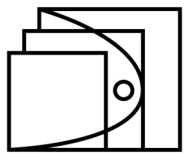
WebThree

Everything you need to know about Web3 and the World’s update.

Agustin Cortes



www.lirn.io | www.lirners.com

For those who’ve seen the light of cognition and learn for the sake of learning.

The autodidacts of life.

May we learn so much, we lose our minds and gain new ones.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

x

About the Author

Hello world, I believe having context pertaining to a person you are learning from is vital in your learning experience. It sets the primer and creates a perception that bridges your information. My name is Agustin Cortes, and a little overview about me is that I am an autodidact edtech founder who gets monomaniacal obsession about new domains every few months. These domains can range from cognitive psychology to socioeconomic systems.

Currently, I am obsessed with how web3 will change the world not just from a technological standpoint but from an economic and social outlook. I decided to write this because I felt that there wasn't a single resource that gave the holistic viewpoint of the change that web3 is bringing. Most of the information on the web is scattered and is focused on the tidbits of what is happening, rather than focusing on the core concepts of web3. A lil fun fact is that when I started writing this, I was reading the Bible and found out that the epistemological definition of the word bible means the book of books. In a way, that is the goal for this book; make it the book of books for web3. In other words, this single book covers the entire spectrum.

Knowing that there are constant changes in Web3, this book will constantly be updated to ensure all information is valid. In the possible near future, we may even get this officially published. The funds of this book will be allocated to creating Lirn.io's protocol for an economy of education.

1.

Intro

“The internet consists of transactions, relationships, and thought itself.” - **John Perry Barlow**

Web3. You’re hearing about it everywhere. There is a real-time shift of companies focusing their priorities on building in this new space. Your friends are talking about NFTs. Some people on Twitter are discussing something called DAOs. You see that cryptocurrencies have a market cap of billions of dollars; Bitcoin even reached a market cap of over a trillion dollars. This massive activity flux has made you curious to learn more, but you do not know where to start.

There are a few things that evolve at the speed of web3. I mean very few things in the timeline of human history. The rate of the exchange of information is unprecedented. Countless corners of the world are diving in and contributing to this change. Even if you are obsessively learning the space, it is hard to stay updated on a day-by-day basis. New ventures, stories, concepts, and lessons get documented every day. It is important to note that even though the changes of web3 are happening at an incomprehensible rate, all major changes are happening on foundations.

That brings the purpose of this book. The goal here is to create a linear understanding of all the foundational pieces of information on web3. Essentially, everything you need to learn in web3, so you understand what is going on. This ebook is broken down into two core components. Conceptual and technical. For clarity, we will be discussing more on the abstractly conceptual workings of web3, but we will touch upon technical elements. Let’s dive in.

2.

Internet History to Web3

The Internet

“The Internet is the global system of interconnected computer networks that communicates between networks and devices. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The origins of the Internet date back to the 1960s.” - **Wikipedia**

The early Internet was a network that had an exclusive operational system for devices. The first official name was the ARPANET(Advanced Research Projects Agency of the United States Department of Defense). That is a marvelous achievement in itself; humans established the network infrastructure for the future operations of the world. All the predecessor innovations from the sciences led us to this feat. However, its biggest limitation was that the resources available were centralized and the information available was a preconceived taxonomy to a body of knowledge. Information was siloed and limited in this manner. Within a few years, the internet would meet the world. Here comes the World Wide Web to the rescue.

Web1

“I was excited about escaping from the straightjacket of hierarchical documentation systems…. On the web, scientists could escape from the sequential organization of each paper and bibliography, to pick and choose a path of references that served their own interest.” - **Timer Berners-Lee**

In 1989, a computer scientist named Time Berners-Lee wrote “Information-Management: A Proposal” to introduce a new way to share information. This proposal was the genesis of what is known as Web1. With Web1, information becomes decentralized compared to the how the internet network handled information. The introduction of new rules and protocols allowed information to be referenced and shared in a novel way. An information highway has emerged. This new highway was called the World Wide Web.

One of the innovations that came with Web1 was the browser. A browser is a portal to the world wide web. What happens is that your device syncs real-time information and renders a website’s screen. The information the browser requests lives in a server, which is something you can view like a memory box. The servers deliver the information to the browser in a precise manner. This is called the Hypertext Transfer Protocol (HTTP). A few years later, HTPPS was upgraded to HyperText Transfer Protocol Secure (HTTPS). This hypertext transfer protocol allows a server to deliver specific information packets to the browser, which will render a website. Your device can get information from anywhere in the world. An English author named H.G. Wells coined a concept called the World Brain. The premise of the World Brain is what Web1 was about to create.

Web2

“The whole human memory can be, and probably in short time will be, made accessible to every individual…” - **H.G Wells**

Read & Write. Those two words define what is known as the Web2 era. In Web2, users can now send information back to the servers that were delivering the information in Web1. The essence of this process is called User Generated Content (UGC). Websites were now able to capture user-generated content and work with that data. Since data can be many things from emails, names, addresses, images, forums, etc., companies can create multiple types of products. In this excerpt, we will only be discussing data the user intentionally submits, not tracked data. Let’s use Twitter as an example.

Twitter is a relatively simple application. It takes in your personal information to create an account, and it allows you to send text-based content known as tweets. All the content on Twitter are tweets from other users. If users could not send

information to the database, Twitter would not have data to render. It would be an empty skeleton with no information flowing in. Web2 allowed countless new applications to emerge and create the internet that we know. Operating with these rules seems fine and dandy, but there is a problem for the users. The people in the platform literally create the content and information, but the companies take in all the profit. View it as you do all the work for a project, but you do not get any form of independent ownership for your work. You just get a couple of likes. Not having ownership or getting compensated for your work is an issue that Web3 could solve.

3.

Web3, Blockchain, and Smart Contracts

"Decentralization doesn't mean an absence of leaders, but an abundance of them." - **Balaji Srinivasan**

You can not build Web3 without blockchain. For now, we will give a high overview of blockchain, and then we will dive deeper into the upcoming sections. What's happening with Web3 is that we are at a new level of the internet. We learned about Web1 and Web2; what could blockchain do that'll make the world so different? Decentralization is an effective one-word to summarize the change.

Let's go back to Web2 to give a real example. Let's say you create an account on Twitter, and you build up your information on the platform. When you want to create an account on Facebook, you have to start from scratch. That's the norm for us, right? Since every company has its own databases, we need to make an account specifically for their database. Well, that is because all the data on the web is centralized on these companies' servers. That's a broken system for navigating the internet, and here is how blockchain solved it.

In the simplest terms possible, a blockchain is a database that has no owner, its data is accessible to everyone, and the data stored will never be changed. These components are the heart of Web3. By having data accessible, decentralized, and immutable, a new shared source of truth can emerge. This feat is creating one of the most innovative systems we've seen in decades, possibly centuries. Blockchains create a sociological and technological change that impacts everything from climate change to economics to the metaverse.

Smart Contracts

Various blockchains are built on the essence of code called Smart Contracts. They might sound intimidating, but what a smart contract does is run code to execute automatically, control, or document actions onto a blockchain. The best analogy of a smart contract can be used by referencing a vending machine. When you insert your money into the vending machine, select the item you want, the vending machine will disperse the item, and you will receive your item. The steps of the vending machine are done automatically. Smart contracts follow the same automation concept, but they add data onto a blockchain. Smart contracts get more complicated than vending machines because there are many more variables in the process, which could leave vulnerabilities for hacks and security issues. Now that we covered Web3, Blockchains, and smart contracts, let's plunge into the fabric that makes up web3. Let's start at the base of everything. Philosophy.

Layer 0

"Learn to ask of all actions, "Why are they doing that?", starting with your own." - **Marcus Aurelius**

The philosophy of blockchain has a fascinating origin. However though, before diving into philosophy, we need to discuss some core definitions. First, we will start with decentralization. Decentralization is the distribution of functions and powers away from a central authority. Basically, it means no central ruler, and the power gets distributed among stakeholders. The premise is to move power away from a central authority. Decentralization operates as a spectrum, meaning there will be levels of control in certain areas. You will hear decentralization be used a significant amount in web3, so it is crucial to have a base understanding of it.

The following vital definition to discuss is immutability. Immutability is something that can not be modified once it gets documented. The most common usage of immutability is when working with databases. With immutable databases, the registered data can not change once information goes in. In other words, it gets set in stone.

Let’s move onto the concept of value. We will focus on two forms of value, extrinsic and intrinsic. In economic definition, value is a measure of the benefit provided by a good or service to an economic agent. This type of value is extrinsic and is generally measured relative to currency units. On the other hand, intrinsic value is an unmeasurable worth. Think of the value of happiness, health, belief, community, or concepts like this. Intrinsic value can’t be measured, but it does exist. Blockchain provides both types of value for people. Value is a complicated subject, and we will discuss it in further detail in the value theory section.

The last areas I’ll address here are economics and sociology. These two fields are the invisible forces that make people believe and work in blockchain. Economics is the social science of focusing on producing, distributing, and consuming goods and services. The concept of Economics will be fundamental to be aware of because once you see how blockchains operate, you will know that they have their economic system. That same system then becomes validated through sociology. The study of society, human social behavior, patterns of social relationships, social interaction, and aspects of culture associated with everyday life will be fundamental to understand because blockchain is the way society operates. These two fields are the socio backbones of Web3.

Bitcoin and the Origin Philosophy

“Bitcoin is a swarm of cyber hornets serving the goddess of wisdom, feeding on the fire of truth, exponentially growing ever smarter, faster, and stronger behind a wall of encrypted energy.” - **Michael Saylor**

On the Halloween of 2008, an anonymous mastermind named Satoshi Nakamoto introduced a whitepaper called Bitcoin to a community of cryptographers. It documented how to create a secure value exchange between peer-to-peer with no central authority. (Bitcoin is commonly referred to as digital gold since gold is a universal value storage.) Bitcoin became valuable because it solved multiple technological and economic issues that cryptographers, computer scientists, mathematicians, legal scholars, cypherpunks, and others have tried to solve for several decades.

The idea of creating internet money or a storage of value was attempted by cryptographers and cypherpunks several times before Bitcoin. In 1998, Nick Szabo created Bit gold, a mechanism for a decentralized digital currency. In 2002 Adam Back formally introduced Hashcash, a mechanism to prevent exploitation and spam from validating an exchange of value. Bit gold, Hashcash, and other predecessor progressions led to the emergence of Bitcoin.

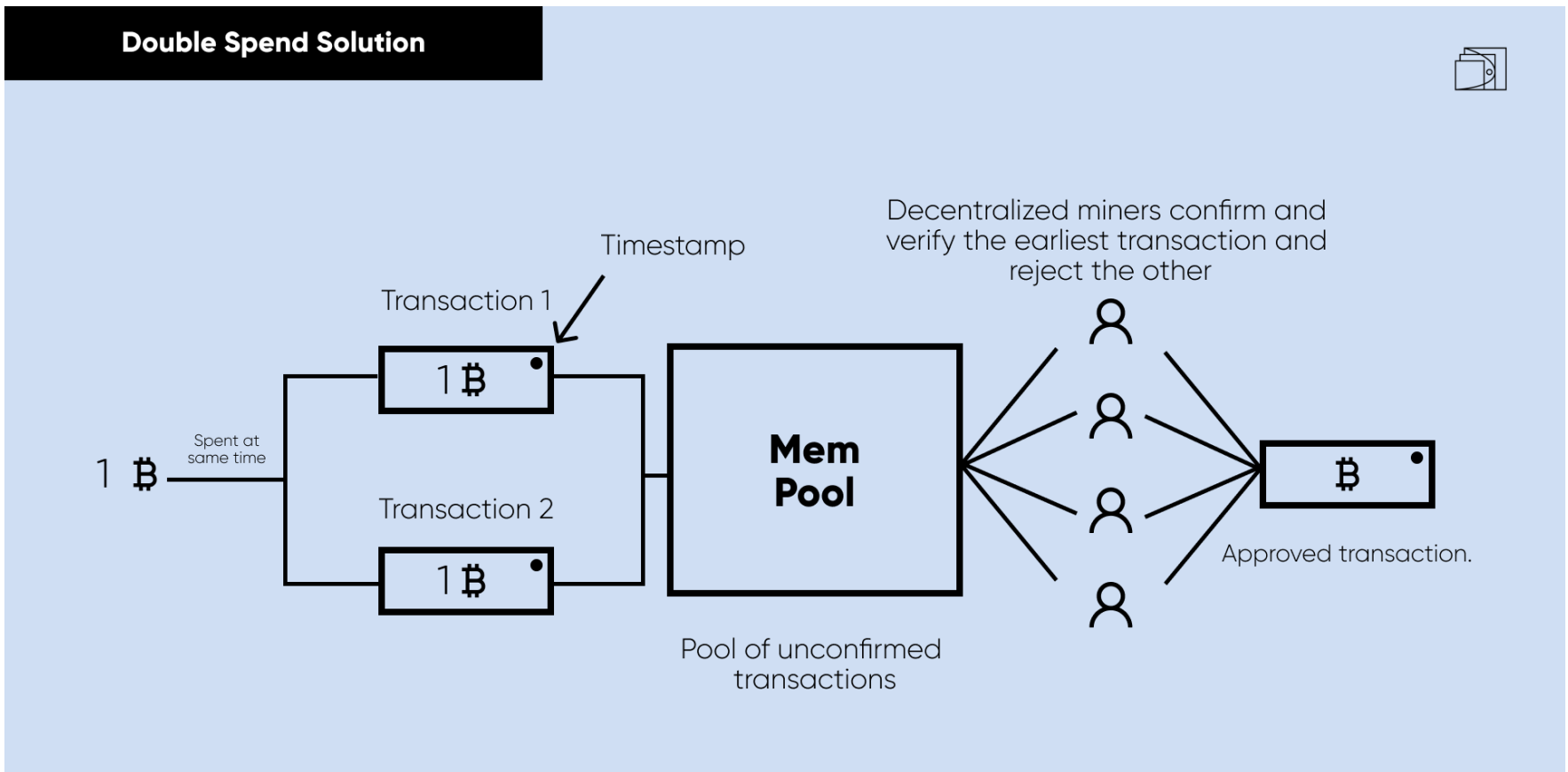
1: Double Spend Problem

One of the most significant problems Bitcoin solved is the double-spend problem. Double-spending is when someone could simultaneously spend a digital currency more than once. If a double-spend transaction goes through, it will create a discrepancy between the spending record and the amount of currency available. There are two ways a double-spending can happen. Either by simultaneously spending the money twice or by reversing a transaction once the buyer got the product or service they were paying for. A technical programmer could manipulate the protocol to control their usage of money in their favor, but Bitcoin has a process to prevent this.

The reason digital money has this vulnerability is that bad players can easily replicate digital and digital money takes time to register transaction activity. For Bitcoin, it takes up to ten minutes for data to get added onto the blockchain, so within those ten minutes, a bad actor can spend their money multiple times since it isn’t registered yet.

Bitcoin solves the double-spend problem by creating a pool of unconfirmed transactions. Each transaction gets sent to this pool, and a decentralized group of verifiers validates the transactions. So let’s say someone spent the same $10 of Bitcoin twice; what would happen is the two transactions would go to the pool, and verifiers would validate the first transaction. The second transaction would get reverted by the network.

Once the transaction gets approved, it becomes immutable data on the chain. Having a decentralized validity mechanism allows the integrity of information to be legitimate. Solving the double-spend problem is a grand accomplishment because it will enable digital money to work. We will go into further detail about the underlying operations of data movesinside a blockchain when we reach the consensus mechanism section of this book.



2: Miners

Miners validate transactions and create the new coins inside a blockchain. Bitcoin was the first blockchain to incentivize and reward people for keeping data added onto the blockchain legitimate. What's unique about adding data through miners is that they coordinate in a trustless peer-to-peer manner. Operating in a decentralized manner means each miner can operate in the network independently without a third-party central authority.

A miner can be a validator and a creator of blocks. The blockchain will reward the creator of a block the network reward. In the case of Bitcoin's blockchain, the miner gets rewarded in Bitcoin. The process that miners go through starts with miners competing against each other to solve a mathematical puzzle. The first miner to solve the puzzle will be legible to package transactions into a block. Other miners will independently check the data of the block presented, and if they validate it, the block gets added to the blockchain. The miner that won the puzzle and got the block onto the blockchain receives the Bitcoin. Different blockchains have their own approach to mining, but the premise is to do decentralized coordination for the validity of the information.

3: Belief in Bitcoin and Blockchains

With people realizing the capabilities of Bitcoin, a community of believers started to form. These believers started frantically discussing and building the

possibilities on Bitcoin. Bitcoin introduced a new concept of money and people believed. This new idea of money broke the paradigm and got its first price point of economic value within a short time. The first time Bitcoin price value was on October 12, 2009, when Martti Malmi, a Finnish developer that helped Satoshi work on Bitcoin, sold 5050 Bitcoins for $5.02. This transaction gave 1 Bitcoin the value of $0.0009. By mid-2011, Bitcoin's price reached $32, that's a 40,000% growth in 2 years. As more people started to believe and trade Bitcoin, blockchains gained more validity.

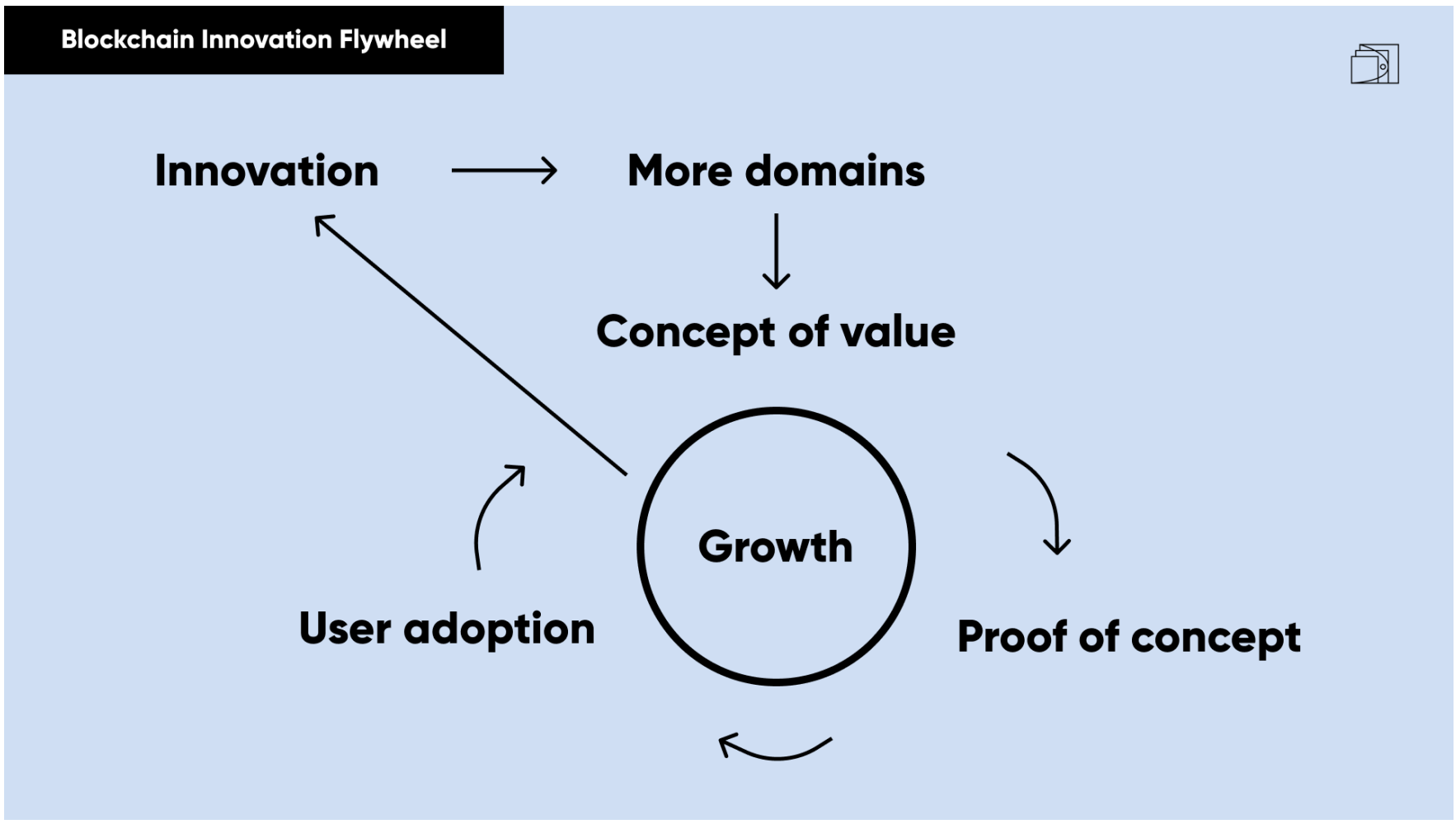
A new sociological philosophy emerged, and Bitcoin was paving the way for further innovation. Bitcoin created a new system that allowed people to trust each other without having a central authority involved. Operating without a central authority creates a new dimension for social sciences like economics, sociology, game theory, finance, system theory, and more.

The Emergence of Other Chains

"One computer for the entire planet." - **Gavin Wood**

With Bitcoin being the first blockchain to solve digital money's core problems, the concept of blockchain gained sociological validity. As more and more people got involved, the breadth of the possibilities started outreaching. Soon, the emergence of new blockchains started. In 2013, Vitalik Buterin realized that a blockchain system for the value of computation needed to be created. Vitalik emerged the genesis of Ethereum. Vitalik assembled a co-founding team with scientists and entrepreneurs. The co-founders are Gavin Wood, Charles Hoskinson, Anthony Di Iorio, and Joseph Lubin.* Bitcoin paved the way, Ethereum broke the ice, and now there are dozens of different types of blockchains, each focusing on their own mechanism. Blockchains allow people to use economics, sociology, and technology to create new systems for value exchange.

** Gavin Wood started another blockchain called Polkadot. Charles Hoskinson started another blockchain called Cardano. Anthony Di Iorio is reported to have left crypto and disappeared from the web due to safety concerns.* Joseph Lubin started a blockchain company called Consensys. *



When concepts start compounding in momentum, it is known as the flywheel effect. In the beginning, something takes a lot of effort to gain momentum, but it will gain even more speed once it does.

4.

Layer 1

“Engineering is about rigorous analysis, design, and verification of systems; all assisted by tools that reconcile theory with practice. Engineering is also a discipline of responsibility: ethically and professionally accountable to what you build." - **Trent McConaghy**

Here we will be discussing blockchain in greater detail. When people in web3 refer to layer 1 (L1s), they refer to a specific blockchain and its protocol components. Layer 1s are blockchains that have their own systems and mechanisms for operating. These systems are engineered with solid technical intricacies. People in the community also call L1 the mainnet. Let’s dive into what exactly a blockchain is and how it works.

Blockchain Technicalities

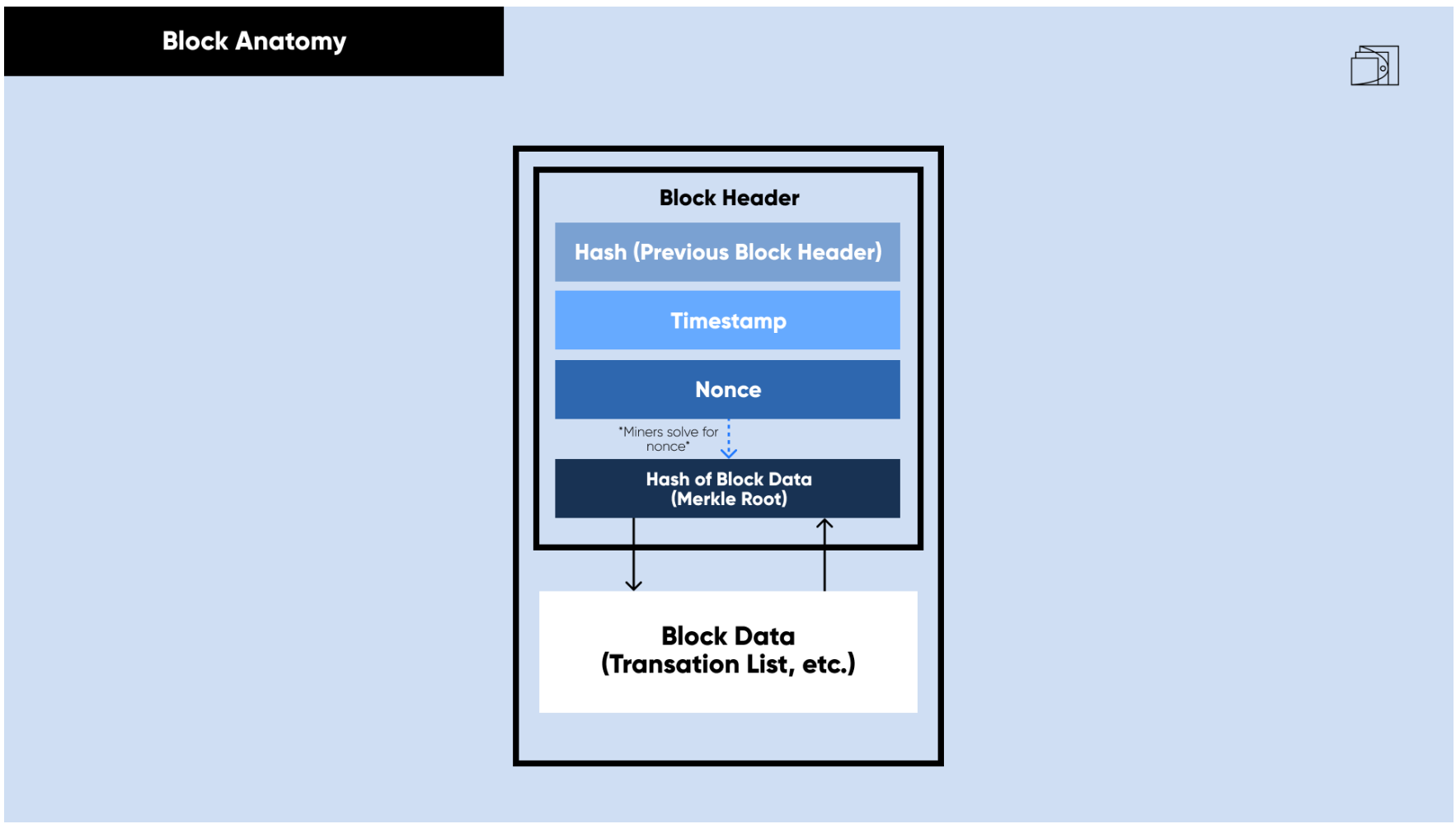
Before we explain what a blockchain is, we have to understand the building blocks. To understand blockchain, you have to have a collective understanding of multiple variables. In this chapter, we will take a look at technical variables that create a blockchain. We will begin with blocks.

1: Blocks

A block is a data structure that has a header that stores an ID number, a nonce (number used once), a timestamp, a previous block’s hash, and its own hash (Merkel Root). A block also stores a transaction list. In simple terms, a block in a blockchain, is a block with specific holding specific data that sends that data onto the following block to create

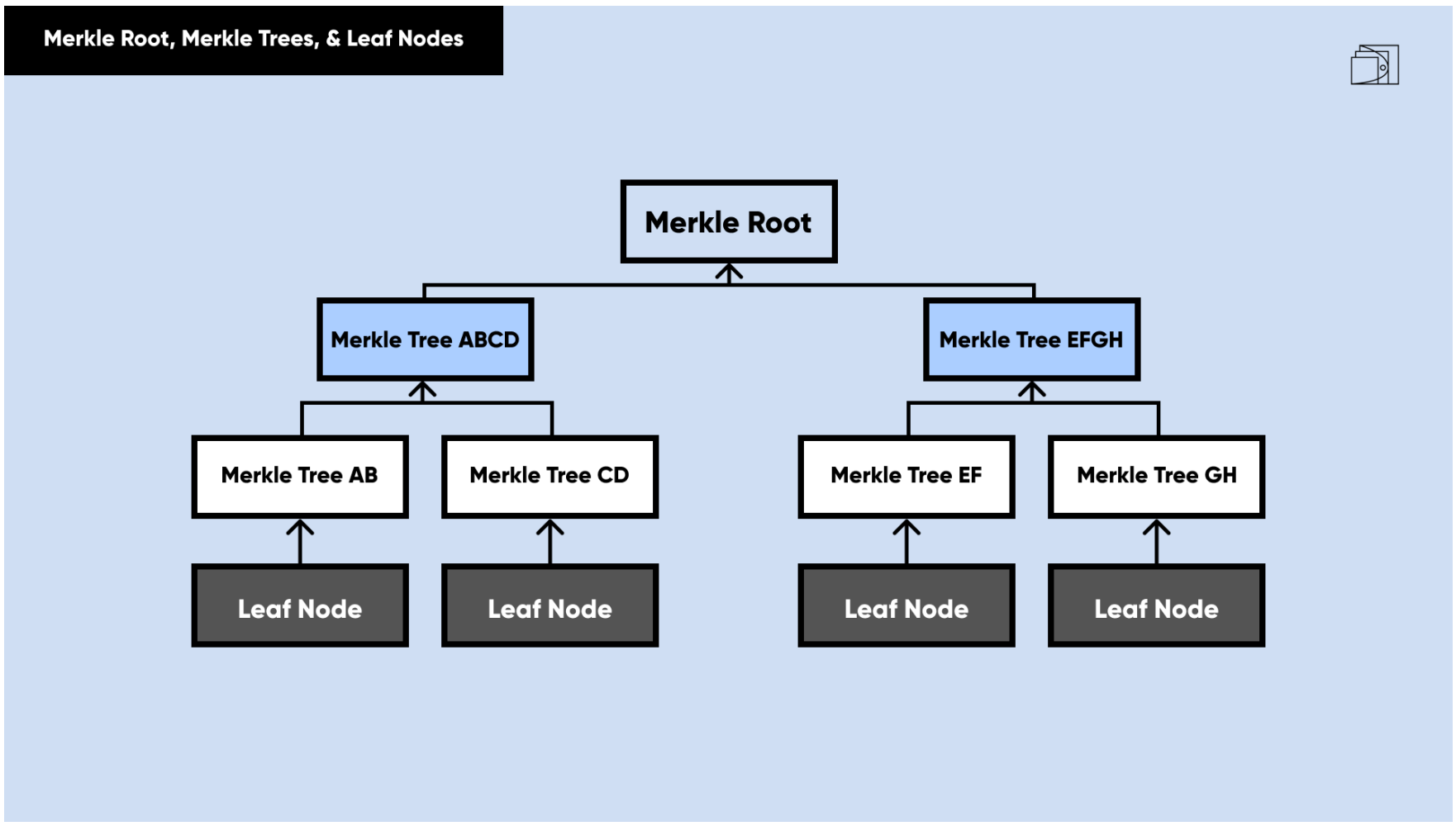
a chain of data. (For context, a block that sends data to another block is known as a parent block.) Miners validate the appropriate blocks and if approved they will add it to the chain. Once data is on-chain, it’s impossible to change. Having the data linearly sync block to block creates a specific mechanism of the flow of information known as a blockchain.

Here’s a visual representation of a blockchain to help piece the information.



2: Merkle Tree, Hashes, Nonces, and Cryptographic Hashing

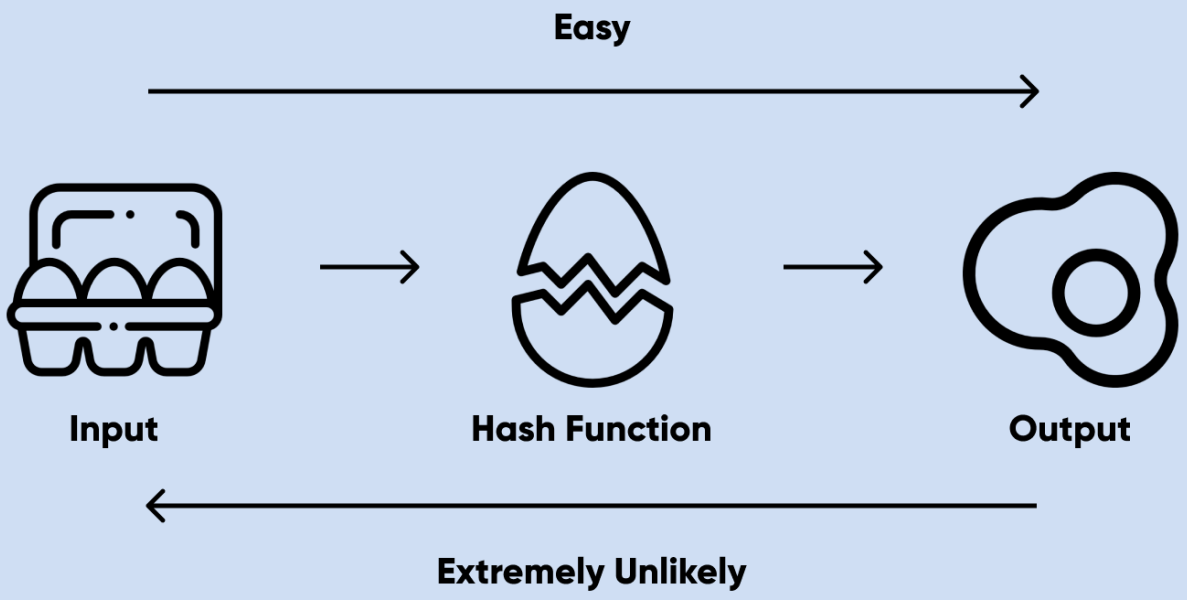
A Merkle tree is a data structure method to prove the integrity of transactions and reduce memory size. The way memory is optimized by Merkle trees creating hashes. A hash is an encrypted output of information that can be used as a digital identifier. Most blockchains use an encryption formula named SHA-256 which randomly encrypts data and is decrypt-proof.



Let’s explain this in detail. Blockchains use Merkle trees for packaging more transaction data onto a block. For example, instead of adding 100 transactions, those transactions can be packed into a single Merkle tree. A transaction in this context is called a leaf node. Merkle trees are powerful because they can create layers of packaging information. Let’s say that there are 1,000 transactions in a block; if one Merkle tree can package 100 transactions, then there will be 10 Merkle trees. We now have 10 hashes that can identify the 1,000 transactions. The 10 Merkle trees can be paired once again to minimize memory. Merkle Trees A and B can create another Merkle Tree called Merkle AB and the same can apply to the remaining trees. These pairs become child trees but still carry all the parent trees’ data. The child pairs can pair with other child pairs to the point that they create a Merkle Root. The Merkle root is the hash of the block. The power of Merkle Roots is that they allow proof of data and minimize memory storage to verify the records.

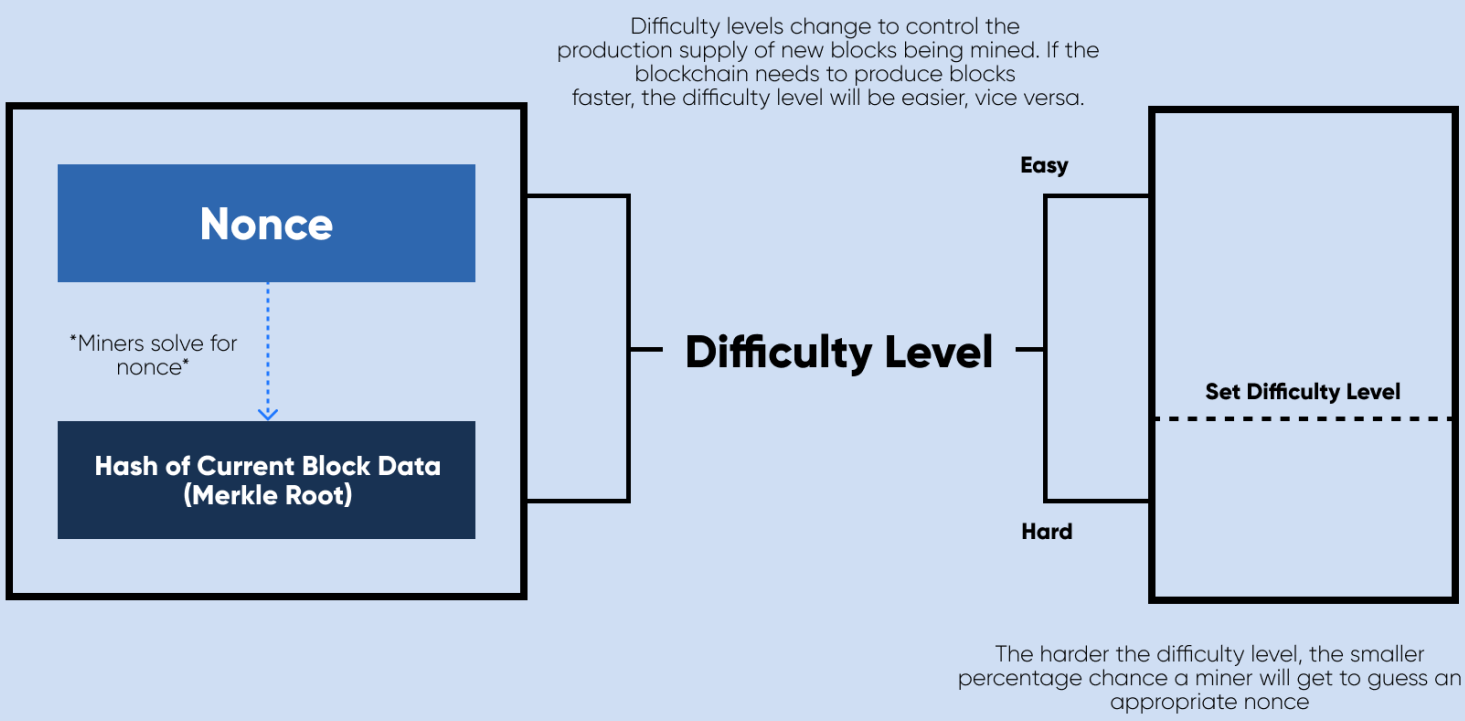
For example, if Merkle Roots didn’t exist, if a miner wanted to download the blockchain, the miner would have to download all the transactions in the blockchain. Hypothetically let’s say that the memory size was 100 gigabytes. With Merkle trees and roots, the memory size the miner would have to download would be 5 gigabytes. This is also known as cryptographic hashing.

Encryption is not Reversible



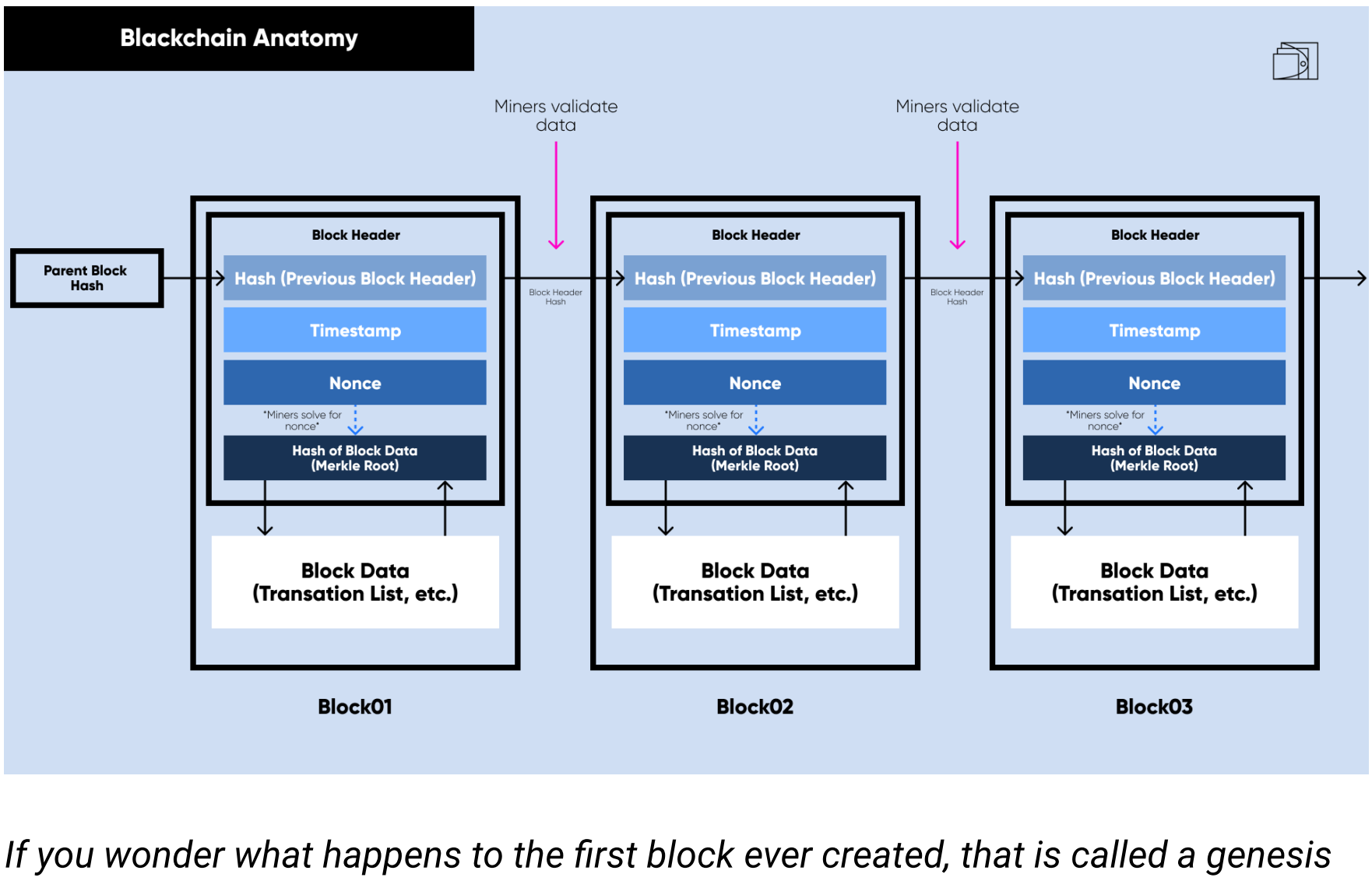
A block will also always have a nonce (number used once). The purpose of a nonce is to be encrypted and give out the block's current hash. Miners encrypt billions of nonces in pursuit to get the correct number that yields the appropriate hash. The nonce is a variable that must be found and validates the concept of proof of work. Each blockchain will have a difficulty level to guess a valid hash. The difficulty level is a way to decrease the chances of a miner getting a correct nonce. Blockchains implement difficulty levels to stabilize the production of new coins. The miner that guesses the nonce correctly earns the network reward. The network reward is the coin the blockchain distributes out. For example, in Bitcoin, the network reward is Bitcoin.

Difficulty Level



Blockchains are a Source of Truth

Now that we tied the meaning of Merkle roots, hashes, nonces, and miners, we can fully describe a blockchain. A blockchain is a sequential chain of data blocks that is decentralized. There is no central authority that validates the activity in a blockchain, rather decentralized miners coordinate to keep the legitimacy of data. The miners are rewarded for validating transactions and growing the blockchain. Since data in blockchains move linearly and get cryptographically hashed, all miners work with the same blockchain. Since hashes are the vehicles of data, any change in a transaction will completely change the merkle trees and root. If any miners try to change data inside blocks other miners will prevent this data from being added to the chain.

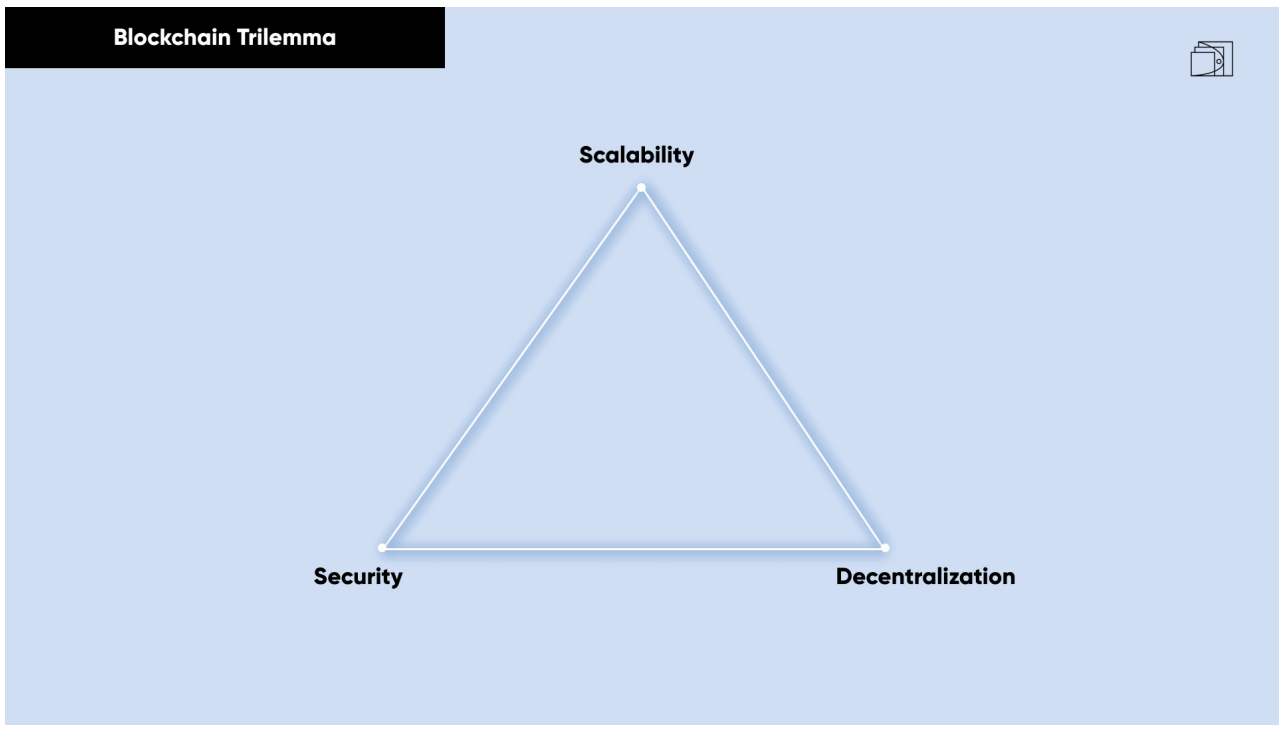


If you wonder what happens to the first block ever created, that is called a genesis block that kicks off the blockchain. Usually, the first transaction in a genesis block is called a coinbase transaction.

Now that we know that a blockchain is a chain of data, let's talk about the core issues that web3 is facing, also known as the blockchain trilemma. Scaling, decentralization, and security are foundational to blockchain, but as the complexity emerges, one or two areas get compromised to solve issues. This concept was coined by Vitalik Buterin when discussing core issues developers face when building blockchains.

5.

Blockchain Trilemma



Decentralized Ownership and Consensus Mechanisms for Security

A public blockchain (there are private blockchains, but we won't be discussing those) is a blockchain with data accessible to anyone. Anyone can download a public blockchain's data and stay updated with real-time transactions. Data accessibility allows decentralization, and game theory shines. By having open access to the ledger, people can now be incentivized to ensure that the information added is legitimate. A blockchain incentivizes people to work together is called a consensus mechanism. Investopedia has an excellent definition: " A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies." In layman's terms, this is a way to get people to agree on what is defined as true.

There are two popular consensus mechanisms: the security forefronts for blockchain; Proof of Work (PoW) and Proof of Stake (PoS).

Each has their own merits and flaws. Bitcoin uses the Proof of Work consensus mechanism, a form of cryptographic proof that uses energy consumption to verify that a certain amount has been expended. This energy consumption aims to make miners make billions of attempts to get the correct nonce for the upcoming block to get the reward. These verifiers are also called miners, which is probably what you've heard more about in web3. So the goal for PoW is to make miners consume energy to keep the blockchain information legitimate and earn the network reward.

In a summarized manner, Proof of Stake is a consensus mechanism where the mining power is correlated to the number of coins owned by the miner. We will discuss coins in detail in the tokenomics section, but in essence, a coin is the network reward in the blockchain. Currently, Etheruem uses PoW but is moving to use PoS. In Ethereum, the coin is called Ether, so in the case of PoS, the more Ether owned by the validator, the higher the mining power they have. PoS solves the excessive need for computation power because mining power is now based on the percentage of ownership staked. So if a miner has 5% of the total coin supply, they can potentially mine 5% of the blocks. The game theory behind this mechanism is that the miners will behave in the best interest of the blockchain because they can lose coins if caught acting maliciously. Hence, the value of the blockchain goes up, their earning do too, so it is a win-win for the blockchain and the miner. On top of that, this allows for massive scaling improvements.

Consensus mechanisms are a way to set trustless coordination for security. A Blockchain can face some of these attacks: the Finney attack, race attack, 51% attack, Sybil attack, DDos, Routing attack, and more. PoW and PoS so far have been highly effective in holding security and avoiding exploitations on blockchains. Security will never be perfect, and hackers are becoming much savvier in finding exploitation. The good news is that a major blockchain has not been hijacked directly and overtaken by hackers. However, hacks targeting projects built on a blockchain is a typical security issue. Here's a story on how a project on Ethereum got hacked, and it ended up changing the blockchain itself.

In 2016, Ethereum experienced a massive hack called the "DAO Hack," leading to Ethereum forking. The high overview of the hack was that a decentralized autonomous organization (we'll cover DAOs in upcoming sections) received what was estimated to be about $150 million US dollars worth of Eth. The DAO's

purpose was to allocate capital provided by investors, and the investors would get returns on the money they put up front. Essentially, a decentralized venture capital firm. Within a few weeks, a hacker exploited the smart-contract code and sent Eth to their wallet. The hacker left with about $50 million US dollars worth of Eth, which led to a huge discussion about the future of Ethereum. The hacker had a significant amount of all the distributed Eth in existence. And this was a huge security risk for when Ethereum was to convert into a Proof of Stake consensus model. Remember how with PoS, the more you own, the more mining power you have? With the hacker having so much Eth, they would be able to be an extremely strong bad player in the PoS consensus mechanism. Being aware of this, the Ethereum team did what is known as a hard fork, which is when a blockchain makes a copy of itself but changes some information. Ethereum did a hard fork and created a chain that reverted the hack. The chain that stayed with the data of the hack became known as Ethereum Classic.

Growing Pains. Scaling.

“Pain is part of growing up. It's how we learn.” - **Dan Brown**

As blockchains get more user adoption, complexity starts arising. For example, getting data into a block starts getting more expensive because more users compete to get into blocks. Some blockchains, like the Solana, want to optimize for scalability, but they dilute their decentralization. Ethereum focuses on decentralization and security but struggles with scalability, leading to extremely high transaction fees to get data onto the mainnet.

Let’s discuss what transaction fees are and how they work for a blockchain. At a high overview, it is relatively simple. Users have to pay a fee on every transaction they initiate to try to get their data onto the blockchain. The amount of computation needed to add the transaction onto the blockchain is what determines the amount for the transaction fee. In the Ethereum network, a transaction fee is called a gas fee. By definition, gas is the unit that measures the amount of computational effort required to execute specific operations. The fee is paid to a miner who does the computation power to validate the transaction and add it to the block. Once a miner adds your transaction to the block, the data will now be part of the blockchain.

Things start to get complicated when several people compete to get their data

onto the block. Scaling payments is a major technical issue of blockchains. Remember how we defined a blockchain as a collection of memory-sized blocks that stores records? Well, the memory size of each block and the speed it gets mined at becomes the core variables to how much transaction fees are going to cost. If the block size is small and it takes several minutes to mine a block, it will be more difficult for users to add their data. Getting transactions onto the blockchain falls under the principle of supply and demand. Small block sizes and slow mining rates create a low supply of blockchain real estate, and as more users come on board, the more demand there will be. Transaction fees are a massive problem on the scalability spectrum. Let’s observe the current headaches that Ethereum is experiencing.

Currently, in the Ethereum blockchain, it takes about 14 seconds to mine a block and can process 15 transactions per second. So this means the average block size has 210 transactions (15 * 14 = 210). A low amount of transitions is terrible news for users who want to add data onto the blockchain because as there are more and more users, people are willing to pay more in fees to get one of those 210 spots in the block. Back to supply and demand, this creates an auction for users willing to pay the most fees to miners to add their data. Miners take in the bids and then start competing among themselves for their offer to get onto the blockchain. Competing to add data on-chain creates a loop of using more computation power, increasing the transaction fee. Ethereum has prioritized fixing these transaction fees and is focusing on multiple processes.

One of the most significant changes in Blockchain history is close to happening. Ethereum is scheduled to move away from a Proof of Work consensus mechanism to a Proof of Stake (PoS) mechanism. It is estimated that Ethereum will be able to handle up to 100,000 transactions per second when it migrates to PoS. Switching consensus mechanisms is no easy feat, and Ethereum has had issues accomplishing this.

Other real-time solutions are happening in Ethereum to help with scaling. These are called L2 solutions. What happens is, transactions are processed off the mainnet chain and later added on. These L2 solutions cleverly find ways to process the data from their chain and add it onto the mainnet at a subfraction of cost. At the moment of writing, L2s on Ethereum quickly pick up user traction and capital allocation.

Centralization

Solana is a new blockchain that is picking up massive steam because it is a blockchain that can scale and have no transaction fees. Typically users are paying a few cents to add data onto the blockchain. Solana is one of the most interesting chains due to how fast its market cap is rising (We'll discuss market cap in the DeFi chapter). Many projects and innovations are happening inside the Solana blockchain. However, one of the narratives against Solana is that it is relatively centralized. If we recall the Blockchain Trilemma of dealing with scalability, security, and decentralization, Solana scores high in scalability and security but ranks lower in decentralization.

Solana started a venture-backed project where early investors got the majority of the coins at a low price. It is common to reward early investors in blockchain business as there is a higher risk of entering new projects. Usually, projects do something called an ICO, an initial coin offering, to distribute ownership in return for capital. For the most part, these ICOs give the majority of ownership through a public sale, which is when anyone could have access to purchase. Solana did more of a centralized distribution by providing an above-average ownership allocation to private investors and not public sales. Around 60% of the coins are controlled by the project's founders and the Solana Foundation, with only 38% reserved for the community. The majority of the coins being owned in a centralized manner could be hazardous. One example is how an owner with an excessive amount of coins can do market manipulation by causing panic sales if they start dumping their coins.

A few other centralization factors are the hardware requirements needed to become a miner in the network, and the majority of projects built on Solana are closed-based. Let's talk about hardware first. Currently, users have to be thousands to obtain high-end hardware capable of running the network. In contrast with other networks, people can use simpler hardware. Solana co-founder Anatoly Yakovenko is aware of this issue and prioritizing methods to allow different scales of hardware to gain accessibility.

Let's now discuss closed-based projects, meaning projects do not share their codebase. Not sharing codebases is counter-culture to the original aspect of blockchain, which started open-sourced. In other networks like Ethereum and

Bitcoin, open-source all the code. When code is open-sourced, other builders can take that code and leverage it to create similar projects. There isn’t anything wrong with having closed source projects, but the narrative argues that the blockchain culture was built around openness and decentralization.

Okay, now that we talked about the trilemma of blockchains, let’s take a turn into the field of economics. In my opinion, grasping the holistic viewpoint of how economics and blockchain are coming together gives the ultimate enlightening on what web3 could become. There is a lot of complexity and a mesh of subjectivity as there is for any social science, but we will cover the main components that bridge web3 and economics.

6.

Cryptoeconomics

“Our choices are always in accordance to the prevailing value systems of our environment.” - **Sunday Adelaja**

With the emergence of blockchain systems maturing, a new field in economics is arising. This field is called cryptoeconomics. The term was casually introduced in the Ethereum developer community in 2014 and has picked up formality. There is no universal agreement on what cryptoeconomics can be defined as because it is still under development. The best definition I’ve seen has been “Cryptoeconomics is the study, analysis, and design of economies built on blockchain infrastructure to incentivize human behavior.” The process of designing economies is a complicated thing to do because complexity arises with the infinite amount of possibilities each agent can have. Sometimes cryptoeconomics will be referred to as tokenomics. The main distinguisher is that cryptoeconomics focuses on the economics to create a blockchain, and tokenomics focuses on a token on top of a blockchain.

Economics Overview

The foundation of economics allows people to securely represent underlying resources to exchange value in an information system. Okay, if that’s the foundation, then what is economics? Mirriam-Webster has a great and straightforward definition that goes as follows: “A social science concerned chiefly with description and analysis ofthe production, distribution, and consumption of goods and services.” Beneath all those words, I view economics as the study of the exchange of value.

Economics is such a vast field that it overlaps with other domains such as mathematics, sociology, psychology, political science, and now blockchain.

We can break down the analysis of economics into two main categories—macro and micro, which leads to the subfields of macroeconomics and microeconomics. Macroeconomics focuses more on the entire spectrum of the economy, mainly the indicators of gross domestic product, unemployment, inflation, and other significant economic variables. On the other hand, microeconomics focuses on how individuals respond to dynamic economic conditions. It's important to note that traditional macro and microeconomics are focused studies in the post-industrial era. Blockchains are so big now that Cryptoeconomics has emerging macro and microeconomic systems, leading to the premise of economies.

Economies

The product of economics is an economy. Wikipedia has a great definition of an economy: "*An economy is an area of the production, distribution, and trade, as consumption of goods and services by different agents. It is generally defined as a social domain that emphasizes the practices, discourses, and material expressions associated with producing, using, and managing scarce resources.*

A given economy is a set of processes that involves its culture, values, education, technological evolution, history, social organization, political structure, and legal systems, as well as its geography, natural resource endowment, and ecology, as main factors. These factors give context, content and set the conditions and parameters in which an economy functions. In other words, the economic domain is a social domain of interrelated human practices and transactions that does not stand alone.

Economic activity is spurred by production, using resources, labor, and capital. It has changed over time due to technology and innovation (new products, services, processes, expanding markets, diversification of markets, niche markets, increased revenue functions)."

Thanks again, Wikipedia.

That overview gives us the critical parameters of an economy. All the variables used in traditional economies are now being used to build blockchain economies. Moving our current understanding of economic variables is profound because we can now make economies in a new way. If we look back at what a blockchain is, we will realize that one of the most important aspects is that all the data in the blockchain is accessible. Data accessibility will change how economies will work because we now have a new source of truth.

1: Ledgers

If economies are the product of the exchange of value, then ledgers are the databases tracking all the activity. By definition, a ledger is a book that registers economic activity. That's a simple concept, but it wasn't until a few centuries ago that ledgers changed how humans operated. Before ledgers, there was no official documentation of exchange of value. Imagine exchanging a product or service, and there isn't a form of validating the exchange. The absence of registering and documenting economic activity stunned human progression, and once ledgers came to be, the world started flourishing. Historians believe that the usage of double-entry bookkeeping, which is what current economic systems are built on, was one of the pillars for economic flourishment. Double-entry bookkeeping is simply tracking debits and credits between people. Ledgers became the base for financial infrastructure. Under the fancy financial jargon, banks are just the central institutions that use ledgers to track the exchange of economic transactions. Ledgers may not sound too exciting, but they are the tool that allows humans to operate at the scale that we are today collectively. Let me give an example of one of the most powerful ledgers in existence.

The economic system of the United States fiat currency operates off a central ledger. Actually, all countries around the world operate off ledgers. The US Dollar (or any currency) is the currency that encapsulates the shared value among the agents (people). This unit of value is a product of a government, and the government needs a system to track its economic data. The United States government, specifically the Federal Reserve, is in charge of managing the ledger of the United State's economy. Essentially, the FED is the central ledger, and Federal Regional Banks use sub-ledgers. The purpose of using a central ledger is to implement monetary policies to maximize employment, stabilize prices, and moderate long-term interest rates. Monetary policies are influential factors in

economic development, and they carry exponential impact. For example, cryptocurrencies got banned in China, excluding law-abiding Chinese people from participating in these new economies. Government ledgers are centralized and operate through bureaucratic and political operations.

A common potential issue called the Principal-Agent problem arises when centralized operations and power dynamics are introduced. The Principal-Agent problem is when one entity can make decisions on behalf of another entity. Enabling one entity to have absolute decision-making power creates a dilemma if two entities have different incentives and are against each other. Political scientists dedicate a significant amount of effort to finding solutions to this problem, but people still argue that the people in government sometimes still act in their personal interest. Crypto natives emphasize that a blockchain, a decentralized ledger (blockchain), removes the Principal-Agent problem because a centralized power can not make decisions for their favor.

By using a decentralized ledger, centralized powers can not create policies in their personal favor. On top of that, all the economic transactions that partake on a blockchain are accessible to anyone, disrupting the exclusiveness of centralized information. In their true power, ledgers map economic relationships by being the source of truth of the economic activities. As government officials look at the data of centralized ledgers to make decisions about monetary policy, the blockchain community can now see the open ledger and vote towards changes if necessary. It is important to note that blockchains are still novel and in infancy. However, some governments are moving towards using blockchain as their source of economic truth. El Salvador is the first country to make Bitcoin its legal tender. The following sections won't be heavily blockchain-centric. Still, economic principles are essential to understanding how cryptoecomics is built out.

2: Agents

Economic agents are individuals, businesses, organizations, or governments that are decision-makers in some aspect of the economy. Economic transactions occur when two agents agree to the value or price of the transacted good or service, commonly expressed in a specific currency. Two types of common agents are the buyers and the sellers of a product or service. Other types of agents could be monetary policymakers, banks, and firms. To put this concept into a metaphor, you can view an agent as a node in the economy, and the relationships between the

nodes are the economic activity. If there are no agents, then there is no economic activity going on in the economy. This concept of agents migrates perfectly over into blockchains economies. However, a core question arises if we think about it at the meta-level. What and why are agents exchanging in the first place?

Value Theory

Perhaps one of the most essential words in economics is value. Value is a very complicated subject to put in semantic definition because there is a lot of nuance to a possible meaning. It has a touch of philosophy and can be puzzling to articulate. It is common to tie value to a monetary definition, but value is more than that. The simplest explanation for value is “A principle of what is important or desired.” I like that definition because it captures all value essences from an external and internal point. Fortunately, economists have given the concept of value a tremendous amount of thought and have defined two main value types; extrinsic and intrinsic value. A high overview to distinguish these two is saying extrinsic value “from the outside,” and intrinsic value is from “the inside.”

We will define each type of value in further detail in this section. Equally exciting is that economists started stating that the emergence of blockchain systems is creating new economic designs for both extrinsic and intrinsic value in recent years. Let’s start with defining extrinsic value first.

1: Extrinsic Value

“Values are determined by priorities.” - **Suzy Kassem**

Extrinsic value can best be defined as the value used to help us get something else. The perfect example of this would be currency. A currency is the extrinsic unit of value that people use in exchange for a product or service. Extrinsic value is a relatively simple concept to understand because it leads to binary outcomes. For example, the US dollar is an extrinsic form of value because agents use it in exchange for a product or service. It is important to note that the US dollar itself does not have value, rather the utility that the dollar carries value.

2: Intrinsic Value

Extrinsic value focuses more on external components, and on the other hand, intrinsic value is more stand-alone and can not be quantified nor utilized. Some theorists call it “objective value” because it is an independent form of value that brings us value. Intrinsic value can be defined as the value that something has “in itself.” I know that sounds super philosophical, and that is because it is. Intrinsic value may be puzzling to understand, but there are a lot of merits in understanding it because it is what makes humans so dynamic. Intrinsic value merges concepts from economics and philosophy. Let me define intrinsic value further.

Something that has intrinsic value has value for its own sake. It is in a state that can not be derived or quantified. Some great examples of things that have intrinsic value are satisfaction, art, truth, friendship, cooperation, security, integrity, and others. In philosophy, intrinsic value is heavily tied to virtues and ethics.

I think integrity is a great one to take a further look at as an example. Integrity is the consistency of actions, values, methods, measures, principles, expectations, and outcomes. If we take a step back, we could realize that we can pack that definition into what blockchains do. That’s just one form of intrinsic value. Blockchains also focus on security, truth, cooperation, and other values. If you take a philosophical viewpoint, blockchains carry a lot of forms of intrinsic value, which leads to magnetism that attracts people, unlike a few things do. Some people compare blockchains to religions as people devote so much passion and personal commitment to the ideology. You can find articles talking about the blockchain holy wars. Okay, now that we spoke on value theory, it is now time to talk about what makes humans do things in the act of obtaining value. We are talking about incentives.

3: Incentives = Extrinsic + Intrinsic Value

There is an invisible force that makes every human being do things. This force is called an incentive. The reasoning for an incentive can be one’s self-interest without a reward, or someone can do it for the sake of getting a reward. Blockchains are incentive machines because they allow people to do things at a grand level. My favorite breakdown of this was by Trent McConaghy, an ai researcher, founder of the Ocean Protocol, and coined the term Token Engineering. Trent broke down how blockchains are incentive machines to get people to do

things. He gave the example of Bitcoin. The consensus mechanism proof of work that Bitcoin uses is exceptionally secure and uses high amounts of energy. The miners who are the ones that receive the network reward are incentivized to handle the costs of the hardware and electricity usage. Bitcoin started in the deep webs of the internet with a few passionate people. Within a decade, it now consumes more electrical power than some countries (we will talk about the environmental issues of crypto at the end of the book). The miners are just one type of agent incentivized in the Bitcoin economy. Buyers are incentivized to promote the network because the more people come on board, the more valuable the coin starts to accumulate perceptually.

Knowing what we know about extrinsic and intrinsic value, we can see the components tied to blockchain. Bitcoin can carry extrinsic value because it can be used as a medium exchange, just as a currency would. It has intrinsic value because it is secure, based on trust, cooperation, decentralization, faith, and other forms of value. Combining these forms of value creates a flywheel for the agents involved in the economy. The more people see and use the coin's value, the more value the economy attracts. The increase in value is why Bitcoin has reached over a trillion-dollar market cap in a relatively short time. Bitcoin is not the incentive machine out there. As more blockchains come around, the more specialized the incentives and forms of value start to arise. The encapsulation of these rewards is also known as tokeonomics.

In my opinion, viewing things from a macro viewpoint and attaching the knowledge of economics to web3, you start to get the complete picture of why things are working. Okay, with that being said, we can now transition into some of the most talked-about areas of web3. Cryptocurrencies.

7.

Cryptocurrencies

“All money is a matter of belief.” - **Adam Smith**

Cryptocurrencies will probably be one of the first things you hear about when learning about web3. You will hear stories about how some currencies (also called coins) bring exponential returns and that there’s always a new hot coin on the rise. Cryptocurrencies are a recent phenomenon because they carry a lot of principles that traditional currencies have. It is important to note that cryptocurrencies are in their infancy, and there is a lot of uncertainty in the space. There is a lot of volatility in cryptocurrencies, and I emphasize that this is not financial advice, rather an educational curriculum on the subject.

Cryptocurrency and Fungibility

Let’s start by defining what a cryptocurrency is. By definition, a cryptocurrency is encrypted data on a blockchain designed to work as a medium of exchange. These currencies are created by quantifiable units called coins or tokens. These tokens are what is known as fungible. In the context of money, $100 can be represented by a single $100 bill or by five $20 bills, ten $10 bills, one hundred $1 bills, or any combination of bills that sums up to $100. Fungibility seems like a fairly intuitive concept, but we’ll discuss how things can be non-fungible and still carry value. Cryptocurrencies are the fungible representation of the value of a blockchain.

One thing to distinguish here is the difference between a coin and a token. A coin is the network reward of a blockchain how Eth is the coin for Ethereum. A token is a reward built on top of a blockchain that is not the

blockchain's network reward. Sometimes these are also called Alt Coins. On Ethereum, there is something called ERC-20 tokens, which are fungible currencies that anyone can create. Let's say If I were to create a currency on top of Ethereum and call it Tint Coin, it would be a token because I am building it on the Ethereum blockchain and not on my own blockchain. I will interchange the usage between coin and token quite often. Okay, moving from here, let's look at what gives a coin market value.

1: Market Cap

Each blockchain will make their cryptocurrency have a fixed supply or endless circulation. The supply of a cryptocurrency leads to coin circulation, which is how many coins have been distributed. For example, Bitcoin has a fixed supply of 21 million Bitcoins, meaning that there not be more than 21 million bitcoins in existence. For example, Bitcoin has a fixed supply of 21 million, but the way Bitcoins get mined, miners will mine the last coins in 2140. The fixed supply amount was hardcoded into the production code by Satoshi.

On the other hand, Ethereum has an endless circulation supply, and they have processes to combat inflation. More about that soon. Something worth noting is that about cryptocurrencies is that all transaction activity is stored on the blockchain ledger and accessible for everyone to see. So the economic value of a price starts to get affected when supply and demand come into the picture.

Based on the coin circulation and buyers' demand, the price can go up and down. The total economic value of a blockchain is known as a market cap. The market cap is calculated by knowing the price per coin multiplied by how many coins are in circulation. Let's give a live example. At the time of writing, Bitcoin is around $48,000, with about 18.9 million Bitcoins in circulation, equating to about $904 billion. Calculating the market cap is a relatively simple process but where things get complicated is the reasoning of why people want to buy or sell the coin.

Supply and Demand

As we mentioned in the economic section, the more economic activity agents engage in, the more the economy expands. So if more people start using a cryptocurrency, its economy starts increasing, leading to a change in the supply and demand of the coin. More usage of the coin leads to an increase in demand,

and it starts impacting the available supply for sale. People will have different incentives to engage in the market. Some people will focus on being traders, which is when they actively buy and sell the currency to strike profit. Other people may believe that the coin's value will increase, so they hold or are also known as hodl. By hodling, the supply for sale goes down, and as more people buy, the value goes up. Regardless of the reason for someone changing the supply and demand of a cryptocurrency, it derives from their incentives. Whether it is based on extrinsic or intrinsic value, people dictate the economy and the market of the chain.

1: Exchanges (CEX, DEX)

People can obtain a cryptocurrency through mining or, more commonly, by buying them on exchanges. An exchange is a middleman to buy and sell crypto. Under the hood, an exchange's operations are complicated due to the amount of technicality they take to build, but the premise is that buyers and sellers use the exchange to buy and sell. You tell the exchange how much of a cryptocurrency you want to exchange from fiat or another cryptocurrency. The exchange handles the transaction and takes a small percentage fee. That's the business model of exchange.

There are two types of exchanges in crypto. There are centralized exchanges like Coinbase, FTX, Binance, and others. They are called centralized because they have to follow regulation policy and collect information about their users. When people talk about centralized exchanges, you might hear something called KYC (know your customer). The other type of exchange is a DEX (Decentralized Exchange). A DEX is a platform that allows peer-to-peer exchanges without the need for a middleman. DEXs are attractive to traders because the markets operate differently from CEXs by being more effective in preventing price manipulation and allowing traders to stay anonymous (No KYC).

Exchanges are not new, they've been used for centuries in traditional finance, but the innovation of crypto allows for new purposes. More than likely, the first time you get crypto, you will do it through an exchange, even more likely a CEX. They make it seamless for consumers to start purchasing or exchanging crypto. It is now time to start talking about one of the first mainstream adoptions of crypto. DeFi.

8.

Defi

“DeFi is an open and global financial system built for the internet age – an alternative to a system that's opaque, tightly controlled, and held together by decades-old infrastructure and processes. It gives you control and visibility over your money. It exposes you to global markets and alternatives to your local currency or banking options. DeFi products open up financial services to anyone with an internet connection, and they're largely owned and maintained by their users.” - **Ethereum.org**

Decentralized Finance (DeFi) is an open blockchain-based form of finance with no central financial intermediary, allows anyone to join, and operates autonomously through code (smart contracts). DeFi is a global economic system no longer tied to a central government. Crypto and fiat currencies are now competing on a market valuation, taking us to a new paradigm of financial infrastructure. Assuming that their government hasn’t banned crypto as China did. DeFi allows people to move assets in a unique manner that wasn’t possible in traditional finance. Anyone with an internet connection can get started in the DeFi economy. This level of accessibility brings more inclusivity to people who’ve previously been marginalized in financial systems. In simple words, DeFi allows people from around the world to be part of an open financial structure and operate financial assets in a new manner.

The same concepts of traditional finance apply to DeFi, things like using a currency to trade, insuring against risks, operating loans, earning interests, and other financial capabilities but at a new level of operations. Innovations like Liquidity Pools, Flash Loans, Liquidity Mining, Stable

Coins, and other feats have given DeFi its wings. Let’s begin with talking about how money moves in DeFi.

Liquidity Pools

A liquidity pool is a collection of funds stored inside a smart contract. What is unique is that all transactional activity is handled autonomously with no central authority. DApps (Decentralized Applications) like Uniswap, Sushiswap, Curve Finance, Bancor, and others started to use liquidity pools to create markets for the exchange of cryptocurrencies.

A liquidity pool works because it allows people to buy or sell no matter how high the cryptocurrency’s price, time of day, or a seller or buyer. In contrast with traditional finance, trades are operated through what’s known as an order book, which is when buyers and sellers submit their order to an exchange with a specific price point for what they want to buy or sell. When a buyer and seller meet at the same price, the exchange executes the transaction. With DeFi, there is no central mediator, and the transactions can happen at any time or at any price. Sales automatically happen because liquidity pools run off algorithms called automated market makers (AMM). Let’s break AMMs down.

Automated Market Makers

AMMs allow for liquidity to happen at any time because the trading is done internally with the liquidity pool’s cryptocurrencies. A special formula allows for AMMs to work; it’s quite simple. The formula is tokenA_balance(p) * tokenB_balance(p) = k. This is called the constant formula because the variable k is a constant balance, and it will dictate the price of the other assets. The tokens are the assets inside a liquidity pool. Following this formula will give the quantitative amount and price of the assets inside the liquidity pool. The formula will create a dynamic price point of the assets inside the liquidity pool as there is a change in the supply and demand. A simpler form of this formula is x * y = k but will not be using this formula.

Let’s do a mathematical metaphor for the constant product formula tokenA_balance(p) * tokenB_balance(p) = k. Let’s use token A as Ethereum with a balance of 10 and a price of $5,000. Token B will be Bitcoin with a balance of 1 and a price of $50,000.

So to recap our assets, 10 Eth tokens = $50,000 and 1 Bitcoin = $50,000. This gives us the constant of 2,500,000,000 (50,000 * 50,000).

Our formula would like like
10(5,000) * 1(50,000) = 2,500,0000,000

So now let's say we want to trade 1 of Eth for Bitcoin. We'd have to figure out the price points for each asset with the constant product formula.

Since we are moving 1 Eth, we now have 9 Eth at a new price and the variables to change our constant. Here is how the math would play out.

First, we have to find the new value of Bitcoin in the pool to find the latest price of Eth.
We add the 5000 from the 1 Eth sale onto the original amount of Bitcoin 50,000. This gives us a sum of 55,000, and we use this number to divide the constant.

2,500,000,000 / 55,000 = 45,454

This is the new price of 1 Bitcoin in the liquidity pool. The price went lower because there is now more Bitcoin inside the liquidity pool when we exchanged Eth for it. The price change may be confusing at first glance but converting Eth into Bitcoin makes Bitcoin less valuable because there's more of it in the liquidity pool.

Next, we have to find the price of Eth.

9(x) * 1(45,454) = 2,500,0000,000
9(x) = 2,500,0000,000 / 45,454
9(x) = 55,000
x = 55,000 / 9
x = 6,111

We need to make sure our numbers are correct. Our new price values should equal our constant.
9(6,111) * 1(45,454) = 2,500,000,000.

Bingo, we got new price updates inside our liquidity pool that are automatically updated by a smart contract. As you can see, the lower the supply of one asset becomes in a liquidity pool, the more expensive it becomes, so the goal is to try to keep the ratio 50:50 to keep a stable price. However, when the supply fluctuates, traders come in to trade if they see an opportunity. For example, if they see that the Bitcoin price is lower in this liquidity pool than in exchanges or other pools, they can swap some Eth and get the Bitcoin at a cheaper price. Following that, the trader can trade the Bitcoin at an average market price on another pool or exchange to profit. Moving crypto like this is also known as arbitrage trading. Automated Market Makers move billions of dollars of cryptocurrencies. In 2019, market predictions estimated that about $10 billion was locked in DeFi and liquidity pools, and at the end of 2021, there is an estimate of $97 billion.

You may be wondering how liquidity pools get the funds to grow. Anyone can provide the funds in a liquidity pool. A holder with cryptocurrency can stake their tokens into the pool, and they will receive returns from the AMM transaction fees. The returns that the investor gets are called the Yearn. It is common in the industry to call this liquidity mining. Some platforms will offer higher yield percentages, but that usually comes at a risk. Sometimes bad smart contracts could lose all the funds in a pool to a vulnerability, and all investors lose their money. This field is very novel, and there have been significant flaws that have lost billions of dollars.

Flash Loans

Another innovative component to DeFi is flash loans. Aave was the first DApp to introduce the capability to do uncollateralized loan options in DeFi. Flash Loans are rapidly executed loans where the principal amount needs to be paid back within the same transaction. A flash loan can revert if the principal amount is not paid in the transaction. The smart contract will only be approved if the principal amount is paid. Flash loans are still very experimental, but some users utilize them to do transactions where users will spend less on fees. Let’s say that you liquidate your coins from a liquidity pool, but many people are causing the take-out percentage to be higher than usual. You can use a flash loan to convert your initial coin to another coin and then exchange the new coin at a lower percentage fee.

Stable Coins

Stable coins are cryptocurrencies that are pegged to the US dollar. Meaning one stable coin equates to one US dollar. Essentially stable coins are utility tokens built upon another coin's blockchain. The point of a stable coin is to be a cryptocurrency that is not volatile. Their value of stable coins to users is that they offer the convenience of privacy and security of crypto while offering the stability of fiat money. Stable coins are a haven for traders as they are utilized for trading in liquidity pools. Trading with stable coins allows for lower transaction fees, instant trades and allows risk-free procedures from centralized tracking. On top of that, stable coins earn a significantly higher interest rate when staked than compared to fiat currency.

A stable coin works in two ways: fiat collateralization or smart contract manipulation. A stable coin should be backed by fiat collateralization, meaning that there should be a fiat dollar for every stable coin. On the other hand, we have algorithmically pegged stable coins (APSC). Both have their pros and cons. Fiat collateralized tokens are less volatile but more difficult to audit and can be more vulnerable to someone within the protocol to steal some tokens. ASPCs are more volatile, but there are algorithms to get one US dollar price point. The algorithms use smart contract manipulation to change the number of coins in your wallet dynamically, so the value stays at $1 or a money printing and bond reward system to adjust the price to $1.

Okay, so now that we got an overview of DeFi, it's time to talk about perhaps one of the most essential things in web3. Essentially your identity on the web. Wallets.

9.

Wallets

“You are what you do, not what you say you’ll do.” - **Carl Yung**

A wallet, also known as an address, is your identifier on the blockchain. It points to all the wallet’s data on the blockchain. I like to view a wallet as the digital passport for blockchain. Every action you add to the blockchain is a stamp to your wallet, just like when you travel to a new country, you get a stamp on your passport. The more actions this wallet has on the mainnet; the more data is tied to it. Before we dive further into wallets, we need to talk about the heart of web3. Encryption. I mean, it’s called crypto for a reason, and here is why.

Public and Private Keys

A wallet comprises two core components: a public key and a private key. A public key is an address that is available for anyone to see. If you look at any transaction on the blockchain, there will always be public addresses interacting with each other. When people share their wallet address, they usually share their public address, not their private keys. Public keys only allow you to read data, not create data.

The creation of data is done with your private key. A private key is what gives the signature of approval to the transaction. You can view your public address as your email and your private key as your password. Private keys are your digital signature. Whenever you approve a transaction, you use your private key as a digital signature for validity since you should be the only one with access to it. Both hot and cold wallets have something known as a seed phrase, a phrase of 12 words that you must input to log in to your

seed phrase, you will never be able to recover your wallet. More on that at the end of this section. So to summarize the two components of a wallet, your public key is the address on the blockchain, and your private key is your digital signature of approval for a transaction.

Asymmetric Encryption

Having two types of keys is known as asymmetric encryption. You have a key to read and decrypt information (public key), and you have a key to create and encrypt data (private key). Having two keys is an essential usage of cryptography because it allows people to send information safely. In comparison, there is something called Symmetric Encryption when there is only one key to encrypt and decrypt data. There is a huge security vulnerability in giving the key to someone else. Anyway, the key is delivered, whether it's via email, text, letter, or any possibility, it would introduce the risk of someone else obtaining the key and gaining access to all the information.

On top of that, the person you trusted with the key can give a copy to someone else, and the new person will be able to decrypt any information tied to the key. The encryption and decryption availability is why asymmetric encryption is the solution. Data will stay more protected and only be decrypted by those it was intended for.

Cold Wallet and Hot Wallet

You’re probably going to hear the terms hot wallet or cold wallet. They have interesting names, but they are pretty easy to understand. A hot wallet is simply a software wallet; Where you use an application to get your public and private keys. Hot wallets are much easier to use and are meant for everyday crypto users. If you are a bit savvier and want to focus on security, you would probably get a cold wallet. A cold wallet is a hardware wallet that keeps your crypto offline. Cold wallets are tough to hack since they don’t have vulnerabilities from the web. If you have your cold wallet, no central app, government, or exchange can revoke your crypto, allowing for sovereign ownership. However, since you physically need the wallet, there’s nothing you can do to claim your crypto if you lose it.

Ownership and Identity

Perhaps one of the most compelling parts of a wallet is that you own the data inside of it. Since data from blockchains are decentralized, no central authority can revoke the data inside a wallet. Anything a wallet adds to the mainnet will be there permanently.

Decentralization leads to a central identity that wasn't available before. Let me explain how centralized sites prevented people from building their identities on the web. Every time you sign up for a web2 app, you have to create a new account on their database. So when you sign up on Facebook, Twitter, Reddit, etc., all your information stays siloed because each database is tied to the company. Having data be siloed in different databases isn't optimal as a user because your data can travel with you when you join new platforms. It starts from scratch every time you sign up on a new site. For example, if you have 100,000 followers on a platform, you can not bring them to another platform.

On the other hand, all future DApps will share a single database with blockchains, meaning that all information tied to your account can move from platform to platform. Information ownership is not linked to applications anymore and allows individuals to build a more robust online identity. Imagine that you accomplished 1,000 tasks on one platform, have 100,000 followers on another platform, launched five projects, and own 100 NFTs; all that information could be tied and verified to your identity now. The days of individuals not owning their information will be gone with web3.

Another big talking point in crypto is how users are at the mercy of central platforms. We see this especially with social media platforms becoming more aggressive on deplatforming accounts. The viewpoints of why people should be deplatformed are subjective that cross over to ethical and political standpoints. Still, the premise is that a central authority can shut down anyone if they feel like it. Sometimes the reasoning for excluding an account may be "just," and sometimes, it may not be. People are advocating that the future of social media will lean more towards a decentralized approach where it will be harder for a platform to ban users.

A decentralized social platform could work by allowing users to sign up with their

wallets. Since the ownership of the wallet is tied to the blockchain, the DApp will not be able to delete the wallet. The app could ban that specific address, but it won't be able to delete it. On top of that, the DApp could introduce tokenomics to allow wallets to receive tokens for the activity they bring on to the platform. Venture capitalists and builders mention that social media on web3 has not had its Satoshi moment, which means that there isn't a DApp that has figured out how to get product-market fit. Maybe you can be the creator of that.

1: Lost

One of the biggest issues with wallets is that it is lost forever if you lose access to your account. There are no processes to recover your account. Losing your seed phrase is an ultimate tragedy in web3. It is not like losing your password in traditional logins. The reason for that is that there is no way to decrypt information to reveal your password, nor is there a database that can grant the creation of a new password. There have been many accounts with millions of dollars in crypto that get locked out, and there is no way to pull out the crypto. So now that we touched on wallets let's dive into one of the most exciting fields in web3. NFTs.

10.

NFTs

Non-fungible tokens are probably the most recent craze that has attracted new users into web3. NFTs are an exceptional innovation because they mesh economic, sociological, and technological viewpoints. It is common for some people to love them and for some people to despise them. Both sides can follow extreme narratives, and both have their validity. I will be discussing NFTs from an optimistic viewpoint and focus on the potential buildout they can bring to the world. If we look at the technological and socioeconomic components, we can see that NFTs get something novel to the world. We can now verify digital ownership of an asset with NFTs. That sounds quite simple, but there is an incredible amount of complexity that NFTs are solving. First, let's define what NFTs are and how they could shape the future.

A nonfungible token is an identifier that is one of a kind, and its ownership is registered on a blockchain (not just a JPEG). It is called nonfungible because these tokens have unique value and can not be equally interchanged for other assets. If you recall, when we discussed cryptocurrencies, we mentioned that cryptocurrencies are fungible, meaning that people can predict the token's value and are easily interchangeable. The currency's value can be summed up and precisely quantified, while for an NFT, it is entirely unique and dynamic. For example, the value of a painting can range from $10 to $10,000,000. A painting is nonfungible because its uniqueness will dictate its interchangeability with other products or currency. What's exciting about this space is that any object can become an NFT by simply adding it onto a blockchain.

Ownership

In my opinion, one of the most powerful components of an NFT has to do with ownership. As we mentioned in the wallet section, once the data of a transaction gets added to the mainnet, the only way to change ownership will be if the private key approves another transaction. Once you own an NFT, it is yours until you decide to sell it or possibly burn it (discard it). Some people say they can own an NFT because they can download the image, but ownership is not tied to the blockchain. These groups of people are called “right clickers” because you right-click to download an image on the web. Right clickers do not have their wallet being the NFT owner in the mainnet, hence not truly owning the NFT on-chain.

Having ownership of a digital identifier in a decentralized blockchain is a game-changer to economics. It is the introduction to property rights in a new aspect. Since an NFT can essentially be anything, anything can be created and owned digitally. You can see how this can lead to the conversation about the metaverse, but let’s save that for the ending parts of this book. Going back to NFTs, they give the digital world a method for actual validity of ownership. Verifying digital ownership is monumental because we have never accomplished validity like this before. Before, people could save and upload things, but there was never legitimate ownership on a shared ecosystem. Now all digital identifiers can be tied and verified on a blockchain. This concept is a paradigm shift way to how the internet will operate.

Let me emphasize what I mean on this point a bit more. Let’s go back and take a look at the history of trade. Trade has been around for as long as humans have existed. It is coordination for the exchange of value. Throughout the centuries, new innovations progressed trade. When trade started, it was limited to local villages, and then cities became central hubs for business. People made more sophisticated trade routes, and merchants used animals and carts to carry more items. Fast forward a few centuries, and we now have 18 wheeler trucks, cargo boats, airplanes, and a logistics system to move trade at a scale never seen before. However, this trade is only done for physical items as there was no legitimate way to trade items over the internet. The reason was that there wasn’t a shared agreement on ownership since the items were digital. As more people adopt blockchains and see that they are truth-ledgers and can verify ownership wallet to wallet, trade in the digital era has begun. It is a novel way for trade to be

experienced, now in the digital realm.

1: What Gives an NFT Value?

One of the biggest questions there is when it comes to NFTs is, “what gives it value?”. Well, there are many answers. Good thing we covered value theory in the earlier sections. You see, NFTs are dimensional products that can carry extrinsic and intrinsic value. Most commonly, the extrinsic form of value will be tied to an NFT’s social signal or utility. The extrinsic value of an NFT will have an external purpose and usage. This value can range from an NFT’s social symbol of wealth to a ticket to gain exclusive information or a financial instrument that yields you tokens.

On the other hand, some NFTs are purely based on intrinsic value. Some people enjoy buying NFTs for the pure sake of appreciating art, because they believe in the team’s mission, or they like the creators. People in the community commonly refer to this as “no roadmap, just vibes,” meaning that they are only buying the NFT because they like it and are not focused on an extrinsic form of value. Both extrinsic and intrinsic value gives people incentives to purchase NFTs, which some sales have been documented in the 8 figure ranges now.

Some NFTs can not be bought but instead only earned. For example, we can now create a digital certification for proof of completion or attendance into an NFT. This means that the wallet owner can now have a digital identifier in their wallet that they earned for meeting the requirements. In this example, we could take a look to see if someone has proof of attendance and they did it themselves. Since NFTs are unique, and all data of the NFT is trackable, we could verify that this person earned this NFT legitimately and didn’t cheat by having someone else swap it over to them.

2: Dangers of Speculation

There is a lot of speculation in the NFT space, people buying into projects hoping that the value of NFT goes up. When this is done irrationally, it is called “aping” because it is very primitive behavior. Buying off pure speculation could be a damaging and risky form of allocating capital. Unfortunately, when it comes to spending money, our cognition sometimes doesn’t allow us to think things through properly, and it could introduce the possibility of bad spending. It is not common to

hear that people come out financially damaged because they made bad NFT purchases. NFTs could be expensive, and it is an unregulated market, so bad spending may put certain people at financial risk. It is important to be cognizant that if you purchase NFTs, there is a high risk of losing money.

3: Are NFTs Assets?

Defining if an NFT is an asset is a difficult question to answer. The answer is yes and no. NFTs are broad products that can be viewed as assets or consumer products. If the intended creation of an NFT is to create a return on investment for its buyer, then it should be tagged as an asset. Even more, it could be classified as a security. In the United States, the SEC can define an asset as a security if the future proceeds depend on the work of others. Meaning if people purchase an NFT in expectation that the operating team will make the NFT a financial instrument that will bring a return on investment, the SEC could deem it a security. If all NFTS get classified as a security this would mean that the creators of the NFT need to follow US regulation laws to comply and not violate the laws. Please note that I am not a financial advisor nor have in-depth competence with regulations. The field is so novel that even experts in the area are figuring out the dynamics of NFTs.

4: What Type of NTS are There?

NFTs are very diverse in not just art but also the product type. An NFT can range from a certificate of proof, to a 1 of 1 art piece, to a unit in a collection. It is an exciting time for the space because many innovations are happening due to more buyers and sellers entering the market. The massive explosion of demand took Opensea, the most popular NFT marketplace, to process $328 million in July to $3.4 billion in August. That was a 10x growth in a single month. With that money movement, people start flocking in and building new things.

A. Proofs

NFTs can represent proof of identity, completion, attendance, or any conceptual area tied to ownership. Being an edtech founder here is one of my favorite ways NFTs can prove education. Let’s say that you earned an NFT that is proof of completion for a course. This course has the prestige of carrying a lot of validity. Only a few people can be skilled enough to pass the course.

On top of that, the creator of the NFT is a highly respected institution that people admire. Even outsiders know that this NFT carries a lot of validity because it is extremely challenging to get, and a credible source distributes it. So then, if someone showcases that they have that NFT in their wallet, people will trust that this person knows their stuff. This person has proof of completion with the NFT. Earning this NFT makes its type different because the purpose is tied to a specific user, and its value is earned. Hence transferring to another person defeats its purpose.

B. 1 of 1s

1 of 1 NFTs are mostly collector-centric. An artist only creates one piece and only allows one owner. Imagine if Picasso was selling a painting. People would spend a lot of money to buy this piece because there's only one, and Picasso created it. Technically any artist can make 1 of 1s, but the ones that get the most recognition are those by artists that have a massive influence.

C. PFP Collections

Usually, a team creates a theme-based collection that is made up of several units, sometimes ranging from a few to several thousand. Units inside a collection are perhaps the most popular type of NFTs. These units are often used as a PFP (profile picture) to represent ownership and commitment to the collection. From what I've seen, these types of NFTs have brought the most innovation to the space. The reason collections are so powerful is because it allows individuals to build a new identity based on the theme of the project. On top of that, getting like-minded individuals who share the belief with the theme fosters a solid community. Within these types of NFTs, you will see the word community because people can now access and have ownership to identifiers that align with their beliefs.

On top of that, these collections can also operate as a business. It is quite common for a collection to have something known as a roadmap. Essentially, it is a documented vision board with milestones the team hopes to accomplish with funding from selling the NFTs. As a collection gets more and more recognition, the more ambitious the roadmap

becomes alongside the community's strength. Perhaps one of the most impressive collections to arise is the Bored Ape Yacht Club (BAYC). At the time of writing, Yugalabs, the creators of the BAYC and MAYC (Mutant Ape Yacht Club), have traded about 390,000 Eth, which comes out to be about $1.56 billion. The crazy thing is that all that happened within a year. There are plenty of other collections generating impressive numbers and fostering strong communities.

D . Digital Items

Many conversations have circled how video games will create NFTs so the players can now have ownership over the products they purchase. In this case, let's say that a player bought a special helmet for his character. The player can now sell that helmet to another player and get most of the transaction revenue. Owning digital items would be a revolutionary aspect of gaming because players never owned digital items. NFTs in the gaming space sounds exciting, but what is currently happening in a social climate is that specific gaming demographics despise NFTs. Companies have had to pull back NFT initiatives because certain gamers have threatened to stop supporting companies that support crypto. Their reasoning ranges from NFTs not being legitimate to crypto being bad for the environment. These points carry validity weight, and we will discuss this in further detail in the Philosophy, Law, and Ethics of Web3 section.

11.

DAOs

Decentralized Autonomous Organizations. The name says it all. The purpose of a DAO is to allow individuals to contribute to an organization with no central hierarchy autonomously. This organization can be a business providing a service, a nonprofit community, or any form of people collectively working together. The way a DAO gets established is usually by a group of people that focus on providing a purpose, recruiting early members, and then obtaining some form of funding. Money for a DAO can come in many forms, whether it is self-funded by the team, grants, or sometimes the DAO can have a product that generates revenue.

There isn’t an established norm of what contributors can expect when joining a DAO. Some DAOs focus more on exclusivity where users have to pay to gain access, some you have to apply for, and some are completely open, and anyone can contribute at any moment. The premise of a DAO is to be decentralized, but since decentralization is a spectrum, there will be different levels to it.

DAOs are a fascinating form of coordination because they can solve problems that traditional organizations have not been able to. People in the community call this “transcending orgs” and believe that allowing people to contribute to an organization autonomously can change the world. One of the best narratives I’ve heard about this transcending org is if we want to solve massive global issues, we need a valid international operation process. For example, if we’re going to plant 10 trillion trees to combat climate change, we’d need the world’s coordination to achieve that due to its scale.

Centralization in DAOs

Even though DAOs focus on becoming decentralized, there are elements of centralized power. There is usually a core team of members with authority over certain aspects of the DAO. It is typical for the core team to approve the roadmap, set compensation rates, officially represent the DAO and other areas. Most DAOs prioritize making all core team operations transparent and inclusive of opportunity. The culture does revolve around openness and transparency. So far, it does seem that there needs to be a degree of centralization for DAOs to work.

Contribution

Typically when you want to contribute to a DAO, the responsibilities are documented of what tasks need to be accomplished, what team does what, and when deadlines are. It is common for DAOs to be broken down into guilds, which are groups focusing on one area of operations. One exciting comparison point here is that you need permission to start working in a traditional job, but in DAOs, you can begin working as soon as you'd like. Effective DAOs will have an internal system for progress tracking and internal communications. Just like a strong company would.

Contributors might work alone or work in the guilds to provide solutions. As the contributor proves their competency and completion to the DAO, they can gain recognition. The gain in recognition could lead to gaining a position with more responsibilities. It is important to note that in DAOs, there isn't a traditional form of hierarchy where there is a CEO and the officers report to the CEO. Instead, it is a horizontal organism where the collective community moves the DAO forward.

Fluid Employment

DAOs operate similarly to companies and open an alternative career development route. Working in this manner is a new concept to the way people work, and it will take a lot of time to refine and create a structural process. This new way of work needs to be proven because there are a lot of risks that traditional employment already solves. Areas focusing on income taxing, company health insurance, retirement plans, etc., are going to have to be addressed by DAOs to make sure contributors can be stable in the workforce.

What makes DAOs compelling for some people is that they can allow for fluid “employment.” Compared to traditional employment, their entire career focus revolves around their hired company when someone joins a company. With DAOs, users can simultaneously work in other DAOs because the structure is more fluid. On top of that, the amount of time dedicated to the work is up to the contributor, meaning working hours can range from 7 hours a week to 50 hours.

Payments

Payments in DAOs are still in their infancy stage, and there are a few ways they currently are being done. Let’s start with the most simple—full-time work. Just like in a traditional career, when you are under full time, it means it takes up the majority of the time. What is different in full-time DAOs is that the legal restrictions are not the same. DAOs are less competitive, meaning that you can have your full-time role in a DAO but still be in other DAOs. Being full-time is more correlated to the amount of time rather than the legal limitations of regular jobs. A few DAOs require full-time workers to sign anti-competitive clauses, but it is not as common in the DAO scene. Perhaps in the future, as DAOs evolve, they will adopt more of a traditional structure.

1: Tokens

Some more savvy DAOs can create an internal token that owners can exchange in liquidity pools. Having tokens does mean that the DAO has to have its backers and that the tokenomics behind it are strong enough to support a currency. So let’s say that a new contributor joins a DAO, proposes a new project, coordinates with the team to complete it, and delivers it promptly. The DAO will weigh the relevancy of work and allocate tokens to this contributor. The benefit of DAOs paying in their token is it works as capital compensation, and if the value of the token increases, their treasury now has more capital to spend. Sometimes the tokens are not financially valuable, and they are social tokens to represent a symbol of recognition.

2: Bounties

Perhaps the simplest payment method is bounties. People will reward these fixed amounts of capital if someone solves the problem (the bounty). Bounties are most commonly known in software development, where developers are paid for finding errors in the code. However, DAOs can pay bounties for nontechnical tasks as well.

Since the price is fixed, the contributor can decide if they want to take on this bounty in the first place.

Let’s do a hypothetical experience on how contributing to a DAO can become a new form of employment for someone. Let’s begin our story with someone named Jose finding a DAO that focuses on providing a solution this person is passionate about. Let’s say it is reforming post-secondary education. Jose joins the DAO’s discord channel and converses with community members who share similar beliefs. From here, Jose gets inspired and writes a well-thought-out blog post on how the future of education can look like. He presents it to the community, and everyone loves it. The DAO wants to upload this piece onto the DAO’s blog and give him recognition. From here, the DAO has a task to get a meeting with theUnited States Secretary of Education. Jose starts leveraging his social followings and fortunately gets a few connections that set up the meeting. The DAO recognizes Jose’s accomplishments by giving him some funds. Jose and other members of the DAO collectively worked together to create a policy plan that will allow for the accreditation of autodidactic learning activities. The meeting takes place, and the Secretary of Education grants the DAO $5 million to start building. All the progress and competence Jose has displayed makes him one of the most respected individuals in the DAO and spearheads new projects. He even became part of the core member team. From sharing his viewpoint about a passionate subject, Jose now makes a healthy amount of money and creates a massive impact in a space he cares about.

Jose’s example is just one example of how individuals can get great opportunities through a DAO. Some people will take more of the flexible approach where they jump around from DAO to DAO and contribute to specific areas. There is a lot of exciting movement in DAOs, and the evolution is not slowing down. If DAOs prove themselves to the world, we may now approach the world problems we are trying to solve differently.

12.

Culture and Communities in Web3

Culture is the invisible fabric that creates the operating system within people. The combination of social behavior, beliefs, and knowledge make certain conduct that acts as a guideline for behavior among people. Adopting culture is a social learning experience through explicit instruction and observations. Culture will be a big part of your web3 journey.

It is imperative to distinguish that some regions of web3 will have different cultures. Cultural differences can range from blockchain beliefs to social etiquette. For example, the Bitcoin folks value self-sovereignty and stand on many contrarian viewpoints. Ethereum folks value decentralized creation and are focused on building innovations. DeFi folks appreciate open markets and less bureaucratic operations, so they create open trade. NFT folks value ownership of digital property, so they spend high amounts of money to purchase. Each of these areas can have sub-sectors to get more specific on their culture. The amount of culture domains in web3 is astonishing.

Even though there is incredible diversity, general concepts and words are shared among the web3 space. WAGMI, gm, fren, anon, ser, degens are some of the words you will be exposed to when you’re exploring the social terrain of web3. Currently, Twitter is the primary social platform where crypto folks engage; this side of Twitter is called CT(Crypto Twitter). Reddit and other forums have fantastic communities, but it seems that the information rate on Twitter is at a higher output.

When a collection of people with similar interests actively

engage, a community forms; communities are social units where people with commonalities get together. As you start exploring the domains of web3, you will meet others who share the same interest as you and will probably begin to get embedded into communities. You might be wondering what's the difference between a DAO and a community and simply put, a community is just a social group. At the same time, a DAO is an organization with a purpose to execute. There are many ways communities are getting fostered, but one of the most common is to join their Discord. It's just a giant group chat that can be divided into topics of conversation. Community members actively chat with each other discussing various subjects on Discord.

The reason communities could be so prevalent in web3 is because the space is challenging, novel, and impactful. These are some of the attributes that help build camaraderie. It is common knowledge that humans bond differently based on specific variables. The conceptual context of web3 is a cocktail for people to connect. An excellent example of this would be when things are challenging, humans become more receptive to receiving support, and those providing support intrinsically feel better. Some interesting social theory studies discuss that bondages between soldiers that went through war together are embedded deeply into their psyche. The concept is that the more difficult an experience shared with people will foster a stronger bond. Now comparing going to war and learning web3 are extremities, but the premise is that learning web3 will be challenging. Communities are a great place to get that support that can help you.

When things are novel, people are always curious about a new potential. Some evolutionary psychologists believe that curiosity about novelty is what helps humans progress and innovate. The novelty scale of web3 is enormous, so a great number of people are coming together to learn this field. The collective act of seeking this new novelty brings people together. A metaphor for this could be exploring new terrain. To increase your chances of having a successful voyage, it is best not to do it alone and be alongside people who are willing to work together.

Another main pull for web3 is the concept of impact. The ability to exert energy into an idea that you believe will have a massive power of change has opened. With web3, people can become creators and builders of new grand concepts. Blockchains are allowing for essential areas of life to be disrupted, and people can participate in these changes. It is no longer that this level of impact was esoteric

and available to certain people. For example, before, to create a massive impact in tech, you had to physically live in Silicon Valley because that’s where all the people and innovation were happening. Those who weren't in the peripheral location of the valley were excluded. On top of that, the culture of information used to be much more closed source was in contrast with web3, open-source rules, and the innovation is happening through the web. Communities are the people that foster their beliefs together to work on something that could have a massive potential impact.

13.

Metaverse

History and the Future of Web3

This section of the book will be more subjective as it derives from my viewpoints and narratives. It is important to dedicate a section to discuss epistemological areas that focus on the boundless territory to develop new forms of thinking. At the end of the day, our human tendency is to build narratives based on the stories and information we get exposed to.

Technology: *“The change and manipulation of the human environment.”*

Maybe this book should’ve begun by discussing the origins of technology and what it has done for humanity. I didn’t decide to talk about the concept of technology initially because I assumed that the average reader could generally grasp the impact technology has already made on humanity. However, I do believe that even though we can acknowledge the relevance of technology’s impact, we are constantly cutting it short and can not fathom its true impact.

Britannica has my favorite definition, and it is “The change and manipulation of the human environment.” We now usually think of technology only tied to the digital spectrum, but technology is not just that. Humans harnessing technology is an effective utilization that no other living species can do on our scale. Hundreds of books cover the origin and progression of technology, but I want to give a quick linear overview of how the past leads to the future. Essentially, we are leveraging technology today as a

stepping stone into a new paradigm. In this paradigm, everything could be different. From the way matter interacts to the social dynamics. The possibility for humans to create the metaverse.

From Tools to Bits

Homo-sapiens, also known as Humans, started as a primitive animal that eventually became the omnipotent species on Earth. This power and leverage did not come from our physical strength but from our capabilities to exert cognition. Our cognition allowed us to increase our chances of survival in various manners ranging from coordination with other humans to changing the environment. One of the most crucial exertions of cognition was the creation of tools. In this context, we'll define a tool as an item that increases influence or power for the desired outcome. Tools became the extension that allowed us to scale technology. For example, when humans needed to hunt, they sharpened rocks and tied them to long sticks to throw. Sharpening rocks was the first step to creating tools of weapons. The tools of weapons allowed humans to obtain food more efficiently. Humans started a linear progression of advancing tools to create massive advancements in technology.

Most of the significant technological advancements humans have created have predecessors. When we look at urbanization and the population changes moving to more centralized locations, it was only possible with the leverage of agriculture. With agriculture, people had a system to manipulate their environment and have food for growing centralized populations. When urbanization started to advance, it led to an acceleration of trade. With cities, merchants had more availability to trade at a more grand scale. As trade evolved, it led to innovations in finance, where currencies and ledgers started to get used among society. Finance and trade were the stepping stones to the industrial boom where products began to become commodities, and a new wave of commerce and operations emerged. This new wave introduced a complexity where we needed the help of computational machines to solve. Computers and hardware started accelerating the process of information, and soon, we invented the bit. A binary digit. The smallest variable of information. From the bit, we created the internet and the world wide web. This web accelerated the number of information computers from around the world sending information to each other. Software started emerging from this and it quickly started to eat the world. Meaning it was becoming more

and more prominent in our lives. Hardware and software are now extensions of our lives, and they're leading us to the new paradigm—the metaverse.

Atoms to Bits to Batoms

The metaverse can become as grand as the universe we know. Anything and everything can exist in this space. We can program the rules of physics, and we'd be able to experience this new universe through hardware and software. An omnipotent software would create this experience and would similarly simulate our known universe. A simulated universe may sound like sci-fi, but if we look at how we neurological process stimuli, we'll see that it's not too far away.

Let's take a moment to discuss how we experience reality through our cognition. Talking about thoughts and experiences may enter the philosophical realm since reality is a slippery axiom to define. I'll focus on a neurological definition since we could view it more empirically.

Here is how our brain processes stimuli and converts it to our reality. It starts with our brain processing stimuli through senses (sight, touch, smell, taste, hear). This makes neurons release neurotransmitters (chemicals) that generate electrical output to other neurons. This electrical output ripples out to activate multiple brain components, which in return yields an emotion or thought. An emotion can be defined as the chemical reaction your body is experiencing, and thought is the cognition in your mind.

Emotions and thoughts are how we experience reality in our known universe. For example, you are reading this book. You are touching a piece of hardware, using your sight to read the words, and processing the information into a thought. Feeling the hardware and processing the stimulus to converge a thought is your experience of reality at the moment. You will have the same principles of processing stimuli through your senses to create an emotion or thought for anything you do in life. From when you take a bite of your favorite food to hugging your loved ones, it is all processed stimuli that make you feel and think in a particular type of manner. Now imagine if you put on some hardware that emulates the experience of processing stimulus from the real world. You wouldn't be able to distinguish reality from the simulated environment. Atoms will not be Batoms, a bit atom. If this becomes a reality, we'd be entering a new existing

paradigm. We can experience everything imaginable differently because we can now control to an extent what variables we are inputting into the simulation.

Things get even more complicated with the rules of law in this space. No central government will be the creator of the metaverse, meaning that we will create the regulations and protocols in a way we've never seen before. Will the rules follow similar concepts in political science, or will this be an emergence of a new domain? No one knows what will happen, and a bunch of complexity will arise, but as humans always do, we create processes that lead to coordination. From a pragmatic, optimistic viewpoint, I think it will never be perfect, but the processes will get better over long enough timescales.

You may be wondering how web3 will lead to the emergence of the metaverse. As any future behaves, it is unpredictable, but I would like to theorize that web3 will be the invisible infrastructure that builds the metaverse. Just how society has built their governments and methods of coordination, we will build the new systems on web3 with blockchain technology. The new systems of the metaverse will operate from the immutable data in blockchains and the autonomous protocols we establish. The metaverse will be a social experiment pushing humanity to a new level.

Transhumanism

With the metaverse, we'd be entering a transhumanism standpoint. This can be defined as "a philosophical and intellectual movement which advocates the enhancement of the human condition by developing and making widely available sophisticated technologies able to enhance longevity, mood and cognitive abilities greatly, and predicts the emergence of such technologies in the future." Transhumanism is a broad concept and leaves a lot of room for nuance. The truth is that there is too much complexity happening to cultivate an accurate prediction for this futuristic era.

As we learned throughout the book, web3 is the new protocol for the internet's update, and we are at the forefront of it. Blockchains are now the ledgers of our truth, and we are building cryptoeconomic systems with this new technology. Human coordination will reach new heights, and the world's operating system will experience an update. The best we can do is educate ourselves and become

future builders. Throughout history, there are short windows of opportunity to become pioneers. We are in a window of opportunity and have the chance to be the pioneers of this new era. May we prepare for this world's update and build a better future for humanity with webthree.

As you know, learning never stops; I will add more information to this book. The areas I plan on covering next are listed below.

- Oracles
- SPV (simplified Payment Verification Nodes)
- Crypto Cities
- System Theory
- Miner Extracted Value
- L2s & Side Chains
- Quantum computing vs. encryption

Please stay alert for future updates, and I will be emailing the revised version in the near future. Twitter is my favorite web2 platform to share ideas @tintology. Also, I plan on making this a free resource in the near future. Once my startup gets enough capital to maintain a healthy runway, I will make this free.

Thank you.

REFRENCES

Zargham, M. (2018, July 2). Token Engineering 101: Why Engineering Is Necessary. | By Michael Zargham | BlockScience | Medium. Medium. https://medium.com/block-science/token-engineering-101-why-engineering-is-necessary-3bac27ccb8b7

Balasanov, S. (2018, December 13). How To Make Bonding Curves for Continuous Token Models | By Slava Balasanov | Relevant Community. Medium. https://blog.relevant.community/how-to-make-bonding-curves-for-continuous-token-models-3784653f8b17

Registry, T. C. (2018, November 23). The Token Curated Registry Reading List | By Token Curated Registry | Medium. Medium. https://medium.com/@tokencuratedregistry/the-token-curated-registry-whitepaper-bd2fb29299d6

McConaghy, T. (2020, September 7). Web3 Sustainability Survey. A Review Of Web3 Ecosystem Funding... | By Trent McConaghy | Ocean Protocol. Medium. https://blog.oceanprotocol.com/web3-sustainability-i-survey-of-ecosystem-funding-programs-ffa2bb235df5

Brekke, J. K., & Alsindi, W. Z. (2020, November 18). Cryptoeconomics | Internet Policy Review. Internet Policy Review. https://policyreview.info/glossary/cryptoeconomics

Barlow, J. P. (2016, January 20). A Declaration Of the Independence Of Cyberspace | Electronic Frontier Foundation. Electronic Frontier Foundation. https://www.eff.org/de/cyberspace-independence

Walden, J. (n.d.). Past, Present, Future: From Co-ops To Cryptonetworks. https://www.google.com/url?q=https://jessewalden.com/past-present-future-from-co-ops-to-cryptonetworks/&sa=D&source=docs&ust=1640669353256986&usg=AOvVaw2TnpWMqJ8aUrHBDKq_iG62

REFRENCES

Khanna, P., & Srinivasan, B. S. (2021, December 11). Great Protocol Politics. Foreign Policy. https://foreignpolicy.com/2021/12/11/bitcoin-ethereum-cryptocurrency-web3-great-protocol-politics/

Iredale, G. (2021, May 30). Byzantine Fault Tolerance - A Complete Guide. 101 Blockchains. https://101blockchains.com/byzantine-fault-tolerance/

Proof Of Work. (n.d.). https://www.google.com/url?q=https://en.wikipedia.org/wiki/Proof_of_work&sa=D&source=docs&ust=1640669243148515&usg=AOvVaw3aNlYHxZWhyGu1qEYlCZA0

C. (2021, October 21). Merkle Trees & Merkle Roots: Bitcoin & Blockchain | Gemini. Gemini. https://www.gemini.com/cryptopedia/merkle-tree-blockchain-merkle-root

M. (2018, October 19). Coinbase Transaction Explained - Mycryptopedia. Mycryptopedia. https://www.mycryptopedia.com/coinbase-transaction-explained/

P. (2018, December 28). Genesis Block Explained - Mycryotpedia. Mycryptopedia. https://www.mycryptopedia.com/genesis-block-explained/

Blocks-size?scale=1&timespan=all&showDataPoints=true. (n.d.). Blockchain.com. https://www.blockchain.com/en/charts/blocks-size?scale=1&timespan=all&showDataPoints=true

Block Hashing Algorithm - Bitcoin Wiki. (n.d.). Block hashing algorithm - Bitcoin Wiki. https://en.bitcoin.it/wiki/Block_hashing_algorithm

The Truth About Blockchain. (2017, January 1). Harvard Business Review. https://hbr.org/2017/01/the-truth-about-blockchain

REFRENCES

Blockchain - Wikipedia. (2016, May 23). Blockchain - Wikipedia. https://en.wikipedia.org/wiki/Blockchain

Cypherpunk - CLC Definition. (n.d.). cypherpunk - CLC Definition. https://www.computerlanguage.com/results.php?definition=cypherpunk

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/en/bitcoin-paper

Szabo, N. (1994). Smart Contracts . Smart Contracts. https://www.google.com/url?q=https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html&sa=D&source=docs&ust=1640668881225957&usg=AOvVaw1BD57r_OI6UfLs_0WPvess

Smart Contracts Defined | IBM. (n.d.). Smart contracts defined. https://www.google.com/url?q=https://www.ibm.com/topics/smart-contracts&sa=D&source=docs&ust=1640668805476199&usg=AOvVaw2HJ-yEd4Lm727sTNhLleJS

Ryan, C. (2021, January 4). The Anatomy Of Bitcoin’s Adoption Cycles. clearblockinsights. https://www.google.com/url?q=https://www.clear-block.io/research/adoption-cycles&sa=D&source=docs&ust=1640668744306704&usg=AOvVaw3ECHrcF3vYdPaD7WM0gt8h

What Is A Database?. (n.d.). https://www.google.com/url?q=https://phoenixnap.com/kb/what-is-a-database&sa=D&source=docs&ust=1640668714543420&usg=AOvVaw0j1E8h3AjnhETPND0LPf7Y

REFRENCES

N. (n.d.). Web 1.0 To Web4: A Brief History Of The Evolution Of Internet Technologies |
Hacker Noon. Web 1.0 to Web4: A Brief History of The Evolution of Internet Technologies | Hacker Noon. https://hackernoon.com/web-10-to-web4-a-brief-history-of-the-evolution-of-internet-technologies-tl64341x

Press, G. (2015, January 2). A Very Short History Of The Internet And The Web. Forbes.
https://www.forbes.com/sites/gilpress/2015/01/02/a-very-short-history-of-the-internet-and-the-web-2/?sh=5b2246e57a4e

Craig, W. (2021, June 15). The History Of the Internet In a Nutshell: From 1960s To Now.
WebFX. https://www.webfx.com/blog/web-design/the-history-of-the-internet-in-a-nutshell/