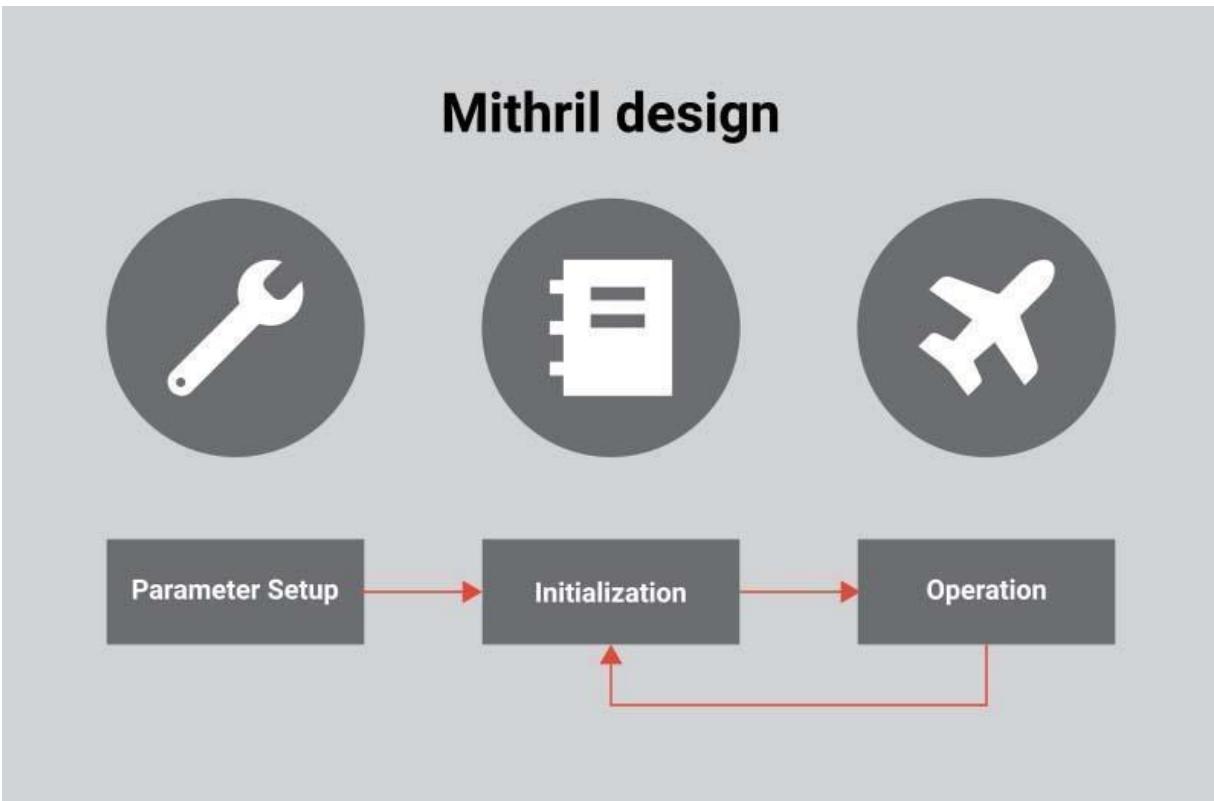


Figure 64. Mithril design

Parameter setup

Users must do the following to set up a Mithril protocol:

- Make sure the group where the cryptography will take place is set up correctly.
- Select the index range M , which represents the number of elections to be held
- Determine the quorum size K , which is the minimum number of election winners required to accept a signature.

It's also crucial to provide the proof system a reference string. This may be done in a transparent way without relying on any high-trust assumptions.

Initialization

Users should update the state distribution during this phase. This informs all stakeholders as to the stake they hold. Then it's up to each stakeholder to register their keys. This may occur both on and off the chain.

Finally, users must stake and compress their test keys, which is accomplished via the Merkle tree. Mithril signatures may be checked against a single hash that represents the Merkle tree using this function. As a result, the state size required to validate a signature may be kept small.

Operation

Users may create, collect, and validate Mithril signatures while working with the chain. Producing signatures entails users attempting to determine if the signature they created is indeed a winner in one of the concurrent lotteries. If this is true, the users' signatures will be broadcast. If enough signatures from separate lotteries support a specific message, they may be combined into a single Mithril signature. It may then be broadcast and checked by anybody using the proof system's reference string and the short Merkle tree hash of stake distribution.

A single user may utilize Mithril to produce a signature as follows:

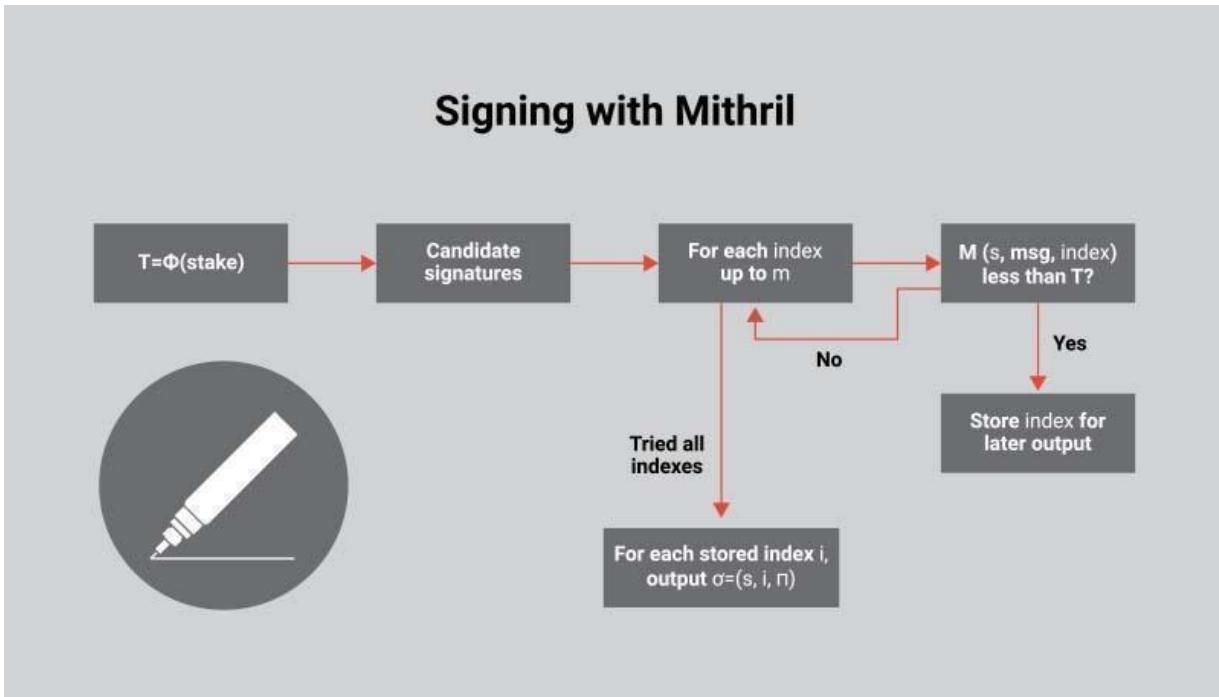


Figure 65. Signing with Mithril

To get their score threshold T , a user will first verify how much stake they have and then run it through a score function. Then they'll try to come up with a candidate signature S . They will assess whether the candidate's signature created corresponded to the message they had just signed for each index. The lottery index number they're comparing it against should similarly give a score value smaller than their threshold T . If this is correct, the candidate signature they supplied won the lottery on that specific index number. They'll try again if they don't succeed the first time.

Users may have one or more indexes for which their signature S is valid after checking all available indexes. They may generate a separate signature for each of those indexes, consisting of their candidate signature, the index number for which it is legitimate, and the evidence that their score is comparable with the registered stake.

Mithril network architecture

The following graphic displays the network architecture of using Mithril on Cardano:

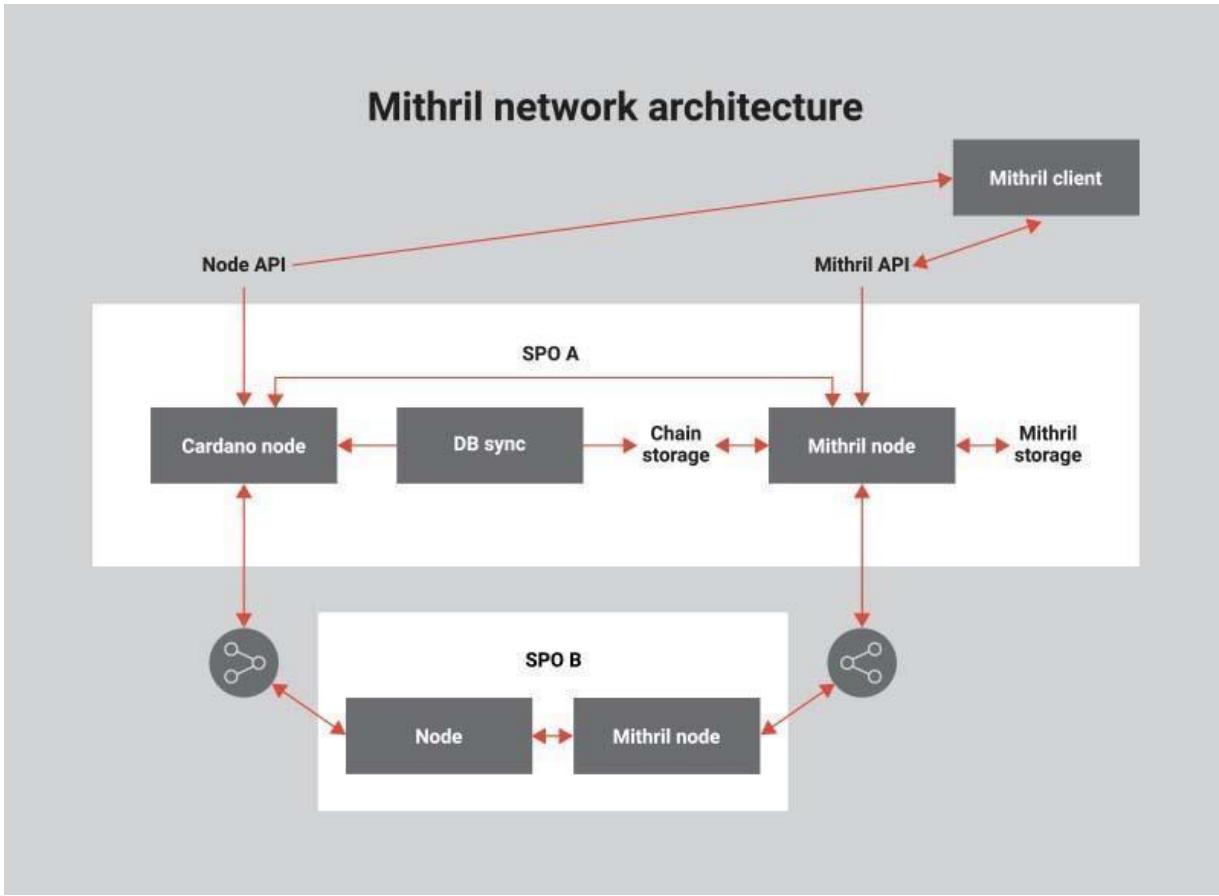


Figure 66. Mithril network architecture

The link to the Cardano peer-to-peer (P2P) network, the Mithril node's P2P network, and the Mithril client connected to the node managed by a SPO are all high-level representations of software surrounding a stake pool operator (SPO).

The Mithril node on the SPO platform connects to its validated blockchain on local storage and executes the protocol to generate Mithril certificates, which are stored in the Mithril storage. Mithril certificates that have been created may be verified throughout the whole network. As a result, the SPO may share the whole Cardano blockchain as well as a list of valid Mithril certificates. When the Mithril client joins the network, it asks for a list of Mithril certificates and the Cardano blockchain's longest chain.

Many SPOs can participate. The Mithril client will next check that the obtained Cardano blockchain is properly confirmed by the certificates. The whole operation is lightweight and does not need the use of large amounts of network storage or compute power. Furthermore, Cardano complete node sync and Mithril fast sync techniques are not mutually exclusive - they may be used simultaneously. The full node sync will validate Mithril fast sync later.

Mithril use cases

Mithril makes full node clients or applications like Daedalus more efficient.^[838] It assures that the whole node data is synchronized quickly and securely, saving time and resources like computation, network exchange, and local storage while maintaining high-level security assurances.

Mithril may also be used in light clients and mobile apps, guaranteeing a trustless approach. Another big benefit is that Mithril signatures may be used to operate sidechains. The primary blockchain may link to several sidechains, each with its own consensus process. Mithril offers advantages in lightweight blockchain state verification, allowing certificates to securely authenticate the present state of a blockchain as well as the validity of forward and backward transactions.

Finally, Mithril may be used in stakeholder-based voting systems and governance solutions regardless of the voting protocol's complexity. Mithril signatures may be used for tally verification that is both secure and light. This is also effective in governance when stakeholders participate in a decentralized decision-making process and deliver a simple and verifiable end conclusion.

Real world applications

Several companies have shown interest in using Mithril into their blockchain applications. Galois,^[839] a leading research and development business specializing in formal methods, cryptography,

and hardware, will create the first Mithril prototype based on IOG's research. Due to its quick prototyping capabilities, Galois will develop Mithril in the Rust programming language. Smaller signatures with BulletProofs^[840] will be presented first, followed by production-ready implementations, and lastly formal proofs of correctness.

Mithril Progress Update

Roy Nakakawa (Product Manager for Mithril) and Mithril Architect Arnaud Bailly provided an update in the Cardano360 May 2022^[841]

...as we all know, booting and synchronizing Cardano nodes is a slow process that requires downloading and verifying all the blocks, comprising the chain, one after another. The goal of Mithril is to leverage the existing Cardano network of SPOs to provide certified snapshots of this chain state. Those snapshots could be in different forms....but we could also imagine providing snapshots, certified snapshots, of the full UTXO set, which would make it possible for light wallets to rely on those kinds of certificates. The interesting thing is that those certificates produced by the Mithril protocol have the same security properties that the underlying consensus that drives Cardano has, which is the Ouroboros Praos protocol.

This means that Mithril clients have the same trustless guarantees as normal Cardano node users would. An important thing that we want to be able to do is provide this feature on top of the network, and without interfering with the normal operation of the Cardano network, in a non-intrusive way. So Mithril would strictly be an additional feature and provide additional service, on top of the existing network.

How does Mithril work?

Mithril works thanks to some clever cryptographic schemes, which takes into account the amount of stake each owner owns, to produce signatures. So at some interval, some predefined intervals, the stake owners will attempt to sign the current state of the chain depending on the Mithril parameters, and the

amount of stake they own. They will be able to issue one or more signatures...

One analogy that you can use to think about it is the lottery. So depending on the amount of stake, you draw tickets from a lottery, and depending on the amount of stakes you draw, depending on the amount of tickets you bought, your chances of having a winning ticket are higher. And so this is the same for Mithril ...you can potentially have several winning tickets. Once enough winning tickets have been drawn, over all the stake pool owners, then a certificate can be issued which provides a certified signature of the current state of the chain from a share, some share of the stakeholders, from some predefined share... and this is what we call a snapshot.

Now the snapshot is made available to clients, and the clients can verify it, they can verify these snapshots by checking the aggregate signatures from all the lottery winners, so to speak, and so from all the signers....and check that they are actually legit and this check also rests on checking that the stake distribution is legit, and this is done through checking the chain certificate down to some general certificate ...and once they have verified the validity of certificate, then now they can just download the snapshot itself, bootstrap the node, without having to go through the hassle of verifying everything.

Mithril has progressed, especially in the Mithril aggregator component. The first step was to implement somewhat advanced mathematics, which were not available 'out of the box' in standard primitives that are available on the market. This library, which we call 'Mithril core', is now more or less feature complete. So the whole foundation part is ready. What we are currently working on is the first version of what we call the Mithril network, with the goal of making it fast and easy to bootstrap a Cardano node. They all have moving parts to get right. We have this notion of a signer, the signer part will be run by SPOs (stake pool operators), responsible for issuing signatures of snapshots, so drawing the lottery tickets, as I explained before. We have

the Mithril client, on the other side, which will validate the certificates and download snapshots.

...an important role is played by the Mithril aggregator. So the Mithril aggregator is the party that is responsible for aggregating signatures to create certificates that will be used by clients.

Also, even more importantly, the aggregator will be responsible for storing and distributing the snapshots themselves. These snapshots are somewhat huge, like tens of gigabytes, really for a mainchain. Potentially, we all know that this will keep growing over timeso signing and delivering those is a problem, which you can imagine, it's just like delivering a movie, like a high-resolution movie, in 4k (parts). It's also several tens of gigabytes. So how do you do it efficiently?

...the aggregator really has a very important role in making that efficient for all the clients. What we're doing now, for the sake of simplicity, and for really the first step, is to implement this aggregator in a centralized way and to have the Mithril signers and the Mithril aggregator communicate with each other directly through some calls, but the end goal is really to have a fully decentralized industry solution.

It's something that we have already started thinking about, and we'll be working in this first MVP, is really to have the signers and the aggregators work in a decentralized way so that new aggregators could be easily built up, and with different ways of distributing those snapshots of aggregated signatures and delivering the value to the clients, potentially with innovative distribution schemes. So think IPFS (InterPlanetary File System) or even BitTorrent, if you think about it, could be used for that with different business models, and different incentives.

Next phase of Mithril?

We are in the final stages of cleaning up the code in preparation for open sourcing the whole library. So we plan to open source after the (Consensus 2022) conference, somewhere around June, and also provide some friendly documentation to help everyone get started on Mithril. The short-term goal is to reach a

stable enough state of the system, that we can put it in the hands of the community members for beta testing on testnet. In a few months from now, once we have enough, once we have gathered enough momentum and enough experience from running on the Testnet, the next step will be general availability on the mainnet.

To learn more about Mithril, delve into the research paper[\[842\]](#) and look back at the Cardano 2021 Summit talk.[\[843\]](#) You can check the official site for the latest updates: mithril.network/

April 18, 2022, Twitter Space ‘Sunday Chat with Charles’ Re: Light wallets. CH:[\[844\]](#)

So there's two sets of things that need to happen for this problem to get totally solved. One side of things is that we need a program to ensure that there's great competition and wallet diversity. So certified wallets are the key there, and that's a high priority for me and I'm pushing very hard for the Cardano Foundation to get something done there. They're the objective neutral party that ought to maintain that program. I can certainly launch one at IOG, but I'm now competing in this space and so I have a conflict of interest.

So that's one dimension of it. The other dimension is that there needs to be a collection of technologies that kind of need to be built out, like wallet infrastructure and smart contract infrastructure in the Cardano space and make sure that those are open source and widely available. Our hope was that that would be developed by the Yoroi ecosystem and that didn't quite occur, for a variety of reasons, and that's OK. They're certainly working hard, but it didn't happen on their side.

So in the second half of 2021, we (IOG) made the decision to enter the light wallet space. We hadn't been there. We'd only been in the full node space, which is Daedalus. We spun up a team, it's quite a large team now, and we're building a collection of infrastructure and technology, which will all be open source.

First Mithril, which will give you full node security on a light wallet, but a light wallet user experience to the DApp store and other things, and just making sure that that looks really good. We're going to be making sure that that gets out this year. The sooner the better, and every month, we'll make sure the user experience improves for every user. It's going to start with the browser, but very quickly we'll get into the cell phone and then I think that's going to kind of create a standard that the rest of the light wallet people can follow, and they can borrow some of that infrastructure and they'll be able to bring their own competitive tech. dcSpark has also entered and they created a great product called Flint, and that continues to evolve as well.

So there's a lot coming, a lot of competition coming. And everybody has a flavor and as long as there's good standards, that ensures security and quality. That allows you to distinguish between a scam and not a scam. We'll exit the year with a lot of good options. So it's not just solving the problem in one particular case. That's not good for any consumer, if there's only one useful wallet. You need to solve the problem with multiple solutions that are all good.

.....

So crypto's ideal, not just because it can be sent person to person. You don't have to wait in a line or expose yourself. The other thing is it can be concealed, and that's a very powerful thing. I don't want anybody to know that I just got \$200 when everybody living in my neighborhood lives off of \$50 a week. So if I can get that money discreetly, and nobody knows I got it, I can keep it secret. Then there's a safety factor there with that privacy.

So it's really important to us, for our mission, to make sure that it works well on a phone. It's really important that that ecosystem gets developed and this is just one of those things when you have new protocols. Building a light wallet ecosystem, you have to build it from scratch.

Bitcoin didn't have a good light wallet game until about 2012, 2013...and even then, it still took some time and that was four or five years after protocol launched. And so we're kind of following that same path. And there's been some unique factors that have slowed down certain things. But we did design these protocols with light wallets in mind, that preserve inclusive accountability.

So unlike Bitcoin, where you have to trust the central actor, for Cardano you don't with Mithril support, and that's something that we value so much that we brought in bespoke developers from very expensive firms and pay them \$3k a day just to do some of the cryptographic engineering because I want to make sure that actually gets out this. And all of that's open source, and anybody who's building a light wallet will be able to use those libraries to ensure that their wallets also have inclusive accountability. It's not just a unique feature to an IOG product, it's truly open-source software.

April 20, 2022, '4/20 Hangout with Charles' Twitter space, [\[845\]](#)

L2 scaling solutions, ZK roll ups... CH:

Zero knowledge crypto is a really cool topic. It's actually becoming one of my favorite topics since it's so incredible, you always say that you get to meet your heroes ...and there were a handful of academics I really looked up to and I really enjoyed when I was growing up, on the computer science side. One was Phil Wadler, and I just loved his papers, they were so much fun to read...and it created a love of functional programming early in my life and now I work with Phil Wadler, that's an honor and a privilege.

Another was Silvio Micali, and Silvio was much like Wadler. In the 1980s, he was just in 'Beast mode' and he was going around solving everything, and Micali actually helped create

zero knowledge cryptography and now Micali is actually in the cryptocurrency space, and he created Algorand. So it's surreal that you can be on panels and engage and have dinner with these people that are like legends standing up on pillars. So that's just a side note, but it's a fun one.

Zero knowledge crypto... The easiest way of explaining it is usually the allegory of a cave. So let's say that you're walking in a forest one day, and then you come across this cave, and it has two entrances, and you decide to go down one of those entrances, and as you go, you can find a scroll and a code word written on it. And then, as you keep walking, you see this big golden door, and you decide to read the code word. When you do, the door opens up... and it leads to a chamber, and in that chamber is this huge treasure. It's a really beautiful, special place and then you notice there's another door, and you go through that door. It comes out the other side. So if you were to draw it, you would kind of like this U, where the butt of U, the bottom part of it...those two parts open up into a chamber.

Ok, so let's say that you want to sell the treasure inside the cave. Well if you go and just tell people that you have access to it, you can open the door. How do you prove to them that you know that? You could tell them the password, in which case they already have the thing of value, and then they could just kill you... or they'll just have to believe you on blind faith that you know that password.

Well, what you could do is design an experiment. So because both doors are linked, the only way that you can go down the right path, and exit the left path, is going through the cave. So that means that you have to have had the password or gotten lucky.

So here's what you do. You design an experiment, a trial...and you said ok, I'm going to randomly go down a tunnel, the right tunnel or the left tunnel ...and then you're going to randomly

shout into a tunnel, and I'm going to come back that way. So let's say I go down the left tunnel and you shout 'left'.. i just turn around and go back, I don't actually have to go through the door, but let's say i go down the left tunnel you shout right, the only way i could have done that is by actually going through those doors.

So every time you do this trial, you have a one in two chance of getting it, cumulatively it's 'one over two to the n'... so basically after 5, 10-15 trials, there's no way probabilistically that you could have done that correctly, unless you had the password. What makes this really cool, and zero knowledge, is an outside observer witnessing this event, doesn't know if you two have collaborated or not, so they've actually gained no knowledge.

So if you and the person who's testing you said OK, the patterns could be left, left, right, right, left, right, left, right, right, something like that... You could just do that, and you never actually have to know the password, but the person asking is the only person convinced, and so that's what they call a zero-knowledge proof. It's basically something where you're proving you know something without revealing it, but you're only proving it to the person who is asking, and any outsider gains no additional knowledge.

So these were a curiosity, back in the 1980s and 1990s, and they were real fun thing as a thought experiment, for people at MIT to play around with, but they didn't really have a lot of use cases until we started creating interactive communication protocols, where you're trying to broker that somebody is somebody, or somebody knows something.... And then cryptographers start constructing more elaborate systems.

The system that I just mentioned is an interactive two-party system. There is a person who's doing something...that's the prover, and there's the person accepting that, which is what's known as the verifier. But in the case of cryptocurrencies, these

are non-interactive protocols. You shouldn't have to wait for somebody to come online to be able to spend your Bitcoin. You shouldn't have to be able to wait for your stake pool operator to do something to spend your ada... so you need them to be non-interactive and so a new generation of zero knowledge proofs were created and they're called SNARKS, succinct non-interactive arguments of knowledge...

It created things of two different axes...on one axis, it allowed you to prove interesting things about a larger, more generic set of information. And then on the other axis, they reduce the amount of interaction required, for those proofs to be valid. The initial wave for them required a bootstrap, and that was called a 'trusted setup'. You may, in literature, see it's something called 'toxic waste', and they're basically some group of people who have to get them together, do something to get it started, and as long as you trust that they did that right, then everything downstream of that is non-interactive.

Now we have the next generation of these things, where they actually don't require a trusted setup, and also you are more generic in the statement of things that you can do. So a lot of people ask, well, what's the point? Why do we care about this technology? Why is this useful to me as a consumer? OK, let's say you go to a bar, and you get carded. When you show your driver's license to the bartender, you reveal more than just your age. You reveal your precise age. Oftentimes, the driver's license has an address on it. If you're an organ donor or not, a picture of you, your gender, you reveal some of them... I think they put Social Security numbers on the driver's license, military ID, and even more, a passport. You get all this stuff that the bartender should not know.

The bartender is looking for a threshold condition. Are you above or below the drinking age? That's all they need, it's a Boolean yes or no. Are you over 21?... at or over 21? So what a zero-knowledge proof can do is, for an identity system with

digital ID, you can prove to that bartender that you're over at the age of 21, but reveal nothing else about you. No other metadata, and an abstraction you can do that for any challenge response protocol. Are you a US citizen or not? Is the money that I've received taxed or not? Are you fully compliant with laws in the state of Colorado? or not? Yes or no. These types of things. Are you eligible to see this information? Yes or no. You remove that judgment in that respect.

Now the other application is, do you own this money or not? Zero knowledge proofs are perfect for this application, because basically you're proving that the money exists and that you have the right to spend it, but you're not revealing which money it is, and you're not revealing who you are. So that's why they're used in privacy systems.

Now where do rollups come? Well recursion is where you basically say, well, hang on a second here, what if I take the state of the entire system?... All of the moving pieces of the system, and I basically say that as the state gets updated, I refresh a proof recursively, so one generates the next one, and you kind of roll them up, so that you, at any given time, only have one universal proof, or collection of them, and then when you look at the state of the system, you're able to verify that there's been a chain of events to lead to that, that's legitimate.

Now why is it useful? if you look at technology like mina^[846] ...what are they doing? They're basically attempting to build entire blockchain systems that have constant sized-blockchains, or the use case is the system grows logarithmically to the size of the chain. In other words, very, very slowly relative to the amount of data that's inside of it.

...and frankly, this is the only way, in practice, to be able to, in the long term, run a blockchain system, because otherwise, you'll have a situation where the system is in the yottabytes.^[847] You know, it's so vast and large and voluminous, that only

Google or the NSA or a massive data warehouse, can preserve the state of the system. And in other words, you have to completely trust a centralized actor, which defeats the entire point of decentralization. So because this is the only way to preserve inclusive accountability, and because they provide amazing advantages for scalability, mobile clients in a litany of other applications ...they're among the most studied of all mathematical structures in the cryptocurrency space.

...and you see lovely papers like Plumo.^[848] You see lovely papers like PlonK,^[849] ...we wrote a paper called Sonics.^[850] There's a lot of very fertile, beautiful active research. Some are very complicated and involve incredibly deep cryptography. That is elegant, but because it's complicated, it has a high probability of having a problem.

...and other parts of the crypto are very simple, for example what we did with Mithril, for Cardano, and which is being implemented for our light wallet solution, which is very lightweight, but still has a lot of power in giving you full node security with a light client. Every year this is an area that evolves at a pretty rapid pace. Now for us in Cardano, what we've done is we've done two things.

One, usually proofs are constructed as an interactive process by a collection of actors. So we're working a lot on the plumbing to do that in a Layer 2 capacity. Mithril, in particular, we're building a network subnet for that. Second, what we've done is put a lot of cryptographic primitives into Cardano... like secp256k1 support and pairing-based crypto support through BLS support... coming in the Vasil hard fork here in June, that are foundational to many of the schemes that people would use, whether it be bulletproofs or PlonK, or other things. So this in essence, these built-ins and these primitive supports make it much easier for third parties to port things that have been done on other blockchains to Cardano.

Now we're also examining the crypto itself, and we have a whole group of people in our organization who are exclusively working on these privacy primitives, and we've written some foundational groundwork paper... like how do you upgrade a SNARK system? to replace it from one primitive to another?

We've also written a paper on private computation. So how do you go from just a transaction to a smart contract? that's private state... and we wrote a paper called Kachina for this. So we're working on these things and there's a lot we've learned, and there's a lot of moving pieces for it, but it's one of those 'move in inches' type of a deal, but we're all moving together and we're all learning together, so it's actually become very fertile in that respect. And ultimately, I think it's one of the bedrocks of blockchain technology. It's one of the foundational requirements of it, that preservation of inclusive accountability.^[851]

Lace

At Consensus 2022, which took place in Austin, Texas, IOG announced their new light wallet *Lace* (lace.io) was in development. Charles Hoskinson ran through a demo^[852] explaining that *Lace* will not just be a wallet but a platform enabling users to tie together identity, voting and DApp Store experience. *Lace* will clearly be pivotal for Cardano adoption.

IOG's full node implementation is the *Daedalus* wallet, which is a desktop client that is fully synchronized with the blockchain history. Full node wallets are an excellent alternative for more advanced users, but because they carry a full copy of the blockchain, they use a lot of resources and take a long time to sync. As a result, a full-node wallet may not be suitable for users that want immediate access to their funds. As Cardano expands into more mainstream countries, particularly in emerging nations, a viable alternative is necessary. *Lace* will focus on driving adoption by offering a great user experience.

It will initially support the basics: storing your ada, sending/receiving ada, storing NFTs and delegating your ada. Long term it will integrate with Atala Prism (IOG's Decentralized Identity solution) and the DApp Store, enable Catalyst voting and be interoperable with other blockchains.

In an interview^[853] with Eleanor Terrett for FoxBusiness, Charles Hoskinson talked more about Lace:

We love trying to think about how to build a great consumer experience. There's a lot of things that need to be pulled together. A wallet is kind of a misnomer, in that cryptocurrency wallets are usually only there to store and transact assets... but when you look at cryptocurrency in 2022, you have identity, you have DApp interactions, you have rich metadata, you have tax compliance... you have so much going on... you have collectibles inside these wallets now.

So what we wanted to do was build a very consumer-friendly platform that evolves very quickly. So every 6 to 9 weeks, new features and functionality come out. It gives you kind of a Swiss army knife of cryptography, so you can do some very complicated things over time like multisig transactions, partial delegation and proxy keys^[854] ... but ultimately you go multi-chain, multi-asset. It's a place to store your digital life in that respect. So it's a place where you can interact with people, a place where you can share identity, multiple identities which you can share. Identity for GameFi, one for compliance, one for friends, one for NFTs... all these types of things.

It's also a place where you can start consolidating and getting a common view of the DApp space. DApps are very fragmented right now, and you usually have to go to a website and there's a poor user experience interacting with them, lots of clicking, lots of different windows...it would be much better if you had a beautiful DApp Store, one-click install, you have it, it's there, it

works. Get it to work on the browser, on the phone, on the desktops and make it fast and beautiful.

The other thing is that we have such great relationships, like with Carnegie Mellon University. We have been working with them for a while, and they have one of the best Human Computer Interaction Groups in the world. So we have all these user experience and user interface problems when using cryptocurrencies... you have to enter 24 key words, you have to do all this stuff, it's very easy to lose your money, lose your keys... It would be very cool to collaborate with them on projects where we need to do better. Maybe your (wallet) restoration could be a picture, instead of keywords, these types of things.

So it's really nice to have a platform where, not only can we make technological innovations, and integration innovations and kind of bring everyone together and unify... but also user interface innovations to ultimately make using cryptocurrencies easier for people... because if you want to go from 10 million to a billion people, that delta is usability, not functionality. Usually your functionality is great at 10 million but it's the 'best kept secret'. The billion is only when you have great usability in that respect.

Tiered Pricing as the network scales

Cardano's adoption will keep growing as demand for decentralized finance grows. IOG's research team are continually reviewing methods to ensure that all users have equal access and throughput. The Cardano network will stretch and develop in order to fulfill the need for smart contracts and DeFi. Similarly, the transaction fee model used by Cardano will need to be upgraded.

The existing approach is straightforward and equitable: every transaction is processed equally, and users cannot change their priority by paying greater fees. This strategy works effectively as long as the throughput capacity is similar to the demand.

However, there are certain disadvantages. With more people using Cardano, there will come a point when not all transactions will be able to be included on the blockchain, even if the parameterization is tweaked. Although boosting the main chain's capacity and/or routing transactions to Hydra or other layer 2 solutions will help relieve this issue, the core system must remain adaptable in all potential scenarios and at all times.

In the event of a denial of service (DoS) attack, this is significant. With the system as it is, an attacker may take advantage of the system's fairness and pass their harmful spam off as legal transactions, causing everyone else to wait longer. There are safeguards in place (for example, in relation to transaction propagation over the peer-to-peer network) that make an attack like this impractical. However, for further security, the network should be able to raise the costs of such attacks without endangering the system's fairness and price efficiency.

In 2022, members of the IOG's research team began working on this issue. The solution presented preserves the cornerstones of Cardano transaction processing (predictability, fairness, and cheap access) while addressing the challenges that may develop as demand grows. For blockchains, IOG's method proposes an innovative transaction fee structure. The design's major feature is dividing each block into three 'tiers' depending on the use case. Each tier is intended for various sorts of transactions and accounts for a certain proportion of the maximum block size. The tiers, as well as the recommended division that IOG considered, are as follows:

- fair (50%)
- balanced (30%)
- immediate (20%)



Figure 67: Tiered pricing: a block can be split into three tiers.

Going from right to left from the graphic above... ‘Balanced’ and ‘immediate’ function by having a distinct ‘fee threshold’ for each. Transaction issuers would define the tier of service they need in order to be included in a block. This may be accomplished by imposing a transaction fee cap. Then, beginning with the ‘immediate’ tier, the ‘balanced’ tier, and lastly the ‘fair’ tier, each block would be filled. Within the same tier, similar transactions would be charged the same rate. To make this decision easier, each transaction would only be paid the smallest fee that would ensure its inclusion in the block. Fees for ‘immediate’ and ‘balanced’ tiers would be dynamically and deterministically adjusted after each block (using demand levels in prior blocks) to guarantee that each tier consumes its desired percentage of the block.

The distinction between ‘immediate’ and ‘balanced’ tiers is the manner in which fees are changed, notably the ‘speed’ with which they change given the present load. The ‘immediate’ service threshold would always be greater than ‘balanced’, reacting more quickly to demand and assuring that the transaction requesting it would be served as quickly as feasible. The ‘balanced’ threshold would be slower to adapt and more stable, making it inappropriate for time-sensitive transactions, but it would provide a lower, more consistent price in exchange for a longer, more variable waiting period.

The ‘balanced’ and ‘immediate’ tiers are designed to manage transactions with varying degrees of urgency, while the ‘fair’ tier is designed to handle everyday transactions. The ‘fair’ tier is meant to be a refinement of Cardano’s present approach, keeping fees low (or even stable, by pegging to a basket of commodities/flat, as discussed in IOG’s blog [\[855\]](#) on stablefees) and eliminating any uncertainty for users. This tier would work similarly as Cardano does now (May 2022), as long as demand is minimal, and transactions fit inside half of the block.

However, if demand grows, a unique mechanism for ‘fair’ tier transactions will be activated. The approach would use a priority function to filter transactions in a fee-independent way. Giving precedence to transactions based on the age and quantity of their UTXOs is an example of this. The sum of the quantity of each input multiplied by its age, then divided by the total size of the transactions in bytes, would be the priority of a given transaction. This priority might be used with a threshold (updated dynamically after each block) to reject transactions with too low a priority. By constantly offering a cheap way into each block, such a method ensures liveness for each transaction at a low and predictable price, limiting the impact of a malicious attacker, or a rush in demand, on pricing.

The notion of the multiplier, which IOG established in the stablefees concept, is also extended and clarified by the tiered pricing approach. As a result, each of the three tiers has a deterministically computed multiplier, whose value is determined by the congestion of the appropriate tier in prior blocks. The ‘fair’ tier always has a multiplier of 1.

This technique differs from existing pricing approaches, such as those employed by Bitcoin or Ethereum (even allowing for Ethereum Improvement Proposal EIP-1559), [\[856\]](#) in which each transaction must surpass a variable fee to be included in a block. The disadvantage of this strategy is that the fee that everyone must pay is determined by the ‘richest’ customers. Worse again, this is the fee that the

wealthiest users pay to have it turned into a block ‘immediately.’ Furthermore, since the ideal bidding strategy is not obvious to users, these sorts of transaction fee mechanisms might unwittingly ‘shape’ demand or inadvertently raise prices, even if the fees are largely a function of supply and demand.

The multi-tiered strategy is more polished. It recognizes that not every transaction has the same requirements, allowing several use cases to take place at the same time and allowing users to easily choose the service they want. Tiered pricing allows for predictable and fair fees while reducing congestion on the main chain in this manner. Tiered pricing, when combined with design changes that concentrate on improving the main chain’s raw throughput capacity and processing power, demonstrates how Cardano will be able to handle any transaction processing demand.

February 2022 release

IOG are combining many code releases in 2022 to increase the ecosystem’s delivery predictability. The first big upgrade of 2022 was in February. IOG will continue optimizing, scaling, and adding new features via fresh release deployments in the next weeks and months. IOG will do this via well-defined incremental upgrades that aggregate new technology stack features into more manageable monthly releases. The February release was the first of three significant code releases in 2022, with the others coming in July and October.

Predictability is the driving force for this grouping approach. Cardano has seen substantial growth, and it is projected to continue to do so as 2022 progresses. Companies that depend on Cardano’s infrastructure may better prepare with key upgrade dates locked down. The February release included a number of significant changes and improvements:

- Ability to generate transactions that comply with the Concise Data Definition Language (CDDL) using the node’s native tools

CLI, rather than relying on third-party tools.

The way computers store data when they're executing is not necessarily a great way to store data when you're trying to send it across the network. When data is taken out of the computer's memory and passed on to another peer to propagate a block, it's important that a representation is taken out of the computer's memory and put through a process which is known as serialization.^[857] Serialization takes the data object and represents it in a way that is efficient for transport.

IOG uses Concise Binary Object Representation (CBOR) for serialization. It's based on JSON,^[858] used extensively in web development. The change IOG made was to CDDL. CDDL (Concise Data Definition Language) is like a schema for CBOR. IOG tried to enhance this schema for their underlying serialization representation. As a result, sending data across the network was now done more efficiently.

- Support for transactions with multiple signatures in incremental stages. While it was already possible to have a Cardano transaction signed by many entities using their private keys (equivalent to a joint bank account), this update allowed for incremental signing of a transaction. Instead of needing to sign the transaction simultaneously, one party could now sign it first, and then send it to the other
- SPOs could now check the leadership schedule using a new CLI tool. This tool allowed SPOs to inspect the slots where the SPO delivering the command will mint a block for the following epoch. Some were concerned that this capability raised security concerns, however the tool is structured such that each SPO may only examine their own impending schedule. They are unable to verify the schedules of any other SPOs
- A CLI tool for inspecting local mempools. This is a developer tool that allows you to view the local mempool, which is where

transactions are stored before being included in a block. This feature enabled developers to track the status of a transaction before it is put to a block

- A command-line tool for estimating script costs. Node users could now estimate the cost of executing a Plutus script with more accuracy. This is helpful since it allows developers to see what resources (memory / CPU limits, etc.) they're using when building smart contracts or validation scripts, which is especially valuable for creating Plutus transactions. Developers could now see how much resources their scripts would need while running on-chain.

The February release was just the beginning and laid the foundations for future upgrades during 2022, with an emphasis on the hard fork combinator (HFC) events in June (Vasil) and October (Chang). October's update is named in memory^[859] of Philip Chang, the Voltaire Product Manager who sadly passed away.

Input Endorsers

By separating transactions into pre-constructed blocks, input endorsers increase block propagation speeds and throughput (amount of data transferred). This increases block propagation consistency and enables increased transaction rates.

Input endorsers are due to be released later this year, 2022. John Woods (former IOG head of Architecture) is confident input endorsers are going to be a 'near end game solution' for Layer 1 scaling, putting Cardano on the top of the pile when it comes to throughput for Layer 1. It's a mechanism which will enhance the process for block production and block propagation on Cardano.

The current process is to scoop transactions out of mempool, forge a block, then send it on to peers. With input endorsers, blocks will be created on an ad hoc basis, signed and counter-signed, and will be flying around the network on a near second-by-second basis.

The existing network Ouroboros Praos, where a block is generated every 20 seconds, is adequately meeting user demands. Input Endorsers will, however, keep Cardano ahead of the curve for the demands coming down the tracks with more and more businesses deploying on Cardano, as Plutus and Marlowe mature.

Currently, blocks are responsible for both consensus and holding transaction data. Input Endorsers divide each block in two. One of the blocks is responsible for consensus, with the other faster block assigned for holding transaction data.

The consensus block will essentially be freed up from its duty of managing transaction data. It will now have a pointer (using ‘reference semantics’) to the block holding the transaction data. This will reduce bottlenecks and the 20 second wait time, enabling blocks to be streamed constantly. The result is ‘a super fast layer 1’ as Director of Architecture, John Woods, outlined in his April 2022 Cardano 360 update.[\[860\]](#)

Input Endorsers were muted as far back as the original Ouroboros paper in 2016. Similar to block producers (BP), input endorsers (IE) are described as a stakeholder entity, in the sense that the amount of stake delegated to them affects their capacity to function.

According to Section 8.1 of the paper:

Input-endorsers create a second layer of transaction endorsing prior to block inclusion. [...] Note that input-endorsers are assigned to slots in the same way that slot leaders are, and inputs included in blocks are only acceptable if they are endorsed by an eligible input-endorser.

also

Note that blocks and endorsed inputs are diffused independently with each block containing from 0 up to d endorsed inputs.

IOG researcher Peter Gaži explained the input endorsers concept^[861] at the Cardano Summit 2021.

Input endorsers echo some concepts discussed in a paper called *Prism: Scaling Bitcoin by 10,000x*^[862] which is complemented by a video presentation^[863] on *Prism* (not to be confused with IOG's *Atala Prism* Decentralized Identity solution).

Professor Aggelos Kiayias gave a more detailed explanation in his video^[864] whose formulas and math are beyond the scope of this book. It's clear, however, that input endorsers are kind of an anthology of the best of Cardano as they leverage the power of Mithril, the Extended UTXO model, previous research on ledger combiners and the foundations established by previous Ouroboros iterations.

In the video, Prof Kiayias explained Ouroboros uses a 'longest chain' protocol^[865] similar to Bitcoin, except it is based on proof of stake.^[866] So it inherits all the decentralization and security benefits of Bitcoin, but with much less energy expenditure. 'Longest chain' protocols have serious performance limitations in terms of throughput. If a pipe represents a consensus protocol, where width is the throughput and length is the settlement time, then we want a nice wide, short pipe.

Based on research^[867] IOG published at the *ACM Computer and Communications Security Symposium* in 2021, it's possible to derive the upper bound for the throughput in a longest chain protocol. This works out to be only 8%, leaving 92% of the throughput capacity untapped. Ouroboros *Leios*, and specifically input endorsers, will resolve this critical shortcoming.

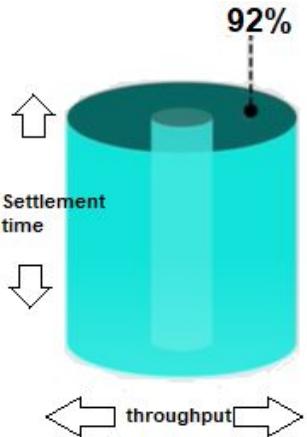


Figure 68: Longest chain protocol represented as a pipe

As mentioned previously, Ouroboros uses a networking strategy of applying *backpressure* to cope with times when there is peak demand for transaction processing. The system processes what blocks it can, while transactions wait in line to be pulled in for processing. Under peak traffic conditions, transactions will still be processed, but they have to wait their turn.

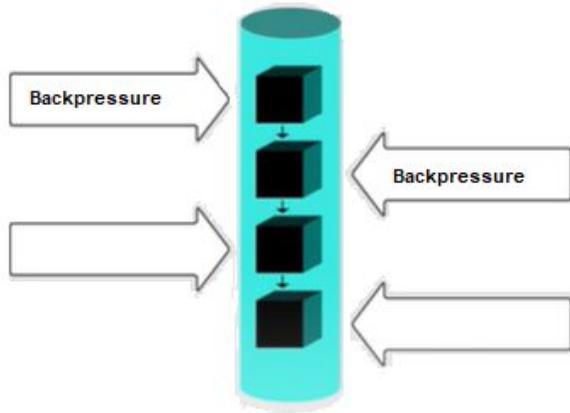


Figure 69: Backpressure networking concept

Input endorsers release segments of mempool (or ‘backup mempools with special privileges’ as a user on Stack Exchange [\[868\]](#) referred to them) to float around before they’re considered for processing in a mainchain block. These floating segments of mempool are called ‘input blocks’. This allows block producers to free up space in their mempools so they have more capacity to pull

transactions in. Mempool segmentation needs to be concurrent across all block producers.

IOG plans on adopting practices from spread spectrum communications^[869] to ensure there is minimal overlap between input blocks. Valid input blocks are checked as with longest chain blocks, but additionally, they are attested via the issuance of Mithril certificates. This means input blocks are transformed into verified transaction batches to be included in the mainchain by reference only. Input blocks' transactions and scripts are processed externally from the mainchain block validation. Longest chain 'ranking blocks' are used to organize or 'rank' these floating input blocks.

The serialization nature of longest chain protocol resolves 'double-spending' in input blocks. This strategy also leverages the strengths of the Extended UTXO model as script execution and validation occurs away from mainchain validation. The goal of higher throughput is now possible as the idle 92% capacity can now be utilized. The graphic below captures all the moving parts to input endorsers.

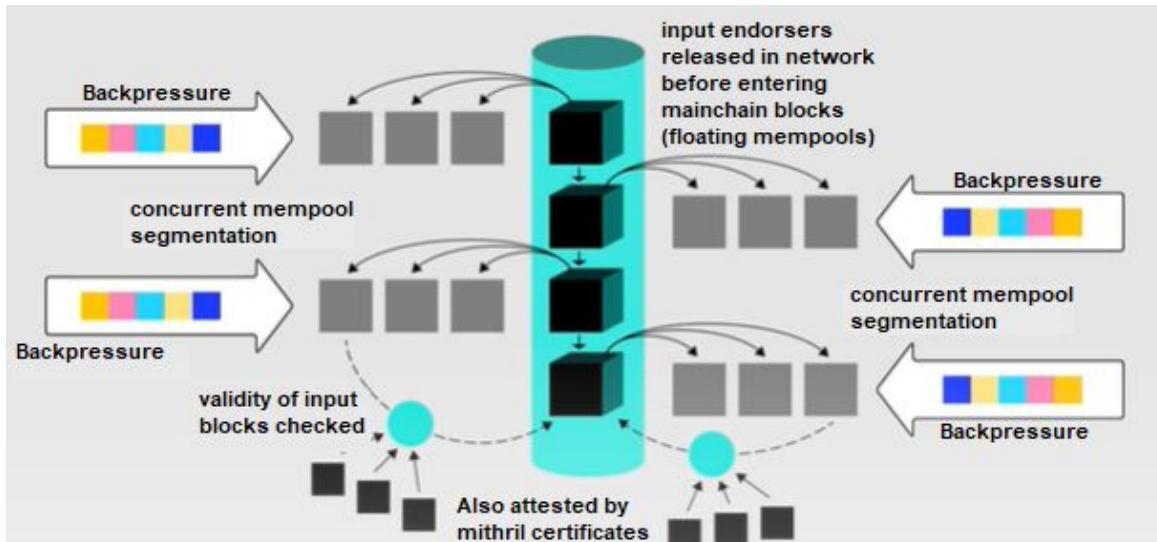


Figure 70: Input Endorsers graphic adapted from Professor Kiayias explainer video

As Prof Kiayias states in the video, this feature is still under development and details of its implementation will be published at a later date.

April 13, 2022. Re: Upcoming features for second half of 2022, Surprise AMA. CH:[\[870\]](#)

There are a few more things, like input endorsers, babel fees, the sidechain stuff that's coming at the end of the year, October and beyond... and those things are going to really double down and add to what makes Cardano so incredibly special. It's a hard thing to invent an entirely new field of science. If you think about these weird distributed systems that don't have centralized authority, they have to have resistance against all of these Byzantine actors that can come from anywhere in the world, and the very same set of people who maintain the system, are potentially a set of people who are trying to attack the system. It's a weird new field of science and there's only about 13 years of history behind it, and we've made such meaningful and significant contributions, and we've built great foundations for all of these things.

To see those foundations come to life, and become vibrant, and start flowering and producing downstream effects is so cool... and seeing all the interconnectivity of it. Mithril is interconnected with the sidechain strategy, which is interconnected with the Hydra strategy, which is interconnected with Ouroboros.. and all the magic of Ouroboros and the heterogeneity that Ouroboros provides is interconnected to all these things... wow...

Years ago, we were talking about it on blackboards and we said, 'if only we could do this and this...' and this is the year where we actually get to play around with it, and see it, and also to see what the community is doing with Cardano.

WingRiders (wingriders.com) just came out, I tweeted that this one was special because they added so much... staking while doing TVL (total value locked) stable coin support, a lot of really cool off-chain design patterns... It's an example of a very refined DEX, much more so than a lot on the market right now ...and the other ones will copy and emulate and learn ...and so there's

a rapid evolution that's occurring So I suspect that everybody's going to say 'hey we should catch up' ...but the fact that these things are evolving so quickly, is just a testimony to the quality of this community, and the quality of the technology ...and this is pre-Vasil! when Vasil comes out in June (September) you're just going to see a whole new wave of things like stable coins and other things... algorithmic stable coins like Djed and so forth that are kind of waiting for it (Vasil).

April 20, 2022, '4/20 Hangout with Charles' Twitter space, re: What can drive crypto adoption? CH:[\[871\]](#)

Yeah, it's a great question and the answer is I don't know, and it's a partial answer, but I could hazard a guess and so, in hazarding a guess, you have to argue by analogy, and so when you look at things like the Internet. It was really hard, in 1994, to sell the internet to people.

...you sounded like a stark raving mad person ...you're like ok, ok... so here's what's going to happen, like people are going to pay to have all these wires installed into their houses... and then they'll upgrade their computers and everything ..and then somehow some way, people are going to then make content and put it up there for no money...and build communities by themselves and autonomously connect to each other. And then we have to build all these protocols and new software...and then we're going to find out that infrastructure is not fast enough, and we have to add more infrastructure, like trillions of dollars of this stuff... and everybody in the whole world is going to do it, and they're going to do it in like 10 years. And if you miss out, then you're going to lose all these opportunities to create new businesses. Like if everybody's there, you have to find stuff. So you need a search company, and if all the people are there, they're going to want opinions. So you're going to be like a bulletin board company, and they're going to want to buy and

sell, so you'll need a town bazaar ...It's like you just go on and on....

They're like uh-huh uh-huh...and is the internet in the room with us today? is it here right now? I mean you just sound like a crazy person... and now when you look back at it, you're just like, 'oh yeah it's obvious, of course it's on the internet, it's great'... when i was growing up my mom was like don't talk to strangers, don't get into strangers cars, and now we literally have an app that summons a stranger for you, to get into his car, and he'll drive you somewhere, it's called 'uber'. It's like wow society's gone bonkers.

So when you ask, 'how do we get people to hold cryptocurrencies?' Well, I guess maybe the analogous answer is just to offer so much value in things that they're interested in, that they just happened to be in the room where the crypto's at, so they're going to just start naturally using that. So if that's where the video games are, and that's where the music is, and that's where the celebrities are, and that's where their information sources are, and that's where their human interactions happen to be. They're not going to want to leave that room to go engage in a commercial transaction. They're going to stay in that room to do that, and so the people who offer the capacity to do that, in a friction-free, very usable way, will end up being the predominant way people spend money.

Ok, so if you can get to that mindset, and that level of quality and infrastructure, then I think crypto will win, if it happens to be an asset... Now the danger is that those assets don't have to be cryptos. They could be CBDCs (Central Bank Digital Coins), they can be a litany of other instruments that are digital native, but don't carry the same values...and I don't know how to make people value the things that I value. I don't know how to make people value privacy. I don't know how to make people value decentralization. It is disheartening as hell to be in an industry, where you see people gain so much market cap, who don't give

a flying f\$ck at all about the level of decentralization their currency has, and when their network collapses, they just kick it and turn it back on... and they say, ‘that’s how it should be.’

Or you see the People’s Republic of China rate things, and the things that are right at the top are heavily centralized or federated. Of course they say ‘that that’s the case because that’s their model, God damn it’ ...and yet consumers seem to flock to these things, they seem to invest in these things and think these things are great bets. So it’s definitely a challenge and I think the only way to solve it is probably by having the collective community, as a whole, emergently sell that, as opposed to just ‘Charles Hoskinson is going to figure this out’.

I’ve got you guys as far as I have the skill to get you, I’ll still do the AMAs and the Twitter spaces, and I’ll talk until I’m blue in the face. But the next wave has to be done by the community and there has to be a demonstration of it, or...

Or it’s got to be done by crisis. There’s a whole lot of people in Ukraine right now, that think ‘boy this whole decentralization thing is a pretty good idea’ because they just survived the mother of all cyber-attacks from Russia and there’s a lot of IDPs (internal displaced persons) and displaced people who now aren’t able to access their digital lives, and if they lived in a blockchain structure, they’d still have access to it. So 35 million people just got sold on the idea of resilience and decentralization, and transnational standards.

It’s sad that that’s the price of admission to learn these types of things, but that’s where they’re at, and so that’s an opportunity, when peace comes, to go and sell that and say, ‘hey, let’s make sure moving forward this never happens again in this particular way.’

...and that’s a permanent constituency. And there are a whole lot of people who went through Covid who saw the propaganda

and the misinformation, and the consolidation of the media, and the agenda that was pushed upon us...and just how crazy it was. And now they say, ‘boy, deplatforming is a real thing. Boy, this is really bad propaganda. Boy, these people are lying to us. We need decentralized media. We need decentralized social media. I think we should have freedom of expression. That’s a human right, we should definitely make sure we have that power.

So it's easier to sell them on that particular idea. So the burden is on the entrepreneurs now, the millions of people in the Cardano ecosystem, to recognize each of those categories and scratch that itch, go take care of that particular problem... and bring those people permanently into the ecosystem, and then, since they're here, convenience will set in, and they'll want decentralized money in addition to that, and they have it with ada and stable coins derived from it.

May 2022. Charles Hoskinson, Update from Washington^[872]

IOG sent a delegation to meet lobbying groups, advocacy groups, meetings with congressional staff and staff of the US senate.

I, for one, have always been optimistic, and I'm not so cynical to believe that nothing can be accomplished. I think a lot of very well intended, good people do want to see things move forward and a lot of well-intended people do want to see this industry continue to survive. I was surprised by how many allies, adherents and advocates, even amongst government officials, that I met while I was here in Washington...but proof is an action, it's not in words and we will see over the next year or so what happens.

Now we, as a community, our strength has always been our capacity and ability to hang together, and to show our work. We will continue, as a community, testing governance experiments. We will continue, as a community, to get ever more decentralized and resilient, and diverse... and we as a community will continue to innovate. Many of the things we are doing in Cardano are not just about scalability and performance

and DevX (developer experience) and quality of code but have a lot to do with the social elements of a cryptocurrency.

It is a very rare and unique opportunity, that each and every one of you is participating in the construction of a digital government, as much as you are participating in the construction of a protocol...and everything about how decisions are made, how we change things, is inevitably going to be up for grabs, by those who are willing, not those who are privileged, which is a special thing.

I think there's a lot that Washington can learn from us, as an ecosystem, and the things that we do could potentially have deeper ramifications than just the governance of Cardano as a whole. So it's a conversation, it's an engagement, and there's a lot of work to do, there's a lot of places we have to go, there's a lot more shoe polish that has to be worn off, and a lot more trips to Washington...but if they're as productive as this one, that I took, then that's a good sign.

[...]

I really do want to close with one final point. I did discover that certain members of the Bitcoin community are actively telling lawmakers to write into legislation that everything, but bitcoin is a security....to write into legislation, every attempt possible to delegitimize or outright ban, proof of stake cryptocurrencies. This was extremely disappointing and disheartening. I like to believe that despite the fact that we have political differences, or technological differences, or differing financial incentives, that we would fight these things in the marketplace of ideas and the marketplace of users and traditional competition. The attempt to co-opt the US Federal Government, and legislative process, to ban your competition is anathema to every single thing the Bitcoin movement was founded upon.

This is the behavior of multinational banks, it's not the behavior of people who came from libertarian principles, and free market

principles. It's disgusting, it's reprehensible, and it's unbelievable that people would tell the staff of members of congress and senate to do these things. Saw the messages, saw the emails, heard it from many different sources and we know who you are. So it's childish, it doesn't really have much of an impact, and frankly it delegitimizes the people saying and doing it, but it does show that our industry has a long way to go. We have to be mature, we have to be adults, and we have to acknowledge that problems have occurred.

When tens of billions of dollars get lost in a matter of a week, and the people responsible for that will probably still walk away with millions, if not billions of dollars, and many people were warned that these things could happen and there are no consequences or perceived consequences, this is an invitation for heavy regulation. This is an invitation for sweeping legislative changes, that in hindsight, could be very damaging or problematic to our industry. For some reason, a lot of people don't seem to want to call out this behavior. They just say, 'let's move on and pretend like it didn't exist', and the fact that maximalism has gotten to the point where dirty tricks are being played, and people are trying to convince politicians now to encode maximalist principles into US law, is another example of just the fractious nature, and the childish nature and the immature and irresponsible nature, of some members of this industry.

I think we can all be better, and I sincerely hope that the other leaders in the space show up here and express themselves in productive, positive ways, and are willing to collaborate and cooperate on some basic principles.... like the standards of smart contracts. The definitions of things like decentralization...trying to create regulatory frameworks that actually make sense, as opposed to ones that are just extensions of things that came up for in the 1930s.

I'm willing to work with pretty much anybody. If any leader of the cryptocurrency space called me tomorrow, and said 'let's do something together', I'll pick up the phone call and have that conversation. It's for the greater good of this industry, as a whole, and I'd like to believe that there's at least more than one person willing to do that, and if we work together, collectively, we command as an industry, trillions of dollars of economic value and a very strong voice.

If we compete with each other, and fight each other, finger point, name call or attempt to use the process to damage each other's competition, we will neither accomplish that end nor will we achieve the end of legitimizing and stabilizing the industry. Rather we will hand it to the legacy actors, who will never give it back. It's a choice we have to make, we have to hang together, or divide, fall apart.

Vasil & Chang Releases

Scaling Cardano in 2022		
February	June: Vasil	October: Chang
CLI transaction creation	Plutus version 2.0	Governance
Leadership schedule	Enhancements to crypto primitives (VRF, KES)	Smart contract evolution
Multi-signature capabilities	Script collateral handling	Performance
Local mempool monitoring		
Script cost estimation		

Figure 71: Cardano hard fork combinator (HFC) event schedule

Cardano has come a long way in a short space of time. The Byron

era was slow and frustrating, but it led to the creation of the hard fork combinator and the steady release cadence we've seen since. It wasn't long ago when the idea of proof of stake was ridiculed, now it's self-evident. The extensive research and meticulous implementation of prior eras mean developers are building on granite. There has already been the unexpected NFT boom on Cardano, a result of the right features and easy user experience. When I was wading through the jargon, studying for my masters (2018), I remember thinking at the time a term like non-fungible token (NFT) would never catch on. Now NFTs are on the verge of going mainstream. The ecosystem has matured with dozens of companies building on Cardano. The *Lace* light wallet platform will soon cater for Catalyst voting and partial delegation. But it's just one wallet competing in a thriving ecosystem.

Cardano has stayed true to its principles, even when it was inconvenient. The incentivized testnet (ITN) could have been a cryptocurrency in its own right, but it was just an *orderves* before Shelley mainnet. Cardano has approached development from a different angle to other 'build first, fix later' blockchains. With hacks and scams now weekly news in the industry, this methodical and sensible approach is a breath of fresh air. There is still much to do, and many questions unanswered. Will the Vasil hard fork attract new developers to Cardano? Will input endorsers be an 'end game' scalability solution? What will multi-resource consensus look like? When will support for partial delegation and proxy keys arrive? Will the US Senate really ban encryption?

Charles Hoskinson reflects on progress to date and gives a sneak peak of the future in his 'Let's Talk Roadmap and Governance' update.^[873] One thing is certain, there will be plenty to write about for the next edition of *Cardano for the Masses*.

Appendix: Cardano Architecture

Much of Cardano's architecture is updated regularly, especially after major hard forks like Vasil. It's always best to check the documentation and the latest component release notes. [\[874\]](#)

CardanoDocs [\[875\]](#) is overdue for a refresh, however, the developer portal [\[876\]](#) is well maintained (at time of press).

Cardano was built in modules, with interconnected components that may be leveraged in a variety of ways. The Cardano 'platform stack' is made up of these components. They collaborate behind the scenes to assist the development and usage of the live Cardano blockchain. The relationship between Cardano's system components is shown in the diagram below:

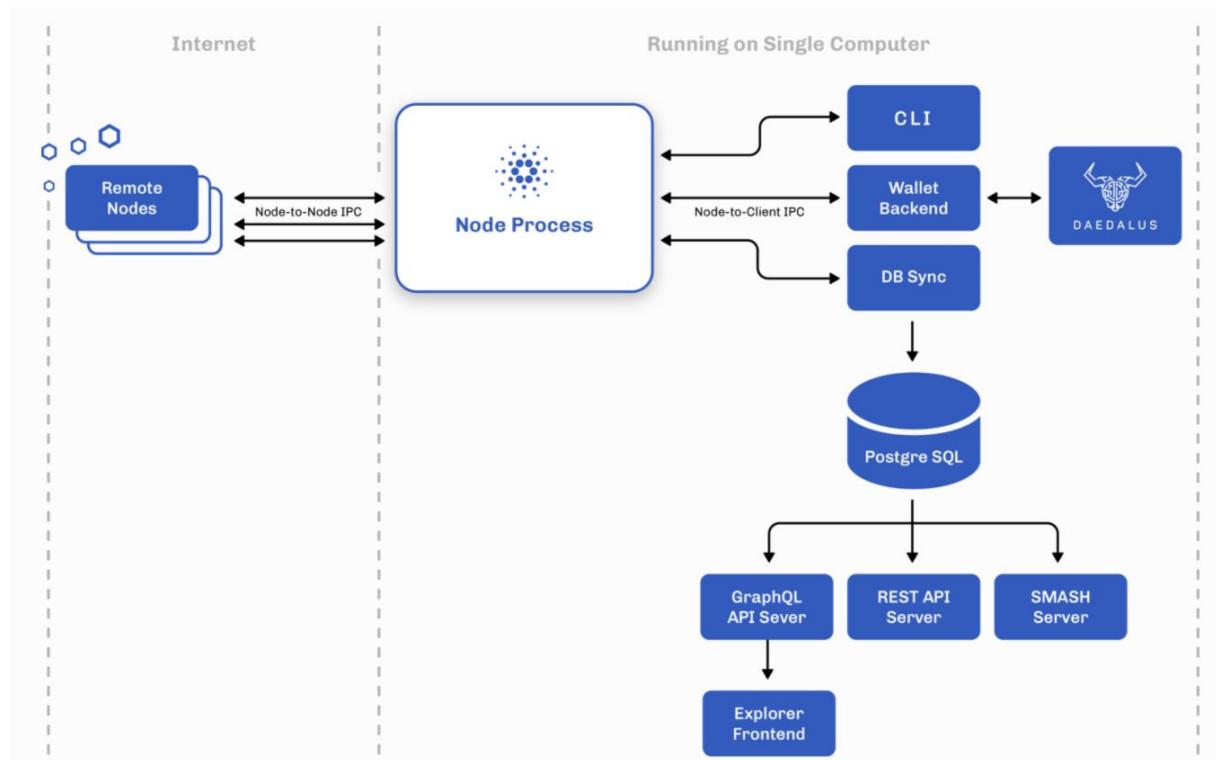


Figure 71: Cardano architecture overview

Cardano's present implementation is very modular. It consists of the following parts (various deployment use cases will need different

combinations of these):

- Cardano Node [\[877\]](#)
- Command line interface (CLI) [\[878\]](#)
- Cardano wallet [\[879\]](#)
- Cardano db-sync (synchronizes blockchain data with a relational database)
- GraphQL API server (Apollo)
- Rosetta API (blockchain communication protocol)
- Adrestia [\[880\]](#)
- REST API components [\[881\]](#)
- SMASH server

The Daedalus wallet isn't part of the core stack, but it communicates with the other components.

Developers should also familiarize themselves with:

- cardano-addresses [\[882\]](#): module providing mnemonic (backup phrase) creation, conversion of mnemonics to seeds for wallet recovery, and other address derivation functionalities
- cardano-ledger-specs [\[883\]](#): formal specification, executable models of the ledger rules.
- bech32 [\[884\]](#): Haskell implementation of the Bech32 address format (BIP 0173)

Cardano Node

The cardano-node is the node's top-level repository, including components from other packages such as consensus, ledger and networking, configurations, CLI, logging and monitoring. Wallet and explorer features are no longer included on the node. The wallet and explorer backends are two independent components that connect with the node through local Inter-Process Communication (IPC) [\[885\]](#) in separate external processes. The Cardano node is a program that runs on your computer and serves as the backbone of the network, allowing anybody to join the decentralized blockchain. Daedalus is a full-node wallet, which means that if you run it on your local PC, you are essentially contributing to the network's operation.

The networking layer

The networking layer comes next. Each Cardano node is connected to a distributed infrastructure that handles the blockchain and related services. The network is made up of nodes that connect with one another in order to keep track of the distributed ledger, process transactions, and interact with user wallets and other services. The network's core is made up of decentralized nodes known as stake pools, which work together to verify blocks and add new ones to the chain. They are backed up by relay nodes that handle network connections and define the network's overall structure. The Daedalus wallet and other services connect to this network through specialized nodes to monitor and submit transactions on-chain.

Cardano nodes keep in touch with each other. Communication between the nodes is enabled through a collection of mini-protocols. Each mini-protocol implements a fundamental information exchange need, such as notifying peers of new blocks, sharing blocks as required, or distributing new transactions throughout the Cardano network. Mini-protocols are defined by the network protocol version for connection reasons.

So nodes are in charge of:

- Running the Ouroboros protocol
- Validating and relaying blocks
- Producing blocks (not all nodes)
- Informing other local clients about the status of the blockchain

You may only truly trust nodes that are self-operated. This is why Daedalus keeps a background full node running.

Node process

The cardano-node is the node's top level, and it contains other subsystems, the most important of which are consensus, ledger, and

networking, as well as CLI, logging, and monitoring.

Node-to-Node IPC protocol

As part of the Ouroboros consensus mechanism, the node-to-node Inter-Process Communication (IPC) protocol allows for the transmission of blocks and transactions across nodes.

The node-to-node protocol is a hybrid protocol made up of three ‘mini-protocols’:

- chain-sync: This command is used to follow the chain and get block headers[\[886\]](#)
- block-fetch: This command is used to retrieve block bodies
- tx-submission: This command is used to forward transactions.

On a single long-running Transmission Control Protocol (TCP) connection between nodes, these mini-protocols are multiplexed. To allow for peer-to-peer (P2P) settings, they may be executed in both directions on the same TCP connection.

The overall protocol - as well as each mini-protocol - is built for a trustless environment in which both parties must protect themselves against Denial-of-Service (DoS) threats. Each mini-protocol, for example, employs a consumer-driven control flow, in which a node asks additional work only when it is ready, rather than having work pushed to it.

The protocol is modular and evolvable: version negotiation is used to agree on the set of mini-protocols to use, allowing for the inclusion of new or updated mini-protocols without breaking compatibility.

Node-to-Client IPC

The node-to-client IPC protocol enables local apps to communicate with the blockchain via the node. Wallet backends and blockchain explorers are examples of such applications. These apps access the

raw chain data and query the current ledger status through node-to-client communication. It also allows users to enter new transactions into the system.

The node-to-client protocol is similar to the node-to-node protocol, but it employs a separate set of mini-protocols and local pipes instead of TCP connections. As a result, it is a low-level, limited interface that only shows what the node can do natively. The node, for example, gives users access to all of the chain's raw data but does not allow them to query it. Dedicated clients, such as cardano-db-sync and the wallet backend, are in charge of delivering data services and higher-level APIs.

Three mini-protocols make up the node-to-client protocol:

- **chain-sync**: This command is used to follow the chain and get blocks
- **local-tx-submission**: This command is used to submit transactions
- **local-state-query**: This command is used to query the status of the ledger.

Instead of only block headers, the node-to-client version of chain sync contains complete blocks. This eliminates the requirement for a separate block-fetch protocol. The local-tx-submission protocol is similar to the node-to-node tx-submission protocol; however, it is simpler and returns transaction validation failure data. The local state query protocol allows users to query the current ledger state, which includes a wealth of information not immediately visible on the chain.

Visit the Cardano Docs [\[887\]](#) to learn more about the Cardano node communication protocols and networking protocol design.

Cardano cli (command line interface)

The CLI tool on the node is the system's 'Swiss army knife.' It can accomplish practically anything, but since it's text-based and lacks a GUI, it is not for novice users.

The command-line interface (CLI) tool can:

- Get data by running queries on the node
- Complete and submit transactions
- Construct and sign transactions
- Keep track of cryptographic keys

For more details visit the Cardano Docs GitHub page[\[888\]](#)

Cardano wallet

For interacting with the wallet, the Cardano wallet component includes a HTTP[\[889\]](#) application programming interface (API) and a command-line interface (CLI). It may be utilized as part of a frontend like Daedalus (daedaluswallet.io), which offers a user-friendly wallet experience that allows you to keep track of your ada and send and receive payments. Daedalus includes a complete Cardano node that records the whole history of the Cardano blockchain as well as validating all blocks and transactions for fully trustless and autonomous functioning.

Daedalus is made up of two parts: a wallet interface and a backend. The user sees and interacts with the frontend GUI (graphical user interface). The backend is a service process that keeps track of the user's wallet and does all of the 'donkey work,' such currency selection, transaction creation, and submission. The node-to-client IPC protocol is used by the backend to communicate with a local node, while the HTTP API is used to communicate with the frontend. The wallet may also be interacted with via the backends' CLI. The wallet backends' API may also be utilized outside of Daedalus. This is a simple approach for software developers to interface Cardano with other systems and apps.

A full Cardano node is running behind the scenes in the wallet. Unlike a light client wallet, it loads the whole shared ledger and verifies all transactions, ensuring the blockchain's security for all

participants. Most users should start with Daedalus. The landscape is changing however with the likes of dcSpark's (dcspark.io) relatively new Flint Wallet (flint-wallet.com). The Mithril^[890] protocol (Chapter 9) will enable more and more light wallet options.

Key features

- Simple installation with bundled Cardano node setup in a single click
- Wallets and encrypted private keys^[891] are kept locally and are not shared with third-party servers
- Trustless operation using a locally operating complete Cardano node that independently verifies the blockchain's entire transaction history
- Participates in the Cardano protocol to support the Cardano network
- Mnemonics phrases for wallet backup and restoration
- Support for staking
- Complete independence from third-party servers and services
- Create a paper wallet to keep your money safe while you're not connected to the internet.

Downloading Daedalus

You should only ever download the Daedalus wallet from the official website. As Cardano becomes more popular, more and more scams^[892] target ada holders.

For more information about Daedalus visit IOG's dedicated Helpdesk page^[893]

Some other wallet types:

- NamiWallet (NamiWallet.io) is a Browser extension / Simple UX
- Eternl (eternl.io) is another Browser extension / Mobile app
- dcSpark's Flint wallet is EVM compatible

Cardano DB Sync

The Cardano node holds the blockchain and the accompanying information required to validate it. This design philosophy focuses on lowering code complexity, as well as computational cost and resource use, by keeping the node's local interfaces to a bare minimum and relying on external clients to offer a range of helpful interfaces and additional functionality. The node does not offer a user-friendly query interface for searching existing blockchain data. A separate component provides this data service, which uses a Structured Query Language (SQL) database.

DB Sync is the component that monitors Cardano chain activity and logs blocks and transactions in PostgreSQL. It powers cardano-graphql^[894] as a middleware^[895] component. To provide higher-level interfaces for blockchain discovery, DB Sync saves blockchain data obtained from [cardano-node](#) in an intermediary database. It also supports services like the Cardano Explorer, a graphical user interface that reflects the blockchain data in an understandable way and enables a variety of queries to get Cardano blockchain data from PostgreSQL. The Cardano GraphQL API is a cross-platform implementation of the GraphQL data query language.

Cardano DB Sync components:

Db Sync acts as a client, connecting to the local node and synchronizing with on-chain activities. The on-chain data is then mapped to the relational model using the PostgreSQL database.

Cardano users and developers may use DB Sync to find out particular information on block production and recent transactions. Block metadata, which allows users to follow the chain and investigate transactions inside blocks, is included, but cryptographic signatures are not.

The database does not contain cryptographic signatures, but it does save enough data to track the sequence of blocks and examine the transactions inside them.

The PostgreSQL database is meant to be read-only by other programs. The database structure is fully normalized, [\[896\]](#) reducing data inconsistencies (specifically with the use of foreign keys from one table to another). Postgres Views [\[897\]](#) may be used to create more user-friendly database queries by joining tables together.

- cardano-db : offers a set of data types and methods that may be used by any Haskell application that needs to communicate with a database. It specifies the database schema in particular
- cardano-db-tool : Cardano-db-sync databases are managed using this utility (create, run, validate and analyze migrations).
- cardano-db-sync : serves as a Cardano node by following the chain and storing the data in a PostgreSQL database
- cardano-db-sync-extended : cardano-db-sync-epoch-data is a simple modification to cardano-db-sync that maintains an extra table with epoch data
- db-sync-node : built to save data in a PostgreSQL database using a locally running Cardano Node.

Cardano-db-sync and cardano-db-sync-extended are completely interoperable and share the same database structure. The sole difference is that the extended version keeps track of an Epoch table, while the non-extended version creates but does not keep track.

To be versatile, the db-sync-node is developed in a very modular approach. It uses a Unix domain socket to connect to a locally operating cardano-node (one that is linked to other nodes in the Cardano network across the internet using TCP/IP). Db-sync-node retrieves blocks, maintains its internal ledger state, and saves bits of each block in a PostgreSQL database on the local machine.

PostgreSQL is a relational database that is used to convert on-chain data into a relational representation. It uses the normalization approach to hold relational data without duplication, addressing individual user demands and constraints.

The interaction between the system components is shown below:

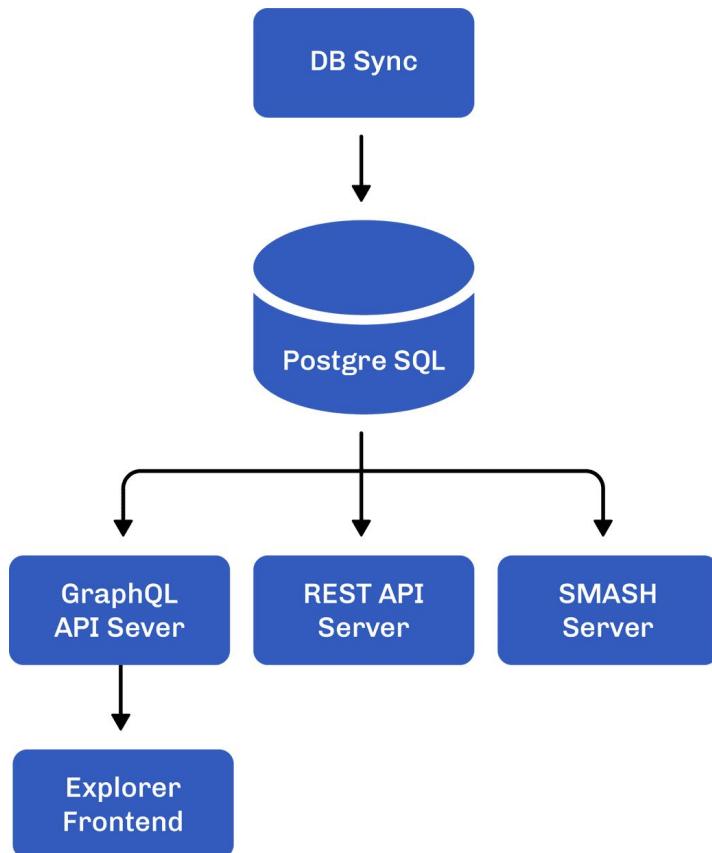


Figure 72. PostgreSQL

GraphQL and REST API expose an interface to the data contained in the database that can be accessed from programs such as an Excel spreadsheet. The Frontend explorer is the most user-friendly tool; it pulls data from the primary database and displays it in an easy-to-use GUI. Another component, the SMASH server, collects stake pool information and delivers a list of legitimate stake pools with validated metadata to pool operators and delegators.

Best Practices:

This section explains how to use the Cardano DB Sync component properly. Here are some examples of what a Cardano DB Sync instance on a certain network might be used for:

- Look up the information of any block, transaction, address, or stake pool on that network, generally using the hash or an index into another database
- For a certain epoch, get the balance of any stake address
- For each epoch, check the amount of ada that has been delegated to each stake pool.

Sample queries may be found here: Sample Cardano DB Sync queries.[\[898\]](#)

Recommended Hardware for Cardano DB Sync

For cardano-db-sync (with both db-sync and the node operating on the same system), IOG propose the following hardware:

- A Linux distribution (for example: Debian, Ubuntu, RHEL, CentOS, Arch)
- 8 Gigabytes of RAM
- 2 CPU cores
- 50 Gigabytes or more of disk storage

The db-sync and PostgreSQL servers should be installed on the same system, if possible. There is a lot of data traffic between db-sync and the database during syncing (when historical data is fetched from the blockchain). Traffic to a local database is substantially quicker than traffic to a database located on a local area network (LAN) or remotely.

To use cardano-db-sync, you must first have a cardano-node operating locally. See the building and running instructions[\[899\]](#) for further details.

Sample Cardano DB Sync queries

The psql program that comes with PostgreSQL is used to conduct queries. You can connect to the database using the following commands from the cardano-db-sync git checkout:

```
PGPASSFILE=config/pgpass-mainnet psql cexplorer
```

IOG include a set of sample SQL queries in the documentation that run against the `db-sync` database.

IOG's 'Cardano Docs' also include a section[\[900\]](#) which demonstrates how Cardano users may access blockchain data stored in the database, how to operate with the PostgreSQL database and its numerous queries.

Note: If you want to build and execute anything in this repository, avoid using the master branch and instead use the most recent release tag.

To learn more, Go to 'Cardano DB Sync' GitHub repo[\[901\]](#)

Carp – dcSpark's replacement for db-sync

Carp is a new Cardano indexer[\[902\]](#) that stores its data in a Postgres database (SQL). As outlined in the last section, db-sync is a SQL database-powered indexer, used in practically all Cardano projects. Db-sync was started by IOG and preserves all of the Cardano blockchain data in one big database, allowing you to access practically everything you need. Carp aims to improve upon db-sync by being more flexible, modular, faster and developer-friendly. Read more about how dcSpark plan to make Carp the indexer of choice for developers in their blog.[\[903\]](#)

It's always best to DYOR (do your own research) in such cases and find what works best for your use case. You can find help on sites like Cardano Stack Exchange. See *What are the benefits of using Plutarch?*.[\[904\]](#) The protocol enhancements that arrived with the Vasil HFC (hard fork combinator) event affect Plutus Core, therefore benefitting all these options including Plutarch (which is an alternative to Plutus Tx).

GraphQL API Server

The GraphQL API offers a query interface to all blockchain data through GraphQL, which is a suitable alternative for web-based client applications (for example, JavaScript or other browser-based languages) that communicate with other services using HTTP/REST APIs. It's a replacement for the database's SQL interface. For accessing chain data, application developers have the option of using SQL or GraphQL. The Apollo Server,^[905] an open source, spec-compliant GraphQL server that works with any GraphQL client, is used to build the API.

Cardano API that is cross-platform, typed, and queryable. The project includes a docker-compose stack^[906] that serves the included cardano-graphql-server Dockerfile, the expanded hasura Dockerfile, and cardano-node-ogmios, as well as numerous packages for assembling GraphQL services to fulfill unique application needs. The schema is written in native .graphql, and it's used to create a TypeScript^[907] package for client-side static typing. If you need to send a signed and serialized transaction to the local node, you can use the mutation provided.

Apollo Server^[908] provides the NodeJS execution engine through an HTTP endpoint, as well as Prometheus^[909] support for open-source metrics and operation filtering to prevent unexpected requests. Consider just importing the executable schema from the @cardano-graphql/api-* packages if you want additional control over the server or want to connect the schema to an existing service.

GraphQL is a query language and execution environment for a variety of computer languages with server and client implementations. The language is suitable for defining most domains and can be encoded for network transmission. It also hashes schema implementations for assurance.

Javascript (JS) is often referred to as the 'language of the web'. JS, along with TypeScript (a superset of JS), has the greatest pool of production-ready libraries, developers, and interoperability. GraphQL

Code Generator^[910] created TypeScript definitions for the schema, which are accessible on npm.

Ogmios (ogmios.dev) is a Haskell-based protocol translation service that runs on top of cardano-node. It uses WebSockets to provide a JSON interface and allows programs to communicate with Ouroboros' client mini-protocols through remote procedure calls.

Go to 'Cardano GraphQL' in the GitHub repo^[911] for more details.

Rosetta API

The Rosetta application programming interface is a high-level interface that attempts to make the integration process simpler, quicker, and more reliable, so you can write once and use it everywhere. To make Cardano integration easier, IOG designed a one-of-a-kind [cardano-rosetta](#)^[912] implementation. This interface is especially beneficial for exchanges, since it allows them to connect with the Cardano blockchain using the same interface they use for other blockchains.

Rosetta is a collection of open-source tools and specifications for integrating with blockchains. Rosetta offers a high-level interface that can be adapted to operate with any chain and serves as a general-purpose integration framework. Rosetta's mission is to make the integration process simpler, quicker, and more reliable, so you can create once and deploy your blockchain everywhere.

To make the process of integrating with Cardano as simple as possible, IOG developed their own [cardano-rosetta](#) implementation. [Bitcoin-rosetta](#)^[913] and [ethereum-rosetta](#)^[914] also exist. The only thing that all implementations have in common is that they all use the same interface.

The argument for integrating with Rosetta is that a single interface may communicate with all blockchains that have implemented that interface in a smooth manner. This is especially beneficial for exchanges, since they can connect with the Cardano chain using the

same interface that they use to deal with other chains (Bitcoin, for example.) To accommodate the different chain implementations, blockchain-specific operations^[915] are interpreted.

Getting started with Rosetta

The Data API^[916] and the Construction API^[917] are the two main components of the Rosetta API. These APIs work together to let you read and write to blockchains in a consistent format using a standard communication protocol. The rosetta-specifications repository contains the specs for these APIs.

Read the Rosetta API specification for further information. View the Flow of Operations^[918] for an overview of the interactions.

Developer examples, exchange examples, and API calls^[919] may all be found here.

For more in-depth details Go to ‘Cardano Rosetta’ in the GitHub repo and visit the official Rosetta website.^[920]

Rosetta use cases

The following are some examples of typical Rosetta use cases:

- Sending transactions^[921]
- Staking key registration and delegation^[922]
- Withdrawals^[923]
- Sending transactions with single multi assets^[924]

Adrestia

Adrestia is a suite of solutions that enable integrating with Cardano simpler. It consists of a number of Application Programming Interfaces (APIs), Command-Line Interfaces (CLIs), and Software Development Kits (SDKs). Integrating with any blockchain may be difficult for exchanges and developer partners. Technology advances at such a rapid rate that keeping up with the speed of change might be impossible. The Cardano development and release process is

presently moving at a rapid speed. Managing multiple software development work streams operating at various rates might seem like changing the engine of a plane while in flight.

Cardano's mission is to build decentralized applications, systems, and society with unrivaled security and long-term viability. It was built to be the most technologically sophisticated and ecologically friendly blockchain platform available, providing a safe, transparent, and scalable template for how people, organizations, and society work, communicate, and create.

In order to achieve these goals, IOG needed to figure out a means for their partners to connect with Cardano quickly, effortlessly, and reliably, regardless of what was going on below the hood. IOG sought to build a uniform manner through which all upgrades to the core node could be readily accepted by everyone, regardless of the speed and frequency of future rollouts.

IOG engineers founded the Adrestia team to assume responsibility for establishing all the web APIs and libraries that make Cardano available to developers and application builders, in order to make that integration and engagement with Cardano simpler and quicker. Users will always be able to interact with the node with ease, allowing developers to concentrate on speed and scalability. Adrestia was named after the goddess of rebellion because IOG want everyone to be able to interact with Cardano using these new interfaces, resulting in a 'revolution' in accessibility.

The Adrestia team's objective is to offer a consistent integration experience through Web APIs so that developers know what to anticipate between Cardano roadmap revisions. Users may browse the chain, perform transactions, and more, regardless of whether they are a wallet developer or an exchange.

The following are the APIs:

- cardano-wallet: An HTTP REST API for maintaining UTXOs, as well as other features
- cardano-submit-api: An HTTP API for submitting signed transactions on the Cardano blockchain
- cardano-graphql: A blockchain exploration API based on HTTP GraphQL.

Several low-level libraries make up the SDK:

- cardano-addresses: mnemonic manipulation, address creation, and derivation
- cardano-coin-selection: Coin selection and fee balancing algorithms
- cardano-transactions: Transaction-building and-signing utilities
- bech32: Implementation of the Bech32 address format^[925] in Haskell (BIP 0173).

Maintenance is simplified in addition to giving a flexible and productive approach to interface with Cardano. It takes less time to upgrade integrations between versions when there is consistency. This familiarity lowers the cost of maintenance. The program may then be deployed in days instead of weeks. At the end of the day, everyone can keep up with change. To get started, visit IOG's Adrestia project repo and review their user guide.

[Github](#) hosts Adrestia's components and associated repositories.

Cardano Docs includes sections on Integrating with third parties^[926] as well as Running stake pools and delegation for exchanges^[927]

REST API Components

An HTTP REST API for dealing with a local node is supported by two Cardano components:

- A dedicated transaction submission component with a single endpoint for transaction submission

- Access to blockchain data through a query component. This is a legacy component that was created to help people migrate from the Byron period. Any apps that use it now should consider switching to the GraphQL API or the SQL interface.

The reasoning for this is that since the REST API is no longer supported, there is no incentive for new apps to utilize it to query chain data. Because GraphQL does not yet support tx submission, the submission API is currently the sole HTTP-based API for tx submission. This means that any application developers who want to use web-tech APIs (rather than scripting APIs, low-level, or Haskell APIs) may use the REST API for tx submission.

Stake Pool Metadata Aggregation Server (SMASH)

Stake pool activities are at the core of Cardano decentralization, allowing servers throughout the network to establish consensus. The Ouroboros proof-of-stake consensus algorithm enables pool operators to agree on transaction validity and sign a block, which is then immutably recorded on the Cardano blockchain.

The Cardano network expands as more stake pools join the protocol. Operators create pools, recruit delegates, stake ada, earn rewards, and take a small share to cover operating expenses before distributing the remaining funds to pool members.

Decentralization of nodes is a crucial component. However, to maintain track of stake pool information and make it easier for delegators to choose a pool, it's critical to make sure that information about each stake pool is current and accurate. The impact of negative actors on the system, such as prospective attackers, spoof pools, and trolls, is limited as much as possible.

The Stake Pool Information Aggregation Server (SMASH) is a server that collects off-chain metadata provided by stake pools when they

register on the Cardano blockchain. This information comprises the stake pool's name, ticker symbol, web address, and so on.

In the Cardano architecture, a metadata aggregation server has two purposes:

1. Off-chain storage of stake pool metadata; and
2. To allow the monitoring of stake pool metadata without the need of a central censor.

The information is stored off-chain and referenced to during pool registration on the blockchain. SMASH gathers off-chain data to make accessing it easier, faster, and more reliable for wallets and other applications.

The SMASH server also solves the need for a centralized censorship body to monitor the content of stake pool information. Most wallet users and stake pool managers, for example, would want to be able to regard stake pool ticker names as distinct trademarks. A fair, on-chain method for resolving ticker name disputes would be much too complicated. Instead of verifying uniqueness on the chain, metadata aggregation might potentially ensure it via filtering. Various bodies may deploy several aggregation services with different strategies for filtering stake pool information. This allows wallet users and other stake pool metadata consumers to pick which policy, if any, to follow.

Policies in SMASH may be set up to filter information based on block lists or reserved ticker names. Daedalus may be set up to work with any SMASH server.

Although IOG originally ran the Smash server, the server code is open source and may be installed by anybody. As a result, IOG expects that the Smash strategy for decentralized metadata will be supported by the community in the future. For ada holders who like to support stake pool companies with a specific emphasis, Daedalus will enable them to create any server of their choosing and browse

bespoke stake pool listings - for example, charity pools, bare metal pools, or pools from a certain location.

How does SMASH work?

Smash is a system that is always updating. IOG was initially in charge of the IOG Smash server's maintenance and metadata curation as its operator. Stake pools that perform badly may be removed from Daedalus' presentation. Illegal or malicious metadata content, impersonation, the use of ticker names that were previously registered on the Incentivized Testnet (when this is not the same stake pool/operator), intellectual property rights violations, or stake pools that are no longer active are all factors taken into account when making such decisions.

Smash is a resource to help the community, most people will be familiar with it from the Daedalus delegating tab. Stake pool metadata may be gathered, retrieved, and stored in a semi-centralized setting using a SMASH server. The server is usually held by a single operator, who is then in charge of its upkeep as well as the curation and evaluation of stake pool metadata. It also allows for the resolution of disputes regarding offensive or duplicated stake pool ticker names, as well as the delisting of operators who have been proved to be bad actors.

Anyone may deploy the SMASH server code and become an operator because it is open source. Daedalus will eventually enable users to configure whatever server they choose and browse bespoke stake pool listings. Cardano's integrity and reputation are dependent on genuine registered stake pools, the absence of duplicate ticker names or trademarks, and the removal of material that users are likely to find offensive. SMASH was created to provide Cardano users with easier access to verified stake pool information and navigation choices.

The original version of SMASH was developed by IOG and is now used in the Daedalus delegation center, allowing users to see

accessible stake pools with verified names, ticker symbols, websites, and descriptions. With its standardized structure for publishing legitimate stake pools with validated information, SMASH's functionality enables stake pool operations and the delegation ecosystem.

SMASH Use Cases

Delegators, stake pool operators, exchanges, and wallets may install and use SMASH to assure a better degree of metadata accountability and upkeep as SMASH was launched to address metadata performance and privacy problems. The operators are then exchanges, wallets, or other SPOs that can verify and handle this information, as well as curate it for censorship through the delisting function.

For example, exchanges may utilize SMASH to get stake pool information and compare it to the on-chain registered hash. The exchange may then double-check existing metadata (size restrictions, content, and so on), manually construct new stake pools, and reserve their ticker names. It will be possible to delist a stake pool that has a duplicated ticker name, counterfeit, or inappropriate material.

Apart from censorship, there are many additional reasons to maintain SMASH servers: for example, an operator may opt to offer only charity pools or pools from a certain area for ada holders who wish to support locally operated stake pool enterprises.

More operators are likely to employ SMASH servers for metadata management. More servers will be added to a list of recommended SMASH servers in the Daedalus wallet as they become available.

The SMASH Handbook[\[928\]](#) in the official Cardano Docs goes into the command line intricacies of installing, running and delisting a SMASH server.

SMASH Handbook

The Stake Pool Metadata Aggregation Server (SMASH) Handbook gathers all presently accessible information regarding SMASH, including history, reasons for its creation, and technical specifics.

There are 5 main parts in this Handbook:

1. **Introduction:** A primer on the foundations of SMASH.
2. **Learn about SMASH:** This section provides an overview of the capabilities, reasoning, and use cases of SMASH.
3. **Installing the SMASH server:** This section contains information on how to install the SMASH server, as well as essential commands and testing instructions.
4. **Running the SMASH server:** This section discusses how to set up testnet and mainnet nodes, as well as how to generate SMASH and run tests.
5. **SMASH metadata management:** This section covers the intricacies of interacting with the IOG SMASH server, as well as how to delist a pool and report any problems to the operator.

This handbook is for Stake Pool Operators (SPOs) who wish to register their pools' information, as well as anybody interested in learning more about what SMASH is and how it operates.

To study SMASH in more detail, Go to ‘SMASH’ in the GitHub repo[\[929\]](#)

Constantly evolving stack

Plutus, the native smart contract language[\[930\]](#), as well as additional smart contract development languages like Marlowe[\[931\]](#) for finance and Glow (glow-lang.org) for DApps, will be incorporated into the Cardano stack iteratively during the Goguen era. IOG are producing new and enhanced components to compile Plutus, Marlowe, and Glow scripts, submit them to the blockchain, and interact with them.

The Alonzo protocol update built on previous token upgrades. Plutus pioneers and partners assisted in testing Plutus Core and were involved in the user acceptance process prior to mainnet launch. Plutus and Marlowe components, including both interpreters, have been formally included to Cardano's platform stack.

Glossary

[1]

Cardano360 - February 2021, youtu.be/YXaK0cvgoFQ?t=2184

[1] Sunday AMA 05/17/2020, www.youtube.com/watch?v=-CJ5pcullgg&t=690s

[2] IOHK Library, iohk.io/en/research/library/

[3] **OG** (crypto Original Gangster) is slang for a founder of any early crypto blockchain such as Vitalik Buterin, who invented Ethereum. A crypto OG can also refer to an early investor in Bitcoin or Ethereum.

[4] ‘A brief (and fascinating) history of money’,
www.britannica.com/story/a-brief-and-fascinating-history-of-money

[5] A **blockchain** is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. A blockchain is ‘an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.’

[6] **Bitcoin (BTC)** is a cryptocurrency and a payment system that uses a public distributed ledger called a blockchain. Invented by a single (or potentially a group) under the Satoshi Nakamoto alias. On 31 October 2008, Bitcoin was introduced to a cryptography mailing list and released as open-source software in 2009. There have been various claims and speculation concerning the identity of Nakamoto, none of which has been confirmed. The system is peer-to-peer, so transactions take place between users directly, without an

intermediary. These transactions are verified by network nodes and recorded in the blockchain, which uses bitcoin as its unit of account.

[7] A **cypherpunk** is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change. Originally communicating through the cypherpunks email list, informal groups aimed to achieve privacy and security through proactive use of cryptography. Cypherpunks have been engaged in an active movement since the late 1980s.

[8] Satoshi Nakamoto (2008) ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, bitcoin.org/bitcoin.pdf

[9] A **genesis block** is the first block of a block chain. The genesis block is almost always hardcoded into the software of the applications that utilize its block chain. It is a special case in that it does not reference a previous block.

[10] Bitcoin Source Code Walkthrough, drnealaggarwal.info/bitcoin-source-code-walkthrough/

[11] Bitcoin’s logo, decrypt.co/43923/bitcoins-logo-the-story-of-the-big-orange-b

[12] **Sound money** is money that is not liable to sudden appreciation or depreciation in value.

[13] **Price discovery** is the process of determining the price of an asset in the marketplace through the interactions of buyers and sellers.

[\[14\]](#) **Non-fungible token (NFT).** Such a token proves ownership of a digital item in the same way that people own crypto coins. However, unlike crypto coins, which are identical and worth the same, an NFT is unique. A craze started with the Christie's auction of *Everydays: the First 5,000 Days*, a collage of 5,000 digital pieces on March 11, 2021. Mike Winkelmann, known as Beeple, created the digital art and made an NFT of it. Bidding started at \$100. It sold for \$69.3m. Ten days later, Twitter co-founder Jack Dorsey sold an NFT of the first tweet for 1,630.5 ether (\$2.9m) and donated the proceeds to charity. NFT became the Collins Dictionary's word of the year for 2021. However, when the buyer of Dorsey's NFT tried to sell it a year later, the highest bid was just \$6,800. Ultimately, the value of an NFT is determined solely by what someone is willing to pay for it.

[\[15\]](#) 'Five biggest bitcoin transactions in history',
www.cryptovantage.com/news/heres-the-5-biggest-bitcoin-transactions-in-history/

[\[16\]](#) **Decentralization** is the process by which the activities of an organization, particularly those regarding planning and decision making, are distributed or delegated away from a central, authoritative location or group.

[\[17\]](#) Charles Hoskinson's Keynote from Dcentral, Austin 2022,
youtu.be/tf13d8TDWJ4?t=383

[\[18\]](#) The Edinburgh Decentralization Index,
www.bbcode.org/edinburgh-decentralization-index.php

[\[19\]](#) Addressing Blockchain's Hidden Trade-Off,
www.youtube.com/watch?v=FSByg_sdjaM

- [\[20\]](#) **Fiat money** has been defined variously as:
- Any money declared by a government to be legal tender
 - State-issued money which is neither convertible by law to any other thing, nor fixed in value in terms of any objective standard
 - Intrinsically valueless money used as money because of government decree
 - An intrinsically useless object that serves as a medium of exchange, also known as fiduciary money.

[\[21\]](#) In economics, **hyperinflation** quickly erodes the real value of a local currency as the prices of all goods rise. This causes people to minimize their holdings in that currency as they switch to more stable foreign currencies (hard currency).

[\[22\]](#) **Distributed ledger technology (DLT)** is a protocol or database that is consensually shared and synchronized across many sites, institutions, or geographies, accessible by many people, and enables the secure functioning of a decentralized digital database.

[\[23\]](#) A **consensus protocol** is a fault-tolerant mechanism that is used in blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies.

[\[24\]](#) BOOK Token : The Path to Decentralize Knowledge, book-token.medium.com/book-token-the-path-to-decentralize-knowledge-1ee651d657c3

[25] **Decentralized identifiers (DIDs)** are a type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (such as a person, organization, thing, data model or abstract entity) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities.

[26] **DID document**: a set of data describing the DID subject, including mechanisms, such as cryptographic public keys, that the DID subject or a DID delegate can use to authenticate itself and prove its association with the DID. A DID document might have one or more different representations.

[27] Charles Hoskinson on How did Ron Paul inspire you,
www.youtube.com/watch?v=jqiLVxSAt8w

[28] Slot Leader Episode 1: Interview with Charles Hoskinson,
www.youtube.com/watch?v=YT0PXYBEnuE, Charles Hoskinson: The Future of Blockchain in Africa, www.youtube.com/watch?v=m3eSEPrJ-1A

[29]

Open-source software (OSS) is software in which source code is released under a license in which the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose.

[30] Slush pool, slushpool.com/home/

[31] Cypriot Financial Crisis,
www.theatlantic.com/business/archive/2013/03/everything-you-

need-to-know-about-the-cyprus-bank-disaster/274096/
[32]

Charles Hoskinson and Brian Göss, 'Bitcoin or how I learned to stop worrying and love crypto', www.udemy.com/course/bitcoin-or-how-i-learned-to-stop-worrying-and-love-crypto/

[33]

Programmability is the capability within hardware and software to change; to accept a new set of instructions that alter its behavior. Programmability generally refers to program logic (business rules), but it also refers to designing the user interface, which includes the choices of menus, buttons and dialogs.

[34]

Ethereum is a decentralized, open source blockchain with smart contract functionality. Ether is the native cryptocurrency of the platform. Ethereum was conceived in 2013 by programmer Vitalik Buterin. Additional founders of Ethereum included Gavin Wood, Charles Hoskinson, Anthony Di Iorio and Joseph Lubin.

[35] Bitfund, www.crunchbase.com/person/xiaolai-li

[36]

Project Invictus, bitcointalk.org/index.php?topic=229315.0

[37]

Stablecoins are cryptocurrencies designed to minimize the volatility of its price, relative to some 'stable' asset or a basket of assets. A stablecoin can be pegged to another cryptocurrency, fiat money, or to exchange-traded commodities. Stablecoins redeemable in currency, commodities, or fiat money are said to be backed, whereas those tied to an algorithm are referred to as seigniorage-style (not backed).

[38]

Decentralized Exchanges (DEX) are peer-to-peer (p2p) online services that allow direct cryptocurrency transactions between interested parties. ErgoDEX and WingRiders are just two of many on Cardano.

[39] **Mt Gox** was a bitcoin exchange based in Tokyo. Launched in 2010, three years later it was handling 70% of all bitcoin transactions worldwide. In February 2014 Mt Gox suspended trading, closed its website and exchange service, and filed for bankruptcy protection from creditors. In April 2014, the company began liquidation proceedings.

[40] Cardano, Crypto Toxicity, & Institutional Collapse, youtu.be/5-vsU-Olhl?t=1405

[41] Dan Larimer, everipedia.org/wiki/lang_en/dan-larimer

[42] The History of BitShares,
how.bitshares.works/en/master/technology/history_bitshares.html
[43]

Colored coins are a class of methods for associating real-world assets with addresses on the Bitcoin network. Examples could be a deed for a house, stocks, bonds or futures.

[44]

Omni (formerly **Mastercoin**) is a digital currency and communications protocol built on the bitcoin blockchain. It is one of several efforts to enable complex financial functions in a cryptocurrency.

[45]

Charles Hoskinson Interview ‘Ivan on Tech’,
youtu.be/dWW_RRgAxKI?t=3500

[46]

A **maximalist** is a person who holds extreme views and is not prepared to compromise.

[47]

Non-Interactive Proofs of Proof-of-Work (NIPoPoWs) are short stand-alone strings that a computer program can inspect to verify that an event happened on a proof-of-work-based blockchain without connecting to the blockchain network and without downloading all block headers. For example, these proofs can illustrate that a cryptocurrency payment was made.

[48] **Proof of stake (PoS)** is a type of algorithm by which a cryptocurrency blockchain network aims to achieve consensus. In PoS-based cryptocurrencies the creator of the next block is chosen via various combinations of random selection and funds committed (ie, the **stake**). In contrast, the algorithm of **proof-of-work-based** (PoW) cryptocurrencies such as bitcoin uses mining; that is, the solving of computationally intensive puzzles to validate transactions and create blocks.

[49]

Bitcoin Alliance Canada, www.coindesk.com/bitcoin-alliance-launches-canada

[50]

The Erica Show EP9 - Charles Hoskinson, youtu.be/l35h0xW47-Y?t=904

[51]

Initial coin offering (ICO) is a means of crowdfunding via use of cryptocurrency, which can be a source of capital for start-up companies and open-source software projects. In an ICO, a

percentage of the newly issued cryptocurrency is sold to investors in exchange for legal tender or other cryptocurrencies such as bitcoin or ether.

[\[52\]](#)

A **smart contract** is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts were first proposed by Nick Szabo in 1996. Proponents of smart contracts claim that many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both. The aim with smart contracts is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting.

[\[53\]](#)

A **Founders' Agreement** is a contract that a company's founders enter into that governs their business relationships. The Agreement lays out the rights, responsibilities, liabilities, and obligations of each founder.

[\[54\]](#)

Hard fork: a total overhaul of the network's protocol, resulting in a shift in operational flow from one model to another. Cardano has a unique mechanism, called the hard fork combinator, for executing hard forks with minimal disruption. See Chapter 4.

[\[55\]](#)

Bitcoin Cash is a cryptocurrency created in mid-2017. A group of developers wanting to increase Bitcoin's block size limit prepared a code change. The change, called a hard fork, took effect in August 2017 and the cryptocurrency split in two. At the time of the fork anyone owning bitcoin was also in possession of the same number of Bitcoin Cash units.

[\[56\]](#)

Crypto tokens are digital assets that are built on a cryptocurrency blockchain. A blockchain is a digital ledger that stores information in

blocks that are linked. This information can be transaction records or full-fledged programs that operate on the blockchain, which are called smart contracts. The 'coin' of a cryptocurrency is a token. In effect, it's the digital code defining each fraction, which can be owned, bought and sold.

[57] The **DAO** was a decentralized autonomous organization (DAO) that was launched in 2016 on Ethereum. After raising \$150 million USD worth of ether (ETH) through a token sale, The DAO was hacked due to vulnerabilities in its code base.

[58] Charles Hoskinson on leaving Ethereum,
www.youtube.com/watch?v=AWSI78nh6jc

[59]

Polkadot is a blockchain network being built to enable Web3, a decentralized and fair internet where users control their personal data and markets prosper from network efficiency and security. Polkadot is the flagship project of the Web3 Foundation.

[60]

Cardano, crypto toxicity, & institutional collapse, youtu.be/5-vsU-OlhI?t=21

[61]

The future will be decentralized | Charles Hoskinson |
TEDxBermuda, www.youtube.com/watch?v=97ufCT6IQcY

[62]

A **crowdsale** is a type of crowdfunding that issues tokens that are stored on the user's device. The tokens can function like a share of stock and be bought and sold ("equity tokens"), or they can pay for services when the service is up and running ("user tokens").

[63]

Cardano CrowdSale, www.nasdaq.com/articles/iohk-launches-cardano-blockchain-ada-now-trading-on-bittrex-2017-10-02

[64]

The Erica show EP9 - Charles Hoskinson, CEO of Input Output, youtu.be/l35h0xW47-Y?t=611

[65]

In computer science, **formal methods** are a particular kind of mathematically based techniques for the specification, development and verification of software and hardware systems. The use of formal methods for software and hardware design is motivated by the expectation that, as in other engineering disciplines, performing appropriate mathematical analysis can contribute to the reliability and robustness of a design.

[66]

Ethereum 2.0 is a new version of the Ethereum blockchain that will switch to a proof of stake consensus mechanism, moving from the original, existing proof of work mechanism.

[67]

Crypto Twitter is a term to describe the Twitter subculture and community that surrounds the topics of blockchain and cryptocurrency.

[68]

The **tragedy of the commons** is a situation in a shared-resource system where individual users, acting independently according to their own self-interest, behave contrary to the common good of all users, by depleting or spoiling that resource through their collective action.

[69]

Prof. Aggelos Kiayias, iohk.io/en/team/aggelos-kiayias

[70]

A **Sidechain** is a blockchain that runs in parallel to the main blockchain. Tokens can be transferred and synchronized between the main chain and the sidechain.

[\[71\]](#)

The **Shinkansen** is a high-speed railway in Japan. Initially, it was built to connect distant Japanese regions with Tokyo, the capital, to aid economic growth and development.

[\[72\]](#)

Solana's Wormhole Hack Post-Mortem Analysis, extropy-io.medium.com/solanas-wormhole-hack-post-mortem-analysis-3b68b9e88e13

[\[73\]](#)

Haskell is a general-purpose, statically typed, purely functional programming language with type inference and lazy evaluation. Designed for teaching, research and industrial applications, Haskell has pioneered a number of programming language features.

[\[74\]](#)

Prof Phil Wadler, iohk.io/en/team/philip-wadler

[\[75\]](#)

Plutus is a suite of programming tools for creating Cardano smart contracts.

[\[76\]](#)

Marlowe is a programming language created specifically for the creation of financial smart contracts. It is restricted to financial applications and is intended for finance professionals rather than programmers.

[\[77\]](#)

Crypto 17, www.iacr.org/conferences/crypto2017/

[\[78\]](#)

Gazi1, Kiayias, Zindros (2018), ‘Proof-of-Stake Sidechains’,
eprint.iacr.org/2018/1239.pdf

[79]

Dynal Patel, ‘Incentivized Testnet: what is it and how to get involved’,
iohk.io/en/blog/posts/2019/10/24/incentivized-testnet-what-is-it-and-how-to-get-involved

[80]

Charles Hoskinson on leaving Ethereum, www.youtube.com/watch?v=AWSI78nh6jc

[81]

Surprise AMA! 12/12/2020, www.youtube.com/watch?v=GIVU8ZiVUL0

[82]

Ledger: a distributed ledger (also called a shared ledger or referred to as distributed ledger technology) is a consensus of replicated, shared, and synchronized digital data geographically spread across sites, countries, or institutions. There is no central administrator or centralized data storage.

[83]

In telecom networks, a **node** is either a redistribution point or a communication endpoint. The definition of a node depends on the network and protocol layer referred to. A physical network node is an active electronic device that is attached to a network, and is capable of creating, receiving, or transmitting information over a communications channel.

[84]

Block: a record of recent network transactions. Each block also includes the data necessary for blockchain management, such as an encrypted record of the preceding block. Each finished block is followed by the creation of the next block to continue the chain.

[85]

A **cryptographic hash** is a math algorithm that maps data of an arbitrary size (often called the ‘message’) to a bit string of a fixed size (the ‘hash value’, ‘hash’, or ‘message digest’). It is a one-way function, that is, a function that is practically impossible to invert. Cryptographic hash functions are a basic tool of modern cryptography.

[\[86\]](#)

Address: a data structure used to express different types of information in transaction outputs. To identify between various networks (eg, mainnet or testnet), each address has a network discriminant tag and a proof of ownership (who owns the transaction output). Delegation options and script references are also included in some addresses.

[\[87\]](#)

Reward: an amount contained in each new block that is paid out to the stakeholder by the network.

[\[88\]](#)

Coined by Vitalik Buterin, who led the creation of Ethereum, the ‘**blockchain trilemma**’ sets out the challenges developers face in creating a blockchain that is scalable, decentralized and secure, without compromising on any facet. Blockchains are forced to make trade-offs between these three aspects:

- decentralization: creating a blockchain system that does not rely on a central point of control.
- scalability: the ability of a blockchain to handle a growing number of transactions.
- security: the ability of a blockchain to operate as expected, and defend itself from attacks, bugs, and other unforeseen issues.

[\[89\]](#)

A **pure function** is a function that has the following properties: first, its return value is the same for the same arguments (no variation with local static variables, non-local variables, mutable reference

arguments or input streams from input-output devices); second, its evaluation has no side effects (no mutation of local static variables, non-local variables, mutable reference arguments or inputs and outputs).

[\[90\]](#)

MMT Chakravarty, S Coretti, M Fitzi, P Gazi, P Kant, A Kiayias, and A Russell (2020) ‘Hydra: fast isomorphic state channels’. eprint.iacr.org/2020/299.pdf

[\[91\]](#)

In the decentralized ecosystem, a **Layer 1** refers to the blockchain protocol itself. **Layer 2** refers to a technology that operates on top of a blockchain to improve its scalability and efficiency. For example, Bitcoin is a Layer 1 network, and the Lightning Network is a Layer 2 to improve transaction speeds. Hydra is a layer 2 protocol built on top of Cardano, layer 1.

[\[92\]](#)

Stake pool: a stable, block-producing server node that aggregates the stakes of several stakeholders (in Cardano’s case, ada owners) into a single entity, or pool.

[\[93\]](#)

Saturation: a stake pool is saturated when it has more stake delegated to it than is optimal for the network. The saturation level is expressed as a percentage. When a stake pool achieves 100% saturation, the rewards start to shrink. The saturation mechanism was created to avoid centralization by encouraging ada owners to delegate to several stake pools, and operators to build more pools to keep receiving maximum rewards. Saturation aims to safeguard both the interests of ada holders delegating their stake and the interests of stake pool operators (SPOs).

[\[94\]](#)

Blockchain **governance** brings together norms and culture, laws and code, and the people and the institutions that are needed to run

a system and ensure its stability in the long term. Governance, including voting and a treasury for long-term funding, is the focus of the Voltaire stage of the Cardano roadmap.

[95]

Project Catalyst is a series of experiments that seek to encourage the highest levels of community innovation. Catalyst is bringing on-chain governance to Cardano by allowing the community to determine priorities for growth (see Chapter 8).

[96]

Let's talk Cardano - Interview with Charles Hoskinson,
www.youtube.com/watch?v=NX3fGKMd004

[97]

IOG GitHub: github.com/input-output-hk/

[98]

Functional programming is a rigorous style of building the structure and elements of computer programs that treats computation as the evaluation of mathematical functions and avoids changing the properties of the data being processed. It is a ‘declarative’ paradigm in that programming is done with expressions or declarations instead of statements. In functional code, the output value of a function depends only on its arguments, so calling a function with the same value for an argument always produces the same result. This is in contrast to imperative programming where, in addition to a function’s arguments, the global state of a program can affect a function’s resulting value. Eliminating side-effects, that is, changes in state that do not depend on the function inputs, can make understanding a program easier, which was one of the motivations for the development of functional programming.

[99]

Prof Aggelos Kiayias, ‘The Ouroboros path to decentralization’,
iohk.io/en/blog/posts/2020/06/23/the-ouroboros-path-to-decentralization/

[\[100\]](#)

Byzantine fault tolerance (BFT): A Byzantine fault is a condition of a computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component has failed. The term takes its name from an allegory, the ‘Byzantine Generals Problem’, developed to describe a situation in which, to avoid catastrophic failure of the system, the system’s actors must agree on a concerted strategy, but some of these actors are unreliable.

[\[101\]](#)

Slot: Within an epoch, a set duration of time. Time is separated into numbered slots for each epoch. Active slots are those that are occupied by blocks.

[\[102\]](#)

In cryptography, a **verifiable-random function (VRF)** is a pseudo-random function that provides publicly verifiable proofs of its outputs’ correctness.

[\[103\]](#)

Epoch: a set group of slots that constitute a period of time (currently 5 days).

[\[104\]](#)

A **script** is a generic term for an executable program used in the ledger. In the Cardano blockchain, these are written in Plutus Core.

[\[105\]](#)

A **decentralized application** (DApp, dApp, or Dapp) is an open-source project that runs on a blockchain network. The distributed nature of these networks provides users with transparency, decentralization, and resistance to attacks.

[\[106\]](#)

IOG audits, github.com/input-output-hk/external_audits

[107]

Some Brief Comments on Process, www.youtube.com/watch?v=T4hjGjredpw

[108]

The Boolean satisfiability problem (abbreviated **SATISFIABILITY** or **SAT**) is the problem of determining if there exists an interpretation that satisfies a given Boolean formula. It asks whether the variables of a given Boolean formula can be consistently replaced by the values TRUE or FALSE in such a way that the formula evaluates to TRUE. If this is the case, the formula is called satisfiable. On the other hand, if no such assignment exists, the function expressed by the formula is FALSE for all possible variable assignments and the formula is unsatisfiable.

[109]

'Country ranking', ccaf.io/cbeci/index/comparisons

[110]

Oettler (2022), 'Nothing at stake / Costless Simulation', blockchain-academy.hs-mittweida.de/courses/game-theory-blockchain/lessons/attacks-on-proof-of-stake-pos/topic/nothing-at-stake-costless-simulation/

[111]

Anthony Quinn, 'Combinator makes easy work of Shelley hard fork', iohk.io/en/blog/posts/2020/05/07/combinator-makes-easy-work-of-shelley-hard-fork/

[112]

Staking involves holding funds in a cryptocurrency wallet to support the security and operations of a blockchain network, and in return receive staking rewards. In other words, staking is the process of actively participating in transaction validation (similar to mining) on a proof-of-stake (PoS) blockchain.

[113]

Slashing is a mechanism used by some PoS protocols (but not Cardano) to discourage harmful behavior and make validators more responsible. They help keep the network secure because, without slashing penalties, a validator can use the same node to validate blocks on more than one chain or do so on the wrong chain.

[\[114\]](#)

A **multi-asset (MA)** ledger can do the accounting for or interact with more than one type of asset. Cardano uses native tokens to provide this feature.

[\[115\]](#)

Plutus: a Turing-complete programming framework for constructing functional smart contracts. Plutus is a Haskell-based programming language.

[\[116\]](#)

A system is said to be **Turing complete** if it can be used to simulate any Turing machine. This means that this system is able to recognize or decide other data-manipulation rule sets. Turing completeness is used as a way to express the power of such a data-manipulation rule set. Virtually all programming languages today are Turing complete. The concept is named after English mathematician and computer scientist Alan Turing.

[\[117\]](#)

The **Unspent Transaction Output (UTXO)** model is commonly used in the field of Distributed Ledger Technology (DLT) to transfer value between participants. A UTXO is the technical term for the amount of digital currency that remains after a cryptocurrency transaction. You can think of it as the change you receive after buying an item. Much more on this later, Chapter 5.

[\[118\]](#)

Metadata: a collection of extra data expressing transaction circumstances or owner information. Metadata is used in smart

contracts to indicate the circumstances under which a transaction should take place.

[119]

Adam Hayes, (2022) '10 important cryptocurrencies other than Bitcoin', www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin

[120]

Dogecoin is a cryptocurrency featuring a likeness of the Shiba Inu dog from the 'Doge' internet meme as its logo. Introduced as a 'joke currency' in 2013, Dogecoin quickly developed its own online community and reached a capitalization of US\$1bn in 2018.

[121]

Ergo (ergoplatform.org) is a proof-of-work smart-contract platform that enables new models of financial interaction, underpinned by a safe and rich scripting language built with flexible and powerful zero-knowledge proofs (Σ -protocols).

[122]

Peer review is the evaluation of work by one or more people with similar competences as the producers of the work (peers). It functions as a form of self-regulation by qualified members of a profession within the relevant field. Peer review methods are used to maintain quality standards, improve performance, and provide credibility. In academia, scholarly peer review is used to determine an academic paper's suitability for publication.

[123]

'Polkadot consensus', wiki.polkadot.network/docs/learn-consensus

[124]

A Kiayias, A Russell, B David, R Oliynykov (2017) 'Ouroboros: A provably secure proof-of-stake blockchain protocol' citations, [scholar.google.com/scholar?](http://scholar.google.com/scholar?cites=9760004817031418890&as_sdt=2005&sciodt=0,5&hl=en) cites=9760004817031418890&as_sdt=2005&sciodt=0,5&hl=en

[125]

J Garay, A Kiayias, N Leonardos (2014) 'The bitcoin backbone protocol: analysis and applications', eprint.iacr.org/2014/765.pdf

[126]

Cardano roadmap, roadmap.cardano.org/en/

[127]

A **cryptocurrency wallet** stores the public and private keys which can be used to receive or spend a cryptocurrency. A wallet can contain many public keys but only one private key, which must be kept safe from loss or theft. Once a private key is lost that ends the life of that wallet. The cryptocurrency itself is not in the wallet. The cryptocurrency is decentrally stored and maintained in a publicly available ledger called the blockchain. Every piece of cryptocurrency has a private key. With the private key, it is possible to digitally sign a transaction and write it in the public ledger, in effect spending the associated cryptocurrency.

[128]

Cardano Explorer, explorer.cardano.org/en

[129]

Delegation: By delegating the stake related to their ada holdings to a stake pool, ada owners participate in the network and collect rewards each epoch (five days). Delegators are rewarded in proportion to the amount of stake delegated.

[130]

Slot leader: an elected node that has been chosen to construct a block in the current slot. An arbitrary election takes place based on the proportionate stake.

[131]

How to buy Cardano ada cryptocurrency for beginners,
www.youtube.com/watch?v=3MEO-lm6OSg

[\[132\]](#)

Cardano wallets, www.cardanocube.io/collections/wallets

[\[133\]](#)

How to choose a stake pool, iohk.zendesk.com/hc/en-us/articles/900002174303-How-to-choose-a-stake-pool

[\[134\]](#)

How safe is it to delegate to a stake pool?, iohk.zendesk.com/hc/en-us/articles/900002046123-How-safe-is-it-to-delegate-to-a-stake-pool-

[\[135\]](#)

How to delegate to a stake pool, iohk.zendesk.com/hc/en-us/articles/900005718683-How-to-Delegate-to-a-stake-pool

[\[136\]](#)

Staking and delegating for beginners, forum.cardano.org/t/staking-and-delegating-for-beginners-a-step-by-step-guide/36681

[\[137\]](#)

How to delegate from the Yoroi wallet, forum.cardano.org/t/cardano-shelley-how-to-delegate-from-the-yoroi-wallet/38230

[\[138\]](#)

IOHK | Cardano Whiteboard; overview with Charles Hoskinson, www.youtube.com/watch?v=Ja9D0kpksxw

[\[139\]](#)

First-principles thinking is one of the best ways to reverse-engineer complicated problems and unleash creative possibilities. Sometimes called ‘reasoning from first principles,’ the idea is to break down complicated problems into basic elements and then reassemble them from the ground up.

[\[140\]](#)

Scorex project, iohk.io/projects/scorex/

[141]

IOHK research papers, iohk.io/research/library/

[142]

The **Transmission Control Protocol (TCP)** is one of the main protocols of the **Internet Protocol (IP)** suite. Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World-Wide Web, email, and file transfer rely on TCP.

[143]

Why Cardano?, why.cardano.org/

[144]

Duncan Coutts, ‘Cryptocurrencies need a safeguard to prevent another DAO disaster’, iohk.io/blog/cryptocurrencies-need-a-safeguard-to-prevent-another-DAO-disaster/

[145]

In defense of peer review, www.youtube.com/watch?v=3-rbn73cUEk

[146]

Separation of concerns is a design principle for separating a computer program into distinct sections, so that each section addresses a separate concern. A concern is a set of information that affects the code of a computer program.

[147]

Hoskinson announces a new system to tackle both security & privacy concerns, ambcrypto.com/hoskinson-announces-a-new-system-to-tackle-both-security-privacy-concerns/

[148]

Wet code and dry, unenumerated.blogspot.com/2006/11/wet-code-and-dry.html

[149]

The **semantic gap** characterizes the difference between two descriptions of an object by different linguistic representations, for instance languages or symbols. According to Hein, the semantic gap can be defined as "the difference in meaning between constructs formed within different representation systems". In computer science, the concept is relevant whenever ordinary human activities, observations, and tasks are transferred into a computational representation.

[150]

The **Ring of Gyges** is a mythical, magical artifact mentioned by the philosopher Plato in his *Republic*. It grants its owner the power to become invisible at will. Through the story of the ring, *Republic* considers whether an intelligent person would be just, if they did not have to fear reputational damage if they committed injustices.

[151]

Ari Juels, Ahmed Kosba, and Elaine Shi, 'The Ring of Gyges: using smart contracts for crime', www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf

[152]

RootStock is a smart-contract peer-to-peer platform built on top of the Bitcoin blockchain. Its goal is to add value and functionality to the core Bitcoin network by the implementation of smart contracts as a sidechain.

[153]

Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum.

[154]

Jeevak Kasarkod, ‘Zeppelin: a secure smart contracts open-source framework for blockchain applications’,
www.infoq.com/news/2016/10/zeppelin-secure-smart-contracts/
[155]

Liquid Haskell, ucsd-progsys.github.io/liquidhaskell-blog/
[156]

Why Cardano? CCL, why.cardano.org/en/introduction/cardano-computation-layer/
[157]

Broadly speaking, **modularity** is the degree to which a system’s components may be separated and recombined, often with the benefit of flexibility and variety in use. The concept of modularity is used primarily to reduce complexity by breaking a system into varying degrees of interdependence and independence across and ‘hide the complexity of each part behind an abstraction and interface.’

[158]

A combinator is a technical term used to indicate the combination of certain processes or things. In the case of Cardano, a **hard fork combinator** combines protocols, thereby enabling the Byron-to-Shelley transition without system interruption or restart. It ensures that Byron and Shelley ledgers appear as one ledger.

[159]

Post Conference recap, thoughts and an AMA 04/21/2019,
youtu.be/pBXZVrBQ6U8?t=3325

[160]

Permissioned v permissionless. At the simplest level, the distinction lies in whether the design of the network is open for anyone to participate – permissionless – or limited only to designated participants, or permissioned.

[161]

Post-Roadmap Comments and Some Reddit Questions,
youtu.be/nwMZFGHo1p4?t=2162

[\[162\]](#)

Chimeric ledger (explained), www.youtube.com/watch?v=3nZQUpuqgcY

[\[163\]](#)

Secure **multi-party computation** (also known as secure computation, **multi-party computation (MPC)**, or privacy-preserving computation) is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptographic tasks, where cryptography assures security and integrity of communication or storage and the adversary is outside the system of participants (an eavesdropper on the sender and receiver), the cryptography in this model protects participants' privacy from each other.

[\[164\]](#)

Thoughts on cross chain communication, sidechains, NiPoPoWs and Litecoin, www.youtube.com/watch?v=HvIAgDEUC4o,

[\[165\]](#)

The acronym IELE (pronounced YELL-eh) stands for two things: The IELE Virtual Machine (VM) or the IELE Assembly Language. It's discussed more later.

[\[166\]](#)

Wrapped tokens are a way to use cryptocurrencies on blockchains other than the blockchain they were originally built on. Wrapped tokens are backed 1:1 by their underlying asset, which is stored in a digital vault

[\[167\]](#)

Litecoin is a peer-to-peer cryptocurrency and open-source software project released under the MIT/X11 license. While inspired by, and in most regards technically nearly identical to Bitcoin (BTC), Litecoin has some minor technical differences such as almost zero transaction fees.

[\[168\]](#)

Transaction (Tx): an instance that reflects the system's sending and receiving of currencies.

[\[169\]](#)

Blockstream is a blockchain technology company led by co-founder Adam Back. Blockstream intends to develop software to 'break off' transactions from the bitcoin network and charge a fixed monthly fee to allow people to use alternative 'sidechains'. Blockstream employs a large number of prominent Bitcoin Core developers.

[\[170\]](#)

Special Edition New Year's AMA 2020, [youtu.be/GtWt68kp1dg? t=777](https://youtu.be/GtWt68kp1dg?t=777)

[\[171\]](#)

Chancellor on the brink of second bailout for banks,
www.coindesk.com/podcasts/the-breakdown-with-nlw/13-years-on-the-meaning-of-chancellor-on-the-brink-of-second-bailout-for-banks/

[\[172\]](#)

'Now that India has pulled back from banning crypto, here's how it plans to develop digital currency on its own terms',
fortune.com/2022/02/02/india-crypto-ban-plans-develop-digital-currency-taxes-regulation-bitcoin/

[\[173\]](#)

Special Edition New Year's AMA 2020, [youtu.be/GtWt68kp1dg? t=7282](https://youtu.be/GtWt68kp1dg?t=7282)

[\[174\]](#)

BitConnect Founder Indicted in Global \$2.4 Billion Cryptocurrency Scheme, www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme

[\[175\]](#)

What We Can Learn From OneCoin, Crypto's Biggest Scam, www.fool.com/the-ascent/cryptocurrency/articles/what-we-can-learn-from-onecoin-cryptos-biggest-scam/

[\[176\]](#)

Payments for \$9 billion bitcoin settlement from Mt. Gox collapse could start in months, markets.businessinsider.com/news/currencies/mt-gox-bitcoin-settlement-payouts-9-billion-dollars-early-2022-2021-11

[\[177\]](#)

Federal Court Orders BitMEX to Pay \$100 Million for Illegally Operating a Cryptocurrency Trading Platform and Anti-Money Laundering Violations, www.cftc.gov/PressRoom/PressReleases/8412-21

[\[178\]](#)

Howey Test: Securities and Exchange Commission (SEC) v. W. J. Howey Co. (1946). The case resulted in a test, known as the **Howey test**, to determine whether an instrument qualifies as an 'investment contract' for the purposes of the Securities Act: '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. The Howey Test has remained a notable determiner of regulatory oversight for many decades. In the past few years, it has been called into question, most frequently in conjunction with discussions about Cryptocurrencies and Blockchain technology'.

[\[179\]](#)

Koan, [everipedia.org/wiki/lang_en/Koan_\(disambiguation\)](http://everipedia.org/wiki/lang_en/Koan_(disambiguation))

[180]

The Future of Digital Asset Regulation, www.youtube.com/watch?v=K4ZM2AIT-s

[181]

Cardano founder steals the show at Congressional hearing on crypto regulation, cryptoslate.com/cardano-founder-steals-the-show-at-congressional-hearing-on-crypto-regulation/

[182]

M-Pesa (M for mobile, pesa is Swahili for money) is a mobile phone-based money transfer, financing and microfinancing service, launched in 2007 by Vodafone for Safaricom and Vodacom, the largest mobile network operators in Kenya and Tanzania. It has since expanded to Afghanistan, South Africa, India and in 2014 to Romania and in 2015 to Albania. M-Pesa allows users to deposit, withdraw, transfer money and pay for goods and services (Lipa na M-Pesa) easily with a mobile device.

[183]

Kiva (commonly known by its domain name, Kiva.org) is a non-profit organization, the world's first online lending platform connecting online lenders to entrepreneurs across the globe. Kiva's mission is 'to expand financial access to help underserved communities thrive.'

[184]

Best of all possible worlds,
everipedia.org/wiki/lang_en/Best_of_all_possible_worlds

[185]

Some Random Thoughts and Updates, youtu.be/ttFptsL5hN0?t=4353

[186]

Tartaglia,
everipedia.org/wiki/lang_en/Niccol%25C3%25B2_Fontana_Tartaglia
[187]

Happy Birthday ADA!, youtu.be/hhAOJyi_3IA?t=27
[188]

She Walks in Beauty, www.poetryfoundation.org/poems/43844/she-walks-in-beauty

[189]

Ozymandias, www.poetryfoundation.org/poems/46565/ozymandias
[190]

Charles Hoskinson - Building a Better World with the Blockchain,
podcasts.apple.com/us/podcast/charles-hoskinson-building-a-better-world/id1553861681?i=1000517944232

[191]

Special Edition New Years AMA 2020, youtu.be/GtWt68kp1dg?t=8496
[192]

Lord Byron, www.bl.uk/people/lord-byron
[193]

OBJ programming language,
everipedia.org/wiki/lang_en/OBJ_%28programming_language%29
[194]

Grigore Rosu, runtimeverification.com/blog/author/grigore-rosu/
[195]

Cardano360 - March 2021, youtu.be/ULBLgPgxtN8?t=1571
[196]

Yoroi mobile wallet, yoroi-wallet.com/

[\[197\]](#)

Jormungandr, everipedia.org/wiki/lang_en/J%C3%B6rmungandr

[\[198\]](#)

Rust is a lightweight, portable programming language from Mozilla that compiles to the web, iOS and Android. Rust is a multi-paradigm, general-purpose language designed for performance and safety, especially safe concurrency.

[\[199\]](#)

Kiayias, Russell, David, Oliynykov (2019) 'Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol',
eprint.iacr.org/2016/889.pdf

[\[200\]](#)

Plutus, developers.cardano.org/en/programming-languages/plutus/overview/

[\[201\]](#)

Off-chain code: The part of a contract application's code which runs off the chain, usually as a contract application. **On-chain code:** The part of a contract application's code which runs on the chain (i.e. as scripts).

[\[202\]](#)

Marlowe, www.bbc.co.uk/programmes/p003k9d6

[\[203\]](#)

A **domain-specific language (DSL)** is a computer language specialized to a particular application domain. This is in contrast to a general-purpose language (GPL), which is broadly applicable across domains.

[\[204\]](#)

In a **synchronous system**, operations are coordinated by one, or more, centralized clock signals. An asynchronous digital system, in

contrast, has no global clock. Asynchronous systems do not depend on strict arrival times of signals or messages for reliable operation. Coordination is achieved via events such as: packet arrival, changes (transitions) of signals, handshake protocols, and other methods.

[\[205\]](#)

Berry Pool, github.com/alessandrokonrad/Pi-Pool

[\[206\]](#)

Raspberry Pi: computer on a credit-card-sized board. Idea developed by Eben Upton and others from Cambridge University's Computer Lab and launched by their Raspberry Pi Foundation. Taking inspiration from the 1980s BBC Computer Literacy Project, the single-board computer running Linux with open-source software was launched in 2012 costing £22 to encourage computing in schools and the developing world.

[\[207\]](#)

Cardano on the Rocks: energy efficient proof-of-stake stake pools, www.youtube.com/watch?v=kXR1UXkM46s

[\[208\]](#)

A **light client**, or thin client is a lightweight computer that has been optimized for establishing a remote connection with a server-based computing environment. The server does most of the work, which can include launching software programs, performing calculations, and storing data. This contrasts with a fat client or a conventional personal computer; the former is also intended for working in a client–server model but has significant local processing power, while the latter aims to perform its function mostly locally.

[\[209\]](#)

Take the green blockchain to the next level with Cardano, finance.yahoo.com/news/green-blockchain-next-level-cardano-192654597.html

[\[210\]](#)

Could Cardano's 'green' cryptocurrency ADA take over Bitcoin and Ethereum?, www.euronews.com/next/2021/08/23/could-cardano-s-green-cryptocurrency-ada-take-over-bitcoin-and-etherium

[211]

What is Cardano? The 'green' crypto that defied Musk's bitcoin crash – and hopes to surpass Facebook and Netflix, www.independent.co.uk/space/cardano-crypto-bitcoin-elon-musk-b1849021.html

[212]

Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', bitcoin.org/bitcoin.pdf

[213]

Dotan and Tochner, 'Proofs of Useless Work: Positive and Negative Results for Wasteless Mining Systems', arxiv.org/pdf/2007.01046.pdf

[214]

An Analysis of Energy Consumption and Carbon Footprints of Cryptocurrencies and Possible Solutions, arxiv.org/pdf/2203.03717.pdf

[215]

Major bitcoin mining region in China sets tough penalties for cryptocurrency activities, www.cnbc.com/2021/05/26/major-china-bitcoin-mining-hub-lays-out-harsher-crackdown-measures.html

[216]

Ethereum's energy usage will soon decrease by ~99.95%, blog.ethereum.org/2021/05/18/country-power-no-more/

[217]

This breakthrough could make Ethereum more environmentally friendly than Bitcoin, fortune.com/2021/05/24/ethereum-bitcoin-buterin-carbon-footprint-proof-of-stake/

[218]

Roundtable with Charles Hoskinson and Alex Chepurnoy | Ergo Pulse, youtu.be/k9a3SYV6FJA?t=3182

[\[219\]](#)

A novel proof of useful work for a blockchain storing transportation transactions,

www.sciencedirect.com/science/article/pii/S0306457321002302

[\[220\]](#)

Bitcoin's growing e-waste problem,

www.sciencedirect.com/science/article/abs/pii/S0921344921005103

[\[221\]](#)

What is Cardano? The ‘green’ crypto that defied Musk’s bitcoin crash – and hopes to surpass Facebook and Netflix,

www.independent.co.uk/life-style/gadgets-and-tech/cardano-crypto-bitcoin-elon-musk-b1849021.html

[\[222\]](#)

UN climate report: It’s ‘now or never’ to limit global warming to 1.5 degrees, news.un.org/en/story/2022/04/1115452

[\[223\]](#)

Oligarchy, meaning ‘few’, and ‘to rule or to command’, is a form of power structure in which power rests with a small number of people.

[\[224\]](#)

A **51% attack** is a hostile takeover of a Cryptocurrency validated via proof-of-work Algorithms through the acquisition of the majority of the network's hashing power.

[\[225\]](#)

In a **Sybil attack**, the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence.

It is named after the subject of the book *Sybil*, a case study of a woman diagnosed with dissociative identity disorder.

[\[226\]](#)

Pledging: when a stake pool operator assigns their own ada stake to support their stake pool. This provides protection against Sybil attacks by preventing pool owners from creating a large number of pools without themselves owning a lot of stake.

[\[227\]](#)

Polkadot staking, wiki.polkadot.network/docs/learn-staking

[\[228\]](#)

Slashing is a mechanism used by PoS protocols to discourage harmful behaviors and make validators more responsible. They help keep the network secure since, without slashing penalties, a validator can use the same node to validate blocks on multiple chains or do so on the wrong chain.

[\[229\]](#)

Profit margin: The stake pool operator takes a portion of total ada rewards before dividing the remainder of the rewards with all of the pool's delegators. If the operator's profit margin is low, they're taking less risks, which means delegators should anticipate reaping more of the rewards for their delegated stake. A private pool is one with a profit margin of 100%, indicating that the operator receives all of the rewards and the delegators get none.

[\[230\]](#)

cost per epoch: The stake pool operator deducts a predetermined charge from the pool payouts every epoch to cover the expenses of maintaining a stake pool. Before the operator collects their profit margin, the cost per epoch is removed from the total ada that is awarded to a pool. Whatever is left is divided evenly among the delegators.

[\[231\]](#)

Multisignature (multi-signature) is a digital signature scheme which allows a group of users to sign a single document. Usually, a multisignature algorithm produces a joint signature that is more compact than a collection of distinct signatures from all users. Multisignature can be considered as generalization of both group and ring signatures providing additional security for cryptocurrency transactions.

[\[232\]](#)

Creating a stake pool, docs.cardano.org/getting-started/operating-a-stake-pool/creating-a-stake-pool

[\[233\]](#)

Establishing connectivity between the nodes, docs.cardano.org/getting-started/operating-a-stake-pool/node-connectivity

[\[234\]](#)

Operational certificates and keys, docs.cardano.org/getting-started/operating-a-stake-pool/creating-keys-and-certificates

[\[235\]](#)

Public stake pools and metadata management, docs.cardano.org/getting-started/operating-a-stake-pool/public-stake-pools

[\[236\]](#)

SMASH metadata management, docs.cardano.org/getting-started/operating-a-stake-pool/SMASH

[\[237\]](#)

Stake pool performance, docs.cardano.org/getting-started/operating-a-stake-pool/performance

[\[238\]](#)

Stake pool ranking, docs.cardano.org/getting-started/operating-a-stake-pool/ranking

[\[239\]](#)

List of registered relays, explorer.cardano-mainnet.iohk.io/relays/topology.json

[\[240\]](#)

Peer-to-peer (P2P): distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. In Cardano this involves sending transactions (or files) directly between nodes in a decentralized system without relying on a centralized authority.

[\[241\]](#)

About the Cardano network, docs.cardano.org/explore-cardano/cardano-network/about-the-cardano-network

[\[242\]](#)

Key pair: Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security. Within the blockchain, these keys are used to process and authorize transactions.

[\[243\]](#)

About node configuration files, github.com/input-output-hk/cardano-node/blob/master/doc/getting-started/understanding-config-files.md

[\[244\]](#)

Configuring topology files for block-producing and relay nodes, github.com/input-output-hk/cardano-node/blob/master/doc/stake-pool-operations/core_relay.md

[\[245\]](#)

Creating an operational certificate with key evolving signature (KES),
github.com/input-output-hk/cardano-node/blob/master/doc/stake-pool-operations/KES_period.md

[\[246\]](#)

Mainnet: The blockchain that has been deployed and is now in use. Assets stored on the mainnet have value, but assets held on the testnet do not.

[\[247\]](#)

cardano-node, github.com/input-output-hk/cardano-node

[\[248\]](#)

cardano-db-sync, github.com/input-output-hk/cardano-db-sync

[\[249\]](#)

cardano-graphql, github.com/input-output-hk/cardano-graphql

[\[250\]](#)

GraphQL in 6 mins, www.youtube.com/watch?v=Ys-aox3oOD8

[\[251\]](#)

Docker is a software tool that makes it easier to deploy applications by using ‘containers’, each of which holds all the parts, such as libraries, that the application needs to run.

[\[252\]](#)

A **testnet** is an alternative blockchain used by software developers to check that their code runs properly before they make possibly costly deployments to a **mainnet**. The testnet uses identical technology and software as the ‘mainnet’ blockchain, in other words a parallel network, except the testnet doesn’t make ‘actual’ transactions with ‘value’ and is intended for testing purposes. Testnet coins are distinct from actual coins on a mainnet, as testnet coins do not have any monetary value.

[\[253\]](#)

Slot leader, developers.cardano.org/docs/stake-pool-course/introduction-to-cardano/

[254]

Saturation: a word that refers to a stake pool that has more stake delegated to it than is optimal for the network. The saturation level is expressed as a percentage. When a stake pool achieves 100% saturation, the rewards start to shrink. The saturation mechanism was created to avoid centralization by encouraging delegators to delegate to multiple stake pools and operators to build up alternative pools in order to keep receiving maximum rewards. Saturation aims to safeguard both the interests of ada holders delegating their stake and the interests of stake pool operators.

[255]

Guidelines for large SPOs, github.com/input-output-hk/cardano-documentation/blob/staging/content/02-getting-started/04-guidelines-for-large-spos.mdx

[256]

In general, **bootstrapping** usually refers to a self-starting process that is supposed to proceed without external input. In computer technology the term (usually shortened to booting) usually refers to the process of loading the basic software into the memory of a computer after power-on or general reset, especially the operating system which will then take care of loading other software as needed.

[257]

An **unspent transaction output (UTXO)** is the technical term for the amount of digital currency that remains after a cryptocurrency transaction.

[258]

Stake Pools, docs.cardano.org/core-concepts/stake-pools

[259]

What is a rollback?,
playground.plutus.iohkdev.io/doc/plutus/explanations/rollback.html
[260]

Rollback: The Cardano network is a distributed system with many nodes operating at the same time. Each node keeps its own local copy of the blockchain, extending it regularly with new blocks. At the same time, the node is talking to some of the other nodes in the network to establish a consensus about what the canonical blockchain should be. Sometimes the node discovers that its local version of the blockchain is different from the canonical one that the other nodes agree on. When that happens, the node has to switch (**rollback**) to the correct blockchain.

[261]

Rewards Wallet: a wallet that contains ada and may be used to delegate stakes. A stake may only be delegated to a single stake pool from a single Rewards wallet. You'll need to construct numerous Rewards wallets and divide ada across them if you want to delegate to more than one stake pool. Split pool delegation has been promised by IOG for some time but has been postponed, to allow focusing resources on other roadmap priorities.

[262]

Balance wallet: your original testnet ada balance, copied from the mainnet through the balance snapshot, is stored in this wallet. This wallet's stake is not transferable, although it may be moved to and delegated from a Rewards wallet.

[263]

Can we use AWS spot instances for guaranteed mining profits?,
stackoverflow.com/questions/51665962/can-we-use-aws-spot-instances-for-guaranteed-mining-profits

[264]

Lars Brünjes, 'Preventing sybil attacks',
iohk.io/en/blog/posts/2018/10/29/preventing-sybil-attacks/
[265]

Double-spending is a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once. Unlike physical cash, a digital token consists of a digital file that can be duplicated or falsified. As with counterfeit money, such double-spending leads to inflation by creating a new amount of copied currency that did not previously exist. This devalues the currency relative to other monetary units or goods and diminishes user trust as well as the circulation and retention of the currency. Fundamental cryptographic techniques to prevent double-spending, while preserving anonymity in a transaction, are blind signatures and, particularly in offline systems, secret splitting.

[266]

Kevin Hammond, 'From Byron to Shelley: Part one, the testnets',
iohk.io/en/blog/posts/2020/04/29/from-byron-to-shelley-part-one-the-testnets/

[267]

Cardano Calculator, cardano.org/calculator/?calculator=operator
[268]

Cardano Mainnet: Pledge Influence Factor Analysis,
www.reddit.com/r/cardano/comments/gfed1l/cardano_mainnet_pledge_influence_factor_analysis/
[269]

Pledge Influence Factors, Effects on Operators and Stakers, with Umed Saidov | TCE 88, www.youtube.com/watch?v=ubWIytFZYGE
[270]

Daedalus Flight is a 'pre-release' version of the Daedalus wallet.
[271]

Anthony Quinn, 'We need you for a Daedalus testing program!',
iohk.io/en/blog/posts/2020/04/01/we-need-you-for-the-daedalus-flight-testing-program/

[272]

Cardano founder shares proxy keys idea to implement,
coinregwatch.com/cardano-founder-shares-proxy-keys-idea-to-implement/

[273]

Proxy signature is a special type of digital signature which allows one user (original signer) to delegate his/her signing right to another signer (proxy signer). The latter can then issue signatures on behalf of the former.

[274]

Rewards sharing and pledge on Cardano, www.youtube.com/watch?v=EAzyN3H8MOA

[275]

Earn 4-6% Staking Cardano (ADA), Available on Kraken Now!,
blog.kraken.com/post/8891/earn-4-6-staking-cardano-ada-available-on-kraken-now/

[276]

Create a simple transaction, github.com/input-output-hk/cardano-node/blob/master/doc/stake-pool-operations/simple_transaction.md

[277] Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

[278]

Why use key evolving signatures, forum.cardano.org/t/why-use-key-evolving-signatures/11133/4

[\[279\]](#)

Tim Harrison, ‘From node enhancement to block leadership... Cardano’s February release’, iohk.io/en/blog/posts/2022/02/28/from-node-enhancement-to-block-leadership-cardano-s-february-release

[\[280\]](#)

In public-key cryptography, Edwards-curve Digital Signature Algorithm (**EdDSA**) is a digital signature scheme using a variant of Schnorr signature based on Twisted Edwards curves. It is designed to be faster than existing digital signature schemes without sacrificing security.

[\[281\]](#)

Surprise AMA 03/19/2020, youtu.be/9rCIM2pLNmo?t=2406

[\[282\]](#)

Transport Layer Security (TLS) and its predecessor, **Secure Sockets Layer (SSL)**, are cryptographic protocols that provide communications security over a computer network.

[\[283\]](#)

Install RTView, github.com/input-output-hk/cardano-rt-view/blob/master/doc/getting-started/install.md/

[\[284\]](#)

Essential Cardano, github.com/input-output-hk/essential-cardano/blob/main/essential-cardano-list.md

[\[285\]](#)

Cardano developer portal, developers.cardano.org/showcase

[\[286\]](#)

BitTorrent is a communication protocol for peer-to-peer (P2P) file sharing which is used to distribute data and electronic files over the

Internet. BitTorrent is one of the most common protocols for transferring large files, such as digital files containing movies or music.

[287]

Comparing 4 decentralized data storage offerings,
www.techtarget.com/searchstorage/tip/Comparing-4-decentralized-data-storage-offerings

[288]

A **gossip protocol** is a procedure or process of computer peer-to-peer communication that is based on the way epidemics spread. Some distributed systems use peer-to-peer gossip to ensure that data is routed to all members of an ad-hoc network. Some ad-hoc networks have no central registry and the only way to spread common data is to rely on each member to pass it along to their neighbors.

[289]

Fernando Sanchez, 'Why They're Calling Cardano the Green Blockchain', iohk.io/en/blog/posts/2021/08/17/why-they-re-calling-cardano-the-green-blockchain/

[290]

About stake pools, docs.cardano.org/getting-started/operating-a-stake-pool/about-stake-pools

[291]

Mempool role in multiple transactions, docs.cardano.org/core-concepts/multiple-transactions

[292]

Kiayias, Russell (2018) 'Ouroboros-BFT: A Simple Byzantine Fault Tolerant Consensus Protocol', eprint.iacr.org/2018/1049.pdf

[293]

David, Gazi, Kiayias, Russell (2017) 'Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain', eprint.iacr.org/2017/573.pdf

[294]

Badertscher, Gazi, Kiayias, Russell, Zikas (2019), 'Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability', eprint.iacr.org/2018/378.pdf

[295]

The framework of **universal composability** is a general-purpose model for the analysis of cryptographic protocols. It guarantees very strong security properties. Protocols remain secure even if arbitrarily composed with other instances of the same or other protocols.

Security is defined in the sense of protocol emulation. Intuitively, a protocol is said to emulate another one, if no environment (observer) can distinguish the executions. Literally, the protocol may simulate the other protocol (without having access to the code). The notion of security is derived by implication.

[296]

State channels refer to the process in which users transact with one another directly outside of the blockchain, or 'off-chain,' and greatly minimize their use of 'on-chain' operations.

[297]

Hydra Head GitHub, github.com/orgs/input-output-hk/projects/21

[298]

Badertscher, Gazi, Kiayias, Russell, Zikas (2020), 'Consensus Redux: Distributed Ledgers in the Face of Adversarial Supremacy', eprint.iacr.org/2020/1021.pdf

[299]

Kerber, Kohlweiss, Kiayias, Zikas (2019), 'Ouroboros Crypsinous Privacy-preserving proof-of-stake', eprint.iacr.org/2018/1132.pdf

[300]

SNARK stands for ‘Succinct Non-Interactive Argument of Knowledge.’ A (zero knowledge) zk-SNARK is a cryptographic proof that allows one party to prove it possesses certain information without revealing that information. This proof is made possible using a secret key created before the transaction takes place.

[\[301\]](#)

Badertscher, Gazi, Kiayias, Russell, Zikas (2019), ‘Ouroboros Chronos: Permissionless Clock Synchronization via Proof-of-Stake’, eprint.iacr.org/2019/838.pdf

[\[302\]](#)

The **Internet of Things (IoT)** is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

[\[303\]](#)

Slot Leader Episode 1, youtu.be/YT0PXYBEnuE?t=2218

[\[304\]](#)

Leslie Lamport, everipedia.org/wiki/lang_en/Leslie_Lamport

[\[305\]](#)

Leslie Lamport, ‘Time, clocks, and the ordering of events in a distributed system’, dl.acm.org/doi/10.1145/359545.359563

[\[306\]](#)

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use.

[\[307\]](#)

Network time protocol, ntp.org/

[308]

The **Bellman–Ford algorithm** computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph. It is slower than Dijkstra's algorithm for the same problem, but more versatile, as it is capable of handling graphs in which some of the edge weights are negative numbers. The algorithm was first proposed by Alfonso Shimbel (1955), but is instead named after Richard Bellman and Lester Ford Jr., who published it in 1958 and 1956, respectively.

[309]

Solana Downtime Series Continues, Network Faces Serious Issues Again, u.today/solana-downtime-series-continues-network-faces-serious-issues-again

[310]

Surprise AMA! 12/12/2020, youtu.be/GIVU8ZiVUL0?t=3061

[311]

Advances in Ouroboros: Scaling for Future Growth,
www.youtube.com/watch?v=xKv94MwSNBw

[312]

Ouroboros Omega,
twitter.com/iohk_charles/status/1357364560504709120

[313]

Lark Davis interview, youtu.be/BptZkkNN3tw?t=575

[314]

Bitcoin **maximalism** is a notion among the faction of cryptocurrency enthusiasts that only bitcoin represents practical and successful cryptocurrency in the long term, and that all other cryptocurrencies - altcoins - are inferior.

[315]

A **denial-of-service attack (DoS attack)** is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. DDoS is a distributed DoS attack.

[\[316\]](#)

Game theory is the study of mathematical models of strategic interaction between rational decision-makers. It has applications in all fields of social science, as well as in logic and computer science. Originally, it addressed zero-sum games, in which each participant's gains or losses are exactly balanced by those of the other participants. Today, game theory applies to a wide range of behavioral relations and is now an umbrella term for the science of logical decision making in humans, animals, and computers.

[\[317\]](#)

Surprise AMA 02/09/2021, youtu.be/K3I3_SAGXEE?t=1350

[\[318\]](#)

Gazi, Kiayias, Russell, Zikas (2020) 'Ledger Combiners for fast settlement', eprint.iacr.org/2020/675.pdf

[\[319\]](#)

Abstraction is used to make models that can be used and reused without having to re-write all the program code for each new application on every different type of computer. Abstraction is usually achieved by writing source code in some particular computer language which can be translated into machine code for different types of computers to execute. Abstraction allows program designers to separate a framework from specific instances which implement details.

[\[320\]](#)

The **mempool (memory pool)** is a smaller database of unconfirmed or pending transactions which every node keeps. When a transaction is confirmed by being included in a block, it is removed from the mempool. You can think of a mempool as being like a ‘waiting room’ where a transaction sits before it is added to a block.

[\[321\]](#)

Stateful services keep track of sessions or transactions and react differently to the same inputs based on that history. **Stateless** services rely on clients to maintain sessions and center around operations that manipulate resources, rather than the state.

[\[322\]](#)

In mathematics, semantics, and philosophy of language, the principle of **compositionality** is the principle that the meaning of a complex expression is determined by the meanings of its constituent expressions and the rules used to combine them.

[\[323\]](#)

Block height represents the number of blocks that were validated and confirmed in the entire history of a particular blockchain network, from the genesis block (or block zero) until the most recent one. Unlike the genesis block, all other blocks contain a reference, or hash, to the block that came immediately before it, and the block height is the number of each block in that sequence. So the block height of the genesis block is #0, and the block height of the first block is #1.

[\[324\]](#)

cardano-cli (command line interface) query command contains subcommand, one of which is tip:
tip: gets the node's current tip (slot number, hash, and block number)

[\[325\]](#)

Anthony Quinn, ‘Combinator makes easy work of Shelley hard fork’, iohk.io/en/blog/posts/2020/05/07/combinator-makes-easy-work-of-shelley-hard-fork

[326]

Surprise AMA 01/10/2021, youtu.be/iLq6mRk2dyg?t=3926

[327]

Solana Sputters Back to Life Following Downtime, Network Restart,
decrypt.co/81004/solana-back-online-following-downtime-network-restart

[328]

Tim Harrison, ‘What the Byron Reboot means for Cardano’,
iohk.io/en/blog/posts/2020/03/30/what-the-byron-reboot-means-for-cardano/

[329]

Duncan Coutts, iohk.io/en/team/duncan-coutts

[330]

Flight versus Mainnet, www.youtube.com/watch?v=jmxuVU-oXKM

[331]

How we will launch Shelley, www.youtube.com/watch?v=g7uySEgt06c

[332]

Cardano Allegra and Mary hard fork changes explained,
www.youtube.com/watch?v=9mjvXjxTks8

[333]

Plutus Core is the programming language in which scripts on the Cardano blockchain are written. Plutus Core is a small functional programming language — a formal specification is available. Plutus Core is not read or written by humans; it is a compilation target for other languages.

[334]

Lambda calculus (λ -calculus) is a formal system in math logic for expressing computation based on function abstraction and application using variable binding and substitution. It is a universal model of computation that can be used to simulate any Turing machine. It was introduced by the mathematician Alonzo Church in the 1930s as part of his research into the foundations of mathematics.

[\[335\]](#)

In math and computer science, the ****Entscheidungsproblem**** (pronounced German for ‘decision problem’) is a challenge posed by David Hilbert and Wilhelm Ackermann in 1928. The problem asks for an algorithm that takes as input a statement of a first-order logic and answers ‘Yes’ or ‘No’ according to whether the statement is universally valid, i.e., valid in every structure satisfying the axioms. By the completeness theorem of first-order logic, a statement is universally valid if and only if it can be deduced from the axioms, so the Entscheidungsproblem can also be viewed as asking for an algorithm to decide whether a given statement is provable from the axioms using the rules of logic.

[\[336\]](#)

A **Turing machine** is a mathematical model of computation that defines an abstract machine, which manipulates symbols on a strip of tape according to a table of rules. Despite the model’s simplicity, given any computer algorithm, a Turing machine capable of simulating that algorithm’s logic can be constructed.

[\[337\]](#)

Surprise AMA 06/05/2020, youtu.be/6pQzQbVgX7c?t=2449

[\[338\]](#)

Cardano Pledge, Rewards, and Network Security with Kevin, Lars, and Duncan | TCE 90, www.youtube.com/watch?v=X-ziLksiPOE

[\[339\]](#)

Guidelines for large SPOs, github.com/input-output-hk/cardano-documentation/blob/staging/content/02-getting-started/04-guidelines-for-large-spos.mdx

[[340](#)]

Prof Aggelos Kiayias, 'The general perspective on staking in Cardano', iohk.io/en/blog/posts/2020/11/13/the-general-perspective-on-staking-in-cardano/

[[341](#)]

Curve Pledge Benefit improvement proposal, github.com/cardano-foundation/CIPs/pull/12

[[342](#)]

Special 4th of July Surprise AMA, youtu.be/1qoeLinJ3rg?t=3278

[[343](#)]

Alexander Russel, iohk.io/en/research/library/authors/alexander-russel/

[[344](#)] Marcin Szamotulski, 'Cardano's Path to Decentralization', iohk.io/en/blog/posts/2020/07/09/cardanos-path-to-decentralization-by-marcin-szamotulski/

[[345](#)]

Decentralization unpacked with Colin Edwards, Duncan Coutts, Lars Brunjes & Shawn McMurdo , youtu.be/mXYIQDUiYI

[[346](#)]

Charles Hoskinson Explains Cardano's Secret Weapon (Project Catalyst), www.youtube.com/watch?v=vQOvX-HAQDQ

[[347](#)]

The role of the blockchain is to prove uniqueness and ownership. **NFTs** came to prominence in 2017 with the CryptoKitties game, in which players buy and 'breed' limited-edition virtual cats. Game

developers use NFTs to allow gamers to win in-game tools, and collectibles. Tokenization of such assets allows them to be transferred as tokens between games and players in NFT blockchain marketplaces. NFTs are now used to sell collectibles such as virtual trading cards, music, images and videos. A fractional NFT allows several people to hold (and trade) a share of an asset, for example a work of art.

[\[348\]](#)

Backpressure: Cardano is designed to automatically deal with heavy traffic. Ouroboros and the network stack function even when saturated. If the network is saturated, Cardano can use the admission control method to regulate and restore normalcy. This is the term ‘backpressure’ mentioned in blogs and documentation, it is basically a strategy for network load management.

[\[349\]](#)

An **NFT drop** is the release of a non-fungible token project. A drop refers to the exact date, time, and generally the minting price of the NFT. Many NFT drops have purchase limits that apply to the number of NFTs you are able to mint in one transaction.

[\[350\]](#)

Coutts, Davies, Szamotulski, Thompson (2020) 'Introduction to the design of the Data Diffusion and Networking for Cardano Shelley', hydra.iohk.io/build/7249613/download/1/network-design.pdf

[\[351\]](#)

Cardano Upcoming NFT Drops, nftcalendar.io/b/cardano/
[\[352\]](#)

IOG's Technical Community, discord.gg/inputoutput

[\[353\]](#)

Multiplexing, docs.cardano.org/explore-cardano/cardano-network/networking-protocol/#multiplexing

[\[354\]](#)

Ouroboros.Network.PeerSelection.Governor, input-output-hk.github.io/ouroboros-network/ouroboros-network/Ouroboros-Network-PeerSelection-Governor.html

[\[355\]](#)

Cardano master branch, github.com/input-output-hk/cardano-node/pull/3363

[\[356\]](#)

Prometheus is an open-source tool for collecting metrics and sending alerts.

[\[357\]](#)

May 2022 Mid-Month Development Update,
youtu.be/tH049RwBMSc?t=313

[\[358\]](#)

Cardano360 May 2022, www.youtube.com/watch?v=Ar_8Lo0nV1s

[\[359\]](#)

A **nonce** is an arbitrary number that can be used just once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.

[\[360\]](#)

Nonce, github.com/input-output-hk/cardano-documentation/blob/staging/content/05-explore-cardano/09-explain-nonce.mdx

[\[361\]](#)

Googleplex, everipedia.org/wiki/lang_en/Googleplex

[\[362\]](#)

FLP impossibility theorem, www.the-paper-trail.org/post/2008-08-13-a-brief-tour-of-flp-impossibility/

[\[363\]](#)

Proof of elapsed time, www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp

[\[364\]](#)

Intel Software Guard Extensions (SGX) offers hardware-based memory encryption that isolates specific application code and data in memory.

[\[365\]](#)

Twitter Space ‘Sunday Chat with Charles’,
[twitter.com/IOHK_Charles/status/1515872352395055109?
s=20&t=ivZvNmtLVKrKk_ZEg-1e_A](https://twitter.com/IOHK_Charles/status/1515872352395055109?s=20&t=ivZvNmtLVKrKk_ZEg-1e_A)

[\[366\]](#)

BlockSpaces Live! #8, youtu.be/jiqK9htpHUG?t=1773

[\[367\]](#)

DES (Data Encryption Standard) and **AES** (Advanced Encryption Standard). AES was introduced to overcome the drawback of DES. As DES has a smaller key size which makes it less secure to overcome this triple DES was introduced but it turns out to be slower. Hence, later AES was introduced by the National Institute of Standard and Technology.

[\[368\]](#)

In telecoms and computer networks, **multiplexing** (aka muxing) is a method by which multiple analog or digital signals are combined into one signal over a shared medium. The aim is to share an expensive resource. For example, in telecoms, several telephone calls may be carried using one wire. Multiplexing originated in the 1870s and is now widely applied in communications.

[\[369\]](#)

About the network, docs.cardano.org/explore-cardano/cardano-network/about-the-cardano-network#gatsby-focus-wrapper
[370]

Network protocol overview, docs.cardano.org/explore-cardano/cardano-network/networking-protocol#gatsby-focus-wrapper

[371]

Digital footprint or digital shadow refers to one's unique set of traceable digital activities, actions, contributions and communications manifested on the Internet or on digital devices. On the World Wide Web, the internet footprint; also known as cyber shadow, electronic footprint, or digital shadow, is the information left behind as a result of a user's web-browsing and stored as cookies.

[372]

A **directed acyclic graph** is a directed graph with no directed cycles. That is, it consists of vertices and edges, with each edge directed from one vertex to another, such that following those directions will never form a closed loop.

[373]

Transaction output: Outputs produced by transactions. They are consumed when they are spent by another transaction. Typically, some kind of evidence is required to be able to spend a UTXO, such as a signature from a public key, or (in the Extended UTXO Model) satisfying a script.

[374]

The **address of a UTXO** says where the output is 'going'. The address stipulates the conditions for unlocking the output. This can be a public key hash, or (in the Extended UTXO model) a script hash.

[375]

A **script output:** A UTXO locked by a script.

[376]

Redeemer: The argument to the validator script which is provided by the transaction which spends a script output.

[377]

A **validator script** is the script attached to a script output in the Extended UTXO model. Must be run and return positively in order for the output to be spent. It determines the address of the output.

[378]

Validation context: A data structure containing a summary of the transaction being validated, and the current input whose validator is being run.

[379]

The term **Parallelism** refers to techniques to make programs faster by performing several computations at the same time.

[380]

Fernando Sanchez, ‘Cardano’s extended UTXO accounting model’, iohk.io/en/blog/posts/2021/03/12/cardanos-extended-utxo-accounting-model-part-2/

[381]

Surprise AMA 04/13/2022, youtu.be/AejphsMjkPc?t=298

[382]

John O’Connor, ‘Welcome to the age of RealFi’, iohk.io/en/blog/posts/2021/11/25/welcome-to-the-age-of-realfi/

[383]

DeFi is innovating at 10 times the rate of traditional finance?, coinyuppie.com/defi-is-innovating-at-10-times-the-rate-of-traditional-finance/

[384]

Atala PRISM is a decentralized identity solution built on the Cardano blockchain. It creates a new approach to identity management, where users own their identity and have complete control over how their personal data is used and accessed.

[385]

Olga Hryniuk, ‘Introducing the new Plutus Playground’,
iohk.io/en/blog/posts/2021/01/25/introducing-the-new-plutus-playground/

[386]

Surprise AMA 08302020, youtu.be/lIz3GnCHbOc?t=993

[387]

TVL (total value locked) in Decentralized Finance (DeFi) on the Ethereum blockchain from August 2017 to April 5, 2022,
www.statista.com/statistics/1237821/defi-market-size-value-crypto-locked-usd/

[388]

Cardano Africa 2021, africa.cardano.org/

[389]

World Mobile X IOHK — Charles Hoskinson, Micky Watkins, and John O’ Connor, youtu.be/WSSpl8Rtif0

[390]

Internet blimps are coming to Zanzibar.,
edition.cnn.com/2022/01/12/africa/world-mobile-internet-balloon-zanzibar-spc-intl/index.html

[391]

World Mobile: Building smart cities, building smart countries,

www.youtube.com/watch?v=5ijAOa6VjzA

[392] Charles Hoskinson Interview - On The Power of World Mobile,
<https://www.youtube.com/watch?v=SSptqZ4y4JI>

[393]

Whale is a cryptocurrency term that refers to individuals or entities that hold large amounts of Bitcoin or any other cryptocurrencies. Whales hold enough cryptocurrency that they have the potential to manipulate the currency valuations.

[394]

Charles Hoskinson explains how he will know that Cardano has achieved ‘Success’, cardanofeed.com/charles-hoskinson-explains-how-he-will-know-that-cardano-has-achieved-success-356.html

[395]

The future will be decentralized | Charles Hoskinson | TEDxBermuda, www.youtube.com/watch?v=97ufCT6lQcY

[396]

Blockchain finally comes of age with the world’s biggest blockchain deployment, iohk.io/en/blog/posts/2021/04/27/blockchain-finally-comes-of-age-with-worlds-biggest-blockchain-deployment/

[397]

Tim Richmond, ‘Project Catalyst launches incubator for Africa’, iohk.io/en/blog/posts/2022/04/05/project-catalyst-launches-incubator-for-africa/

[398]

CROW..Live With Charles Hoskinson of Cardano ADA 11/24/20, www.youtube.com/watch?v=z3s6oIBfbfA

[399]

Neither Smart Nor Contracts: Smart Contracts Need a Rebrand, www.netguru.com/blog/smart-contracts

[400]

Surprise AMA 03/31/2019, youtu.be/sc4D2KrvNA?t=2315

[401]

Bitcoin dust refers to the very small amounts of bitcoin leftover or unspent in a transaction that is lower in value than the minimum limit of a valid transaction. Thus, processing the transaction is impossible, trapping a tiny amount of Bitcoin (perhaps 0.00000012 BTC, for instance), in a wallet or address.

[402]

Blockchain Certificates (Academic & Others),
www.unic.ac.cy/iuff/blockchain-certificates/

[403]

Atala PRISM, www.atalaprism.io/

[404]

A hash tree or **Merkle tree** is a tree in which every leaf node is labeled with the hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

[405]

PSG Cardano Wallet API, github.com/input-output-hk/psg-cardano-wallet-api

[406]

CBOR (Concise Binary Object Representation) is a binary data serialization format loosely based on JSON. Like JSON it allows the transmission of data objects that contain name–value pairs, but in a more concise manner. This increases processing and transfer speeds at the cost of human-readability.

[407]

Concise data definition language (CDDL) expresses Concise Binary Object Representation (CBOR) data structures. Its main goal is to provide an easy and unambiguous way to express structures for protocol messages and data formats that use CBOR or JSON (JavaScript Object Notation).

[\[408\]](#)

Transaction Metadata, github.com/input-output-hk/cardano-node/blob/master/doc/reference/tx-metadata.md

[\[409\]](#)

Post Conference recap, thoughts and an AMA 04/21/2019, youtu.be/pBXZVrBQ6U8?t=3557

[\[410\]](#)

Alan McSherry, ‘Getting to grips with metadata on Cardano’, iohk.io/en/blog/posts/2020/11/03/getting-to-grips-with-metadata-on-cardano/

[\[411\]](#)

‘Snoop, Champ, Charles & Clay Nation’ twitter space, April 5, 2022, twitter.com/IOHK_Charles/status/1511402568420929538?s=20&t=dzpXHsegwzrpRRCQ-cfUXw

[\[412\]](#)

Twitter Space ‘4/20 Hangout with Charles’, twitter.com/i/spaces/1IDGLLABeBkGm

[\[413\]](#)

Cardano360 March 2022, youtu.be/r6qNwOE9Bvo?t=3498

[\[414\]](#)

Ethereum ERC20 Contract is a standard for building tokens on the Ethereum Blockchain. Before ERC20 tokens, Cryptocurrency exchanges had to build custom bridges between platforms to support the exchange of any token. For this reason, six rules were created by an Ethereum developer named Fabian Vogelsteller and

placed under the name ERC20, which means ‘ethereum request for comment.’

[\[415\]](#)

ERC721 is a free, open standard that describes how to build non-fungible or unique tokens on the Ethereum Blockchain.

[\[416\]](#)

Token: A cryptographic token that reflects the value as defined by the community, market state, or self-governed entity. A fungible or non-fungible token may be used as a payment unit, a reward, a trade asset, or a data holder.

[\[417\]](#)

What's all the fuss about NBA top shot?,

www.si.com/nba/2021/03/17/nba-top-shot-crypto-daily-cover

[\[418\]](#)

Gas (Ethereum) refers to the fee, or pricing value, required to successfully conduct a transaction or execute a smart contract on the Ethereum blockchain platform. Priced in small fractions of the cryptocurrency ether, commonly referred to as gwei or sometimes nanoeth, the gas is used to allocate resources of the Ethereum Virtual Machine (EVM) so that decentralized applications such as smart contracts can self-execute in a secured fashion. The maximum amount of gas that you're willing to spend on a particular transaction is known as the gas limit.

[\[419\]](#)

'\$300m in cryptocurrency' accidentally lost forever due to bug,

www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether

[\[420\]](#)

3 Reasons Solana Isn't Really Decentralized,

www.makeuseof.com/reasons-solana-isnt-really-decentralized/

[\[421\]](#)

Utility token: a digital token that represents a certain project or environment and has specific capabilities. These tokens may be used as payment units, prizes, or as a means of gaining entry to a particular network.

[\[422\]](#)

Blockchain Vulnerabilities: Vulnerable ERC20 Tokens and How to Avoid Writing Vulnerable Code , www.apriorit.com/dev-blog/555-erc20-token-vulnerability

[\[423\]](#)

What is a native token and how does it compare to ada and ERC20?, github.com/input-output-hk/cardano-ledger-specs/blob/master/doc/explanations/features.rst

[\[424\]](#)

Welcome to native tokens on Cardano!, www.youtube.com/watch?v=PVqsCXh-V5Y

[\[425\]](#)

Blockchain Insights, datastudio.google.com/u/0/reporting/3136c55b-635e-4f46-8e4b-b8ab54f2d460/page/p_wxcw6g0irc

[\[426\]](#)

Interoperability is key to blockchain growth, iohk.io/en/blog/posts/2022/04/28/interoperability-is-key-to-blockchain-growth/

[\[427\]](#)

Tim Harrison, ‘Native Tokens on Cardano’, iohk.io/en/blog/posts/2020/12/08/native-tokens-on-cardano/

[\[428\]](#)

In economics, **fungibility** is the property of a good or a commodity whose individual units are essentially interchangeable, and each of its parts is indistinguishable from another part.

[429] Getting started with native tokens, docs.cardano.org/native-tokens/getting-started

[430]

Learn about native tokens, docs.cardano.org/native-tokens/

[431]

Tokhun, tokhun.io/jonathandickson

[432]

Twitter Jonathan Dickson, twitter.com/JonathanDickson

[433]

Jonathan Dickson Elements NFTs on Cardano,

www.youtube.com/watch?v=F1DR-39RN28

[434]

min-ada-value Explanation, cardano-ledger.readthedocs.io/en/latest/explanations/min-utxo-mary.html?highlight=min%20utxo%20value#min-ada-value-explanation

[435]

PostgreSQL, also known as Postgres, is a free and open-source relational database management system emphasizing extensibility and SQL compliance. See *Appendix: Cardano Architecture*.

[436]

Getting started with native tokens, docs.cardano.org/native-tokens/getting-started

[437]

Getting started with Native Tokens, docs.cardano.org/native-tokens/getting-started

[438]

Minting policies and the multi asset ledger, cardano-ledger.readthedocs.io/en/latest/explanations/policies.html

[439]

minimum-ada-value requirement, cardano-ledger.readthedocs.io/en/latest/explanations/min-utxo-mary.html?highlight=minimum%20ada%20value%20requirement

[440]

Kraken listing process, support.kraken.com/hc/en-us/articles/360001388206-New-coin-listing-requests

[441]

Binance listing process,
www.binance.com/en/support/faq/053e4bdc48364343b863d1833618d8ba

[442]

The Island, The Ocean and the Pond (Soon),
www.youtube.com/watch?v=k8a6tX53YPs

[443]

KEVM devnet, developers.cardano.org/en/virtual-machines/kevm/overview/

[444]

K framework, kframework.org/

[445]

Ethereum Virtual Machine (EVM) is a powerful, sandboxed virtual stack embedded within each full Ethereum node, responsible for executing contract bytecode. Contracts are typically written in Higher-Level languages, like Solidity, then compiled to EVM bytecode.

[446]

Semantics based compilation, testnets.cardano.org/en/virtual-machines/iele/about/semantics-based-compilation/

[447]

Bytecode is a form of instruction set designed for efficient execution by a software interpreter. Unlike human-readable source code, bytecodes are compact numeric codes, constants, and references.

[448]

Goguen roadmap, roadmap.cardano.org/en/goguen/

[449]

Milkomeda on twitter, twitter.com/Milkomeda_com

[450]

Zero-knowledge rollups (ZK-rollups) are similar to optimistic rollups in that they combine a large number of Layer 2 transactions that were executed off-chain and submit them as one transaction.

[451]

Twitter space – ‘Sunday Chat with Charles’,
[twitter.com/IOHK_Charles/status/1515872352395055109?
s=20&t=ivZvNmtLVKrKk_ZEg-1e_A](https://twitter.com/IOHK_Charles/status/1515872352395055109?s=20&t=ivZvNmtLVKrKk_ZEg-1e_A)

[452]

Alan McSherry, ‘Bringing new value and utility to the Cardano blockchain’, iohk.io/en/blog/posts/2020/10/29/bringing-new-value-and-utility-to-the-cardano-blockchain/

[453]

Kevin Hammond, ‘Goguen brings token locking to Cardano’, iohk.io/en/blog/posts/2020/12/02/goguen-brings-token-locking-to-cardano/

[454]

Tim Harrison, ‘Building native tokens on Cardano for pleasure and profit’, iohk.io/en/blog/posts/2021/02/18/building-native-tokens-on-cardano-for-pleasure-and-profit/

[[455](#)]

Michael Peyton Jones, ‘Plutus Tx: compiling Haskell into Plutus Core’, iohk.io/en/blog/posts/2021/02/02/plutus-tx-compiling-haskell-into-plutus-core/

[[456](#)]

API library, github.com/input-output-hk/cardano-node/tree/master/cardano-api

[[457](#)]

Plutus pioneers, developers.cardano.org/en/plutus-pioneer-program/

[[458](#)]

A **feature freeze**, is where all work on adding new features is suspended, shifting the effort towards fixing bugs and improving the user experience.

[[459](#)]

Adam Hayes, ‘10 Important Cryptocurrencies Other Than Bitcoin’, www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

[[460](#)]

CryptoSlate Smart Contract Coins, cryptoslate.com/cryptos/smart-contracts/

[[461](#)]

The DAO Hack Explained: Unfortunate Take-off of Smart Contracts, ogucluturk.medium.com/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562

[[462](#)]

More than \$320 million stolen in latest apparent crypto hack,
www.cnbc.com/2022/02/02/320-million-stolen-from-wormhole-bridge-linking-solana-and-ethereum.html

[[463](#)]

Nikolic, Kolluri, Sergey, Saxena, Hobor (2018), Finding The Greedy, Prodigal, and Suicidal Contracts at Scale,
arxiv.org/pdf/1802.06038.pdf

[[464](#)]

Fernando Sanchez, ‘Cardano’s Extended UTXO accounting model – built to support multi-assets and smart contracts’,
iohk.io/en/blog/posts/2021/03/11/cardanos-extended-utxo-accounting-model/

[[465](#)]

Plutus Pioneer Program, PPP 030101 - Welcome and Introduction,
www.youtube.com/watch?v=X80uNXenWF4&list=PLK8ah7DzglhgK0bEyELK8EzbW0mn6xavC
[[466](#)]

Datum: the data field on script outputs in the Extended UTXO model.

[[467](#)]

Cardano Founder Deals With Concurrency FUD, a Second Japanese Exchange Lists \$ADA,
www.cryptoglobe.com/latest/2021/09/cardano-founder-deals-with-concurrency-fud-a-second-japanese-exchange-lists-ada/
[[468](#)]

More on Concurrency, youtu.be/OVh-eiACtzY?t=325
[[469](#)]

ulimit is a built-in Linux shell command that allows viewing or limiting system resource amounts that individual users consume.

Limiting resource usage is valuable in environments with multiple users and system performance issues.

[\[470\]](#)

UTXO congestion: The effect of multiple transactions attempting to spend the same transaction output.

[\[471\]](#)

Concurrency, the property of program, algorithm, or problem decomposition into order-independent or partially-ordered units.

[\[472\]](#)

A **semaphore** is a variable, or abstract data type, used to control access to a common resource by multiple threads and avoid critical section problems in a concurrent system such as a multitasking operating system. Semaphores are a type of synchronization primitives. A trivial semaphore is a plain variable that is changed depending on programmer-defined conditions.

[\[473\]](#)

SundaeSwap blog on concurrency,
sundaeswap.finance/posts/concurrency-state-cardano

[\[474\]](#)

Cardano-based DEX WingRiders Hits \$44 Million TVL Within 24 hours of Launch, thecryptobasic.com/2022/04/13/cardano-based-dex-wingriders-hits-44-million-tvl-within-24-hours-of-launch/

[\[475\]](#)

Lars Brunjes, iohk.io/en/team/lars-brunjes

[\[476\]](#)

An **automated market maker (AMM)** is a decentralized asset trading pool that enables market participants to trade cryptocurrencies. AMMs are non-custodial and permissionless in nature. Notable examples include Uniswap on Ethereum or ErgoDex on Cardano / Ergo.

[\[477\]](#)

Zahnentferner, Kaidarov, Etienne, Díaz (2021) 'Djed: A Formally Verified Crypto-Backed Pegged Algorithmic Stablecoin', eprint.iacr.org/2021/1069.pdf

[\[478\]](#)

Djed is an algorithmic stablecoin protocol on Cardano announced at the 2021 summit. The Djed is an Egyptian hieroglyph representing stability and durability. Djed behaves like an autonomous bank. More about Djed later in this chapter.

[\[479\]](#)

Front running, also known as tailgating, is the prohibited practice of entering into an equity (stock) trade, option, futures contract, derivative, or security-based swap to capitalize on advance, nonpublic knowledge of a large pending transaction that will influence the price of the underlying security.

[\[480\]](#)

Charles Hoskinson Interview - Latest Cardano ADA Updates, Eth, www.youtube.com/watch?v=Hj9w-fK7mWo

[\[481\]](#)

Jean-Frédéric Etienne, 'Architecting DApps on the EUTXO ledger', iohk.io/en/blog/posts/2021/11/16/architecting-dapps-on-the-eutxo-ledger/

[\[482\]](#)

SundaeSwap blog, sundaeswap-finance.medium.com/sundaeswap-labs-presents-the-scooper-model-678d6054318d

[\[483\]](#)

Maladex blog on concurrency, blog.maladex.com/maladex-solves-concurrency-scales-beyond-memory-limits-and-designs-the-best-possible-cardano-dex-391d7e519e67

[\[484\]](#)

What is ERGO + ERGOdex Concurrency Solution For Cardano,
www.youtube.com/watch?v=xIDINmlFrFM

[485]

Cardano with Paul, www.youtube.com/watch?v=xIDINmlFrFM

[486]

IOHK Lobster challenge, github.com/input-output-hk/lobster-challenge/tree/concurrency-multisig

[487]

Order book pattern, [plutus-apps.readthedocs.io/en/latest/plutus/explanations/order-book-pattern.html#what-is-the-order-book-pattern](https://apps.readthedocs.io/en/latest/plutus/explanations/order-book-pattern.html#what-is-the-order-book-pattern)

[488]

Surprise AMA 04/13/2022, youtu.be/AejphsMjkPc?t=216

[489]

Babel Fish, hitchhikers.fandom.com/wiki/Babel_Fish.

[490]

Babel Fees, iohk.io/en/blog/posts/2021/02/25/babel-fees/

[491] Chakravarty, Karayannidis, Kiayias, Peyton Jones, Vinogradova (2022), 'Babel Fees via Limited Liabilities',

iohk.io/en/research/library/papers/babel-fees-via-limited-liabilities/

[492]

HODL is slang in the cryptocurrency community for holding the cryptocurrency rather than selling it. HODL can also mean 'Hold On for Dear Life' and refers to not selling, even during strong market volatility and poor market performance.

[493]

Roundtable with Charles Hoskinson and Alex Chepurnoy | Ergo Pulse, www.youtube.com/watch?v=k9a3SYV6FJA

[\[494\]](#)

Spot trading is a continuous process of buying and selling tokens and coins at a spot price for immediate settlement. The trader usually intends to gain profits from market fluctuations.

[\[495\]](#)

An **atomic swap** is an exchange of cryptocurrencies from separate blockchains. The swap is conducted between two entities without a third party's involvement. The idea is to remove centralized intermediaries like regulated exchanges and give token owners total control.

[\[496\]](#) Babel fees via limited liabilities, www.youtube.com/watch?v=iJEmRZ6leXE

[\[497\]](#)

Surprise AMA 02/26/2021, youtu.be/6eD_rnII3ms?t=42

[\[498\]](#)

Tether (ticker USDT) is a cryptocurrency that is hosted on the Ethereum and Bitcoin blockchains, among others. Its tokens are issued by the Hong Kong company Tether Limited, which in turn is controlled by the owners of Bitfinex. Tether is called a stablecoin because it was originally designed to always be worth US\$1.00, maintaining \$1.00 in reserves for each tether issued.

[\[499\]](#)

Babel fees - denominating transaction costs in native tokens, iohk.io/en/blog/posts/2021/02/25/babel-fees/

[\[500\]](#)

Special Drawing Rights (SDR), www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR

[\[501\]](#)

The AgeUSD Stablecoin Protocol, github.com/Emurgo/age-usd

[\[502\]](#)

Alexander Chepurnoy, ergoplatform.org/en/hall_of_fame/

[\[503\]](#)

Surprise AMA 04/13/2022, youtu.be/AejphsMjkPc?t=216

[\[504\]](#)

Tether Price History and Everything You Need to Know,
www.rain.bh/learn/tether-price-history-and-information-you-need-for-tether-trading

[\[505\]](#)

Formal verification is the act of proving or disproving the correctness of intended algorithms underlying a system with respect to a certain formal specification or property, using formal methods of mathematics. Formal verification can be helpful in proving the correctness of systems such as: cryptographic protocols, combinational circuits, digital circuits with internal Memory, and software expressed as source code.

[\[506\]](#)

Kovan is a Proof of Authority (PoA) publicly accessible blockchain for Ethereum; created and maintained by a consortium of Ethereum developers.

[\[507\]](#)

Scala is a general-purpose programming language providing support for functional programming and a strong static type system. Designed to be concise, many of Scala's design decisions aimed to address criticisms of Java.

[\[508\]](#)

Ergo Summit 2021 - Entering The New Era - Announcing AgeUSD & The Hardening Upgrade, www.youtube.com/watch?v=zG-rxMCDIa0&t=8366s

[\[509\]](#)

A closer look at the cFund, iohk.io/en/blog/posts/2021/07/28/a-closer-look-at-the-cfund/

[\[510\]](#)

\$ADA: DEX WingRiders Launches, Bringing USDC and USDT Stablecoins to Cardano Mainnet,
www.cryptoglobe.com/latest/2022/04/ada-dex-wingriders-launches-bringing-usdc-and-usdt-stablecoins-to-cardano-mainnet/

[\[511\]](#)

Terra (LUNA) is a Decentralized system focused on enhancing the DeFi space through programmable payments to drive adoption. The Protocol has a native Token, LUNA, and is backed by a host of fiat-pegged Stablecoin. By employing Stablecoin, Terra presents a payment infrastructure void of the shortcomings of traditional payment methods such as Credit card and old Blockchain-based payment systems.

[\[512\]](#)

Terra UST collapse, www.coindesk.com/business/2022/05/09/ust-stablecoin-falls-below-dollar-peg-for-second-time-in-48-hours/

[\[513\]](#)

Terra BTC address,
bitaps.com/2c2daf15ff549f84faf3dde74da288727f4a63724c957bf83a2d263a97779f65/bc1q9d4ywgfnd8h43da5tpcxn6ajv590cg6d3tg6axemvljvt2k76zs50tv4q

[\[514\]](#)

Crypto Market EMERGENCY: UST, LUNA & BTC - What Gives?!,
www.youtube.com/watch?v=x5v67Larlx8

[\[515\]](#)

The tether controversy, explained,
www.theverge.com/22620464/tether-backing-cryptocurrency-stablecoin

[\[516\]](#)

Cardana ADA: I was wrong, www.youtube.com/watch?v=ew-qrNFKWtA

[\[517\]](#)

COTI updates by Shahaf Bar-Geffen, COTI's CEO,
www.youtube.com/watch?v=453M7Pjklbc

[\[518\]](#)

Bitcoin Market Journal, www.bitcoinmarketjournal.com/investors-guide-to-terra-and-luna/arbitrage-behavior-around-luna-and-ust/

[\[519\]](#)

Saturday Night Live AMA 04/18/2020, youtu.be/a3bQ1u4DYns?t=2776

[\[520\]](#)

The (1944) Bretton Woods Agreement established a system through which a fixed currency exchange rate could be created using gold as the universal standard. The agreement involved representatives from 44 nations and brought about the creation of the International Monetary Fund (IMF) and the World Bank

[\[521\]](#)

MakerDAO is an American decentralized company providing a smart contract platform built on Ethereum. Through their asset-backed stablecoin called the DAI, the platform uses a dynamical system of Collateralized Debt Positions (CDPs) and other technological factors as the source of stabilizing value. DAI also responds to emergency conditions relative to the world's major currencies. This allows for the company's other cryptocurrency, MKR, to dilute and sell to raise funds to recapitalize the system.

[\[522\]](#)

Bruno Paleo, iohk.io/en/team/bruno-woltzenlogel-paleo

[\[523\]](#)

'Let's talk Crypto' Twitter space, May 14, 2022,
[twitter.com/IOHK_Charles/status/1525305465105694720?
s=20&t=MdeQMAKTTIBAhzl5Yvf2Ug](https://twitter.com/IOHK_Charles/status/1525305465105694720?s=20&t=MdeQMAKTTIBAhzl5Yvf2Ug)

[\[524\]](#)

Venture capital (VC) is a type of private equity, a form of financing that is provided by firms or funds to small, early-stage, emerging firms that are deemed to have high growth potential, or which have demonstrated high growth. Venture capital firms or funds invest in these early-stage companies in exchange for equity, or an ownership stake, in the companies they invest in. Venture capitalists take on the risk of financing risky start-ups in the hopes that some of the firms they support will become successful.

[\[525\]](#)

In DeFi, **impermanent loss** refers to the loss in value when investing liquidity in a liquidity pool compared to just holding tokens. The event occurs when the price of a user's tokens changes compared to when they deposited them in a liquidity pool. The larger the change is, the bigger the loss.

[\[526\]](#)

A bull market or **bull run** is a state of a financial market where prices are rising. The term bull market is often used in the context of the stock market. However, it can be used in any financial market including cryptocurrencies.

[\[527\]](#)

A **market maker or liquidity provider** quotes both a buy and a sell price in a financial instrument or commodity held in inventory, hoping to make a profit on the bid-offer spread, or turn. The U.S. Securities and Exchange Commission defines a 'market maker' as a firm that

stands ready to buy and sell stock on a regular and continuous basis at a publicly quoted price.

[528]

Kiayias, Koutsoupias, Stouka (2021) 'Incentives Against Power Grabs or How to Engineer the Revolution in a Pooled Proof of Stake System', arxiv.org/pdf/2111.08562.pdf

[529]

Judmayer, Stifter, Zamyatin, Tsabary, Eyal, Gaži, Meiklejohn, Weippl (2021), 'SoK: Algorithmic Incentive Manipulation Attacks on Permissionless PoW Cryptocurrencies', eprint.iacr.org/2020/1614.pdf

[530]

Yield farming is a DeFi term for leveraging DeFi protocols and products to generate high returns that sometimes reach over 100% in annualized yields 'when factoring in interest, token rewards, 'cashback' bonuses, and other incentives.' Yield farming is a way for cryptocurrency enthusiasts to maximize their returns. It typically involves users lending or locking up their funds using smart contracts. In return, users earn fees in the form of crypto.

[531]

Is Do Kwon going to get arrested after Terra's LUNA price collapse?, www.fxstreet.com/cryptocurrencies/news/is-do-kwon-going-to-get-arrested-after-terra-luna-price-collapse-202205191033

[532]

Chitra, Angeris, Evans (2021), 'Differential Privacy in Constant Function Market Makers', eprint.iacr.org/2021/1101.pdf

[533]

The **(TVL) Total Value Locked** into a smart contract or set of smart contracts that may be deployed or stored at one or more exchanges or markets. This is used as a measurement of investor deposits. It is the dollar value of all the coins or tokens locked into a platform,

protocol, lending program, yield farming program, or insurance liquidity pool.

[\[534\]](#)

Slippage refers to the difference between the expected price of a trade and the price at which the trade is executed. Slippage can occur at any time but is most prevalent during periods of higher volatility when market orders are used.

[\[535\]](#)

Criticism from Solana founder,
[twitter.com/IOHK_Charles/status/1532360549857693697?
s=20&t=YIDNMde_QXHGEURpgZj8UA](https://twitter.com/IOHK_Charles/status/1532360549857693697?s=20&t=YIDNMde_QXHGEURpgZj8UA)

[\[536\]](#)

CardanoCube DEXs, www.cardanocube.io/collections/exchanges-dex

[\[537\]](#)

What is impermanent loss?, geniusyield.medium.com/what-is-impermanent-loss-2f03a90a8bcb

[\[538\]](#)

SingularityNET (ticker symbol: AGI) is a decentralized marketplace for Artificial Intelligence.

[\[539\]](#)

DeFi Total Value Locked Hits All-Time High of \$236 Billion ,
www.prnewswire.com/news-releases/defi-total-value-locked-hits-all-time-high-of-236-billion-301412901.html

[\[540\]](#)

Total Value Locked in Defi Nears Lifetime High, Ethereum's TVL Dominates by 54%, news.bitcoin.com/total-value-locked-in-defi-nears-lifetime-high-ethereums-tvl-dominates-by-54

[\[541\]](#)

Unique Cardano (ADA) Wallets Surge to Record High Above 3 Million, cryptopotato.com/unique-cardano-ada-wallets-surge-to-record-high-above-3-million/

[542]

Uniswap is a Decentralized Exchange (DEX) built on Ethereum that utilizes an automated market-making system instead of a traditional order-book. It was inspired by a Reddit post from Vitalik Buterin and was founded by Hayden Adams in 2017.

[543]

DeFi Adoption 2020: A Definitive Guide to Entering the Industry, s3.cointelegraph.com/storage/uploads/view/48c6c4e03f85bc722d76f88c2676478b.pdf?_ga=2.42938214.270418488.1602500005-1231871226.1593587737

[544]

Morgan Stanley warns Ethereum could lose ground to Binance, Solana, and Cardano, making shift to ‘proof of stake’ even more urgent, fortune.com/2022/02/18/ethereum-smart-contracts-proof-of-stake-binance-solana-cardano-morgan-stanley/

[545]

CardanoCube ecosystem, www.cardanocube.io/cardano-ecosystem-interactive-map

[546]

SingularityNET Phase II Launch Sequence Activated: AGI token to be hard-forked to Cardano-compatible AGIX, blog.singularitynet.io/singularitynet-phase-ii-launch-sequence-activatedagi-token-to-be-hard-forkedto-10ede4b6c89

[547]

AGIX converter testnet, testnet.agix-converter.iohk.io/

[548]

Cardano 2021 Summit session on Certification,
summit.cardano.org/sessions/smart-contract-certification-the-why-and-how

[\[549\]](#)

Cardano 2021 Summit DApp Store demo,
summit.cardano.org/sessions/redefining-dapp-discovery-bringing-dapps-to-the-mass-market

[\[550\]](#)

Smart Contract Certification, summit.cardano.org/sessions/smart-contract-certification-the-why-and-how

[\[551\]](#)

Prof. Simon Thompson, iohk.io/en/team/simon-thompson

[\[552\]](#)

Shruti Appiah, iohk.io/en/team/shruti-appiah

[\[553\]](#)

Lace light wallet, www.lace.io

[\[554\]](#)

Consensus 2022, www.coindesk.com/consensus2022/

[\[555\]](#)

DApp Store Plans, summit.cardano.org/sessions/redefining-dapp-discovery-bringing-dapps-to-the-mass-market

[\[556\]](#)

Chainlink (ticker: LINK) is a decentralized oracle network that brings off-chain data into an on-chain format, bridging the gap between isolated blockchains and real-world data.

[\[557\]](#)

Cardano Announces Strategic Collaboration To Integrate Chainlink's Oracles, chainlinktoday.com/cardano-announces-strategic-

collaboration-to-integrate-chainlinks-oracles/

[558]

Parametric insurance is a type of insurance that does not indemnify the pure loss, but ex-ante (Latin for ‘before the event’) agrees to make a payment upon the occurrence of a triggering event. The triggering event is often a catastrophic natural event which may ordinarily precipitate a loss or a series of losses. But parametric insurance principles are also applied to Agricultural crop insurance and other normal risks not of the nature of disaster, if the outcome of the risk is correlated to a parameter or an index of parameters.

[559]

Essential Cardano Oracles, github.com/input-output-hk/essential-cardano/blob/main/essential-cardano-list.md#oracles

[560]

CardanoCube Oracles, www.cardanocube.io/collections/oracle

[561]

Ergo Oracle Pools, ergoplatform.org/en/blog/2021-04-27-chainlink-oracles-vs-ergo-oracle-pools/

[562]

Rollups on Cardano Discussion | Cardano Live #48,
www.youtube.com/watch?v=4DslvkLop04

[563]

Maller, Bowe, Kohlweiss, Meiklejohn (2019), 'Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updateable Structured Reference Strings', eprint.iacr.org/2019/099.pdf

[564]

UTXO alliance announcement, summit.cardano.org/sessions/taking-outputs-as-inputs

[565]

Sharding splits a blockchain company's entire network into smaller partitions, known as 'shards.' Each shard consists of its own data, making it distinctive and independent when compared to other shards.

[\[566\]](#)

EUTXO explainer, docs.cardano.org/plutus/eutxo-explainer

[\[567\]](#)

Why Privacy and Interoperability Will Fuel Exponential Growth in DeFi, www.nasdaq.com/articles/why-privacy-and-interoperability-will-fuel-exponential-growth-in-defi-2021-03-04

[\[568\]](#)

Learning Ergo 101 : eUTXO explained for human beings, dav009.medium.com/learning-ergo-101-blockchain-paradigm-eutxo-c90b0274cf5e

[\[569\]](#)

Olga Hryniuk, 'Concurrency and all that: Cardano smart contracts and the EUTXO model', iohk.io/en/blog/posts/2021/09/10/concurrency-and-all-that-cardano-smart-contracts-and-the-eutxo-model/

[\[570\]](#)

Sebastian Nagel, 'Hydra – Cardano's solution for ultimate Layer 2 scalability', iohk.io/en/blog/posts/2021/09/17/hydra-cardano-solution-for-ultimate-scalability/

[\[571\]](#)

A **distributed system** is a system whose components are located on different networked computers, which communicate and coordinate their actions by passing messages to one another. The components interact with one another to achieve a common goal. Three significant characteristics of distributed systems are:

concurrency of components, lack of a global clock, and independent failure of components.

[572]

AWS vs Amazon: Cloud giant's revenue rises as parent company's profit falls during Q4,

www.computerweekly.com/news/252512961/AWS-vs-Amazon-Cloud-giants-revenue-rises-as-parent-companys-profit-falls-during-Q4

[573]

Gartner OCI scorecard, www.oracle.com/uk/cloud/what-is-iaas/gartner-oci-scorecard/

[574]

Neil Burgess, 'When it comes to DeFi, do your own research',
iohk.io/en/blog/posts/2021/12/09/when-it-comes-to-defi-do-your-own-research/

[575]

Cardano Founder Spills The Beans on 'Fakeness' of Silicon Valley,
www.newsbtc.com/news/cardano/cardano-founder-spills-the-beans-on-fakeness-of-silicon-valley/

[576]

VCs don't understand that Cardano has a community: Charles Hoskinson, cointelegraph.com/news/vcs-don-t-understand-that-cardano-has-a-community-charles-hoskinson

[577]

Guide to Ethereum, medium.com/coinmonks/pauls-guide-to-ethereum-280be582653

[578]

Charles Hoskinson Interview (Halloween Special 2020),
youtu.be/7RmH6w2rMh4?t=1399

[579]

A security token offering / tokenized IPO is a type of public offering in which tokenized digital securities, known as security tokens, are sold in security token exchanges

[580]

Plutus Playground, playground.plutus.iohkdev.io/

[581]

Plutus tutorials, plutus-apps.readthedocs.io/en/latest/

[582]

Plutus explanations, plutus-

apps.readthedocs.io/en/latest/plutus/explanations/index.html

[583]

Plutus github repo, github.com/input-output-hk/plutus

[584]

Validator scripts, docs.cardano.org/plutus/Plutus-validator-scripts

[585]

Plutus Tx: The libraries and compiler for compiling Haskell into Plutus Core to form the on-chain part of a contract application.

[586]

Plutarch, github.com/Plutonomicon/plutarch

[587]

Business logic or domain logic is the part of the program that encodes the real-world business rules that determine how data can be created, stored, and changed. It is contrasted with the remainder of the software that might be concerned with lower-level details.

[588]

The **UTXO set** is the comprehensive set of all UTXOs existing at a given point in time. The sum of the amounts of each UTXO in this

set is the total supply of existing currency at that point of time. Anyone can verify the total supply at any time in a trustless manner.
[\[589\]](#)

A finite-state machine (FSM) or simply a **state machine**, is a mathematical model of computation. It is an abstract machine that can be in exactly one of a finite number of states at any given time. The FSM can change from one state to another in response to some external inputs and/or a condition is satisfied; the change from one state to another is called a transition. An FSM is defined by a list of its states, its initial state, and the conditions for each transition.

[\[590\]](#)

WebSocket is a communications protocol, providing full-duplex communication channels over a single TCP connection. The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP.

[\[591\]](#)

Minting policy, github.com/input-output-hk/cardano-documentation/blob/staging/content/07-native-tokens/01-learn.mdx#minting-policy

[\[592\]](#)

A **toolchain** is a set of programming tools that is used to perform a complex software development task or to create a software product, which is typically another computer program or a set of related programs.

[\[593\]](#)

The purpose of **DB Sync** is to follow the Cardano chain and take information from the chain and an internally maintained copy of ledger state. Data is then extracted from the chain and inserted into a PostgreSQL database. SQL queries can then be written directly against the database schema.

[594]

Cardano Nodes, docs.cardano.org/new-to-cardano/cardano-nodes
[595]

MultiSig scripts, github.com/input-output-hk/cardano-node/blob/master/doc/reference/simple-scripts.md#multi-signature-scripts

[596]

Plutus Playground - Video Tutorial: Compiling and testing a Plutus App, www.youtube.com/watch?v=DhRS-JvoCw8

[597]

Marlowe Playground, alpha.marlowe.iohkdev.io/#/
[598]

A **Chain index** is a database of information obtained from Cardano transactions.

[599]

API alternatives, youtu.be/W2R3zl91U24?t=357
[600]

Mockchain: A testnet version of a blockchain. Used during development, prototyping or testing transactions without fees.

[601]

Ethereum Gas Fees Continue to Rise,
www.analyticsinsight.net/ethereum-gas-fees-continue-to-rise-while-bitget-zero-gas-fee-blockchain-is-booming/
[602]

Absolute vs. Relative Price: Absolute price is the number of dollars that can be exchanged for a specified quantity of a given good. Relative price is the quantity of some other good that can be exchanged for a specified quantity of a given good. Suppose we

have two goods A and B. The absolute price of good A is the number of dollars necessary to purchase a unit of good A. The relative price of good A in terms of B is the amount of good B necessary to purchase a unit of good A.

[\[603\]](#)

Tim Harrison, ‘How we are scaling Cardano in 2022’,
iohk.io/en/blog/posts/2022/01/14/how-we-re-scaling-cardano-in-2022/

[\[604\]](#)

Cooked validators, [github.com/tweag/plutus-libs/tree/main/cooked-validators](https://github.com/tweag/plutus-libs/tree/main/cooked Validators)

[\[605\]](#)

Concurrency, the property of program, algorithm, or problem decomposition into order-independent or partially ordered units.

[\[606\]](#)

Writing a scalable app,
plutus.readthedocs.io/en/latest/plutus/howtos/writing-a-scalable-app.html

[\[607\]](#)

What is the order book pattern?
playground.plutus.iohkdev.io/doc/plutus/explanations/order-book-pattern.html

[\[608\]](#)

Plutus validator scripts, docs.cardano.org/plutus/Plutus-validator-scripts

[\[609\]](#)

Minimum-ada-value-requirement, docs.cardano.org/native-tokens/minimum-ada-value-requirement

[\[610\]](#)

Min-Ada-Value Calculation in Alonzo, github.com/input-output-hk/cardano-ledger-specs/blob/master/doc/explanations/min-utxo-alonzo.rst

[\[611\]](#)

Worked example, github.com/input-output-hk/cardano-documentation/blob/staging/content/10-plutus/06-Plutus-transactions.mdx

[\[612\]](#)

Plutus Pioneers Welcome & Intro., www.youtube.com/watch?v=X80uNXenWF4&list=PLK8ah7DzglhgK0bEyELK8EzbW0mn6xavC

[\[613\]](#)

Datums and redeemers, github.com/input-output-hk/cardano-documentation/blob/staging/content/10-plutus/07-datums-redeemers.mdx

[\[614\]](#)

Plutus transactions model, github.com/input-output-hk/Alonzo-testnet/blob/main/Alonzo-tutorials/Plutus_transactions_tutorial.md#transaction-to-lock-funds

[\[615\]](#)

Plutus HelloWorld, github.com/input-output-hk/Alonzo-testnet/blob/e27563ec0c0c3723376f4d12881cd003a7a7157f/resources/plutus-sources/plutus-helloworld/src/Cardano/PlutusExample>HelloWorld.hs#L47

[\[616\]](#)

EnglishAuction.hs, github.com/input-output-hk/plutus-pioneer-program/blob/024ebd367bf6c4003b482fb4c6db7d745ec85aa/code/week01/src/Week01/EnglishAuction.hs#L103

[\[617\]](#)

Cost model parameters,
plutus.readthedocs.io/en/latest/reference/cost-model-parameters.html

[618]

Plutus bibliography,
plutus.readthedocs.io/en/latest/reference/bibliography.html#id13

[619]

Surprise AMA 03/12/2019, youtu.be/f-rqaTLwWgs?t=1575

[620]

Redeemer validators, bitcoinmagazine.com/articles/thinking-transactions-1401650873

[621]

Cardano testnet, testnets.cardano.org/en/testnets/cardano/overview/

[622]

Peyton Jones, Kireev, ‘The Plutus Platform’,
hydra.iohk.io/build/12983030/download/1/plutus.pdf

[623]

A Formal Specification of the Cardano Ledger integrating Plutus Core, hydra.iohk.io/build/7172824/download/1/alonzo-changes.pdf

[624]

Plutus Tutorial,
plutus.readthedocs.io/en/latest/plutus/tutorials/index.html

[625]

PoolChess on Twitter, twitter.com/PoolChess

[626]

PoolChess PP Lecture notes, plutus-pioneer-program.readthedocs.io/en/latest/plutus_pioneer_program.html

[627]

Plutus: Writing reliable smart contracts, www.amazon.com/Plutus-Writing-reliable-smart-contracts-ebook/dp/B07V46LWTW/ref=sr_1_1, leanpub.com/plutus-smart-contracts

[\[628\]](#)

Plutus on the Cardano Forum,
forum.cardano.org/c/developers/cardano-plutus/148

[\[629\]](#)

IOG Tech Discord, discord.com/invite/w6TwW9bGA6

[\[630\]](#)

Learn You a Haskell, learnyouahaskell.com/introduction

[\[631\]](#)

Haskell and Crypto Mongolia, www.youtube.com/watch?v=ctfZ6DwFiPg&list=PLJ3w5xyG4JWmBVligNBytJhvSSfZZzfTm&index=4

[\[632\]](#)

Register for the Plutus Pioneer Program,
testnets.cardano.org/en/plutus-pioneer-program/

[\[633\]](#)

For Plutus Pioneer Program graduates,
www.reddit.com/r/CardanoDevelopers/comments/pak32y/for_plutus_pioneer_program_graduates/

[\[634\]](#)

March 2021 Cardano 360 Episode, youtu.be/ULBLgPgxtN8?t=3731

[\[635\]](#)

Examples of type-level programming,
stackoverflow.com/questions/24481113/what-are-some-examples-of-type-level-programming

[636]

Marlowe Pioneer Program, pioneers.marlowe-finance.io/

[637]

Niamh Aherne, ‘Learn how to create low-code, low-cost financial smart contracts in the Marlowe Pioneer Program’,
iohk.io/en/blog/posts/2022/05/11/learn-how-to-create-low-code-low-cost-financial-smart-contracts-in-the-marlowe-pioneers-program/

[638]

IOG Workshops, iogmeetups2022.co.uk/

[639]

European Business University, Luxembourg, ebu.lu/

[640]

Cardano Foundation and University of Zurich Partner for Academic Blockchain Research, cryptopotato.com/cardano-foundation-and-university-of-zurich-partner-for-academic-blockchain-research/

[641]

Plutus e-book, www.amazon.co.uk/Plutus-Writing-reliable-smart-contracts-ebook/dp/B07V46LWTW

[642]

Moritz Angermann, iohk.io/team/moritz-angermann/

[643]

John Woods, ‘Slow and steady wins the race: network evolution for network growth’, iohk.io/en/blog/posts/2021/11/22/slow-and-steady-wins-the-race-network-evolution-for-network-growth/

[644]

Nix is a cross-platform package manager that utilizes a purely functional deployment model. Software is installed into unique directories generated through cryptographic hashes. It is also the

name of the tool's programming language, specifically for software configuration and deployment.

[645]

Cardano's 2022 vision: Hoskinson may finally have a release date for 'Mamba', ambcrypto.com/cardanos-2022-vision-hoskinson-may-finally-have-a-release-date-for-mamba/

[646]

Cardano Founder Charles Hoskinson Lays Out 2022 Plans, www.coindesk.com/tech/2021/12/27/cardano-founder-charles-hoskinson-lays-out-2022-plans/

[647]

Cardano Stack Exchange, cardano.stackexchange.com/

[648]

'What is Layer 0?',

cardano.stackexchange.com/questions/8244/what-is-layer-0

[649]

Stack Overflow is a question-and-answer site for professional and enthusiast programmers. It is a privately held website, the flagship site of the Stack Exchange Network, created in 2008 by Jeff Atwood and Joel Spolsky.

[650]

Cardano forum, forum.cardano.org/

[651]

Stack overflow moderators, stackoverflow.com/help/site-moderators

[652]

Stack overflow reputation points,

meta.stackexchange.com/questions/7237/how-does-reputation-work

[653]

Cardano's Project Becomes The World's Largest DAO,
cryptonews.net/editorial/news/cardano-s-project-becomes-the-world-s-largest-dao

[654]

A **wrapper function** is a subroutine in a software library or a computer program whose main purpose is to call a second subroutine or a system call with little or no additional computation. Wrapper functions are used to make writing computer programs easier by abstracting away the details of a subroutine's underlying implementation.

[655]

Learn about Plutus, docs.cardano.org/plutus/learn-about-plutus

[656]

Plutus tutorials, [plutus-](https://plutus.readthedocs.io/en/latest/plutus/tutorials/index.html)
[apps.readthedocs.io/en/latest/plutus/tutorials/index.html](https://plutus.readthedocs.io/en/latest/plutus/tutorials/index.html)

[657]

Plutus explainers, [plutus-](https://plutus.readthedocs.io/en/latest/plutus/explanations/index.html)
[apps.readthedocs.io/en/latest/plutus/explanations/index.html](https://plutus.readthedocs.io/en/latest/plutus/explanations/index.html)

[658]

Plutus scripts overview, [github.com/input-output-hk/cardano-](https://github.com/input-output-hk/cardano-node/blob/master/scripts/README.md#scripts-overview)
[node/blob/master/scripts/README.md#scripts-overview](https://github.com/input-output-hk/cardano-node/blob/master/scripts/README.md#scripts-overview)

[659]

Smart Contracts Best Practice, [docs.cardano.org/plutus/sc-best-](https://docs.cardano.org/plutus/sc-best-practices)
[practices](https://docs.cardano.org/plutus/sc-best-practices)

[660]

Cardano Founder Explains What Users Should Expect From the Upcoming Vasil Hard Fork, [cryptopotato.com/cardano-founder-](https://cryptopotato.com/cardano-founder-explains-what-users-should-expect-from-the-upcoming-vasil-hard-fork)
[explains-what-users-should-expect-from-the-upcoming-vasil-hard-fork](https://cryptopotato.com/cardano-founder-explains-what-users-should-expect-from-the-upcoming-vasil-hard-fork)

[661]

Mid-Month Development Update - April 2022,
www.youtube.com/watch?v=B0tojqvMgB0

[662]

Plutus IR is an intermediate language that compiles to Plutus Core. Plutus IR is not used by users, but rather as a compilation target on the way to Plutus Core. However, it is significantly more human-readable than Plutus Core, so should be preferred in cases where humans may want to inspect the program.

[663]

An **Intermediate representation (IR)** is the data structure or code used internally by a compiler or virtual machine to represent source code. An IR is designed to be conducive for further processing, such as optimization and translation.

[664]

In functional programming, a **monad** is a design pattern that allows structuring programs generically while automating away boilerplate code needed by the program logic. Monads achieve this by providing their own data type, which represents a specific form of computation, along with one procedure to wrap values of any basic type within the monad (yielding a monadic value) and another to compose functions that output monadic values (called monadic functions).

[665]

In cryptography, the **Elliptic Curve Digital Signature Algorithm (ECDSA)** offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography.

[666]

CIP (Cardano improvement proposals), cips.cardano.org/

[667] Secp256k1, en.bitcoin.it/wiki/Secp256k1

[668] Some Brief Comments on Vasil, www.youtube.com/watch?v=Na09S56FwuY

[669]

Pairing-based cryptography has been used to construct identity-based encryption (IBE), which allows a sender to encrypt a message without needing a receiver's public key to have been certified and /distributed in advance. IBE uses some form of a person's (or entity's) identification to generate a public key.

[670]

Homomorphic encryption is a form of encryption that permits users to perform computations on its encrypted data without first decrypting it.

[671]

Vasil Upgrade - The State of Play, youtu.be/fxWfdd2MJOc

[672]

Cardano Vasil hard fork changes explained,
www.youtube.com/watch?v=Tsp9F23dBiM

[673]

Kerber, Kiayias, Kohlweiss (2021) 'Kachina - Foundations of Private Smart Contracts', eprint.iacr.org/2020/543.pdf

[674]

Charles Hoskinson Kachina tweet,
twitter.com/iohk_charles/status/1261328840023961602?lang=en

[675]

Manuel Chakravarty, iohk.io/en/team/manuel-chakravarty

[676]

Zahnentferner (2018) 'Chimeric Ledgers: Translating and Unifying UTXO-based and Account-based Cryptocurrencies',
eprint.iacr.org/2018/262.pdf

[\[677\]](#)

Agda is a dependently typed functional programming language. A dependent type is a type whose definition depends on a value.

[\[678\]](#)

JS arrow function, www.w3schools.com/js/js_arrow_function.asp

[\[679\]](#)

Agile is an iterative approach to project management and software development that helps teams deliver value to their customers faster and with fewer headaches.

[\[680\]](#)

LIVE with Cardano's Charles Hoskinson,
youtu.be/x6TZSBmDWMw?t=5107

[\[681\]](#)

Niamh Ahern, 'The new Mantis: Bringing security and stability to the Ethereum Classic ecosystem', iohk.io/en/blog/posts/2020/12/09/the-new-mantis-bringing-security-and-stability-to-the-ethereum-classic-ecosystem-1/

[\[682\]](#)

Luite Stegeman, 'Looking to the future of Haskell and JavaScript for Plutus', iohk.io/en/blog/posts/2020/06/04/looking-to-the-future-of-haskell-and-javascript-for-plutus/

[\[683\]](#)

Sylvain Henry, 'Improving Haskell's big numbers support', iohk.io/en/blog/posts/2020/07/28/improving-haskells-big-numbers-support/

[\[684\]](#)

JSCert: Formalization of the JavaScript programming language, wp.doc.ic.ac.uk/fswp/project/jscert-formalization-of-the-javascript-programming-language/

[\[685\]](#)

Quickcheck, hackage.haskell.org/package/QuickCheck

[\[686\]](#)

TLA⁺ is a formal specification language developed by Leslie Lamport. It is used for designing, modeling, documentation, and verification of programs, especially concurrent systems and distributed systems

[\[687\]](#)

Marlowe papers, play.marlowe-finance.io/doc/marlowe/tutorials/introducing-marlowe.html#research-based

[\[688\]](#)

In finance, a **contract for difference (CFD)** is a contract between two parties, typically described as ‘buyer’ and ‘seller’, stipulating that the seller will pay to the buyer the difference between the current value of an asset and its value at contract time (if the difference is negative, then the buyer pays instead to the seller).

[\[689\]](#)

In computability theory, the **halting problem** is the problem of determining, from a description of an arbitrary computer program and an input, whether the program will finish running, or continue to run forever.

[\[690\]](#)

Recursion occurs when something is defined in terms of itself or of its type. Recursion is used in a variety of disciplines ranging from linguistics to logic. The most common application of recursion is in mathematics and computer science, where a function being defined is applied within its own definition. While this apparently defines an infinite number of instances (function values), it is often done in such a way that no infinite loop can occur.

[\[691\]](#)

ACTUS (Algorithmic Contract Types Unified Standards) Contract Types are defined based on the underlying contractual algorithm patterns that respectively cover different classes of financial products that each Contract Type pattern is able to express.

[\[692\]](#)

Static analysis, static projection, or static scoring is a simplified analysis wherein the effect of an immediate change to a system is calculated without regard to the longer-term response of the system to that change.

[\[693\]](#)

Writing Marlowe with Blockly, docs.cardano.org/marlowe/writing-marlowe-with-blockly

[\[694\]](#)

Marlowe: Using JS Editor, docs.cardano.org/marlowe/using-javascript-editor

[\[695\]](#)

Using the Haskell editor, docs.cardano.org/marlowe/using-the-haskell-editor

[\[696\]](#)

Static analysis is a simplified analysis wherein the effect of an immediate change to a system is calculated without regard to the longer-term response of the system to that change. If the short-term effect is then extrapolated to the long term, such extrapolation is inappropriate.

[\[697\]](#)

Sample escrow contract, github.com/cardano-foundation/docs-cardano-org/blob/main/marlowe/marlowe-lang-guide.md

[\[698\]](#)

Marlowe tutorials,
alpha.marlowe.iohkdev.io/doc/marlowe/tutorials/index.html
[699]

GitHub Gist allows developers to instantly share code, notes, and snippets. Every gist is a Git repository, which means that it can be forked and cloned.

[700]

MIT AppInventor, appinventor.mit.edu/
[701]

Greenelight Apps,
www.androidblip.com/dev/greenelight_a55fdd36512db0ebd6faad85f5a7e76687f8b28592819d76d5f18ec86f3b1cde.html
[702]

Marlowe embedded in Javascript, play.marlowefinance.io/doc/marlowe/tutorials/javascript-embedding.html
[703]

Marlowe Run, run.marlowefinance.io/
[704]

Marlowe Website, marlowefinance.io/
[705]

Satisfiability modulo theories (SMT) is the problem of determining whether a mathematical formula is satisfiable. It generalizes the Boolean satisfiability problem (SAT) to more complex formulas involving real numbers, integers, and/or various data structures such as lists, arrays, bit vectors, and strings. The name is derived from the fact that these expressions are interpreted within ('modulo') a certain formal theory in first-order logic with equality (often disallowing quantifiers). **SMT solvers** are tools which aim to solve the SMT problem for a practical subset of inputs.

[706]

ACTUS taxonomy, www.actusfrf.org/taxonomy

[707]

ACTUS technical spec, www.actusfrf.org/techspecs

[708]

Bitcoin Script is a simple, stack-based programming language that enables the processing of transactions on the Bitcoin blockchain

[709]

Binance hit by crypto withdrawal suspension,
www.fnlondon.com/articles/binance-hit-by-crypto-withdrawal-suspension-20211101

[710]

Binance suspends SEPA transfers for irish investors,
www.businesspost.ie/investing/binance-suspends-sepa-transfers-for-irish-investors-1ac95e7c

[711]

Cryptocurrency Exchange Fees Are A Mess. Will They Ever Improve?,
www.forbes.com/sites/kenrapoza/2021/10/17/cryptocurrency-exchange-fees-are-a-mess-when-will-they-ever-improve/?sh=477a74be2f4c

[712]

Marlowe Playground Alpha, alpha.marlowe.iohkdev.io/#/

[713]

Kraken feed, api.cryptowat.ch/markets/kraken

[714]

Demo: Cardano's Marlowe Run, www.youtube.com/watch?v=sfLlOlEhSGU

[715]

Marlowe embedded in Haskell, play.marlowe-finance.io/doc/marlowe/tutorials/embedded-marlowe.html

[716]

The **Portable Operating System Interface (POSIX)** is a family of standards specified by the IEEE Computer Society for maintaining compatibility between operating systems. POSIX defines the application programming interface (API), along with command line shells and utility interfaces, for software compatibility with variants of Unix and other operating systems.

[717]

Marlowe CLI Tool, github.com/input-output-hk/marlowe-cardano/blob/cli-blog-april2022/marlowe-cli/ReadMe.md

[718]

Marlowe explainer, docs.cardano.org/marlowe/learn-about-marlowe

[719]

Marlowe tutorials, play.marlowe-finance.io/doc/marlowe/tutorials/index.html

[720]

Prof Simon Thompson on YouTube,

www.youtube.com/user/simonjohnthompson/videos

[721] Marlowe Pioneers 1st Cohort,

https://www.youtube.com/channel/UCX9j__vYOJu00iqBrCzecVw/pla_ylists?view=50&sort=dd&shelf_id=2

[722]

Marlowe docs, play.marlowe-

[finance.io/doc/marlowe/tutorials/introducing-marlowe.html](https://play.marlowe-finance.io/doc/marlowe/tutorials/introducing-marlowe.html)

[723]

Marlowe Pioneer program, pioneers.marlowe-finance.io/

[\[724\]](#)

Potential problems with contracts, play.marlowe-finance.io/doc/marlowe/tutorials/potential-problems-with-contracts.html

[\[725\]](#)

'I may not agree with you but...': Manmohan Singh, Voltaire or someone else – who actually said it?,
www.freepressjournal.in/india/i-may-not-agree-with-you-but-manmohan-singh-voltaire-or-someone-else-who-actually-said-it

[\[726\]](#)

Dash is an open source cryptocurrency and is a form of decentralized autonomous organization (DAO) run by a subset of users, called 'masternodes'. It is an altcoin that was forked from the Bitcoin protocol. The currency permits fast transactions that can be untraceable.

[\[727\]](#)

Tezos (ticker: XTZ) is a decentralized blockchain founded by Arthur Breitman and Kathleen Breitman. The Breitmans also founded Dynamic Ledger Solutions (DLS), a company primarily focused on developing Tezos technology and owns the Tezos Intellectual property. The currency was launched in an initial coin offering (ICO) on July 1, 2017.

[\[728\]](#)

Crowdsales are a popular use for Ethereum; they let you allocate tokens to network participants in various ways, mostly in exchange for Ether. They come in a variety of shapes and flavors.

[\[729\]](#)

Segregated Witness, or SegWit, is the name used for an implemented soft fork change in the transaction format of bitcoin.

[\[730\]](#)

The Tale Of SegWit: Controversy, Civil War & Adoption,
blog.btse.com/segwit/

[731]

Understanding the DAO attack,
www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/

[732]

Ethereum fall out, fortune.com/2016/09/04/ethereum-fall-out/

[733]

Incentive: a method of encouraging members to participate in the network by providing them with a return proportionate to their efforts. By promoting persistent, active, and robust engagement, incentives strive to maintain equality and fairness in a dispersed network of participants. The incentives necessary in Cardano's incentives model are calculated using game theory.

[734]

CIP repo, github.com/cardano-foundation/CIPs

[735]

Pull requests are a feature specific to GitHub. They provide a simple, web-based way to submit your work (often called "patches") to a project. It's called a pull request because you're asking the project to pull changes from your fork.

[736]

CIP biweekly meetings, github.com/cardano-foundation/CIPs/tree/master/BiweeklyMeetings

[737]

Cardano Forums CIP section, forum.cardano.org/c/english/cips/122

[738]

Cardano Ambassadors Program, www.cardano.org/ambassadors/

[739]

Cardano IdeaScale, cardano.ideascale.com/

[740]

Voltaire Roadmap, roadmap.cardano.org/en/voltaire/

[741]

Project Catalyst: implementing Cardano's Governance model with Dr Dor Garbash, www.conferencecast.tv/talk-44699-project-catalyst-implementing-cardanos-governance-model-with-dr-dor-garbash#.talkPage-header

[742]

A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence?, eprint.iacr.org/2018/435.pdf

[743]

Zhang, Oliynykov, Balogun, 'A Treasury System for Cryptocurrencies:

'Enabling Better Collaborative Intelligence', www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02A-2_Zhang_paper.pdf

[744]

Liquid democracy is a form of delegative democracy where an electorate engages in collective decision-making through direct participation and dynamic representation. This democratic system leverages parts of both direct and representative democracy.

[745]

Cardano Network Parameters with Dr. Michael Liesenfeld | Cardano Live #54, www.youtube.com/watch?v=eAs_L68RO-c

[746]

The ETC Cooperative Withdraws Support For The ETC Treasury, medium.com/etccooperative/the-etc-cooperative-withdraws-support-

for-the-etc-treasury-c3f8772fff71

[747]

Tim Richmond, 'Project Catalyst - A virtuous cycle of Cardano ecosystem development', iohk.io/en/blog/posts/2022/05/10/project-catalyst-a-virtuous-cycle-of-cardano-ecosystem-development-investing-in-great-ideas-to-make-positive-real-world-changes/

[748]

Project Catalyst: implementing Cardano's Governance model with Dr Dor Garbash, www.youtube.com/watch?v=Wcl-ZvyeRd8

[749]

Catalyst Telegram Channel, t.me/cardanocatalyst

[750] Jormungandr Node, github.com/input-output-hk/jormungandr/blob/master/CHANGELOG.md

[751]

Project Catalyst Fund6 weekly town hall and Q&A #13 November 2021, www.youtube.com/watch?v=x8134D_lp9o&t=418s

[752]

Dr Dor Garbash, 'Project Catalyst; introducing our first public fund for Cardano community innovation', iohk.io/en/blog/posts/2020/09/16/project-catalyst-introducing-our-first-public-fund-for-cardano-community-innovation/

[753]

Djed update, medium.com/cotinetwork/djed-development-update-421cea2c610b

[754]

Cardano | The First Domino, www.youtube.com/watch?v=W7gGO058rtU

[755]

Crypto Startup Solana Raises \$314 Million to Develop Faster Blockchain, www.wsj.com/articles/crypto-startup-solana-raises-314-million-to-develop-faster-blockchain-11623240001

[[756](#)]

Entrevista CEO IOG Charles Hoskinson e Maria Carmo #Cardano #ada Delege na CARDs ou @cardanistas, youtu.be/rHu6oLTZ7kI?t=3061

[[757](#)]

DARPA: The Defense Advanced Research Projects Agency is a research and development agency of the United States Department of Defense responsible for the development of emerging technologies for use by the military

[[758](#)]

Waves, everipedia.org/wiki/lang_en/waves-cryptocurrency

[[759](#)]

John Greene, ‘DID as a bridge to Microsoft’, cardano.ideascale.com/c/idea/368523

[[760](#)]

Our million-dollar baby: Project Catalyst, iohk.io/en/blog/posts/2021/02/12/our-million-dollar-baby-project-catalyst/

[[761](#)]

Cardano Hotel Barcelona, hotelginebra.com.es/cardano-hotel/

[[762](#)]

Daniel Friedman, iohk.io/en/team/daniel-friedman

[[763](#)]

Weekly Update & AMA - April 22, 2022, www.youtube.com/watch?v=rPBZwEPk5Q8

[764]

Catalyst Natives application, forms.gle/BA8LmtrAWWmHHcY59

[765]

Fund 7 initiatives,

drive.google.com/file/d/193GZuIHuk0zhpTrMiLhcNC4OeEMoRyla/view

[766]

Project Catalyst - Funded Projects Reporting (public MVP),

docs.google.com/spreadsheets/d/1bfnWFa94Y7Zj0G7dtpo9W1nAYGovJbswipxiHT4UE3g/edit#gid=416498551

[767]

'FT x Cardano Blockchain Challenge',

www.seedstars.com/community/entrepreneurs/programs/ft-cardano-blockchain-challenge/

[768]

IOHK youtube channel, www.youtube.com/c/Iohklo

[769]

Fund 8 results, drive.google.com/file/d/1s3jCE7pmoUujy3ASMia-UhFI2KLi_hnf/view

[770]

CIP Editor funded,

twitter.com/SebastienGllmt/status/1525139808926191618

[771]

Catalyst Tracker, bit.ly/FundedProjectsReporting

[772]

Post Conference recap, thoughts and an AMA 04/21/2019,

youtu.be/pBXZVrBQ6U8?t=5003

[773]

Twitter space,
[twitter.com/IOHK_Charles/status/1515872352395055109?
s=20&t=lQdnrPHfNkbLDWjCPfT9aQ](https://twitter.com/IOHK_Charles/status/1515872352395055109?s=20&t=lQdnrPHfNkbLDWjCPfT9aQ)

[[774](#)]

Fitzi, Wang, Kannan, Kiayias, Leonardos, Viswanath, Wang (2022)
'Minotaur: Multi-Resource Blockchain Consensus',
eprint.iacr.org/2022/104.pdf

[[775](#)]

Project Catalyst Fund8 launch - Town Hall #1 February 2022,
www.youtube.com/watch?v=rNZJvzjgduM

[[776](#)]

Catalyst dRep applications, bit.ly/3rSyHvP

[[777](#)]

Project Catalyst FAQ, cardanocatalyst.st/en/faq/

[[778](#)]

Twitter space 'Sunday Chat with Charles',
[twitter.com/IOHK_Charles/status/1515872352395055109?
s=20&t=jbwJYMXSF1zhKUjmNxmEBg](https://twitter.com/IOHK_Charles/status/1515872352395055109?s=20&t=jbwJYMXSF1zhKUjmNxmEBg)

[[779](#)]

Re: Privacy on Cardano, should be decided by the governed '4/20 Hangout with Charles' twitter.com/i/spaces/1IDGLLABeBkGm

[[780](#)]

Live With Charles Hoskinson of Cardano ADA 11/24/20,
www.youtube.com/watch?v=z3s6olBfbfA

[[781](#)]

Ethereum 2.0, everipedia.org/wiki/lang_en/ethereum-20

[[782](#)]

Polkadot bonding, slashing, etc, medium.com/coinmonks/hello-polkadot-5-minting-bonding-staking-slashing-3c1a33c5a005

[\[783\]](#)

Ethereum Casper explained,
academy.binance.com/en/articles/ethereum-casper-explained

[\[784\]](#)

Casper is the implementation that will eventually convert Ethereum into a proof of stake (PoS) blockchain (also known as Ethereum 2.0).

[\[785\]](#)

Eurocript, eurocrypt.iacr.org/2020/program.php

[\[786\]](#)

Crypto, crypto.iacr.org/2020/

[\[787\]](#)

Casper, arxiv.org/pdf/1710.09437.pdf

[\[788\]](#)

Casper paper critique, www.scs.stanford.edu/17au-cs244b/labs/projects/moindrot_bournhonesque.pdf

[\[789\]](#)

Vitalik Buterin Discusses On-chain Governance,
www.youtube.com/watch?v=w-CH_5il9aU

[\[790\]](#)

The **Lightning Network** is a Layer 2 payment protocol that operates on top of a blockchain. It theoretically enables fast transactions between participating nodes and has been touted as a solution to the bitcoin scalability problem.

[\[791\]](#)

Cardashift is a community-run launchpad that raises funds, builds and accelerates startups that are solving social and environmental

issues.

[\[792\]](#)

Fernando Sanchez, 'Introducing Catalyst Natives - How any business can leverage the Cardano innovation engine',
iohk.io/en/blog/posts/2021/11/10/introducing-catalyst-natives-how-any-business-can-leverage-the-cardano-innovation-engine

[\[793\]](#)

The 3 reasons why we choose Cardano to maximize our impact,
cardashift.medium.com/the-3-reasons-why-we-choose-cardano-to-maximize-our-impact-28b2e914e894

[\[794\]](#)

Fund9 launch guide,
drive.google.com/file/d/1kJ8F6doXUIJQRiA5pmSMxXc9feVfF21y/view

w

[\[795\]](#)

Cardano became the most developed crypto project on GitHub in 2021, cointelegraph.com/news/cardano-became-the-most-developed-crypto-on-github-in-2021-santiment

[\[796\]](#)

Tim Harrison, 'How we are scaling Cardano in 2022',
iohk.io/en/blog/posts/2022/01/14/how-we-re-scaling-cardano-in-2022/

[\[797\]](#)

April 20, 2022, '4/20 Hangout with Charles' Twitter space, Re: The slow way is fast way, twitter.com/i/spaces/1IDGLLABeBkGm

[\[798\]](#)

Number of Cardano Addresses Reaches 3.5 Million as ADA Surges by 5%, u.today/number-of-cardano-addresses-reaches-35-million-as-ada-surges-by-5

[\[799\]](#)

Performance engineering: Lies, damned lies and (TPS)benchmarks,
www.youtube.com/watch?v=gpSnyCn2s9U

[800]

Cardano Blockchain Congestion Causing Issues on New NFT Marketplace, finance.yahoo.com/news/cardano-blockchain-congestion-time-high-204500682.html

[801]

Surprise AMA 01/10/2021, youtu.be/iLq6mRk2dyg?t=1057

[802]

The ability of maintaining functionality when portions of a system break down is referred to as **graceful degradation**.

[803]

Coutts, Davies, Szamotulski, Thompson (2020) 'Introduction to the design of the Data Diffusion and Networking for Cardano Shelley', hydra.iohk.io/build/7249613/download/1/network-design.pdf

[804] **Block header:** The portion of a block that contains information about the block itself (block metadata), typically including a timestamp, a hash representation of the block data, the hash of the previous block's header, and a cryptographic nonce (if needed).

[805]

RAM (random-access memory) is a form of computer memory that can be read and changed in any order, typically used to store working data and machine code. A random-access memory device allows data items to be read or written in almost the same amount of time irrespective of the physical location of data inside the memory.

[806]

CIP31, cips.cardano.org/cips/cip31/

[807]

Ergo data inputs, docs.ergoplatform.com/dev/scs/data-inputs/
[808]

CIP32, cips.cardano.org/cips/cip32/
[809]

CIP33, cips.cardano.org/cips/cip33/
[810]

Resident set size (RSS) is the portion of memory occupied by a process that is held in main memory (RAM).

[811]

Cardano node release notes, github.com/input-output-hk/cardano-node/releases

[812]

Live stake: the entire amount of stake held by a stake pool. It combines the pool operator's stake and any stakes that have been delegated to the pool by other ada holders. It may be expressed as a total quantity of ada (e.g. 2M ada) or as a percentage of the network's total ada supply (e.g. 2%).

[813]

row-major order and **column-major** order are methods for storing multidimensional arrays in linear storage such as random-access memory. The difference between the orders lies in which elements of an array are contiguous in memory.

[814]

Milkomeda, dcspark.gitbook.io/milkomeda/
[815]

Mamba sidechain, in 'some updates', www.youtube.com/watch?v=H9wAyW_EcDA&t=485s

[816]

EVM Alpha sidechain, www.linkedin.com/posts/input-output-global_evm-sidechain-activity-6941445505616908288-ysBW?utm_source=linkedin_share&utm_medium=member_desktop_web
[\[817\]](#)

ADA is Exploding with Utility TODAY | ETH TOKENS ON CARDANO | Milkomeda Full Guide, www.youtube.com/watch?v=wbl-iMLv5aE
[\[818\]](#)

Temujin Louie, 'Guest blog: collaborating on Cardano interoperability', iog.io/en/blog/posts/2022/04/27/guest-blog-collaborating-on-cardano-interoperability/
[\[819\]](#)

April 2022 Cardano 360 Sidechains segment, youtu.be/b4x5Oly4shU?t=1231

[\[820\]](#)

June 2022 Cardano360 Sidechains clip, youtu.be/ShBFTaD8nss?t=381

[\[821\]](#)

Isomorphism: corresponding or similar in form and relations.
[\[822\]](#)

TPS on crypto twitter,
twitter.com/bitcoinissaving/status/1437240100807749633
[\[823\]](#)

MMT Chakravarty, S Coretti, M Fitzi, P Gazi, P Kant, A Kiayias, and A Russell (2020) 'Hydra: fast isomorphic state channels'(Section 7 – Simulations), eprint.iacr.org/2020/299.pdf
[\[824\]](#)

Cardano Summit Hydra demo, summit.cardano.org/sessions/hydra-the-multi-headed-scalability-protocol

[825]

Hydra POC, github.com/input-output-hk/hydra-poc

[826]

Sebastian Nagel, ‘Hydra – Cardano’s solution for ultimate Layer 2 scalability’, iohk.io/en/blog/posts/2021/09/17/hydra-cardano-solution-for-ultimate-scalability/

[827]

‘There is an obsession in blockchain designs with transactions per second’, twitter.com/muneeb/status/1258003142450569217

[828]

Cardanians Hydra blog, cardanians-io.medium.com/hydra-cardano-scalability-solution-36b05ddc91cf

[829]

Jourenko, Larangeira, TanakalInterhead Hydra Two Heads are Better than One, eprint.iacr.org/2021/1188

[830]

Prof Aggelos Kiayias, ‘Enter the Hydra: scaling distributed ledgers, the evidence-based way,’ iohk.io/en/blog/posts/2020/03/26/enter-the-hydra-scaling-distributed-ledgers-the-evidence-based-way/

[831]

Hydra on github, github.com/input-output-hk/hydra-poc

[832]

Hydra roadmap, github.com/orgs/input-output-hk/projects/21

[833]

Surprise AMA 04/13/2022, youtu.be/AejphsMjkPc?t=1294

[834]

Wust, et al, (2019), 'ACE: Asynchronous and Concurrent Execution of Complex Smart Contracts', eprint.iacr.org/2019/835.pdf

[835]

Mid-Month Development Update - January 2022,
youtu.be/dt48RqBEZcM?t=592

[836]

Produced blocks: the total number of blocks created by a stake pool in the current epoch. Stake pools are paid in ada for every block they create.

[837]

A **logarithmic scale** is a nonlinear scale used for a large range of positive multiples of some quantity. Common uses include earthquake strength, sound loudness, light intensity, and pH of solutions.

[838]

Daedalus wallet, docs.cardano.org/cardano-components/daedalus-wallet

[839]

Galois, galois.com/research-development/

[840]

Bulletproofs are short non-interactive zero-knowledge proofs that require no trusted setup. A bulletproof can be used to convince a verifier that an encrypted plaintext is well formed. For example, prove that an encrypted number is in a given range, without revealing anything else about the number.

[841]

'Cardano360 May 2022' www.youtube.com/watch?v=Ar_8Lo0nV1s

[842]

Chaidos, Kiayias (2021), 'Mithril: Stake-based Threshold Multisignatures', eprint.iacr.org/2021/916.pdf

[843]

Cardano Summit Mithril talk, summit.cardano.org/sessions/mithril-linking-together-a-stronger-and-lighter-blockchain

[844]

'Sunday chat with Charles',

twitter.com/IOHK_Charles/status/1515872352395055109? s=20&t=UhVSJD7rG0nfH6Yxux4QOg

[845]

April 20, 2022, '4/20 Hangout with Charles' Twitter space, twitter.com/i/spaces/1IDGLLABeBkGm

[846]

Mina protocol, minaprotoocol.com/get-started

[847]

A **yottabyte** is a unit of information equal to one septillion (10^{24}) or, strictly, 2^{80} bytes.

[848]

Plumo, docs.celo.org/celo-codebase/protocol/plumo

[849]

Gabizon, Williamson, Ciobotaru (2022), 'PlonK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge', eprint.iacr.org/2019/953.pdf

[850]

Maller, Bowe, Kohlweiss, Meiklejohn (2019), 'Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updateable Structured Reference Strings', eprint.iacr.org/2019/099.pdf

[851]

Addressing Blockchain's Hidden Trade-Off,
www.youtube.com/watch?v=FSByg_sdjaM
[852]

Lace: a lightwallet platform, www.youtube.com/watch?v=Q4Z83TSdEfg
[853]

Interview with Charles Hoskinson,
twitter.com/i/broadcasts/1eaKbNQkpBqKX
[854]

Re: Proxy Keys. Surprise AMA 11/21/2021, youtu.be/NJcVEJ1a6eg?t=2114
[855]

Prof Aggelos Kiayias, 'Stablefees and the Decentralized Reserve System', iohk.io/en/blog/posts/2021/06/10/stablefees-and-the-decentralized-reserve-system/
[856]

EIP 1559, www.cnbc.com/2021/08/04/what-to-know-about-the-ethereum-london-hard-fork-eip-1559-upgrade.html
[857]

In the context of data storage, **serialization** is the process of translating data structures or object state into a format that can be stored (for example, in a file or memory buffer) or transmitted (for example, across a network) and reconstructed later (possibly on a different computer). When the resulting series of bits is reread according to the serialization format, it can be used to create a semantically identical clone of the original object.
[858]

JavaScript Object Notation (JSON) is an open-standard file format that uses human-readable text to transmit data objects

consisting of attribute value pairs and array data types (or any other serializable value).

[\[859\]](#)

In Memory of Philip Chang, www.youtube.com/watch?v=BUJ0LA0dcqs&t=2346s

[\[860\]](#)

April 2022 Cardano 360 episode, youtu.be/b4x5Oly4shU?t=40

[\[861\]](#)

Ouroboros Family (Input Endorsers), youtu.be/PF1SW7e137A?t=1760

[\[862\]](#)

Prism: Scaling Bitcoin by 10,000x, arxiv.org/abs/1909.11261

[\[863\]](#)

Presentation, Prism: Scaling Bitcoin, www.youtube.com/watch?v=gTJyDtuWvUQ

[\[864\]](#)

Advances in Ouroboros: Scaling for Future Growth,
www.youtube.com/watch?v=xKv94MwSNBw

[\[865\]](#)

The **longest chain** is what individual nodes accept as the valid version of the blockchain. The rule that nodes adopt the longest chain of blocks allows every node on the network to agree on what the blockchain looks like, and therefore agree on the same transaction history. The Longest Chain Rule ensures that the network will recognise the ‘chain with most work’ as the main chain. The chain with the most work is typically (not always) the longest of the forks.

[\[866\]](#)

Proof-of-Stake Longest Chain Protocols: Security vs Predictability,
tselab.stanford.edu/downloads/PoS_LC_SBC2020.pdf
[867]

Gaži, Kiayias, Russell (2020), 'Tight Consistency Bounds for Bitcoin',
eprint.iacr.org/2020/661.pdf
[868]

Input Endorsers on stack exchange,
cardano.stackexchange.com/questions/4626/what-are-input-endorsers-and-how-do-they-make-cardano-more-scalable
[869]

In telecommunication and radio communication, **spread-spectrum techniques** are methods by which a signal generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth.

[870]

Surprise AMA 04/13/2022, www.youtube.com/watch?v=AejphsMjkPc&t=213s
[871]

April 20, 2022, '4/20 Hangout with Charles' Twitter space,
twitter.com/i/spaces/1IDGLLABeBkGm
[872]

Update from Washington, www.youtube.com/watch?v=gHOO_fP75aM
[873]

Let's Talk Roadmap and Governance, www.youtube.com/watch?v=MwP-omMwd3A
[874]

Latest Cardano Component Releases,
docs.cardano.org/tools/release-notes

[875]

CardanoDocs, docs.cardano.org/

[876]

Developer Portal docs, developers.cardano.org/docs/get-started/cardano-components/

[877]

Cardano Node, github.com/input-output-hk/cardano-node

[878]

Cardano Node CLI, github.com/input-output-hk/cardano-node/blob/master/doc/reference/cardano-node-cli-reference.md

[879]

Cardano Wallet, github.com/input-output-hk/cardano-wallet

[880]

Adrestia, input-output-hk.github.io/adrestia/

[881]

REST API, github.com/input-output-hk/cardano-rest

[882]

cardano-addresses, github.com/input-output-hk/cardano-addresses#overview

[883]

Ledger specs, github.com/input-output-hk/cardano-ledger#cardano-ledger

[884]

bech32 command-line, github.com/input-output-hk/bech32#bech32-command-line

[885]

Inter-process communication (IPC) refers specifically to the mechanisms an operating system provides to allow the processes to manage shared data. Typically, applications can use IPC, categorized as clients and servers, where the client requests data and the server responds to client requests. Many applications are both clients and servers, as commonly seen in distributed computing. Methods for doing IPC are divided into categories which vary based on software requirements, such as performance and modularity requirements, and system circumstances, such as network bandwidth and latency.

[\[886\]](#)

Block Header, www.investopedia.com/terms/b/block-header-cryptocurrency.asp.

[\[887\]](#)

CardanoDocs Networking Protocol, docs.cardano.org/explore-cardano/cardano-network/networking-protocol

[\[888\]](#)

CardanoDocs github, github.com/input-output-hk/cardano-documentation/blob/staging/content/02-getting-started/02-use-cli.mdx

[\[889\]](#)

The **Hypertext Transfer Protocol (HTTP)** is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access.

[\[890\]](#)

Olga Hryniuk, ‘Mithril a stronger and lighter blockchain for better efficiency’, iohk.io/en/blog/posts/2021/10/29/mithril-a-stronger-and-lighter-blockchain-for-better-efficiency/

[\[891\]](#)

Cardano Keys, docs.cardano.org/core-concepts/cardano-keys

[[892](#)]

With Cardano Approaching \$3, Charles Hoskinson Issues Scam Warning for Holders, u.today/with-cardano-approaching-3-charles-hoskinson-issues-scam-warning-for-holders

[[893](#)]

IOG's dedicated helpdesk page, iohk.zendesk.com/hc/en-us/categories/360000877653-Daedalus-Mainnet

[[894](#)]

Cardano GraphQL, github.com/input-output-hk/cardano-graphql

[[895](#)]

Middleware is computer software that provides services to software applications beyond those available from the operating system. It can be described as ‘software glue’. Middleware makes it easier for software developers to implement communication and input/output, so they can focus on the specific purpose of their application. It gained popularity in the 1980s as a solution to the problem of how to link newer applications to older legacy systems, although the term had been in use since 1968.

[[896](#)]

Database **normalization** is the process of structuring a relational database in accordance with a series of so-called normal forms to reduce data redundancy and improve data integrity.

[[897](#)]

Postgres Views, www.postgresql.org/docs/current/sql-createview.html

[[898](#)]

Interesting SQL Queries, github.com/input-output-hk/cardano-db-sync/blob/master/doc/interesting-queries.md

[[899](#)]

Building and Running the Cardano DB Sync Node, github.com/input-output-hk/cardano-db-sync/blob/master/doc/building-running.md

[900]

Working with Cardano DB Sync, github.com/input-output-hk/cardano-documentation/blob/staging/content/05-explore-cardano/02-cardano-architecture/04-working-with-db-sync.mdx

[901]

Cardano DB Sync Github, github.com/input-output-hk/cardano-db-sync#cardano-db-sync

[902]

Indexer: Blockchains contain a lot of data and metadata. Dealing with such bulk data can be challenging for DApps and wallets which need to quickly filter data to provide the best user experience.

Indexers speed up this process and there are many different kinds depending on what you're trying to do. SQL databases, like Postgres, are popular because they allow for flexible queries with good performance.

[903]

Carp — New Cardano SQL indexer & replacement for db-sync, medium.com/dcspark/carp-new-cardano-sql-indexer-replacement-for-db-sync-b990243a329e

[904]

What are the benefits of using plutarch?, cardano.stackexchange.com/questions/6996/what-are-the-benefits-of-using-plutarch

[905]

Apollo GraphQL, www.apollographql.com/

[906]

Docker compose, github.com/input-output-hk/cardano-graphql/blob/master/docker-compose.yml

[907]

TypeScript is an open-source programming language developed and maintained by Microsoft. It is a strict syntactical superset of JavaScript, and adds optional static typing to the language.

[908]

Apollo GraphQL, www.apollographql.com/docs/apollo-server/

[909]

Prometheus metrics, prometheus.io/

[910]

GraphQL Code Generator, graphql-code-generator.com/

[911]

Cardano GraphQL Github, github.com/input-output-hk/cardano-graphql#overview

[912]

Cardano Rosetta, github.com/input-output-hk/cardano-rosetta

[913]

Bitcoin Rosetta, github.com/coinbase/rosetta-bitcoin

[914]

Ethereum Rosetta, github.com/coinbase/rosetta-ethereum

[915]

Rosetta blockchain-specific operations, www.rosetta-api.org/docs/1.4.4/models/Operation.html

[916]

Rosetta Data API, www.rosetta-api.org/docs/data_api_introduction.html

[917]

Rosetta Construction API, www.rosetta-api.org/docs/construction_api_introduction.html

[918]

Rosetta flow of operations, www.rosetta-api.org/docs/1.4.4/construction_api_introduction.html#flow-of-operations

[919]

Rosetta API calls, docs.cardano.org/rosetta/api-calls-rosetta

[920]

Official Rosetta website, www.rosetta-api.org/

[921]

Rosetta: sending transactions, github.com/input-output-hk/cardano-rosetta/tree/master/examples#transaction-sending

[922]

Rosetta staking key registration and delegation, github.com/input-output-hk/cardano-rosetta/tree/master/examples#staking-key-registration-and-delegation

[923]

Rosetta withdrawals, github.com/input-output-hk/cardano-rosetta/tree/master/examples#withdrawals

[924]

Rosetta sending transactions, github.com/input-output-hk/cardano-rosetta/tree/master/examples#sending-transactions-with-single-multi-assets

[925]

Bech32 is a segwit (segregated witness) address format specified by BIP 0173 (Bitcoin improvement proposal). This address format is

also known as ‘bc1 addresses’. Bech32 is more efficient with block space. As of October 2020, the Bech32 address format is supported in many popular wallets and is the preferred address scheme for Bitcoin.

[\[926\]](#)

Integrating with third parties, github.com/input-output-hk/cardano-documentation/blob/staging/content/02-getting-started/05-integrating-with-third-parties.mdx

[\[927\]](#)

Running stake pools and delegation for exchanges, github.com/input-output-hk/cardano-documentation/blob/staging/content/02-getting-started/06-running-stake-pools-and-delegation-for-exchanges.mdx

[\[928\]](#)

SMASH handbook, github.com/input-output-hk/cardano-documentation/blob/staging/content/05-explore-cardano/02-cardano-architecture/05-smash-handbook.mdx

[\[929\]](#)

SMASH github repo, github.com/input-output-hk/smash

[\[930\]](#)

Smart contracts here we come, iohk.io/en/blog/posts/2021/04/08/smart-contracts-%E2%80%93-here-we-come/

[\[931\]](#)

Reimagining P2P finance with Marlowe, iohk.io/en/blog/posts/2021/05/26/reimagining-peer-to-peer-finance-with-marlowe/