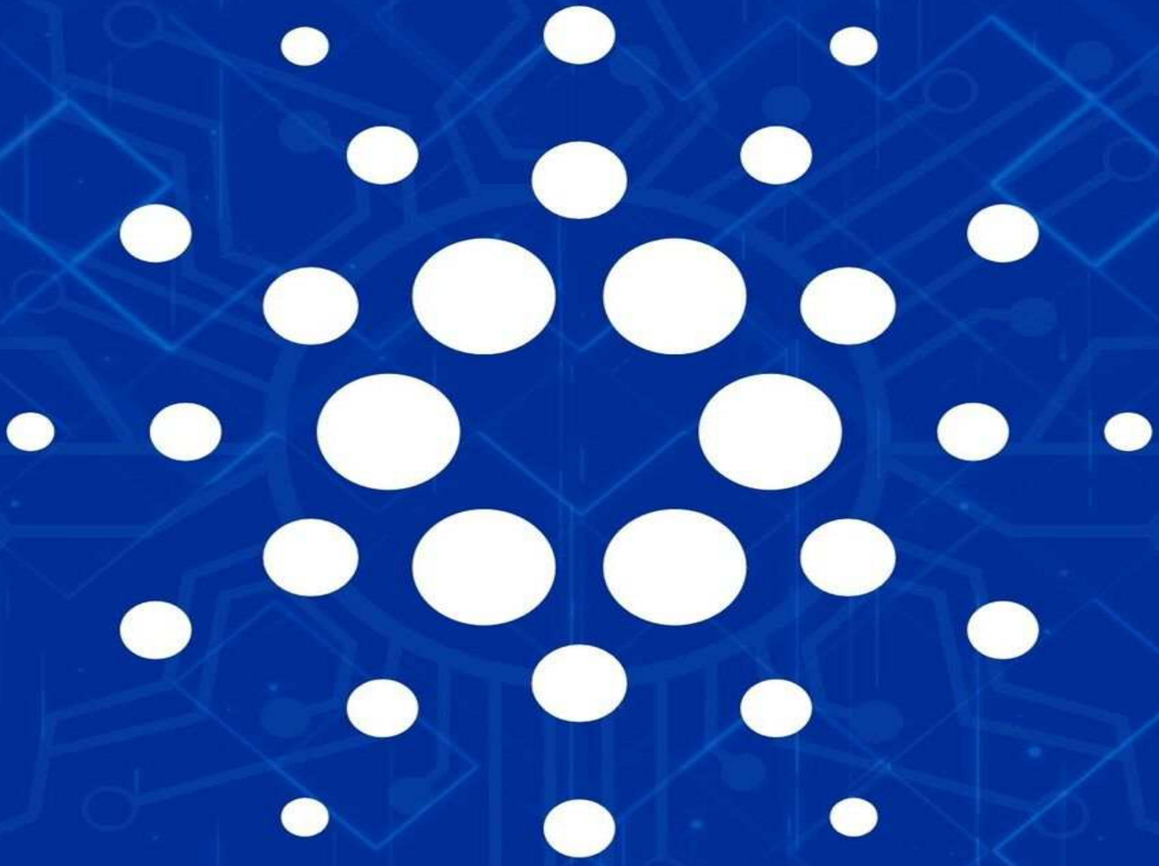
CARDANO

The Essential Guide



Jesse Dvorak

Cardano: The Essential Guide

Everything You Need to Know about the Cardano Blockchain

Jesse Dvorak

Table of Contents

Disclaimer

The opinions contained in this book are mine alone. I do not represent the Cardano blockchain or any of its founding partners in any official capacity. I am merely an enthusiastic user of the Cardano ecosystem.

The information in this book should not be taken as financial advice, legal advice, or any other type of advice. It is only a record of my own knowledge and an optimistic vision of the future.

Who is this book for?

This book is best suited for those who have dabbled somewhat in the cryptocurrency space or have at least heard of the most basic terms in the industry like Bitcoin, Ethereum, Web3.0, or NFTs. There are far too many books already written on the fundamental theory of blockchain technology, the history of Bitcoin, and how these systems will impact the world generally. This book instead focuses on the Cardano blockchain specifically, its utility to the average user, and how it stands apart as an influential leader in the development of the next-generation internet at large.

This book will probably be most useful to four types of readers:

- investors who are looking at throwing some money into this venture in order to seek a return

- developers who want to help build the network

- technologists who are interested in tracking the development of a world-changing technology

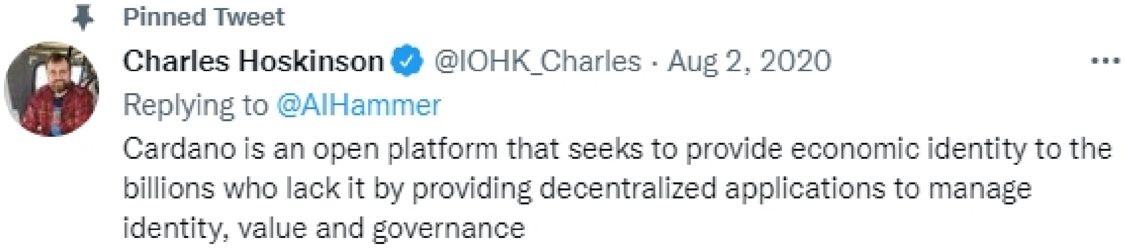
- general users who want to take advantage of the decentralized applications (dapps) that are available for use on the Cardano blockchain

That being said, I have included very concise explanations on how the basics of blockchain and cryptocurrency work because I have found that even people who have invested a ton of time and money into these projects do not always have a full grasp of the true foundations of the technology and are simply jumping on a bandwagon.

I do not want you to be a bandwagon jumper. I want you to know exactly what it is that you are using and why it is that you are investing, if that is what you choose to do.

Use this book as a resource and a stepping off point towards doing your own research and deciding for yourself if Cardano, and the larger world of blockchain, is a project worth pursuing.

Introduction: What is Cardano?



Pinned Tweet

Charles Hoskinson @IOHK_Charles · Aug 2, 2020

Replying 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 **blockchain technology,** and in that way is similar to Bitcoin and Ethereum.

Charles Hoskinson, the founder of Cardano, calls it a “third generation” blockchain. Bitcoin would be first generation, Ethereum second generation, and Cardano third generation. Cardano features the decentralization and security of Bitcoin coupled with the programmability and smart contract capabilities of Ethereum.

Hoskinson’s pinned tweet, seen above, describes in one sentence (albeit a dense one) precisely what Cardano is meant to do. Charles asserts that:

1. Cardano is an “open platform”.
2. Cardano seeks to provide “economic identity”.
3. The lack of economic identity is a problem that affects a large percentage of the world.
4. Cardano aims to handle the problem of economic identity by building a platform that hosts decentralized applications.
5. The applications that are built on Cardano will be able to manage identity, value, and governance for those who use them.

Let’s go through these claims one at a time and breakdown Charles’ vision for Cardano.

Claim #1: Cardano is an open platform.

When Charles talks about the openness of Cardano, he is referring to its decentralization and permissionless nature. Anyone is free to build on and use the platform. No one can be barred or banned in any way. Any transactions that occur are publicly accessible and can be viewed on websites like Cardano Explorer, ADAtools.io, and CardanoScan.io.

The software code by which Cardano is made is also fully open source, meaning that anyone can view the code and use it for their own projects. This code has been posted to Github for easy access.

Keeping the platform open in this way is essential in ensuring that it stays decentralized. The more people building and using the project, the less likely it is that too much control will fall into any one person's hands.

Claim #2: Cardano seeks to provide "economic identity".

Economic identity refers to the ability to tie together a record of transactions with its owner - thereby enabling the creation of a financial reputation.

When I apply for a credit card, the issuer will first check my credit score to make sure that I am the type of person who is likely to be able to pay back any money that is lent on credit. In order for me to have a credit score to check, I need to have an economic identity. The credit card issuer needs to be able to see that I have some sort of proven track record that indicates that I will be able to meet my financial obligations going forward. Failure to provide this proof of reputation on my part would mean that the issuer would refuse to give me the credit card. This, after all, only makes good business sense - handing out lines of credit to people who cannot afford to pay back the money that is borrowed will lead to disaster on both ends of that deal. The issuer also needs to be able to track me down should I fail to pay, and that can only be done if I am tied to an identity. This identity would include contact information like my phone number and address, but it would also be a record of previous loans, purchases, credit card payments, taxes paid, etc. The solidification of this identity is necessary for gaining trust in a system that is controlled by centralized decision makers whose profit rests on a client’s ability to obey the rules of the system.

Claim #3: The lack of economic identity is a problem that affects a large percentage of the world.

According to Charles Hoskinson’s 2014 Ted Talk, 3 billion people, roughly 42% of the earth’s population at the time, are unbanked and undocumented. This is more of an issue in less industrialized African, South American and Middle Eastern countries but also exists in certain parts of modernized countries like India and China. These people may not have basic records that first world citizens take for granted, such as the deed to a house, a car title, government ID, a college degree, a checking account, an electronic medical record, or birth or death certificates. These people do not have a true “economic identity”, and as such they are excluded from first world financial instruments. Giving these people the opportunity to create a formal record of themselves, their property, and their financial reputation will make it profitable for banks to service them - allowing them to get loans, safely store their money, earn interest, and purchase investment instruments like stocks, bonds and real estate and thereby giving them opportunity to build wealth.

Claim #4: Cardano aims to handle the problem of economic identity by building a platform that hosts decentralized applications.

Cardano, as a software platform, is able to host computer programs on top of it called decentralized applications, or “Dapps”. Anyone is free to build and launch Dapps on Cardano, and there are many independent teams working towards that end with the hope of contributing to the decentralized financial infrastructure of the Cardano ecosystem.

The Dapps that are built on Cardano will be able to solve the problem of economic identity in two major ways - firstly, through the facilitation of record keeping so that a person’s financial reputation can be recognized by the legacy banking system, and secondly by building a new type of banking system that is decentralized (thereby free from traditional gatekeepers) which can bypass the legacy system altogether.

Claim #5: The applications that are built on Cardano will be able to manage identity, value, and governance for those who use them.

Charles Hoskinson suggests that in order to handle the problem of economic identity, Dapps will need to be built to manage three particular functions - identity, value, and governance.

The management of **identity** is being tackled with projects on the Cardano blockchain such as Atala PRISM, Blockademia, dHealth, and IAMX. These projects aim to enable users to tie their online identity to things like education credentials, healthcare records, job history, and land ownership.

The ability of users to manage **value** is already assured by the decentralized exchanges that are running on Cardano - Minswap, Muesliswap, Wingriders, and Sundaeswap. These Dapps allow for swapping between tokens that are in the Cardano ecosystem, and will soon feature lending and borrowing as well.

Considerable progress has been made with regards to **governance** on the blockchain through Project Catalyst and the Catalyst voting app. Catalyst allows users to vote on funding grants for new projects being built on Cardano, thereby allowing users to directly influence the future of the ecosystem.

The successful implementation of these three functions, when used in tandem, will allow the Cardano blockchain to fully realize the vision set forth by its founder.

Using Dapps, which are simply lines of code sitting on the blockchain, one can interact with others in such a way that users are either able to **avoid the legacy banking system entirely** because all of their needs are being met, or create enough financial stability that the **use of traditional institutions becomes a real possibility to them**.

As we explore in more detail the underlying technology that makes all of this possible, it will become clear that not only are the stated aims of Cardano achievable, but they are well on their way to becoming reality.

Who is Responsible for Cardano?

Cardano is a decentralized network and so is built and maintained collectively by those who use it. Developers can launch applications on the network, users can access and fund those applications, and people who own the native currency (ADA) can freely move it around as they please from wallet address to wallet address. Stake pool operators ensure the functioning and security of the network by running software that validates transactions and creates new blocks on the chain.

That being said however, there are 4 key entities who are most responsible for the creation, programming, advertising, and maintenance of the Cardano ecosystem.

These are:

1. Charles Hoskinson, the founder of Cardano.
2. IOHK, recently rebranded as IOG.
3. The Cardano Foundation
4. Emurgo

These four entities work together to maintain and improve the network but each has a dedicated function in the Cardano ecosystem.

Charles Hoskinson

“The future must be decentralized. Because it’s not worth living in a future that isn’t.”

- Charles Hoskinson, June 2022 Keynote Address to the Cardano Community

Hoskinson got started in the cryptocurrency space in 2013 with his "Bitcoin Education Project". This project sought to educate the masses about the potential of Bitcoin and had the stated goal of bringing "1 million people into Bitcoin by the end of 2014". It involved the building of courses designed to promote an understanding of what Bitcoin is and how it could be useful in world economics and business. One of his courses still exists on Udemy - "Bitcoin, or How I Learned to Stop Worrying and Love Crypto". Even in these very early years, when the price was only about 100 USD per coin, Hoskinson was excited about what Bitcoin could mean to the world.

Charles Hoskinson's next major achievement in the cryptocurrency space was being one of the 8 original founders of the now famous Ethereum - the second largest cryptocurrency today. Hoskinson and the other co-founders realized that they could use the basic principles of cryptocurrency to create not only digital money but also programs called "smart contracts" that could be used to interact with that digital money. This was the main difference between Ethereum and Bitcoin - Ethereum featured the same type of transferable digital money as Bitcoin, plus the added functionality of smart contracts.

Ethereum was founded in December of 2013, but Hoskinson left the project after a few short months due to disagreements with co-founder Vitalik Buterin on the appropriate business structure of the organization.

In 2015, Charles, along with business partner Jeremy Wood, formed a new software corporation called "IOHK".

Using the resources of his software company, Hoskinson immediately began work on the Cardano blockchain, with its operation officially launching in September of 2017.

Charles is the current CEO of IOHK (Input Output Hong Kong) more recently known as IOG (Input Output Global). Despite the rebranding, many references to Charles' company will still read

“IOHK” as the name has stuck and it isn’t easy to change every citation, directory and web address.

Charles has very regular (almost weekly) AMAs on YouTube where he starts off with a detailed progress report about the current state of Cardano and leaves ample time afterwards to take questions from his live viewers. He is also very involved in the cryptocurrency Twitter and Reddit communities and does his best to respond to the larger issues that crop up there.

I would recommend watching some of his AMAs if you are doing your due diligence on Cardano as a potential investment opportunity. He often gives great insight as to the future plans that are in the works for the Cardano team and loves sharing his vision for what Cardano, and cryptocurrencies in general, should look like as the space develops. The ambitions of a project’s founder are often just as important to that project’s success, if not more important, than the execution.

IOHK

IOG is of course made up of more people than just Charles Hoskinson. As the CEO, he is in charge of the overall direction and high-level planning of the company, but he does no actual software programming - leaving the technical specifics to particular experts in that field.

There is a long list of talented people working for IOG as can be seen on the “team” page of their website. These employees are divided into specific workgroups, such as development, formal methods, quality assurance, business analysis, education, design, web development, product marketing, and talent resourcing. There are currently 416 employees listed, most with pictures and bios. This kind of transparency is well respected in this industry and helps to build trust within the community.

One of the most salient accomplishments of IOG is their ever growing research library, currently made up of over 150 technical papers written to explain and prove some of the most foundational concepts of blockchain theory. These papers are completely free to access by anyone, and are often implemented by others in the blockchain space to back up their own work. One notable example of this is Polkadot's (a competing blockchain) usage of a modified version of the Ouroboros consensus mechanism - a key technology backing the Cardano blockchain.

These papers often start with introductions that are easy to understand even by the average crypto user, but often quickly veer into mathematician-only language. Even so, there are certainly a few that are worth checking out to gain a greater understanding of the theoretical foundation behind Cardano as well as many other blockchain systems. See appendix A for some prime examples.

IOG is Hoskinson's baby and is the organization that is most responsible for the technical improvements in the Cardano blockchain.

The Cardano Foundation

In contrast, the Cardano Foundation is a non-profit whose mission primarily revolves around promoting Cardano in the global community. As their website states, their missions include:

- driving adoption of Cardano
- shaping legislation and commercial standards
- growing the global Cardano community
- ensuring stakeholder accountability
- facilitating partnerships

To these ends, they are active on Cardano's social media, maintaining a presence on Reddit, Medium, Twitter, and LinkedIn, among others. They are also responsible for maintaining some of the official documentation on Cardano's inner workings. In particular, their documentation features a plethora of high-level technical information on some of the computer science behind Cardano's design and implementation. Anyone wishing to know the details of the Cardano network’s basic architecture, its native tokens, or the programming languages Marlow and Plutus should check out this documentation. It is fairly easy to read even for non-computer scientists and features virtually no mathematical language.

The Cardano Foundation aims to make the technology accessible to the masses and get as many people as possible on board with its development.

When you think of the Cardano Foundation, think of promotion and community engagement.

Emurgo

Emurgo is the last piece of the puzzle here. Certainly the least relevant of the three companies to Cardano, Emurgo still has a role to play in the ecosystem. According to its website, Emurgo.io, it is a “global blockchain technology company providing solutions for developers, startups, enterprises, and governments".

Emurgo is not specifically a Cardano company, but is a company that specializes in general blockchain applications. It is however considered to be a founding partner of the Cardano blockchain and was contracted by IOG to create Yoroi, the first wallet in the ecosystem that could be run as a browser extension. Yoroi is regarded as one of the most trusted (albeit also one of the slowest) wallets on the Cardano ecosystem to date.

Emurgo is often referred to as the “commercial arm” of Cardano, but the development of Yoroi is Emurgo’s only real contribution to the platform so far. Emurgo’s relevance to the space will probably fade over time, as the Yoroi wallet is supplanted by faster wallets with more features and better user interfaces (e.g. IOG’s Lace Wallet). However, it will always be remembered as one of the originating institutions of Cardano, and may be contracted for further work in the future.

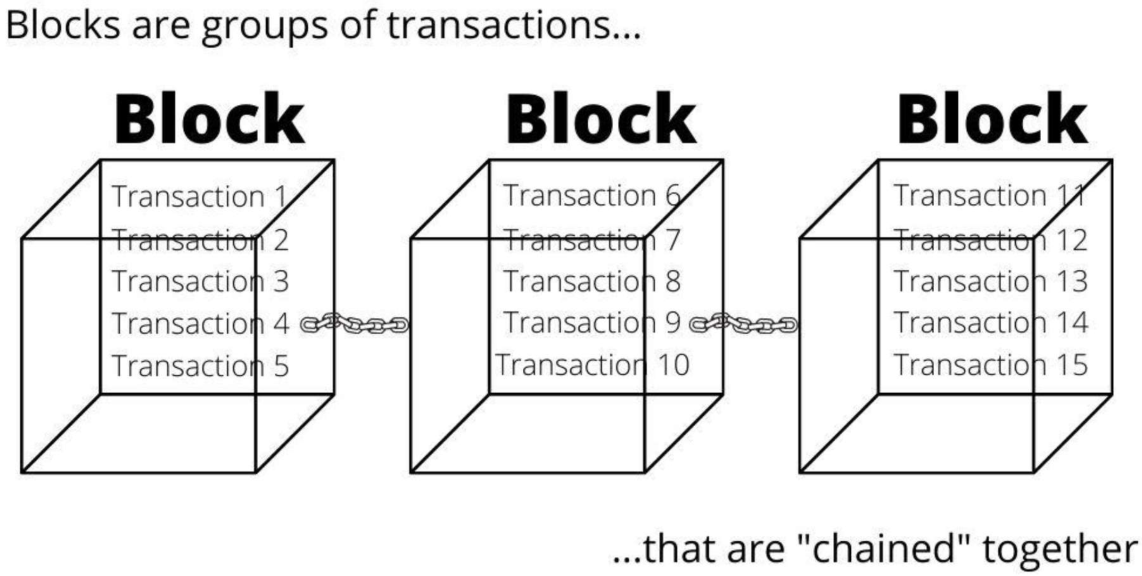
Chapter 1: Cardano's Blockchain Mechanics

"Blockchains are ultimately databases ordering facts and events with guarantees about timestamps and immutability." - Charles Hoskinson, *Why Cardano*

As IOHK researchers tell us in their 2019 paper entitled "Proof-of-Work Sidechains",

> *Bitcoin is the first and most successful cryptocurrency to date. Its core protocol introduced the concept of a blockchain, a type of cryptographic consensus protocol in which transactions are organized into blocks which are then put in a mutually agreed sequence despite the presence of adversarial nodes.*

A blockchain is a new way of creating a permanent ledger, or record of transactions. This ledger is immutable, permissionless and trustless. This means that the record of transactions cannot be changed, is accessible by anyone without any governing authority necessary to grant permission, and there is no need to trust any one entity to ensure that what is recorded is accurate.

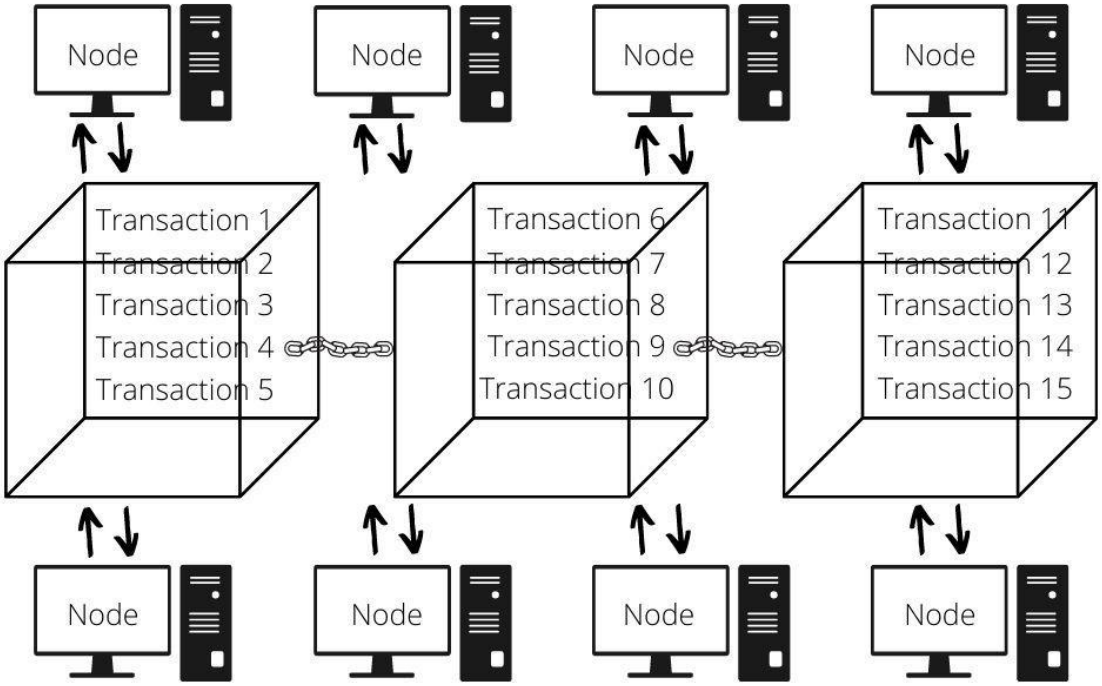


These things are possible because of *decentralization*.

Decentralization is achieved by distributing control of what can be written on the ledger to many **nodes** (members of the system) rather than just one. The greater the number of nodes in such a system, the greater the decentralization and the stronger the immutability, permissionlessness, and trustlessness is.

Because control of the ledger is distributed across many nodes, blockchains are also referred to as *distributed ledger systems*.

These nodes each contain a full copy of the blockchain (ledger of transactions). In this way, each node can ensure that only the appropriate, approved changes have been made to the record by comparing their copy to every other copy.



This would be in deep contrast to a centralized system, where one entity controls the data entirely. Private companies, such as Walmart, control their own data. This data is not monitored or regulated by anyone else. If Walmart decided to tell the public that they sold 1 million toothbrushes that year, how would anyone know that this is “true”? They could ask for receipts, or for some sort of electronic record of transactions. But because Walmart is in control of their own data, there is no way to actually prove for sure the total amount of toothbrushes that were sold by Walmart. This is why for important data collection efforts we expect a separate, disinterested entity to verify the veracity of the data. There needs to be some sort of audit process in centralized systems in order to get the public to trust the accuracy of the records.

The obvious example of this is reported income that will determine tax owed to the government. Businesses report this income, but the report is not always simply believed without verification. In the United States, the IRS is seen as a validator of this sort of data. If the IRS tells us that Walmart made $100 billion this year, we are more inclined to believe it over simply reading it in Walmart’s own report. Why is that? Because now we have 2 sources of data - Walmart reported this income data, and the IRS validated it. With even just one extra entity validating data, we now have increased trust in the validity of what they are saying. But this is still only 2 sources - these 2 entities would only need to form some sort of agreement between them to regain control of the data and change whatever they like. If either entity were to be influenced by the other, the veracity of the data would be compromised. Walmart could convince the IRS that the data was different than it actually was, or the IRS could convince Walmart that the data was different than it actually was. Or possibly both actors could mutually agree to make a change to the data together.

However, adding a third entity to further verify the data would lead to even higher trust in the outcome, as it would be more difficult for 3 separate entities to collaborate on creating a falsity than it would be for 2. Add yet another validator and even more trust is built, and so on and so forth, with each new validator adding a little more trust that the data in question is true. The more separate, uninfluenced entities that exist to validate a data set, the greater the potential that the data is in fact valid. This is because as validators are added to a network, the chance that they will all be working together to produce the same falsity decreases. This truth is the root of why decentralization provides the highest degree of security for a network.

Just remember - **the more entities there are to validate the truth of a piece of data, the more decentralized the network is and the more the record of transactions can be trusted.**

While this is obviously a huge benefit, there is a definite drawback to increased decentralization. With more nodes contributing to a system, there will be decreased speed of transactions as each node needs to be updated whenever a change occurs.

One entity determining truth for everyone is the highest degree of centralization. Every individual determining their own truth is total decentralization. Too centralized, and we cannot trust the data. Too decentralized, and the network would be too slow and expensive.

The ideal would be a correct balance between the two extremes, and that’s where I believe Cardano fits the bill.

The Blockchain Trilemma

This brings us to something called the “Blockchain Trilemma”. Basically there are 3 characteristics that a blockchain wants to have - decentralization, security, and scalability. While all of these are important to a well functioning blockchain, they are tradeoffs of each other. Only two out of these three characteristics can be maximized at any one time.

Decentralization refers to the fact that a lot of people, not just a handful, have control over the network. Security is the network’s ability to resist attacks or attempts to maliciously control the network for private gain. Scalability refers to the ability of the network to handle large volumes of transactions quickly and cheaply.

Focusing on perfecting two of these elements will lead to weakness in the other one. As decentralization increases, for example, more people are added to the network and this will increase cost of transactions and decrease the speed of transactions. More validators ensuring the validity of the data may mean more security, but now there is a difficulty with scalability as the network becomes congested, slow and expensive.

Increasing both security and scalability is possible, such as is the case with traditional company-owned networks such as an internal network of Google or Walmart or Chase. These systems however are centralized - they are owned and controlled by the company. Creating a blockchain like this would be no different than the software we currently use in the legacy system.

Each blockchain on the market today has its own way of handling the blockchain trilemma. All try to improve security as best as they can, as without security a network is essentially useless, but each blockchain must make its choice as to whether or not to sacrifice scalability for decentralization or vice versa.

Cardano’s engineers focused on security and decentralization first, and are building towards scalability solutions second.

This is in contrast to a blockchain like Solana, which has a much greater degree of centralization and as a consequence experiences frequent network outages.

The reason Cardano focused on security and decentralization first is that without decentralization, there is no purpose to making computations on a blockchain in the first place - you could just use a regular, traditional centralized network. And without security, everything built on the network would be in jeopardy and no one would use the network because they wouldn’t take the risk of losing their money. It is clear that to succeed in this space, decentralization and security must be primary. These parameters form the stability that will make scalability even necessary.

Taken from a wonderful Reddit post on the necessity of decentralization on Cardano by u/Cardanians:

> *A blockchain network without a high degree of decentralization does not bring any qualitative change. There is no significant difference between blockchain X and a company server. Decentralization is about the distribution of decision-making power. Decentralization is about cutting out the middlemen and putting more trust directly into the technology. Decentralization needs to be defended and its growth needs to be pursued. Individuals cannot have a strong position in the network. If they gain it, all important characteristics are lost.*

Cardano increases decentralization by providing a monetary incentive for users to host their own nodes. That is, users who host nodes get paid by the system for their service. The fewer nodes there are, the more each one will get paid. This creates a sort of “gold rush” effect as users rush to set up nodes so they can extract the most value from the setup.

As well, it is known that the more nodes in a network, the more resilient that system will be due to the increased decentralization - which benefits all users of that network. Users who see the potential of Cardano will want to run nodes so as to secure the value of their own funds which reside on the network.

Cardano increases security in several different ways, because there are several different types of attacks that can occur, but one notable example is the use of a payment system for using the network that scales with the amount of data sent through it. Because distributed ledger systems (blockchains) are open for everyone to use, their use has to be somewhat expensive to reduce the chances that individual malicious actors disrupt the system for their own benefit. If a system were completely free to use, there would be nothing stopping a malicious actor (sometimes these are referred to as "byzantine nodes" in the industry) from spamming the network and using up all resources thereby effectively shutting down the network.

Cardano, along with other blockchains, handles this potential problem by having implemented a fee structure that charges users funds in proportion to the size and quantity of transactions sent on the network. There is a base fee per transaction, plus a bonus fee added on that scales in proportion to the size of the transaction. In this way, spam of both quantity and size of transactions becomes prohibitively expensive.

Proof-of-Work and Proof-of-Stake: How to Determine What Should Be Written In The Ledger?

As new transactions are made and recorded on a blockchain, every node needs to be made aware of the updated ledger. To do this, new blocks of transactions are published by certain selected nodes. The mechanism of deciding which node gets to create the next block in the chain is called the “consensus mechanism”.

Consensus mechanisms are necessary in blockchain programming because there needs to be a way of making sure that every node in the system has the exact same copy of the blockchain as every other node. It is essential that every node agrees, or has consensus, about what transactions have occurred. If you transfer some ADA from your wallet to a friend’s wallet, every node needs to agree that that happened so that the transaction gets put into the blockchain permanently.

Ouroboros is the name given to Cardano’s “**proof-of-stake**” consensus mechanism. The IOHK paper entitled “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol” lays out the theoretical and mathematical foundations for why Ouroboros is both a secure and efficient consensus mechanism.

Cardano.org succinctly states:

“Ouroboros is the first provably secure proof-of-stake protocol, and the first blockchain protocol to be based on peer-reviewed research.”

“Proof-of-stake” is the general type of consensus mechanism, while “Ouroboros” refers to Cardano’s specific brand of proof-of-stake.

Proof-of-stake (PoS) is often contrasted with Bitcoin's proof-of-work (PoW) consensus mechanism.

Each of these mechanisms are different ways of electing who in the network gets to mint the next block in the chain. PoW is driven by computers solving difficult mathematical problems - whoever in the network solves the problem first gets the privilege of minting the next block. As a reward for doing this, they get some bitcoin dropped into their wallet. This means that the more computing power you have to solve the problem, the more likely you are to mint the next block and the more bitcoin you will collect over time. This process is known as "mining" bitcoin.

Take a look at this high level description of what exactly the Bitcoin proof-of-work blockchain is doing, taken directly from the 2008 bitcoin whitepaper written by "Satoshi Nakamoto":

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Proof-of-stake (PoS), by contrast, allows nodes to put funds at "stake" to increase the chance they will be picked, rather than utilize hardware to solve a math problem. The higher the amount of funds at stake, the greater the chance that that node will be chosen to make the new block. Putting a monetary value at stake instead of scarce physical resources allows the same security protections against malicious actors seeking to subvert the system but does not cost nearly as much in terms of power consumption and computing hardware.

“The rationale behind Proof-of-Stake is that entities who hold stake in the system are well-suited to maintain its security, since their stake will diminish in value when the security of the system erodes” (Bentov et al., 2014).

The eUTXO Model: How it Compares to Etherum and Bitcoin

When navigating the crypto space, you will often hear the term "UTXO" being thrown around, especially when the Bitcoin network is being talked about.

UTXO stands for "unspent transaction output" and it describes the model of transacting that the Bitcoin ledger is built upon. In this model, all transaction inputs are constructed from previous unspent transaction outputs. Think of how you would pay for groceries with cash, for example - if the bill came to $73.80, you might pay the cashier with a $100 bill. In response, you could then receive change in the form of, let's say, a $20 bill, a $5 bill, a $1 bill and 2 dimes. Each of these would be an "unspent transaction output". They are specific denominations of outputs from your grocery transaction, and they can now be spent again in a new transaction. Once one of these UTXOs are spent, they can never be spent again, as they will be either consumed entirely or broken up into new UTXOs.

The Bitcoin blockchain network works like this, as designed by Satoshi Nakamoto. Every wallet on the network contains multiple addresses, with each address corresponding to a particular UTXO value. As transactions are signed by wallets, these UTXOs are "spent" and broken up into further UTXOs when "change" is given, such that no address is ever used twice. Wallets are not tied to single addresses then, but to every address that contains a UTXO that is a part of that wallet. Twenty dollars worth of value on a blockchain, for example, could be divided up into 10 UTXOs of two dollars each, or UTXOs worth five dollars, ten dollars, two dollars and three dollars, or any other such combination.

The system of account for Cardano is called "eUTXO". The "e" at the front of eUTXO stands for "extended" and it refers to the fact that the system is structured so that smart contracts may be put on the platform. Bitcoin follows the UTXO model, which does not allow for smart contracts, while Cardano follows the very similar eUTXO model, which does allow for smart contracts to run on the network and thereby enables the creation of Dapps.

This system of computing contrasts with the way Ethereum is set up. Ethereum uses a so-called “accounts based model” to keep track of its ledger. In this model, transactions are recorded as you would expect them to be when dealing with bank accounts, for example. When currency is sent from one wallet to another, a balance is subtracted from the sending account and added to the receiving account. There are no UTXOs involved - value is simply added and subtracted directly from accounts in exact quantities.

There are advantages and disadvantages to each system from a programming standpoint, and each excels at tasks the other does not.

According to the documentation on the Ergo blockchain, UTXO has the potential for greater privacy, scalability, interoperability, and transaction cost predictability, due to the nature of working with denominations that can only be used once.

From the same documentation, a note on security:

> *The UTXO model has several implications. For a start, each object is immutable - lumps of coins cannot be “edited” like an Account balance is edited when a transaction is made. The balance is calculated from the transaction history when those coins first came into existence.*
>
> *That makes security much simpler because either a UTXO exists in the form that you expect, or it does not exist. With the Account model, you need to carefully check the Account you’re dealing with is in the state it should be (and developers typically don’t do that correctly). This also makes UTXOs more friendly for off-chain protocols, like sidechains and the Lightning Network.*

The programming of an Ethereum-like accounts model is sometimes simpler to work with, but developers who opt to go with a UTXO model (like Satoshi Nakamoto did) generally believe that increased effort in the short term will yield greater benefits in the long term.

Chapter 2: ADA - The Currency of Cardano

The native currency of Cardano is called “ADA”, named after the computer scientist Ada Lovelace. Like all cryptocurrencies, it is stored in a wallet.

Well, sort of. Actually the coins are stored on the blockchain itself, but wallets allow you to interact with the blockchain in such a way that you can view and move your coins.

There are a few wallets of note that should be known by anyone trying to collect some ADA. More wallets will be released as time goes on, with additional features and advanced technology, but the tried and tested first movers will probably be around for a long time. The security of your wallet is paramount, as a bug in a wallet could jeopardize your stored ADA. Therefore some ADA holders will be hesitant to jump from wallet to wallet as new models are released, until those wallets have built a reputation for quality in the community.

There are four main wallets right now that are in use and are well trusted in the community:

1. Daedalus (pronounced dead-ah-lus)
2. Yoroi (pronounced your-oy)
3. Eternl (formerly “CCVault”)
4. Nami

Daedalus is the official wallet produced by IOG. It is a “full node” wallet, meaning that when it is opened it downloads a copy of the entire blockchain. This, in theory, makes it the most secure wallet available. There is no way for the wallet to make a mistake or get something wrong, as it is looking at the complete record of all transactions on the chain. The disadvantage with a wallet such as this is that it does take a significant amount of time to download an entire blockchain when you first open up the wallet, and then while the wallet is up and running it takes up a considerable amount of RAM. On the plus side though, it contributes to the security of the network on the whole, as it is another node in the system and so it is another relay point for verifying transactions.

Being that Daedalus is the official IOG wallet, it is constantly being updated by IOG to keep it secure, fast and functional. It also has a beautiful, clean and efficient user interface. It is my favorite wallet to use because of these advantages. The only real downsides to Daedalus are the time required to download the entire blockchain and the massive RAM usage.

Daedalus is only available as a desktop app - there is no mobile version and most likely there will never be. It is far too hardware-intensive to run on mobile.

Yoroi is produced by Emurgo, and is the official "light wallet" of Cardano. It is trusted and secure, but it is not nearly as fast as other light wallets. It is much faster and less hardware intensive however compared to Daedalus, because it is a light wallet and does not require the download of the entire blockchain. Because of this, it is able to have both a mobile app and a browser extension, so it can be used on smartphones.The tradeoff is that it relies on the integrity of Emurgo's coding to ensure blockchain data is correctly supplied to the wallet. This is true of all light wallets - some degree of trust is needed in the producing company.

Another drawback of Yoroi is that, as of this writing, it cannot fully interact with Dapps. This leaves it at a massive disadvantage compared to the newer Eternl and Nami.

Eternl, formally CCVault, is currently the leading wallet that can be accessed via a smartphone app. It is fast and trusted, although the user interface could use some work. It can interact with Dapps and is much faster than Yoroi.

Nami is the fastest of these wallets. Its speed largely comes from the fact that it is a “one address wallet”, meaning that the speed is gained at the expense of not being able to import multi-address wallets (such as Daedalus, Yoroi, and Eternl) into the Nami interface. That is, you will need to open up a new wallet with Nami and transfer your funds over from your old wallet to achieve full functionality.

This “one address” feature does make the wallet simpler, but it also may make the wallet’s transactions more easily traceable.

Unlike the other wallets, there is no webpage to interact with when you open the Nami wallet. It instead functions only as a browser extension, which adds to its speed and simplicity of use. It can interact with Dapps easily, and seems to be the preferred wallet to interact with the current DEXs on Cardano. It is seen as the “metamask” of Cardano, for those who are familiar with the Ethereum blockchain.

One huge drawback to the Nami wallet however is the fact that you cannot choose what stakepool to delegate your funds to. You may delegate **only** to the **berry** stakepool as of this writing - this acts as the “payment” for using the wallet as that stakepool is owned by the creators of Nami. (More on stakepools and delegation in the next section)

Some other additional wallet options include Flint Wallet, Typhon Wallet, and Gero Wallet.

These wallets are all what I would call “advanced” wallets - they are feature rich, highly customizable, and have a beautiful, clean user interface. They are newer and less proven in the market, however.

All of these wallets exist as browser extensions that can be downloaded from the Chrome web store. Flint wallet is available as a mobile app as well.

Flint wallet is probably the most customizable - you can change settings such as the blockchain explorer that the wallet uses to pull data from as well as the server that is being used. You also have the option of setting a passcode on the wallet so that your wallet is protected even if someone else were to be able to access your browser. Another useful feature of the Flint wallet is the built in graph that allows you to easily see how much value was stored in the wallet over time. Flint also allows you to change how dapps see the wallet - that is, even if Flint itself is not listed as compatible with a certain dapp, you can "inject" the Flint wallet as another wallet that is supported such as Nami or CCVault (Eternl). This feature greatly improves interoperability.

Flint currently runs only on Cardano, but will eventually be compatible with Solana and Ethereum as well.

Typhon wallet is also feature rich - its most compelling addition perhaps being the ability to include custom metadata in a transaction that can be used to describe what the transaction was for, who it was intended for, who it was sent by, etc. Typhon also has a "contacts" tab so that you can save and name commonly used addresses.

Typhon wallet is probably the most detailed wallet and the only wallet that is able to really compete with Daedalus in functionality.

Gero wallet advertises itself as "Your Master Key to Defi". It incorporates a password protection feature that automatically triggers after only a few minutes, ensuring extra security. Gero wallet also contains a built-in "buy" button that links to a third party website that will sell you ADA - at a slight premium, of course - deposited directly into your wallet. My personal favorite feature however is the wallet will show the current ADA price right under your ADA balance, along with a mini graph of the price history.

Many more wallets than these exist, some released and some still in development. I have not personally tried every wallet that exists on the chain however so I cannot personally recommend them, but I'm sure many of them will be faster, more feature rich and with more beautiful interfaces. Each has their own advantages and compromises. Do your own research here to see what wallet works best for you, and report back on the official Cardano subreddit so the rest of us can test it out.

Ensure that when downloading these wallets that you are downloading from the official link. It is possible that fake wallets can be produced that look just like the wallet you are trying to download, but have malicious code in it. The links that I have provided are the official links, but you should still double check and verify these for yourself.

Cardano’s Incentivized Consensus Mechanism

Blockchains, to operate correctly, need to have a way of making sure that each node agrees with every other node on what information should be written in each block. This mechanism is called a “consensus protocol”, and every blockchain has one.

The consensus protocol of Cardano is called “Ouroboros”. Traditionally, the ouroboros refers to the ancient Egyptian symbol of a serpent eating its own tail. Throughout history it was adopted by various cultures and traditions and came to mean many different things for many different people, all revolving around the idea of repeating cycles. For our purposes, it serves as a metaphor symbolizing the circular, self-fulfilling pattern of growth that is built into the Cardano ecosystem.

Cardano’s consensus mechanism is based on the **built-in rewards system** that incentivizes participation in the network.

Cardano’s reward infrastructure is set up as follows:

1. Stake pool operators run specialized software on computer servers, forming “stake pools” which act as nodes in the network.

2. Individual ADA holders “delegate” their ADA holdings to stake pools.

3. Stake pools produce blocks in proportion to the amount of ADA that is delegated to them.

4. Stake pools receive rewards in ADA in exchange for producing blocks and keep a portion of those rewards for themselves (known as a stake pool “fee”).

5. After the stake pool collects its fee, the remaining rewards are distributed to all individual ADA holders who have delegated to a block-producing stake pool in proportion to the amount of ADA that was delegated.

This setup incentivises more users to hold more ADA, as all ADA holders receive a financial benefit in proportion to their stake in the network. As well, users are incentivized to run their own stake pool as they would be able to collect a greater share of the block reward (a “fee”) for doing so.

So where do these rewards that are given out in exchange for block production come from?

Every transaction on Cardano costs a fee for the sender, called a transaction fee. All of the transaction fees that are collected per epoch, along with an amount of ADA from the reserve, are put into a virtual pot. That pot is used to distribute the block rewards to stake pools and stake pool delegators while the rest of it is put into the “treasury”. The pot is divided 80/20, with 80% of the pot going to rewards and 20% going to the treasury - which will be used to fund projects proposals on Project Catalyst that are designed to further develop the ecosystem.

The ADA reserve is similar to the Bitcoin reserve - it is a portion of the total coin supply that has not yet been put into circulation, but is entered into circulation through the rewards given out for block creation. Those nodes which comprise the network must be rewarded for their participation, and this reward is taken out of the reserve supply. In the future, when the reserve supply is dried up, block rewards should be sustained by transaction fees only.

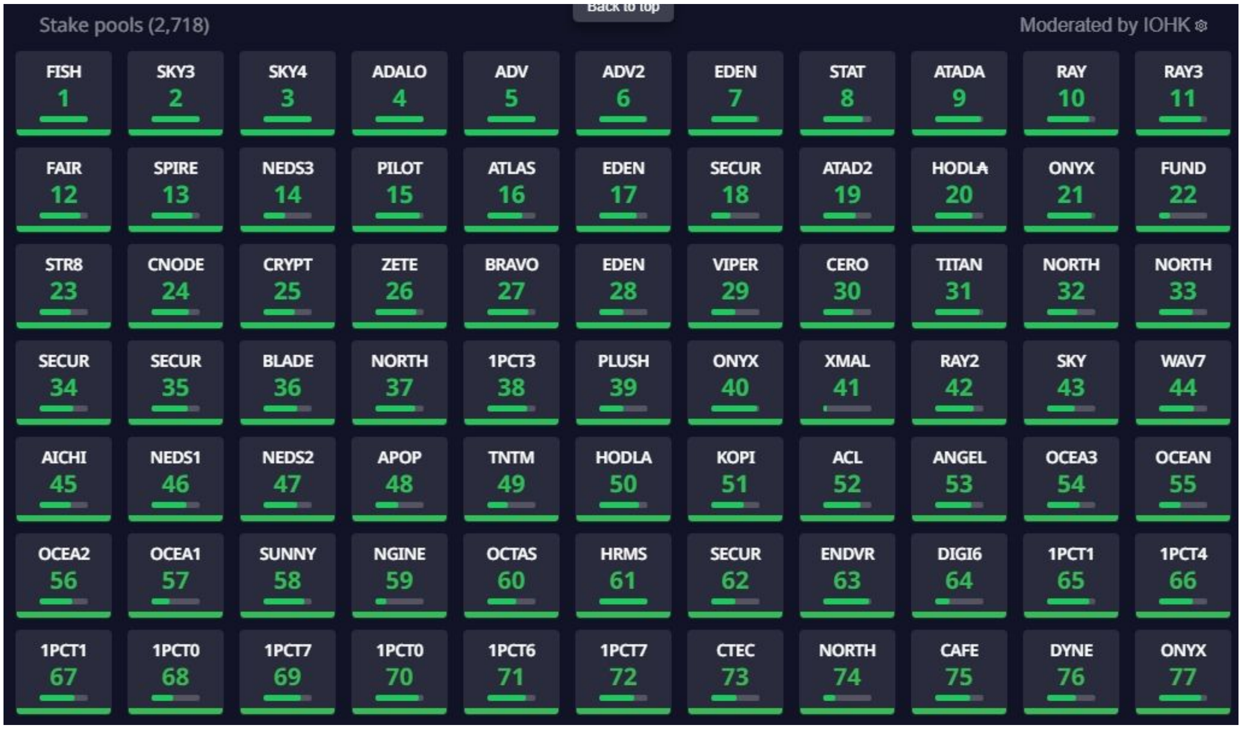
Another interesting component of Cardano's monetary policy is its "ρ" value. This value is a parameter that was initially set by IOHK but in the future will be modifiable by vote. According to an article in ADApulse.io, a higher ρ value would mean a faster rate of funds being pulled from the ADA reserve into circulation. This would equate to greater staking rewards for stake pool operators and their delegators and more money in the treasury. The downside would be that the reserve would run out faster however, meaning that early adopters would be benefitted more but the rewards system would not last long. Therefore a balance needed to be struck between rewarding early adopters of the system and preventing the reserve from becoming depleted too quickly. The value that was chosen was ρ = 0.3%, meaning that 0.3% of the reserves would be pushed into the circulating supply every epoch. This parameter created a reserve half life of about every four to five years.

How to Stake Your ADA with a Cardano Stake Pool

In the Cardano ecosystem, earning passive income through staking ADA that you own is quite easily done. Delegating your ADA to a stake pool can be accomplished through a software wallet - any of the wallets mentioned earlier will do. On every wallet's user interface there should be a tab that allows you to browse the various pools of the Cardano ecosystem so that you can choose one to delegate your ADA to. One of the great advantages of staking ADA is that your funds never need to be locked up. ADA, even while staked, can be moved in and out of your wallet at any time.

In the Daedalus wallet (the official, full node, desktop-only wallet produced by IOHK) there is a beautiful layout of every pool in the system ranked according to potential rewards that you can receive. The rewards that a delegator receives will of course always be in proportion to the amount of ADA that he has staked - the return is usually somewhere around 4.5% annually, give or take. The exact annual return of a stake pool is modulated by a few factors:

1. The pool operator sets a fee that is taken by the pool (higher fees taken by the pool operator mean less total rewards to be distributed among delegators).
2. The more ADA a stake pool has delegated to it, the more likely it is to produce a block and thereby get rewarded with more ADA. This caps off at a certain point however (known as “saturation”), after which increased delegation actually leads to reduced rewards per delegator.
3. Competent operators with reliable hardware ensure a maximum node uptime. If a stake pool ever stops its function as a node in the Cardano network, it can’t produce blocks and so can’t receive rewards.



Stake pools (2,718)

FISH 1	SKY3 2	SKY4 3	ADALO 4	ADV 5	ADV2 6	EDEN 7	STAT 8	ATADA 9	RAY 10	RAY3 11
FAIR 12	SPIRE 13	NEDS3 14	PILOT 15	ATLAS 16	EDEN 17	SECUR 18	ATAD2 19	HODLA 20	ONYX 21	FUND 22
STR8 23	CNODE 24	CRYPT 25	ZETE 26	BRAVO 27	EDEN 28	VIPER 29	CERO 30	TITAN 31	NORTH 32	NORTH 33
SECUR 34	SECUR 35	BLADE 36	NORTH 37	1PCT3 38	PLUSH 39	ONYX 40	XMAL 41	RAY2 42	SKY 43	WAV7 44
AICHI 45	NEDS1 46	NEDS2 47	APOP 48	TNTM 49	HODLA 50	KOPI 51	ACL 52	ANGEL 53	OCEA3 54	OCEAN 55
OCEA2 56	OCEA1 57	SUNNY 58	NGINE 59	OCTAS 60	HRMS 61	SECUR 62	ENDVR 63	DIGI6 64	1PCT1 65	1PCT4 66
1PCT1 67	1PCT0 68	1PCT7 69	1PCT0 70	1PCT6 71	1PCT7 72	CTEC 73	NORTH 74	CAFE 75	DYNE 76	ONYX 77

(Stake Pool Ranking in Daedalus Wallet by IOHK)

You may also choose to delegate to a certain stake pool for a reason other than merely maximizing rewards. Stake pools have a natural incentive to get as many delegators as possible so they can collect as many ADA in fees as possible - to do this, pools will do whatever it takes to advertise themselves and gain some kind of name recognition. This might be done through choosing a fun name for the stakepool, having an interesting backstory, donating some profit to a popular charity, or setting up an educational YouTube channel or other social media.

Stake pool operators will do a lot to promote their stake pool, as the more delegators they have, the more money they themselves will make from their stake pool operation. Their endeavor as a stake pool operator is essentially a small business operation, with the delegators being equivalent to their “customers”. Like all businesses, they need to advertise themselves to get and keep these customers.

This setup creates an incentive for stake pool operators to not only promote their own brand, but also to promote the Cardano network as a whole. The more stakepool operators that there are, the more competition there will be, increasing decentralization and further promoting the Cardano blockchain in the process.

ISPOs - Initial Stake Pool Offerings

There is another interesting use case for the stake pool mechanism that is being utilized by projects that are issuing their own tokens on Cardano.

Given that stake pool operators can increase their fees to whatever percentage they want, some pools are increasing fees to 100% but then distributing their own coin to the delegators. This means that delegators essentially give up, to their stake pool operators, all the ADA that they would have gotten from staking in exchange for whatever other token is being offered.

One popular example is the Genius Yield project that is currently under construction. This project had multiple stake pools set up with 100% fees so that delegators would get GENS tokens deposited into their wallet (usually through a third party mechanism like Dripdropz) while the Genius Yield team collects the full amount of ADA staking rewards from their block creation. Both sides win - delegators get a token that they believe will be more valuable in the future than the ADA they are giving up, and the Genius Yield team gets to keep all of the ADA generated from their stake pools every epoch. This mechanism is a low-risk way for investors to invest and for project creators to fundraise.

Chapter 3: Cardano's Evolution

The Five Eras

Taken from Cardano.org:

> *The Cardano roadmap is a summary of Cardano development, which has been organized into five eras:* ***Byron****,* ***Shelley****,* ***Goguen****,* ***Basho****, and* ***Voltaire****. Each era is centered around a set of functionalities that will be delivered across multiple code releases.*
>
> *While the eras of Cardano will be delivered sequentially, the work for each era happens in parallel, with research, prototyping, and development often in progress all at once across the different development streams.*

The Byron era formed the foundation of the network, the Shelley era allowed for decentralization, the Goguen era gave us smart contracts, Basho is concerned with scalability and Voltaire is all about governance.

These eras each represent an important dynamic of the Cardano blockchain. The sequential layout shows that there was an intentional roadmap in place from the beginning, with each era adding one more layer of complexity and functionality.

The logical sequence of

1. Decentralization
2. Smart Contracts
3. Scalability
4. Governance

reinforces Charles Hoskinson’s mission for Cardano - to build “an open platform that provides economic identity to the billions who lack it by providing decentralized applications to manage identity, value and governance”.

Decentralization of the network handles the “open platform” part, “decentralized applications” are built through smart contracts, “providing economic identity to the the billions who lack it” can only be done if scalability is handled, and on-chain decentralized governance is necessary to safely manage “identity and value”.

Decentralization: The Foundation of a Solid Blockchain

Every blockchain, in order to have any advantage at all over legacy systems, needs to be sufficiently decentralized such that attacks on the system by any minority of malicious actors can be rendered ineffectual.

A large part of blockchain functionality is the successful interaction between nodes in the system. Specifically, every node needs to have a current copy of the blockchain ledger and be able to receive and distribute data on that ledger. If any one node however were to be able to broadcast an update to the ledger that no other node had approved, there would be no “consensus” between nodes and the system would fail. Therefore, consensus between nodes is the essential factor in ensuring the efficacy of a decentralized system.

This ability to form a system-wide consensus was accomplished in the Shelley era of Cardano, when the stake pools were first put online. The establishment of stake pools in the Cardano ecosystem allowed for decentralization, as these stake pools acted as nodes in the network - each one storing and validating transactions to be added to the ledger. Individual ADA holders could delegate, or stake, their ADA with these stake pools and so give them more weight in determining how often they would produce a block on the chain. These stake pools are freely chosen by ADA holders, with the only incentive being the staking rewards that could be collected in exchange for the delegation to a stake pool. This staking mechanism is the backbone of the proof-of-stake consensus mechanism and allows both ADA holdings and the maintenance of the network ledger to be spread out among many people.

This initial layer was the foundation of the network as without decentralization occurring first, no other functionality would matter.

Even though the Shelley era established the basis for decentralization, there is continuous evolution of the degree of decentralization as we move forward into the future. As more stake pools are established (there are over 3000 as of this writing) more individuals will have a say in what gets written in the ledger and what does not. As more individuals buy ADA, the ADA holdings themselves will become more decentralized. Both forms of decentralization are important, especially in a proof-of-stake system where the largest ADA holders have the most say in the outcome of the system.

Smart Contracts: Next Generation Functionality

With the introduction of the Goguen era, smart contracts were enabled on Cardano. Smart contracts allow for the creation of dapps, or decentralized applications. These are programs that live on the blockchain and allow for users to interact with each other and exchange ADA in meaningful, practical or entertaining ways. One of the most prevalent types of dapps used on blockchains are DEXs, or decentralized exchanges. Examples in the Cardano ecosystem include Sundaeswap, Minswap, Muesliswap, and Wingriders. These DEXs are used to exchange one type of Cardano native token for another, and are only possible because of the smart contract code behind them.

DEXs also provide the foundation for DeFi, or decentralized finance. Becoming your own bank through the use of dapps is now entirely possible. Traditional banks are merely third party middlemen that coordinate the transfer of funds between individuals - that service is no longer needed now that smart contracts can act as the intermediary. ADA can be deposited and locked into smart contracts and then withdrawn at a later date, similar to a bank. Loans can be taken against collateral that you put at stake, similar to a bank. Interest can be accrued on assets that you deposit into the smart contract, similar to a bank. There are very few financial services that cannot be accomplished through savvy smart contract usage.

With the propagation of DeFi on Cardano, made possible by the implementation of smart contracts, this third generation blockchain officially enters the race against the current DeFi giant: Ethereum.

There are many other projects utilizing smart contracts in the works as well, including an ADA mixer that will allow users to essentially "wash" their ADA (removing traceability) and various play-to-earn type games.

Scalability: Opening up to the Billions

Scalability, or the ability of a network to accept new users without slowing down or crashing, is a highly focused area of research and development in the blockchain space right now.

Taken from the IOHK paper "Hydra: Fast Isomorphic State Channels":

> *Permissionless distributed ledger protocols suffer from serious scalability limitations, including high transaction latency (the time required to settle a transaction), low throughput (the number of transactions that can be settled per unit of time), and excessive storage required to maintain the state of the system and its transaction history, which can be ever growing.*

With Ethereum struggling with its incredibly high transaction fees due to network congestion, scaling solutions are being developed in all major blockchains at a rapid pace to enable the networks to continue their growth.

Cardano is no exception, and while it is still behind Ethereum in technological progress, the gap is quickly closing.

As I write this in 2022, Cardano is currently in its so-called "Basho era" - meaning that scaling is the primary priority right now. As mentioned previously, creating scalability is difficult in distributed ledger systems because security and decentralization would need to be compromised to do so. Therefore while the original blockchain layer can be optimized for better performance, true scalability requires new, faster networks to be built on top of the original "layer 1". With Ethereum this is already being done - such layer 2 scaling solutions, as they have come to be known, allow for the faster and cheaper use of the Ethereum network by running computations on another chain altogether.

Such scaling solutions will need to be implemented for Cardano also.

So to achieve a network that can scale effectively to accomplish Cardano's goal of "bringing economic identity to the billions who lack it", two things need to happen:

1. The layer 1, Cardano itself, needs to be optimized for speed and efficiency.

2. Layer 2 solutions need to be built on top of Cardano so transactions can be done there and won't clog the layer 1 network and render it unusable.

The official Cardano blog post on this issue of scaling divides the solutions into "on-chain" solutions (a.k.a. layer 1) and "off-chain" solutions (a.k.a. layer 2). I will defer to this reference for the technical details of these implementations, as blockchain scaling solutions can get very detailed and diverse and deserve a book all for themselves.

I will however mention the most important scaling solutions for Cardano so that you will be able to recognize and have a basic understanding of them when they are referred to in more detailed works.

On-Chain Optimization

Block Size Increase - the size of blocks on the blockchain can be increased to expand the data throughput of the system. A larger block size means more storage space for transactions. This upgrade is done easily, but the cost of doing so is that there will be greater hardware requirements for nodes in the system.

As block size is increased, there is always the risk that those nodes that do not have access to the required hardware will no longer be able to participate in the network. However, as the network grows and more nodes (stake pool operators) are added to the system, this is less of a worry.

Pipelining - this is a strategy to decrease the “dead time” between blocks, when the network is effectively doing nothing. The less time between blocks, the more transactions that can be recorded per unit of time.

Input Endorsers - allow transactions to be separated into pre-constructed blocks, thereby “endorsing” blocks before they are minted. This will speed up block propagation times and allow for greater transaction throughput overall.

Right now there is only one type of block, which carries transactions and allows for consensus in the network. With the implementation of input endorsers, there will now be two types of blocks - the slower propagating block that we currently have that will now be designated only for consensus, and a new, much faster block that will carry transactions. In this way, transactions will be streaming across the network constantly while validation of those transactions will still occur every 20 seconds or so as per the original block timing. This allows for vastly greater data throughput of the network.

On Disk Storage - by reconfiguring the blockchain code so that some data is stored on harddrives rather than in RAM, systems that have less RAM will be able to operate more efficiently.

Off-Chain, Layer 2 Scaling Solutions

Hydra - this is the most famous scaling solution for Cardano. It will consist of a few parts, but the most significant will be the ability to open something called “isomorphic state channels” between two parties. These state channels will allow endless, fast, and free transactions to occur between parties while the state channel is open, with only the final result of those transactions being recorded on the blockchain after the channel is closed. This setup will be referred to as one “hydra head”. True to the anatomy of the mythical creature, many such hydra heads will be opened up to increase the total throughput of the system as a whole.

An analogy that is often used to describe how this mechanism works is a game of poker. Using isomorphic state channels, something like a game of poker, with many transactions occurring between players, can occur with **only the final result** of the game being recorded on-chain. This will save a ton of work for the base layer as it will be converting potentially hundreds or even thousands of transactions into just one. This system will thereby free up space for other transactions on-chain. Transactions in this direct P2P format will cost virtually nothing, as they will not actually be stored or computed on-chain. In effect, there will only be one final transaction occurring when the hydra heads are closed.

The novelty of hydra heads is that they are *isomorphic* state channels, meaning that they can utilize smart contract code from the base Cardano layer rather than requiring an entirely new chain or new code to be written. This factor separates it from other layer 2 solutions.

Read more about Hydra and isomorphic state channels in IOHK’s paper “Hydra: Fast Isomorphic State Channels”.

Sidechains - these are additional, separate chains that will be connected to the main Cardano chain via a “bridge”. Value (ADA) will be able to move freely from one chain to the other. One such chain that is in development by IOHK is the “Mamba” chain. By expanding the ecosystem with an entirely separate chain, transactions and value will be able to flow back and forth between these chains while each chain maintains its own parameters and use cases.

For example, you could theoretically transfer value from a high security, low speed blockchain to a high speed, lower security blockchain to allow for increased data throughput and then transfer that value back onto the main chain to restore security. Sidechains can also be used to facilitate interoperability between layer 1 chains, thereby opening up new ecosystems, users, dapps, and programming languages to each of the connected layer 1 systems.

A sidechain that is currently in operation is the Milkomeda C1 sidechain produced by dcSpark. Milkomeda, so named for the collision between the Milky Way and Andromeda galaxies, is a protocol that forms the foundation for the sidechains being built by dcSpark and allows interoperability between layer 1 main chains. The C1 sidechain is the first sidechain built by dcSpark through the Milkomeda protocol and also the first operational sidechain in the Cardano ecosystem. This sidechain specifically bridges the Cardano ecosystem with the Ethereum ecosystem, allowing value to flow between them. Through a novel invention called “wrapped smart contracts”, Cardano users will also be able to access smart contracts that are housed on the Ethereum blockchain without ever needing to move their assets off of Cardano. This type of sidechain that is acts as a bridge between two layer 1 networks helps both of them to scale by allowing the users of each system to utilize the computing resources of the other.

Orbis is another sidechain that is currently in development. While this project will not serve as a bridge to another ecosystem, it does act as a way to increase the throughput of Cardano transactions while still maintaining the security of the base layer. It can do this through a technology called “zkSNARK rollups”. This novel method allows a layer 2 to take transactions from the main chain, process them, bundle the outputs together, and submit them to the main chain in a way that proves that they were executed as intended. These transactions that are executed on the sidechain will never be recorded on the ledger of the main chain - only the outputs that are delivered from the sidechain will be recorded. This allows for greater transaction throughput for Cardano, as less data overall needs to be processed and recorded.

Mithril - named after the extremely light but extremely strong metal of Middle-Earth, this update promises to increase speed and efficiency through the optimization of multi-signature transactions.

These scaling solutions are being developed as a part of the Basho era of Cardano, and are the main focus of development in 2022. Even after we transition into the Voltaire era and shift focus to governance, scaling solutions will continue to be implemented as the network makes room for the billions.

Network Governance and Project Catalyst

One of the main focal points for Charles Hoskinson was the creation of the element of sustainability in the Cardano ecosystem - however, Charles has a slightly different meaning of the word than you might think. When most people hear the word “sustainability" they think of environmental impact, resource conservation, low carbon footprint, etc. While environmental impact isn’t a trivial issue in the cryptocurrency space, this is not what Charles is referring to. He means that blockchains, in order to stand the test of time, must be able to grow themselves and adapt to changing circumstances and thereby “sustain” themselves forward into the future. IOHK, The Cardano Foundation, and Emurgo may not always be around to facilitate the development of the blockchain protocol and so it would be wise to put a system in place that would allow for the users themselves to change and upgrade the network. In this way, Cardano takes on a sort of immortality so long as it has a user base that is still willing to put in work to keep the network alive.

This framework of sustainability is often referred to as “governance”, as it is the system of consensus that allows for the rules to be changed and updated as we move forward in time, similar to a nation-state’s government.

Project Catalyst is a primary part of Cardano’s built in governance infrastructure. It is a system that assures continuous improvement in the network through incentivizing community innovation.

Funding is offered to software developers and others who are willing to work to improve the network. They submit project proposals and try to convince the community that their project is worth funding.

Funding for these projects is allocated from the ADA “treasury” that is built into the monetary policy of Cardano. This treasury is composed of funds taken from the transaction fees that are collected by the network with every transaction sent, as well as the ADA reserve that has yet to be disbursed into the network.

As with almost everything in the crypto world, participating in this system comes with a monetary incentive - **voters** get rewarded in ADA for voting on project proposals, **Community Advisors** get rewarded for writing assessments, or reviews, of project proposals, and **Veteran Community Advisors** get rewarded for judging the quality of Community Advisor assessments.

This three-tiered system minimizes, but unfortunately cannot eliminate, fraud, waste and abuse in the Project Catalyst funding mechanism.

The workflow of Project Catalyst is as follows:

1. Anyone can submit project proposals to the system and ask for funding for their project.

2. So-called “Community Advisors” sort through proposals that are submitted by the required date to ensure they contain all necessary details. These Community Advisors will write up assessments for proposals and judge them based on three factors: **Impact**, **Feasibility**, and **Auditability**. Proposals submitted on Project Catalyst, in order to ensure their legitimacy and promote the highest rate of project completion, should only be funded if they can adequately meet this criteria. Projects should be a relevant solution to the problem they are trying to address (**impact**), they should be reasonably possible to complete by the team submitting the proposal (**feasibility**), and there should be some amount of transparency as to what has been completed already (**auditability**).

3. After assessments are written by the Community Advisors, a higher class of reviewers called “Veteran Community Advisors” review these assessments to ensure they themselves are quality reviews. Veteran Community Advisors will give each assessment a rating of “excellent”, “good”, or “filter out”. Excellent assessments earn three times more rewards than good assessments, and assessments that are filtered out are not rewarded at all.

4. ADA holders who register with the Project Catalyst App are able to vote on these proposals to determine if they will be funded or not. The vote of each ADA holder is weighed in proportion to the amount of ADA they hold in their wallet, thereby allowing those with the most stake in the network to have the most influence on future projects.

After the completion of each round of voting, a results list is published that serves as a record of all of the projects that were voted on and whether or not they received enough votes to be funded. For example, in Catalyst Fund 7 the project “Haskell and Coffee” was voted to be funded and the requested budget of $8200 was granted. This is a small project with the goal of creating an online meetup space that will allow veteran Haskell developers to connect with newcomers to the space so that the next generation of programmers can learn to code in the base language of Cardano. There were also much larger projects that were funded, such as the project “Defending Cardano Staking Ecosystem” which was granted $39,500 to build a system that will help monitor the risk of antagonist or careless stake pool operators and thereby help to secure the blockchain as a whole.

Each fund has many such project proposals divided into several different categories, each with a dollar amount allocated to it. Projects compete for votes to obtain a portion of the money allocated for their particular category. Those projects with the most votes get funded first and so on down the list until all of the money dedicated to the category is exhausted.

In this way the community of ADA holders gets to decide who they will “hire” to improve the network. If they choose correctly, and the proposal submitters honestly follow through on their work, the entire ecosystem benefits and, theoretically, ADA will increase in value. This creates a sort of feedback mechanism that provides the incentive for all Catalyst participants - voters, proposal submitters, community advisors, veteran community advisors - to act honestly. The better the Cardano ecosystem becomes, the more likely ADA holders are to see an increase in the value of their coin. In this way, through financial incentive, decentralized autonomous government can exist.

Chapter 4: Use Cases

It is important to understand that cryptocurrencies in general, and ADA in particular, have definite use cases beyond merely holding the coin and treating it like a stock. The monetary value of cryptocurrencies are often tied to their potential utility and the willingness of people to actually use the network. Therefore, a proper assessment of a coin’s potential value will always include an understanding of its use cases.

Real World Use Case: Banking the Unbanked

In 2014 Charles Hoskinson gave a Ted Talk entitled “The Future Will Be Decentralized”, where he gave a concise outline of the documentation and record keeping problems in the so called “unbanked” world.

In first world countries, the banking system is something taken for granted. Almost every individual has a bank account, a credit score, personal identification such as a driver’s license and birth certificate, a deed to a house, a title to a car, a degree from a university. There are ways of verifying a person’s credentials and ownership over their property because everything is recorded somewhere. In less developed countries, this is not necessarily the case. The information infrastructure is not always there to allow for the correct identification of property and credentials.

This verification issue is sometimes seen in certain rural regions of more developed countries like China and India, but it is generally considered to be much worse in less developed countries such as Sudan and Afghanistan.

Charles Hoskinson saw, even at this very early stage of blockchain development, the potential that decentralized systems held as far as being able to fill this technology gap.

When people think of blockchain technology, they usually think of cryptocurrencies and all of the monetary benefits that come from using digital money. While these uses are of course not negligible, the potential use of storing credentials and records of property ownership on an immutable, distributed ledger system will turn out to be far more valuable to most of the world.

In the same way that currency transactions can be forever recorded on a blockchain, information such as college degrees, car ownership and personal identification can also be stored on a blockchain through the creation of specialized tokens for this purpose. Proof of ownership can then be confirmed as easily as one views his balance in his crypto wallet.

Real World Use Case: Decentralized Finance

Decentralized finance, or DeFi, is another use case of cryptocurrency generally and Cardano specifically. DeFi is not merely a way to provide banking services to those who currently do not have access - it is instead an entirely new type of banking service altogether. Instead of working with a centralized entity like a Chase or Wells Fargo, customers of a DeFi system simply make exchanges with other customers in the system, regulated only by software. There is no person in direct control of DeFi services, and this carries advantages and disadvantages. On the plus side, it ensures that no one can cancel or limit the use of these financial services, as sometimes happens in the legacy banking system. On the negative side, if something goes wrong, there is no one to call who has the power to issue refunds or reverse transactions. Either way, DeFi is a radical new financial technology that can push the agenda of global financial freedom for the average individual.

Real World Use Case: Store of Value

Like bitcoin, ADA also can be used as a store of value to hedge against the rising inflation of fiat currency. ADA has a maximum fixed supply, with a reserve supply that slowly comes into circulation - very similar to bitcoin’s tokenomics. As the supply is fixed, there will only ever be 45 billion ADA. This means that with increased usage of the Cardano network and higher demand for ADA, its value will only continue to rise.

This is in contrast to fiat currency, which gets devalued as the central banks print more money to fund government endeavors.

ADA, like every other cryptocurrency, is currently heavily tied to the price movements of bitcoin. However, we are starting to see that bitcoin is becoming decoupled from the price movements of the legacy stock market. This might be an indicator that investors are starting to use bitcoin and other cryptocurrencies as a hedge against the value of fiat and the rest of the financial markets, making them a good store of value in an otherwise declining environment.

Real World Use Case: Investment Opportunity

When an investor purchases shares in a company, they are not actually buying anything of value.

What I mean is, shares do not have intrinsic value aside from their perceived value in the market. Shares cannot be used as a currency, shares cannot be traded directly from person to person, shares cannot be taken with you or stored separately from an exchange.

Shares are actually fully disconnected from the performance of the issuing company. Share price can be extremely overvalued or extremely undervalued compared to their company's income and growth. Shares only have value because the market says they do, and investors are willing to pay a certain price to own them. Were investors to simply cease all interest in a particular stock, its value would plummet as no one would be willing to buy it and everyone would want to sell it. This sort of situation is possible even with the company itself doing well.

What I am getting at is that there is only artificial demand for shares in a company. There is demand only when it is expected that there will be higher demand in the future. Shares exist solely as speculative instruments, with no inherent utility in and of themselves.

This is not the case with cryptocurrency, and especially isn't the case with ADA. ADA draws its value not only from speculation, but also from the demand that is created by its usage on the Cardano network. As the network grows and attracts more users, more developers, and thus more dapps, the utility of ADA increases as well. Higher demand coupled with fixed supply forces value upwards.

Therefore ADA, unlike legacy financial instruments, becomes both a speculative asset and a utility asset all in one.

Real World Use Case: Decentralized Identity and RealFi

Decentralized identity, or DID, is a major area of development in the blockchain space. While no one DID brand has garnered widespread commercial application as of yet, there are a few projects working in this direction on the Cardano network.

These projects aim to store real-world issued credentials on the blockchain so that they may be retrieved and verified at any time. Because of the nature of the blockchain, once credentials are stored on-chain and attached to an online identity, centralized institutions and government agencies will be able to easily, quickly and certainly verify the identity of users.

Imagine logging on to IRS.gov or your student loan holder or your online bank account and with one click having your verified digital identity transferred into their system. A new username and password for every website you visit would be a thing of the past - all of your accounts would be linked to your digital identity.

The demonstration that is set up for Atala PRISM on their website, https://www.atalaprism.io/, shows the ease with which credentials can be verified and linked to a smartphone app. It also demonstrates the future necessity of such credential verification.

By storing credentials on a blockchain and attaching those credentials to a digital identity, we now have the ability to create **reputation** - which allows for all sorts of advantageous applications.

People of the third world - that is, the developing world - often do not have the means to prove credentials or manage reputation. This greatly impedes events that first worlders take for granted, like getting a mortgage for a house, opening an investment account, or proving graduation from an academic program. With DID services like Atala

PRISM or IAMX that are launching on the Cardano blockchain, anyone with access to a smartphone will be able to record and store their credentials digitally - making it much easier for governments and corporations to verify reputation. This will open the door to opportunities that require some degree of trust or risk assessment.

Real World Use Case: NFTs and Supply Chain Tracking

It is true that a blockchain is fundamentally a record of transactions, but the transactions that are recorded are often linked to data that goes beyond mere additions and subtractions of the blockchain's native currency. This other data can be stored in the form of NFTs, or **non-fungible tokens**. NFTs can be moved around the blockchain similar to how coins like ADA are moved, from wallet to wallet. The main difference between the two however is that 1 ADA is the same as every other ADA, while each NFT is different and identifiable from every other NFT. This attribute of uniqueness allows NFTs to broaden the use case of blockchains greatly.

One way that Cardano specifically is using this technology is to implement the tracking of supply chains and verifying the source of certain goods.Charles Hoskinson, in his 2022 address to the U.S. House Subcommittee on Commodity Exchanges, Energy and Credit, notes that the American beef industry has a need for digital tracking solutions to ensure quality, sourcing, and freshness. He says,

> *Looking, for example, at the beef industry, blockchain technology can be used in many ways including creating significant value for the industry's end-to-end supply chain and more over sustainability and safety, such as grass-fed assurance, trade finance, consumer engagement, consumer feedback, certification and end-to-end traceability.*

IOHK's solution to supply chain tracking is called Atala TRACE and has actually already been used to track the authenticity of wine in Georgia. There currently is not a lot of data on how exactly the system works from a technical perspective (IOHK most likely does not want other companies to simply copy their solution) but it can be inferred that the solution involves the creation of an NFT which contains data on a particular product, and that NFT is linked to a physical QR code that is printed on the product’s container. The QR code will allow a consumer to verify the legitimacy of the NFT as well as the NFT’s location on the blockchain. As the product moves along its supply chain, the NFT will move as well, from wallet to wallet and thereby create a traceable pathway from the originator to the end consumer. The beauty of blockchain technology is that every transaction is publicly verifiable, which means there will no longer be any need to simply “trust” a vendor that they are giving you what is advertised - you will be able to assure yourself that what you are buying comes from the original manufacturer.

Chapter 5: Progress and Expansion on the Cardano Blockchain

NFTs as Art

NFTs (non-fungible tokens) have gained great popularity in the mainstream world recently, especially with certain celebrities and influencers. The way that these NFTs are currently being used however is mostly for art and entertainment purposes rather than anything truly practical.

Non-fungible tokens, each one being wholly unique on the blockchain, are often tied to digital works of art such as .jpgs, .gifs, or audio/video clips. This mechanism however does not really mean that you “own” that .jpg file or whatever it is, but it merely means that you own this one specific link to that .jpg file.

If you show off your NFT on any digital space, another person may simply right click on the image and “save as” in order to steal the image for themselves. They can then take that image and mint their own NFT, thereby also having an NFT of the same file.

Despite this, NFTs have gained so much popularity that they are being used even by those who know very little about crypto and instead are only interested in collecting the work for art’s sake.

The innovation here is not that NFTs allow you to own digital art, but that we now have a way to put a sort of digital signature on artwork that allows for a proof of authenticity to be passed on from seller to buyer. No matter who the NFT is sold to later on down the line, the buyer will be able to verify that what they own is indeed from the original artist. An additional benefit to minting your artwork as an NFT is the possible addition of royalty code - meaning that every time your NFT is sold to a new buyer, a portion of that ADA that was spent on the purchase will be automatically transferred to your wallet. This is quite an advantage and an incentive for artists who have never otherwise been able to enforce royalty payments.

NFTs, while most popular through the Ethereum blockchain, have been gaining popularity on other blockchains such as Cardano due to the extremely high transaction fees required on Ethereum. Cardano NFT (CNFT) marketplaces have opened up that allow for the buying and selling of virtual art as NFTs, including jpg.store and cnft.io.

Average, non-coding users of the Cardano blockchain can also mint their own NFTs using their own artwork (or any image file, really) fairly easily. One such platform is nft maker pro. This platform is detailed and specific and made for serious NFT artists. For a simpler, less detail intensive experience, try Cardano-Native-Token or minterr.io.

Speaking the Language of Cardano: Plutus and Haskell

Cardano is unique in its choice of programming language - it is coded in a language called “Plutus”. Plutus is a slightly modified version of the better known programming language “Haskell”.

Haskell is not a widely used language, which is why Charles Hoskinson continues to be criticized by the developer community for the choice. The fewer people that use a language, the less developers there are to help contribute to your project and the less tools there are to help the few devs that do know the language.

Nonetheless, Charles sticks by his decision, citing the fact that Haskell is a “high assurance” purely functional programming language. “High assurance” here essentially means that although Haskell code is generally considered difficult to write in comparison to other languages, when it is written correctly the code is very error-resistant. This is mainly due to its nature as a purely functional programming language - there is no “state change” as with object-oriented and imperative programming languages. This lack of state change means that once you define something in terms of code, it stays defined in that way forever and cannot be altered. This removes a major source of “bugs” from the code. This feature can, however, be frustrating for developers as it requires a different way of thinking about programming.

Charles Hoskinson himself, when questioned about the difficulty of the language, compares the difficulty of Haskell to the difficulty of using surgical tools - implying that this difficulty is not without purpose.

There is much, much more to learn about the difference between Haskell and the languages used by other blockchains and the advantages and disadvantages of each choice. I will not address all of that here, but if you are interested in going down this rabbit hole I would suggest the following resources:

Cardano Forum: Why Cardano Chose Haskell and Why You Should Care

Youtube: Charles Hoskinson Explaining Why Haskell Was Chosen In An Interview

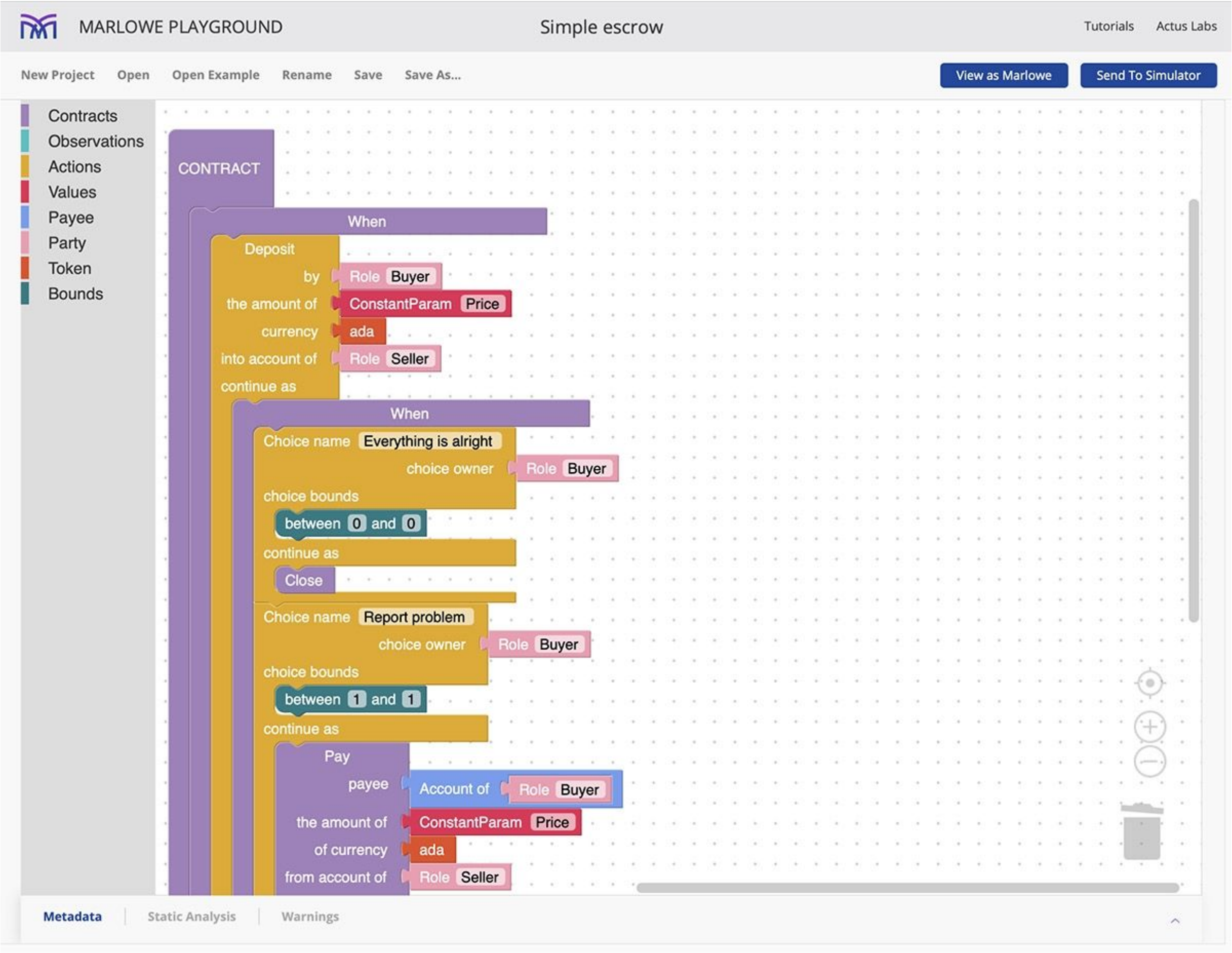
The most popular book for learning Haskell: Learn You a Haskell for Great Good (not made for non-coders unfortunately)

Marlowe: Bringing the Power of Programming to the Financial Industry

Marlow is another programming language that is used in the Cardano ecosystem. Marlowe is what is known as a "domain specific language". It is a highly specialized form of Haskell, narrowed down so that it is easier to use and fewer mistakes are possible. It is designed specifically for the building of financial contracts by people who may be experts in finance but unskilled with coding.

This is accomplished by integrating the code with a visual builder, such that instead of the user seeing strings of code that they would need to manipulate, they simply drag and drop boxes in the correct sequence to form the contract they would like to build.

See example below.



```
CONTRACT
  When
    Deposit
      by Role Buyer
      the amount of ConstantParam Price
      currency ada
      into account of Role Seller
      continue as
        When
          Choice name Everything is alright
            choice owner Role Buyer
            choice bounds
              between 0 and 0
            continue as
              Close
          Choice name Report problem
            choice owner Role Buyer
            choice bounds
              between 1 and 1
            continue as
              Pay
                payee Account of Role Buyer
                the amount of ConstantParam Price
                of currency ada
                from account of Role Seller
```

[Introduction to Marlowe](https://developers.cardano.org/docs/smart-contracts/marlowe/) (https://developers.cardano.org/docs/smart-contracts/marlowe/)

When Marlowe is fully finished, it will allow non-programmers to easily write smart contracts and publish these on the blockchain - thereby further widening the scope of potential Cardano users.

How Cardano Can Be Used: A Summary of Projects

As this space is moving forward technologically at breakneck speed, it would be impossible to record **all** current and upcoming projects here with any real accuracy.

Instead, I can point out the major projects that have already launched on Cardano and those that are scheduled to launch in the near future.

Cardano, the blockchain itself, is only the base layer of the Cardano ecosystem. For the ecosystem to have any real value, the apps that are built on top of the blockchain need to themselves be useful.

Cardanocube.io is a primary tool that can be used to monitor projects on the network. It features a comprehensive list of current and future projects divided into categories such as DEX's, Wallets, DeFi, Marketplaces, Infrastructure, Launchpads, Metaverse, Gaming, Social Media, Lending Services, Stablecoins, Oracles, Identity Management, Payment, Data, Gambling, Community Projects and, of course, Meme Coins.

There are many, many projects launching on Cardano currently, with more constantly being added as developers see the opportunity that Cardano holds. The top projects will change from month to month, as older projects are completed and released and newer projects are dreamt up. Therefore, do not take this list as exhaustive, and do your own research on Cardanocube.io, Builtoncardano.com, or Buildingoncardano.com.

I can't guarantee that these projects are going to work as intended, or that they will even exist by the time you read this, but I tried to curate a list that I believe will stand the test of time.

Here are, in my opinion, the projects with the **highest potential** on Cardano right now:

Muesliswap: The first DEX built on Cardano, it is built on an order book structure and so does not feature liquidity pools or yield farming. It is a simple model of requesting a quantity of a particular token to buy or sell, and hoping that another user will fill that order. It is simple and easy to use, and is often faster than AMM DEXs.

Sundaeswap: The second DEX built on Cardano after Muesliswap, Sundaeswap features an automated market market (AMM) structure that allows for the creation of liquidity pools and yield farming. Users can deposit ADA along with other Cardano tokens into liquidity pools on the Sundaeswap app, receive liquidity provider (LP) tokens to represent their monetary deposit, and then stake those LP tokens to receive a reward over time.

Genius Yield: Branded as an “automated yield optimizer”, this DEX uses AI technology to democratize DeFi and grant its users access to the best possible yield farming opportunities.

Maladex: Another DEX, marketing itself as the “research driven Cardano DEX”. The Maladex team is working on restructuring the mathematics behind liquidity pools in order to reduce the risk of the impermanent loss. Maladex also put together a well written blockchain glossary as a way of contributing to the growth of the space.

ErgoDEX: A DEX on both the Ergo blockchain and Cardano blockchain, allowing for liquidity exchange between the two ecosystems. This is possible due to both blockchains being built on the eUTXO model.

Cardano Mixer: A fully decentralized protocol that allows for anonymity between sender and receiver in a transaction. Funds are sent into the smart contract, held there for a period of time, and then withdrawn. Funds that are withdrawn can never be traced back to the original depositing address.

ADA Handle: A way to “name” a wallet address. Cardano users can purchase a wallet name so that instead of sending to an address that looks like: addr8gqjnpvehqrtpd4g414fcaq7k1u…

The address could be something like “MyMainAccount” or “JoesWallet” or even a very short string like “50”. Each of these names is of course unique, so it is expected that there will be a market for these names to be bought and sold and the “good” names will get taken fast. Also, the shorter the character string, the more valuable and rare the name will be.

The wallet names will be recorded in an NFT, so that the wallet that holds the NFT will also hold the wallet name that the NFT represents. This will allow for the trading and sale of wallet names between users.

Liqwid: A DeFi platform that includes loans and lending services. With this platform, users will be able to borrow stablecoins like djed as well as other currencies by using ADA as collateral. This enables users to withdraw liquidity from their ADA without having to sell it. On the opposite end of the deal, other users can lend out their ADA and provide liquidity to the system, thereby earning interest on their holdings.

Meld: A DeFi platform based specifically around turning crypto into cash through collateralized loans. There will also be functionality to “meld” other cryptos into the Cardano ecosystem, through creating wrapped versions of crypto assets that are native on other chains.

World Mobile Token: A project that seeks to bring internet connectivity to the roughly 50% of the world population that has limited access. Starting with Africa, World Mobile will deploy infrastructure to distribute wifi to underserved populations on a global scale.

Wingriders: Billing itself as “The DEX on Cardano” and featuring a superhero-like mascot with a W on his chest, Wingriders is a feature rich decentralized exchange with a beautiful user interface.

Liquidity pools are open for business and decentralized governance is planned for the future.

Milkomeda: A sidechain project built by dcspark that allows the Cardano ecosystem to interact with assets on the Ethereum ecosystem. It acts as a sort of bridge to allow ADA holders and ETH holders to interact with dapps on the other's blockchain.

Djed: An algorithmic stablecoin that was first designed by IOHK researchers and is now being implemented by a company by the name of COTI. This stablecoin will be pegged to the U.S. dollar and will maintain this price point by using a smart contract to control reserve funds, like a sort of automated banking system.

Babel Fees: Paying Cardano Transaction Fees with Native Tokens

A unique feature of the Cardano blockchain is the development of what is being termed “babel fees”. This technology allows a Cardano user to pay transaction fees in **any** native token that exists on the blockchain. Most other chains, Ethereum included, force the user to pay for their transaction fees with one specific currency - ETH for Ethereum, LUNA on the Terra blockchain, ATOM on the Cosmos blockchain. Cardano is the same way, with all transaction fees being paid in ADA, even if you are only moving other, non-ADA coins. With the implementation of babel fees however, users who would like to move a quantity of WMT (World Mobile Tokens) for example would be able to pay the required fee to move those coins in WMT itself - meaning that no ADA would need to be held in the wallet.

This allows for incredible customization of the Cardano blockchain and fuels the momentum and legitimacy of the projects that have minted their own tokens. ADA will still remain the “reserve currency” of Cardano, and all prices will still be denominated in ADA, but ADA will not be strictly needed at all. If an investor wants to own a wallet consisting entirely of a certain project’s tokens, they will be able to do that.

Non-ADA tokens however will not be automatically taken in place of ADA. Stake pool operators, which validate transactions, must be willing to accept certain tokens instead of ADA. They would also dictate the value of the exchange rate between these coins. In this way, no one is forced to accept anything and all transactions and fees will be based upon mutual agreement.

Taken from IOHK’s blog post on babel fees:

> *The mechanism is of course conditioned on the presence of liquidity providers that possess ada and are willing to issue*

matching transactions. In fact the mechanism creates a market for such liquidity providers. For instance, a stake pool operator (SPO), can publish exchange rates for specific tokens they consider acceptable. An SPO can declare that they will accept tokenX for an exchange rate 3:1 over ada. It follows that if a transaction costs, say ₳0.16, the transaction can declare a liability of ₳0.16 as well as offer 0.48 of tokenX. In the native asset model of Cardano this can be implemented as a single UTXO carrying a token bundle with the following specification (Ada→ -0.16, tokenX→0.48). Note the negative sign signifying the liability.

Chapter 6: Philosophy and Vision

Cardano: The Optimal Expression of a Libertarian Vision

Charles Hoskinson openly admits his involvement with the 2008 Ron Paul presidential campaign. He actively worked to get Ron Paul elected president back then, and he clearly carried forward the values of personal freedom, individual rights, and government transparency that led him to support the candidate originally.

Ron Paul is a fierce advocate of “ending the fed” - that is, pulling the monetary system away from the oversight of a central banking entity like the U.S.’s “federal reserve bank”. He insists that fiat currency as it is currently used, as centralized as it is, leads to a host of perverse economic incentives and inequities that would not exist in a freer, more open and less centrally regulated environment.

Bitcoin (and cryptocurrency in general) is a natural answer to the overregulation inherent in fiat currency - bitcoin is limited in supply, not controlled by any central entity, cannot be stopped or shut down by legislation alone, and can be transferred directly from person to person relatively cheaply and quickly.

One of the fundamental principles of cryptocurrency is that the greater the level of decentralization of a blockchain, the more secure it is and the more free it is. Higher degrees of centralization lead to vulnerabilities due to an excess of influence from a small group of actors. Keeping your money with a totally centralized entity means that you have virtually no control over your funds unless the holding entity permits it, while putting your funds into a decentralized system means that you truly have control over where they are moved to.

Libertarianism takes this exact principle and applies it to political systems rather than just financial systems. While the field of libertarians is diverse, in general it can be said that these lovers of freedom prefer greater decentralization of political power across all sectors of government. It is their philosophy that the greater the centralization of power, the more likely that power is going to be abused and taken advantage of by the controlling entity. One particular example of this is that libertarians are generally proponents of states rights in the U.S. - meaning they seek to empower the right of state governments to enact legislation that is contrary to the will of the Federal government. In this way, the United States as a whole becomes further decentralized - the “nodes” of the network (that is, the 50 states) become more powerful in relation to the highly centralized federal government.

Going down scale even further, counties within states each have their own government, and these can be empowered in relation to the state government so that even each of the 50 nodes of the nation-wide network have their own network of even smaller governments. This system would continue to scale down this way, with every node having its own network of nodes. Decentralization exists in proportion to the power distribution of lower nodes to higher nodes. The more power that is concentrated lower on the scale, the less able the higher nodes would be to take advantage of their position.

Cardano takes this basic libertarian principle of decentralization and implements it not just in its monetary policy but also in its consensus mechanism and its governance system. The way that delegators and stake pools are incentivized (there are over 3000 stake pools as of this writing) plus the Project Catalyst Voting system (all stakeholders get a vote in proportion to their ADA holdings) make for a very decentralized, and thus very libertarian, blockchain network.

Advice to IOG: My Vision for Cardano

I know, I know. Who am I to be giving advice to IOG? I'm just a fan. A supporter. A user.

But as a user of blockchain technology, I can see trends. It's the reason why I'm throwing my chips in with the Cardano ecosystem in the first place.

So here's the rub - this is how you make Cardano successful.

First of all, don't try to directly compete with Ethereum. We aren't going to win. They are just too far ahead of us. Instead, we need to be a different type of blockchain. We need to be the "other" blockchain. The one that started off a bit behind, but has something new and innovative to offer the space. The one that might be slower to market, but does what no one else can. The Apple to Ethereum's Microsoft, if you will.

We are behind on DeFi. We are behind on NFTs. We are behind on transactions per second, DEXs, and ease of development.

So where is our competitive edge?

…
…
…

Digital Identity.

We are the blockchain that has a solution to this. This is where Cardano is going to shine.

Governments, and the internet at large, can no longer rely on Facebook, Twitter, Google and the like to provide digital identity. We have seen what these tech giants are willing to do to silence any form of political opposition. In the past days of the nascent Web 2.0, the then prepubescent social media giants were forced to allow dissident opinions on their platforms - they needed the traffic. These days, due to the de facto monopoly held by the big 5 - Facebook, Instagram, Reddit, Twitter and YouTube - users need these companies more than the companies need users.

Accounts are being banned left and right for doing nothing more than expressing widely held political or philosophical opinions. In the current version of the internet, your digital identity is only yours so long as you obey the every whim of the people in power. For most people, these are unacceptable terms.

Digital identity of citizens cannot be held by a centralized company that serves its own private interests - this will never be a fair system. After all, we currently live in a world where anyone can be deplatformed based on their religion, race, politics or country of origin. Private companies have more than shown their willingness to enforce their own ideological supremacy through the manipulation of digital identity. So long as private companies hold the keys to digital identity on the internet, they have massive power and they will use that power to silence and control the individuals who use their platform.

Therefore a tremendous opportunity has been created for a non-biased digital identity solution to come about. And as the only way to truly ensure something is non-biased is to decentralize it, the only current solution to this problem lies within blockchain technology.

This is where the future of Cardano sits. It may be with the Atala PRISM project or some other similar project, but however it’s done, Cardano needs to be the leader in digital identity if it is going to survive.

Appendix A: Bibliography of Relevant IOG Academic Papers

Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol

Cryptocurrency Egalitarianism: A Quantitative Approach

Filling the Tax Gap Via Programmable Money

Djed: A Formally Verified Crypto-Backed Pegged Algorithmic Stablecoin

Incentives Against Power Grabs or How to Engineer the Revolution in a Pooled Proof of Stake System

Standardized Crypto-loans on the Cardano Blockchain

Cardano Disaster Recovery Plan

SoK: Blockchain Governance

Appendix B: Glossary

Airdrop: a deposit of cryptocurrency into a wallet, usually for free and usually into multiple wallets. Airdrops are generally used as incentives or promotional tools to direct traffic to a new dapp or protocol.

Altcoin: any coin other than Bitcoin. The current largest altcoin is Ethereum.

Bitcoin: The first, largest, and most decentralized cryptocurrency to date.

Block: one unit of a blockchain. A collection of transactions that can be referenced by its number, e.g. “block 324566”.

Blockchain: A distributed ledger system that maintains an immutable record of transactions in a network. It is the foundational technology for Bitcoin and other cryptocurrencies, and it is what allows those currencies to be used as a store of value and a medium of exchange.

Byzantine Node: an “enemy” node, or a node that acts contrary to the interests of the system as a whole.

Charles Hoskinson: founder of Cardano, and co-founder of Ethereum. CEO of IOG (formally IOHK).

Cryptocurrency: digital money which represents a portion of the total value of a distributed ledger system, or blockchain network.

DAO: stands for decentralized autonomous organization. It is an organization that is not run by any person or entity, but acts automatically based on the input of its users.

Dapp: stands for “decentralized application”. This would be any app that functions on a decentralized blockchain.

DeFi: decentralized finance. The trading, lending, borrowing, etc. of cryptocurrencies through decentralized exchanges and applications. It is a way to use bank services without the centralized control of an actual bank.

DEX: decentralized exchange. A primary point of infrastructure for decentralized finance, these allow the exchange of one token for another within a blockchain network. One deployed, exchanges on DEXs are done automatically and not facilitated by any company or person and therefore cannot be stopped.

Distributed Ledger System: this is the type of technology that “blockchain” would fall under. Blockchains are a software solution to the problem of how to distribute a ledger system. It is called a “ledger” system because the main purpose of a blockchain is to maintain an immutable record of transactions. It is “distributed” across many nodes because that is how it remains immutable.

Ethereum: The most popular smart contract platform, and the blockchain that hosts the second most popular cryptocurrency after bitcoin. The original founder and current leader is Vitalik Buterin.

Liquid Democracy: a hybrid between representative democracy and direct democracy. Each voter in the system can choose to vote directly on an issue or delegate their vote to someone who they believe is more qualified to make the decision.

Node: one component part of a network. In distributed ledger systems, nodes act to validate data by coming to a consensus about what transactions should be recorded in the ledger. The greater the number of nodes, the greater the network decentralization.

Project Catalyst: the governance system of Cardano, which allows users to submit proposals for projects that will improve the ecosystem. ADA holders vote on these proposals to determine if they will be funded from the Cardano treasury or not.

Reserve: the ADA that is not in circulation currently. The total amount of ADA that has been created minus the amount that is currently in circulation. The reserve is used to fund block rewards and the Cardano treasury.

Satoshi Nakamoto: creator of Bitcoin and author of the 2008 whitepaper explaining what Bitcoin is. Satoshi Nakamoto is a pseudonym, and the true identity of this person or group of people is unknown.

Seed Phrase: a list of 12, 15, or 24 words that allow a user to access their wallet. Each wallet has a unique seed phrase. No other information or identity check is required to open a wallet other than its seed phrase.

Treasury: a collection of ADA that is set aside for the purpose of distributing funding to the project proposals of Project Catalyst. The treasury is filled through taking a portion of transaction fees and ADA in the reserve.

Stablecoin: a token that is pegged to the price of a fiat currency, usually the U.S. dollar. There are two main categories of stablecoin: algorithmic, and asset-backed. Algorithmic stablecoins maintain a stable price through increasing and decreasing the supply of the coin, by minting and burning it through a smart contract. Asset-backed stablecoins are created through purchasing them with fiat, commodities, or other cryptocurrencies, and thereby deriving their value from those assets.

Staking: cryptocurrency may be “staked” in a proof-of-stake system. This means that a node shows the network how many coins it has and thereby receives the opportunity to create blocks in proportion to the number of coins staked and receive block rewards in proportion to the number of blocks created.

Reserve: The Cardano reserve refers to the ADA that is a part of the total ADA supply but is not yet in circulation. The reserve is used to fund staking rewards and project catalyst proposals.

Vitalik Buterin: creator of Ethereum and its current leader.

Web3: web1 was the read-only internet, where users either created a webpage or read that webpage. It was highly decentralized, as each company had their own separate website and there was little interaction between websites. Web2 was the interactive internet, where users could easily create content on webpages that they did not own (e.g. social media). This version of the internet was highly centralized, as most activity was done on only a handful of centrally controlled social media websites. Web3 will be much more decentralized, as it will be an internet built on top of blockchains and thereby resistant to the influence of centralized entities.

Yield Farming: the process of lending out funds to earn an interest rate. Cryptocurrency is deposited in a liquidity pool to provide funds that will be used by traders to swap between tokens. Fees are paid by traders every time a swap is made, and a portion of those fees will go to the liquidity providers as interest on their investment.

Appendix C: Vetted links to Cardano News and Information

https://adapulse.io/

https://cardanojournal.com/

https://www.coinbase.com/learn

https://roadmap.cardano.org/en/status-updates/

https://www.essentialcardano.io/

https://iohk.io/en/blog/posts/

https://www.adatainment.com/

https://defillama.com/chain/Cardano