Blockchain Technology for Business

Bennett Collen

Dominic Cischke

Boston College

Last Updated: May 2022

The following text is the culmination of a year's worth of work in a constantly changing space. In keeping with the open accessibility of blockchain technology and the need to publish frequent updates, this text is offered for free, online to all.

*Disclaimer: The following text features discussions of specific blockchain technology and/or cryptocurrency assets, products, services, and/or offerings. The authors were not compensated to cover any particular company, asset, product, service, or offering. The authors may be invested in some discussed assets, companies, products, services, and/or offerings. These discussions are merely included to offer additional insight and real-world examples of discussed concepts. The following text should not be considered investment advice and is for educational purposes only. Cryptocurrency and blockchain technology are risky investments.

Table of Contents:

This page intentionally left blank.

Chapter 1: Introduction

Why Study Blockchain?

Blockchain technology is an exciting, new field. It is perhaps the fastest moving field, with new ideas, projects, and technologies being created all the time. Blockchain technology is shaping up to become the infrastructure of the future for the storage, recording, and transacting of digital and physical assets. Blockchain technology has already been applied to create exciting new products and services across a variety of industries. Assets held on blockchains continue to increase in value, far surpassing almost all traditional stores of value. Because the industry is so young and constantly evolving, you can gain an edge in the business world with a strong understanding of blockchain technology and its applications. Knowledge of blockchain technology is in such high demand from businesses that it placed first in LinkedIn's list of the most in-demand hard skills for 2020, ahead of big-hitters such as cloud computing, artificial intelligence, business analytics, and sales.[1]

Why Blockchain Matters to The Internet

So why does blockchain matter? In order to make the argument for why blockchain technology matters for the future of the Internet, we need to look back in Internet history to see where we came from. From here, we can better understand the direction the Internet is headed and see how blockchain technology might fit into the future of the Internet.

Web 1.0 and Web 2.0: The Past and The Present

The very beginning of the Internet is sometimes referred to as "Web 1.0." The websites available for use at this time were static in nature and did not offer much functionality beyond their ability to deliver previously curated content. Web 1.0 functioned primarily as a "content delivery network" for the works of content creators to be viewed by Internet users.[2]

Next came the rise of Web 2.0, the era of which much of our time spent online today most closely resembles. Web 2.0 is largely characterized by the large, centralized social media platforms that we all engage with on a daily basis. In the shift to Web 2.0, a

[1]Anderson, Bruce M. "The Most In-Demand Hard and Soft Skills of 2020." *LinkedIn*, 9 Jan. 2020, www.linkedin.com/business/talent/blog/talent-strategy/linkedin-most-in-demand-hard-and-soft-skills.

[2]Sharma, Madhurkant. "Web 1.0, Web 2.0 and Web 3.0 with Their Difference." GeeksforGeeks, 27 Jan. 2022, www.geeksforgeeks.org/web-1-0-web-2-0-and-web-3-0-with-their-difference/.

rise in user-generated content was observed. The platforms for which users visited began presenting the content of platform users, not the content of the platform itself. Websites have become far more dynamic than those of Web 1.0, allowing for user interaction beyond simply reading the content produced by the website.

During the Web 2.0 era, we have seen the rise of a select few extremely powerful entities that host and have power over a large amount of online communication.[3] Take a moment to consider how few online entities you go through in your navigation of the Internet. Perhaps you use Google services and products for email, web searching, leisure content, or devices to access the internet. You might have a few social media accounts on platforms owned by Meta. Many turn to Amazon for online shopping, grocery delivery, reading, or cloud computing. Beyond a few other companies, there are not many other entities that control a meaningful portion of contemporary online communication.

Web 3.0: The Future

While some may dispute the length to which we have already embarked on the crossing from Web 2.0 to Web 3.0, the fact remains that humanity and the Internet are making the shift, to varying degrees for different users, to tenants of Web 3.0. Web 3.0 is fundamentally different from Web 2.0 in that Web 3.0 seeks to empower independent, connected computers to perform functions that ordinarily require human intervention.

Web 3.0's origins can be traced all the way back to 2001 when an article was published that described "The Semantic Web." The Semantic Web is an extension of the current state of the Internet in which the data of the Internet is machine-readable and computers can take on a participatory role in the Internet ecosystem.[4] Computers of a Semantic Web will be able to take in information from users and autonomously cross-reference databases residing on the Internet to deliver a complete result, comparable to what a person would be able to produce.[5]

With individual computers capable of understanding data and autonomous reference and communication, there is likely a diminished necessity for and reliance on

---

[3]Edelman, Gilad. "What Is web3, Anyway?" Wired, 29 Nov. 2021, www.wired.com/story/web3-gavin-wood-interview/.

[4]Berners-Lee, Tim, et al. "The Semantic Web." *Scientific American*, 17 May 2001, https://web.archive.org/web/20171010210556/https://pdfs.semanticscholar.org/566c/1c6bd366b4c9e07fc37eb372771690d5ba31.pdf.

[5]Shannon, Victoria. "A 'More Revolutionary' Web." *The New York Times*, 23 May 2006, www.nytimes.com/2006/05/23/technology/23iht-web.html.

the services of centralized entities that organize online communication. While it may appear that the removal of these central entities that lie in the middle of (and to a certain degree control) our online lives could provide many benefits to users, this removal also comes with the loss of many components of the Internet that we have come to take for granted. These centralized platforms we use on a daily basis provide important services to users such as information storage and a place for users to convene online. In order to do away with these platforms or even attempt to use the Internet without accessing these existing platforms, new technology and infrastructure is necessary. Here is where blockchain technology can find a central place in the Internet, both today and for years to come.

Blockchain's Place In The Internet's Future

Gavin Wood, a co-founder of Ethereum and the founder of Polkadot (both of which we will discuss later in this book), coined the term "Web3" in 2014 to describe a decentralized online ecosystem of the future that is powered by blockchain technology.[6] Web3 offers a *decentralized* infrastructure to bring the core ideas of Web 3.0 to life: blockchain technology. We will soon dive deep into the details of blockchain technology, but for now a brief description of blockchain is necessary to see how blockchain can fit into and be the central component of the next evolution of the Internet.

Blockchains are a network of independent, connected nodes that form a network which enables trustless consensus between parties. Blockchains are commonly decentralized, meaning there is no central party making decisions for the network. Due to its technical foundations to be discussed soon, blockchain technology provides a simple way to verify the state of stored information.

In keeping with the Web 3.0 trajectory, blockchain technology can be utilized in certain areas of the Internet to facilitate computer-to-computer communication and trusted database retrieval of verifiable state. Blockchain technology can be incorporated to help increase or remove intermediary steps in online transactions and communications.

Web3: Blockchain as The Internet

Perhaps blockchain technology can play a meaningful role in the Internet of Web 3.0, but what if blockchain technology was the central piece of the Internet as described by Web3? What could the future of a blockchain-powered Internet look like?

[6]Edelman, Gilad. "What Is web3, Anyway?" *Wired*, 29 Nov. 2021, www.wired.com/story/web3-gavin-wood-interview/.

A blockchain-powered Internet is one in which users have full control. A true Web3 ecosystem enables users to enjoy the luxuries of the Internet that we enjoy today, without the need for centralized intermediaries. This system is open, transparent, and trusted by users with blockchain technology serving as the backbone. Anyone with an internet connection is able to participate in the system to the same degree as those building the most fundamental applications. There are no central authorities applying censorship power against users to shape the Internet in their image. Users are able to build on top of each other and use the services of pre-existing applications to create newer and even greater applications. The open-source global shared system is constantly growing and evolving. Web3 promises a greater Internet built for the people, by the people.

Book Overview

This book aims to arm you with an understanding of how blockchain works from a technical perspective as well as present many ways that blockchain technology is currently being in business. We will begin in Chapter 2 with what a blockchain is (and is not) and the fundamental concepts of blockchain technology, from cryptography to game theory, that come together to make it function. Then in Chapter 3 we will cover the first use of blockchain technology: Bitcoin. Then we will turn to Ethereum in Chapter 4 where we will see how blockchains can be further enabled to autonomously conduct complex transactions and process logic. Chapter 5 will cover the major challenges that contemporary blockchains face and potential/implemented solutions to address these challenges. In Chapter 6 we will investigate a number of newer blockchains and the unique solutions that these blockchains implement to provide unique value in the hyper-competitive blockchain ecosystem.

Now with a fundamental understanding of blockchain technology and the blockchains available today, we will turn toward business implementations of blockchain technology and important, contemporary topics concerning blockchain technology. Chapter 7 will discuss what a “cryptocurrency” actually is, initial coin offerings (“ICOs”), and other ways that cryptocurrencies are introduced to the market. Chapter 8 will highlight the growing space of decentralized finance (“DeFi”), where blockchain technology is leveraged to provide financial services without a central authority. Chapter 9 will cover the industry of cryptocurrency “mining,” primarily focusing on the Bitcoin mining industry. Chapter 10 will discuss stablecoins and Central Bank Digital Currencies (CBDCs), which have both been topics of heightened discussion for the past few years. Chapter 11 will take us further in-depth on non-fungible tokens (NFTs), which is an area of blockchain technology that has recently exploded in popularity and has found itself in mainstream discussions. Chapter 12 will conclude the book with an overview of blockchain technology use cases beyond those already discussed.

Let's begin with a high-level preview of some of the major ideas we will soon explore:

What is a Blockchain?

Bitcoin and blockchain technology have become tied together in media coverage and public knowledge, but blockchain technology extends far beyond just Bitcoin. While Bitcoin is powered by a blockchain, Bitcoin is not the only blockchain. There are many different blockchains, protocols, and distributed ledgers that power many different use cases. Due to the rapidly evolving nature of this relatively young technology, the definition of and the bounds of what blockchain technology can be used for is continuously changing.

Blockchain technology is a type of distributed ledger technology (DLT) composed of blocks of data that are chained together to create a database. At its core, a blockchain is a digital "spreadsheet" of transactions with no centralized party keeping a master record. Instead, the task of record keeping is shared among the users of the system, which creates a decentralized and distributed ledger. The underlying technology verifies that all users of the system maintain matching records. Blockchain technology and its underlying technologies will be further discussed in far greater detail in the forthcoming chapters.

Blockchain Functions

Blockchain technology creates a tool that can perform various functions; William Mougayar highlights ten of these distinct functions that are central to blockchain technology use cases.[7]

1. Cryptocurrency
2. Computing Infrastructure
3. Transaction Platform
4. Decentralized Database
5. Distributed Accounting Ledger
6. Development Platform
7. Open Source Software
8. Financial Services Marketplace
9. Peer-to-Peer Network
10. Trust Services Layer

[7]Mougayar, William. *The Business Blockchain.* Hoboken: John Wiley & Sons, 2016

As we investigate real-world examples of topics discussed later in this text, pay attention to how these ten functions are leveraged in the use of blockchain technology.

Smart Contracts

Many of the real-world examples discussed in this text incorporate “smart contracts.” Smart contacts are simply computer code that can facilitate, verify, or enforce a contract, transaction, or agreement. When predetermined conditions are met, the computer code will make predetermined executions on the blockchain. Smart contracts are often used in applications of blockchain technology due to their ability to provide “programmable trust.” In a decentralized system with no inherent central authority, smart contracts can be used to provide rule-based decision making and allow the system to continue operating without a central authority. Smart contracts will be covered at length in the next few weeks and will be observed as a central component of many real-world examples of blockchain technology applications.

Use case Overview

The wide-ranging functions and underpinnings of blockchain technology allow it to be applied in many different industries. Blockchain technology has been used in or is gathering excitement for its possibilities in the following fields:

- Finance
- Energy
- Anti-Counterfeit and Fraud Detection
- Supply Chain and Logistics
- Personal Property
- Art
- Voting
- Healthcare
- Identity
- Insurance
- Entertainment

As blockchain technology continues to evolve, the ability to leverage its benefits in more and more sectors continues to expand. While we discuss the foundations of blockchain technology and its current applications, try to think of what other, potentially unexplored industries blockchain technology can be leveraged in.

Chapter 2: How Does Blockchain Work?

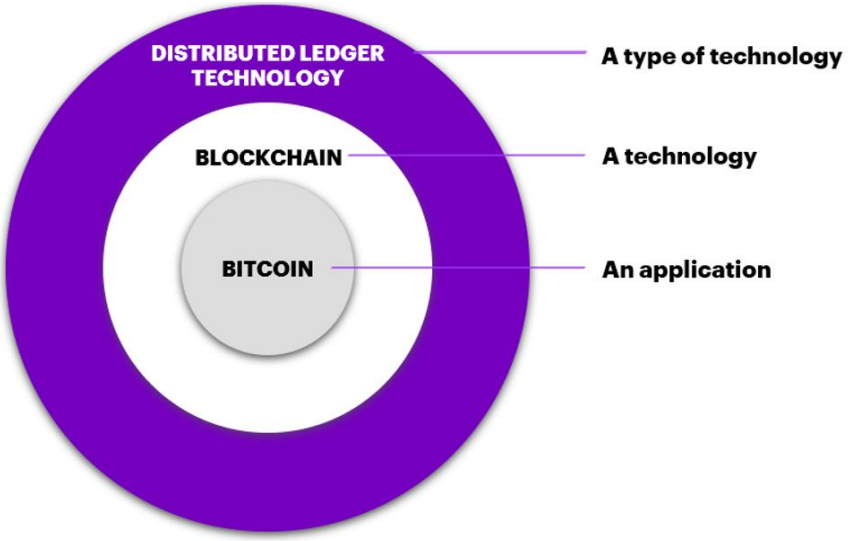
The “Nakamoto” Blockchain

Satoshi Nakamoto created the first blockchain: Bitcoin. The “Nakamoto” Blockchain is the “classic” blockchain from which we will study the fundamentals of blockchain technology. As previously discussed, Bitcoin is not the only blockchain. Subsequently created blockchains have made adaptations from this classic model and we will continue to see further changes to what a blockchain can be as the industry continues to evolve.

Distributed Ledger Technology vs. Blockchain

Distributed Ledger Technology is an umbrella term for **distributed databases**, meaning databases that are managed by multiple parties, across multiple nodes (computers). Distributed databases spread computing power and copies of the ledger across physically dispersed notes. Distributed databases are very common in the world around us. A shared spreadsheet that roommates used to apportion rent costs is an example of distributed ledger technology.

Blockchain technology is a subset of distributed ledger technology. All blockchains are distributed ledgers, but not all distributed ledgers are blockchains. Blockchain technology takes specific approaches to the management of distributed databases such as how the data is stored, secured, added to the database, and how agreements between ledger participants are reached such as its **decentralized** structure.

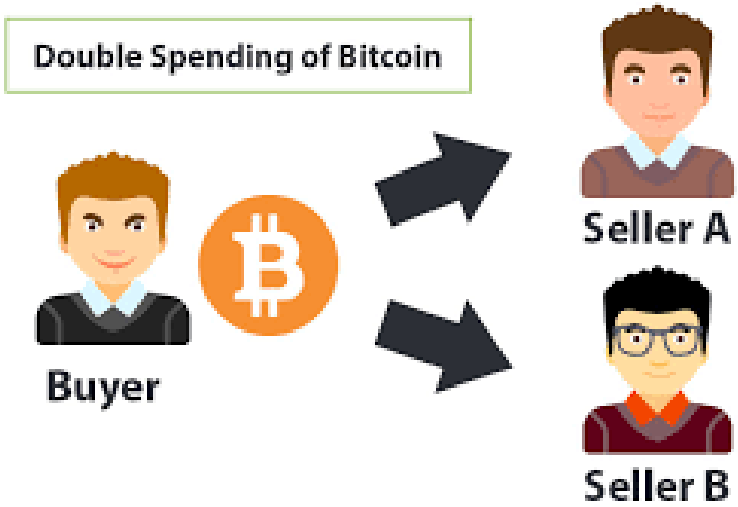


Distributed ledgers that are not blockchains can also have a decentralized database with a different data structure. When used in the context of blockchain technology, the term “decentralized” often refers to the governance mechanism used to manage the data rather than the how the data is structured. In the context of this course, a decentralized database is one that has no central governing body, but rather has decisions be made by the peers of the ecosystem.

The Double Spend Problem

Before blockchain technology came to be, a great barrier existed to the viability of valuable digital assets: the **double spend problem**. Modern-day physical currency is extremely difficult to replicate due to the vast resources necessary to create an identical banknote that defeats all of the security features. However, it is easy to create and disperse a copy of a digital asset. With no central authority to control the authenticity and creation of a digital asset, users could create multiple copies of a single asset and send it to multiple people. The digital asset could quickly spiral into hyperinflation and with the same asset sent to multiple people, faith in the system would be quickly lost.

A digital currency cannot function if a person is able to “double spend” a single dollar. In a decentralized system, the users are equally responsible for keeping track of asset ownership. If Amy sends the same digital dollar to Bob and Charlie, the network-wide agreement on the state of the ledger will be broken. Bob and Charlie will each claim that they own the dollar, and Amy could choose either Bob or Charlie to be the owner of the dollar, or she could decide that she still owns the dollar.



The double spend problem was solved by the Nakamoto Blockchain through the incorporation of multiple existing technologies in a peer-to-peer system discussed below, while maintaining the intended decentralized nature of the system. A blockchain maintains a distributed ledger of ownership that cannot be altered by a bad actor. A user is only able to transact the amount they own and the ledgers of all connected nodes are updated to reflect changes in ownership. In the case of the Bitcoin blockchain, ownership is represented by bitcoins: a finite, fully digital asset native to the Bitcoin blockchain.

This solution was a major contribution by Bitcoin, cited by Vitalik Buterin (Ethereum's creator) as a contribution equal in importance to the creation of a decentralized peer-to-peer digital currency.[8] By solving the double spend problem, the Nakamoto Blockchain made decentralized, digital scarcity possible. Digital scarcity, a critical piece missing from previous digital currency attempts, enables the creation of digital currencies and many other blockchain technology use cases.

Blockchain as a Meta Technology

The Nakamoto Blockchain is a **meta technology**: a combination of multiple existing technologies that creates a new technology. The Nakamoto Blockchain incorporates principles from cryptography, game theory, and software engineering, many of which had already existed and been incorporated into early attempts at creating a digital currency. While Satoshi Nakamoto primarily used pre-existing concepts and technologies, the exact combination of these features in his/her/their creation of Bitcoin led to something truly groundbreaking. Blockchain technology is an excellent example of the whole being greater than the sum of its parts.

Cryptography

Cryptography principles lie at the core of blockchain technology. Many pioneers of blockchain technology were avid participants in cryptography discussion groups such as the "cypherpunks." Three key cryptography concepts power blockchain technology: hashing, keys, and digital signatures.

[8]Buthein, Vitalik. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." *Ethereum*, 2014, https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_White_Paper_-_Buterin_2014.pdf.

Hashing

A **hash** is a unique string or “fingerprint” that helps one verify that a piece of information has not been changed in any way, without the need to check the information itself. When information is converted into a hash through the use of a hashing function, a unique string is generated. If the information is even slightly changed, the hashing function will output a completely different string. This feature allows one to easily check for unwanted changes made to the original information without the need to check through the original information. Hashing functions are one-way functions. This means that given a set of information, a unique hash can be generated, but if one is given a hash, reverse-engineering cannot be performed on the hash to obtain the underlying information. Hashing functions make it extremely easy to create a unique hash for a set of information, while making it nearly impossible to obtain a set of unknown information by using its unique hash.

The Secure Hashing Algorithm (SHA)-256 function used by Bitcoin produces a hexadecimal (base-16 number system using the digits 0-9 and the letters a-f) string of 64 characters in length.

Inputting “Blockchain” into SHA-256 will produce the following string:

625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1

If the input is changed to “Blockchain!” the following string will be produced:

d0d7cc64d0315e6b3a3a2f1cff719a3be3d96e81faf6a9dfa87453bedbb1be19

As you can see, making the slight change of adding an “!” to the end of the input yields a completely different result. Additionally, there is no way to use the resulting hash to know what the input was. If one only has the hash, the only way to find the corresponding input is by randomly guessing inputs and comparing the resulting hash.

Keys

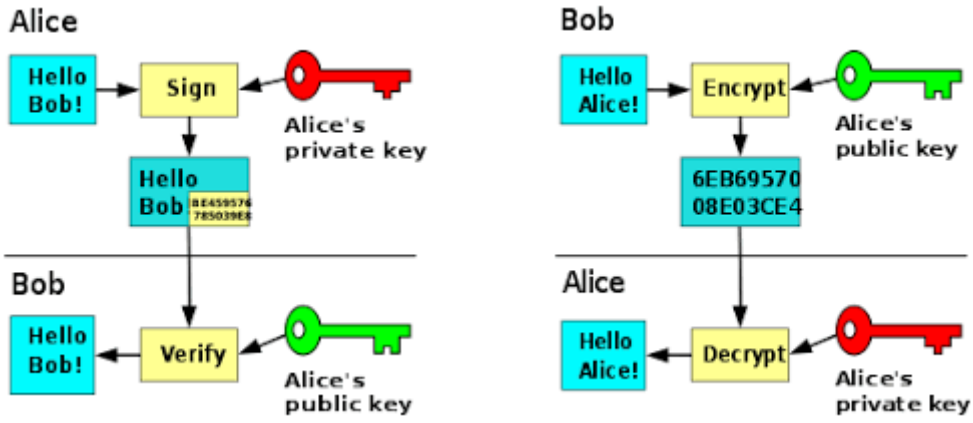
The Nakamoto Blockchain incorporates the cryptography concept of keys through the use of public and private key pairs. The **public key** is the “address” where encrypted information is sent to and received by other network users. The corresponding **private key** is how messages and transactions on the network are encrypted, decrypted, and digitally “signed.” Each network participant has a pair of a public and private key.

An analogy often used to explain the concept of public and private key pairs is the pairing of an email address and one's email password. A person's email address functions as their public key. Email is sent to and from the person's email address. It is a design of the system for your email address to be known publicly, at least by those you interact with on the system. In order to send an email, a sender needs to know the email address of the intended recipient. Similarly, in most email systems, the recipient receives the sender's email address along with the email.

A person's email password functions as their private key. Someone can only send an email from a specific email address with the correct, corresponding password. Unlike public keys, the consequences of another person obtaining one's private key can be severe. If someone obtains your email password, they can garner full control over your email account, including the power to send emails to other individuals from your email. In the case of blockchain technology, if another person obtains your private key, they can send information and transactions (your digital assets) from your address.

Digital Signatures

When sending encrypted information in a blockchain, you "digitally sign" the transaction, by using your private key, in a way that only you as the owner of the sending address can. Mathematical computations occur to prove the authenticity of your **digital signature** on the transaction. Digital signatures can be also used to store data semi-publicly. Someone can verify that you are the authentic signee of sent information as well as when the information was published by observing your signature, while maintaining your sole ability to access the encrypted information with your private key.



Game Theory

In addition to cryptographic principles, blockchain technology incorporates less technologically intense principles such as game theory. Byzantine Fault Tolerance and Network Incentives are two main game theory principles that empower blockchain technology.

Byzantine Fault Tolerance

The Nakamoto Blockchain overcomes an issue to mass-consensus known as the Byzantine Generals Problem, a scenario in which a system's users must be in agreement with each other in order to avoid a system failure, with the problem that some users might be unreliable. Reaching mass-consensus in this scenario achieves **Byzantine Fault Tolerance**, a state in which the system is able to continually operate and reach network-wide consensus, despite the presence of some users with faulty information. Blockchain technology achieves Byzantine Fault Tolerance by having users keep a distributed ledger of the same state and by having the users record changes to all ledgers. This creates a decentralized, distributed ledger shared among the users of the system that is continuously in consensus. Byzantine Fault Tolerance provides that users can trust the legitimacy of the ledger without trusting other users, that good actors and mistakes will not break the system, and that bad actors cannot overtake the system due to mechanisms in place that will soon be discussed.

Network Incentives

The Nakamoto Blockchain and many subsequent blockchains provide **network incentives** to encourage users to be good actors and to discourage bad acts. Blockchain networks require a tremendous amount of computing power to overtake the network. If one is able to gather the resources necessary to overtake a blockchain network such as Bitcoin, the stolen Bitcoin would be devalued due to a loss of faith in the network as users will no longer assign the same value to an asset of a network that has been overtaken. A bad actor will likely find their resources to be wasted in this effort.

The Nakamoto Blockchain and many other blockchains also provide avenues for users to expend the previously discussed resources in a way that secures the network, known as mining. In exchange for securing the network, blockchains often reward users with assets of the network (Bitcoin in the case of the Nakamoto Blockchain).

Software Engineering

Blockchain networks are a system of connected computers working together. Software engineering principles are applied in order to achieve the purpose of a given blockchain.

Internet

The Internet enables communication between all participants in a blockchain network. Blockchains exist on the Internet where users can work together in a peer-to-peer network to keep a distributed, decentralized ledger with a state that all participants agree upon.

Distributed Databases

Going back to the beginning of this chapter, blockchains are a form of distributed ledger technology. Instead of a single central authority maintaining a ledger for all participants, distributed ledger technology provides that the task of keeping the ledger is spread across the network participants. A distributed database, in the form of a distributed ledger for blockchains, provides network participants with the necessary information to validate and conduct transactions without a central authority. Consensus protocols and internal blockchain functions provide that all copies of the distributed ledger are the same.

What is a Protocol?

Blockchains are created by first developing a protocol to coordinate with others, who are not inherently trusted, to achieve an outcome. In the case of the Nakamoto Blockchain, the protocol was developed with the purpose of creating a means of digital cash or store of value that can be transacted on the internet without the need to know or trust other transaction or network participants.

In creating a blockchain protocol, the rules of the protocol are first defined. Many decisions must be made to define the scope, function, and ability of the protocol, such as:

- How do the participants reach consensus on what data gets added to the ledger?
- What constitutes a valid transaction?
- Will the system be public, private, or semi-private?
- Will the system be permissionless, permissioned, or semi-permissioned?
- Will the system be distributed, decentralized, or semi-decentralized?

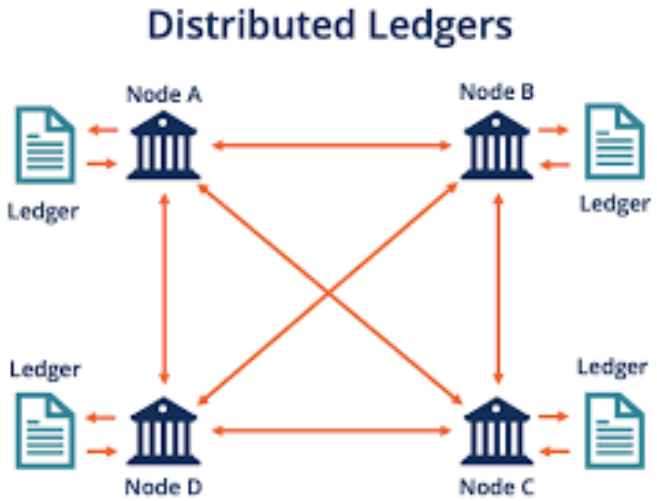
- Can the rules of the protocol as described above be changed in the future, or are the rules set for the lifetime of the protocol once decided upon?

Consensus Protocols

In order to reach agreement between blockchain network users, **consensus protocols** are put in place. The Nakamoto Blockchain decentralizes its consensus among the users. There is no single party that makes decisions for the entire system. Instead, decisions are based upon the predefined protocol. By joining the system, users agree to the terms of the protocol. Through the decentralization of consensus, trust and authority is transferred from a central entity often at the core of many non-blockchain networks to all participants of the system. Decentralized consensus is the foundation of a decentralized architecture.

Blockchain Mechanics

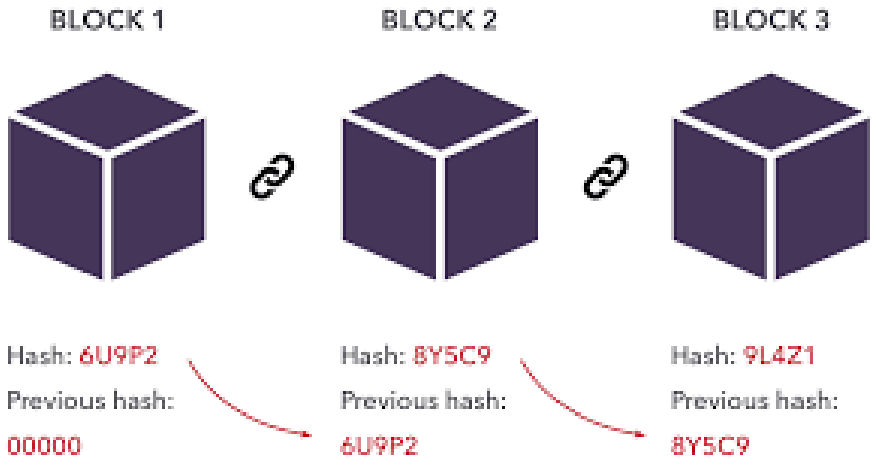
In a blockchain, a network of computers communicate with each other to validate entries to a distributed ledger. All participating computers committed to powering the network (called "**nodes**") have a complete copy of the ledger. New transactions are broadcasted to the network of computers and subsequently verified by the nodes. The verification process is determined by the predefined protocol. The verification of transactions by all nodes maintains the integrity and accuracy of the ledger, as all future entries to the ledger have been deemed as legitimate by all participants.



Once transactions are verified, they go to the **mempool**, which is a grouping of all verified transactions waiting to be included in blocks to be confirmed, executed, and reflected on the blockchain. Verified transactions are pulled from the mempool, often by

selecting the transactions offering the greatest transaction fees, and grouped together into **blocks** of data. New blocks of verified transactions are added to the distributed ledger in regular intervals, as defined by the predetermined protocol. The Nakamoto Blockchain has a 10 minute interval, on average, between the addition of new blocks. It is an intended design of the system for transactions to be grouped into blocks for insertion into the ledger at regular intervals rather than being added to the ledger in real time. This design helps lagging participants to better maintain pace with all other nodes, thus reducing the risk of double spending and differing copies of the ledger in the scenario that some participants have fallen behind the real time updating of the ledger.

When a block of transactions is to be added to the distributed ledger, each node updates its copy of the ledger with the new transaction information contained in the block. Each new block is **chained** to the previous block. Each new block contains a reference to the data in the previous block. Referencing previous blocks provides an important security feature to the immutable nature of a blockchain. Because blocks reference the previous one, changes made to any block in the chain will alter the reference in the next block. A ripple effect will occur to where all blocks after the point of change in the chain will reflect a prior change.



If a blockchain currently has 10 blocks, a change made to block 7 will also alter block 8, thus altering block 9 because block 8 was changed, thus altering block 10 because block 9 was changed. It will be easy to tell that a change was attempted and which block to find the change in. In order for this change to the blockchain to be successful, a bad actor would need to alter the information in block 7, then change block 8 so that the reference to block 7 in block 8 is valid, then change block 9 so that the reference to block 8 in block 9 is valid, then change block 10 so that the reference to block 9 in block 10 is valid, and perform this change in a majority of nodes on the network. With increased size of nodes and computing power, it can become extremely

difficult and at a certain point practically impossible to alter the information contained in a blockchain.

State Machines

Blockchains are known as “state machines.” A **state machine** is a computer that remembers the status of something at a given instance of time. The status that a state machine remembers is known as **state**, which is the set of information stored at a given time. In the case of the Bitcoin Blockchain, the blockchain remembers the state of the distributed ledger.

State can change over time as new information is given. A state machine will keep track of state changes and reflect the correct, current state. More simply put, a state machine keeps track of a set of data and changes to the data over time. Consensus in a network is an agreement on the network’s current state. Blockchains keep track of state in an immutable way. Historical data stored on a blockchain cannot be rewritten. Blockchain databases can only be changed and amended going forward.

The Blockchain Transaction - Bitcoin Example

All of the blockchain fundamentals we have discussed this week enable a digital peer-to-peer transaction network. A complete transaction on the Bitcoin blockchain occurs as follows:

Broadcast

A transaction begins with a sender broadcasting the transaction to the network of nodes of the Bitcoin blockchain. The nodes of the Bitcoin network must then validate the transaction.* A transaction is verified by confirming the digital signature attached to the requested transaction is from the correct address. This step ensures that transactions to send funds from a specific public key can only be initiated by the person with possession of the corresponding private key. Additionally, the balance of the submitting address is checked to ensure the reflected bitcoin balance in the ledger is greater than the amount of bitcoin requesting to be sent. This step ensures that the sender has a sufficient balance to carry out its requested transaction, guarding against double spending and the spending of funds that one does not possess.

Blocks

Once a transaction is verified, it is sent to the mempool of the Bitcoin blockchain. Transactions selected from the mempool are then grouped together into a block of transactions that carries a block size limit of 1 MB. About one to two thousand

transactions are included in each block.[9] The block is assembled with components such as the selected transactions and the previously discussed reference to the prior block.

Mining

Next we get to the mining stage of a transaction's life cycle. Mining is the process through which new blocks are added onto the chain of previous blocks. One all transactions are selected to be included in a block, miners race each other to come up with another block input that yields a hash of the block that is in line with the Bitcoin blockchain's protocol (discussed in detail below in "Proof of Work"). When a miner solves this input, it proposes the block to all other miners.

If the miners agree* that the block is in line with the standards determined by the protocol, the block is appended to the Bitcoin blockchain by way of all nodes adding the block to their record of the Bitcoin blockchain. Transactions of the block are confirmed and finalized. The updated record held by network participants reflects the change in balances caused by transactions of the appended block. Miners are incentivized to agree that a valid block is valid, which results in another network participant getting the block reward, because it keeps the process moving and allows for another opportunity for the miners to win a block reward.

* A majority of nodes (>50%) must be in agreement for consensus in the Bitcoin protocol

Proof of Work (PoW)

The mining step discussed above, native to the Bitcoin Blockchain and many subsequent blockchains, is powered by a process known as **proof of work (PoW)**. Proof of work is the consensus algorithm of the Bitcoin Blockchain and many other prominent blockchains. Computers designated as "miners" perform the protocol's defined tasks to complete the blockchain transaction process. The energy expended and work done by the computers is the "work" in a proof of work system.

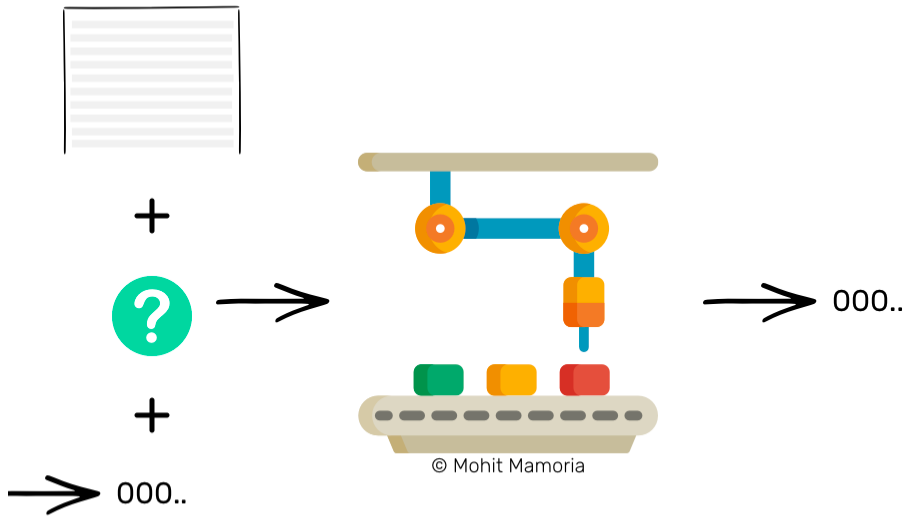
Incorporating Hash Functions

Hashing functions are a core piece of the mining step in a blockchain system. When new blocks are added to the chain of existing blocks, a reference to the previous block is included in the new block. The reference to the previous block is the hash of the previous block. The hash of the previous block is combined with the hash of the transactions of the block to be added to the chain. Finally, these two inputs are combined with one final input to complete the block.

[9] "Bitcoin Average Transactions Per Block." *YCharts*, https://ycharts.com/indicators/bitcoin_average_transactions_per_block.

Miners compete with each other to “seal” the block. Successfully sealing the block is achieved by discovering a final input which along with the hash of the transactions and the hash of the previous block for the hash function yields a hash in line with what the protocol requires. This “final input” is known as the **nonce**.

Mining works to secure the network. By sealing the block and achieving a resulting hash of the block, one can now easily verify the state of the block. The mining process makes blocks immuable in nature. If someone attempts to alter any information held inside the block, the hash of the block’s information will completely change, making it easy for every other network participant to realize that the block’s information was altered. Additionally, the chain reaction of changed hashes will occur on blocks following the altered block due to the previous block reference component of all blocks. In order for a bad actor to successfully alter the information of a previous block, they would have to “re-mine” the desired block and then re-mine all succeeding blocks. In order to accomplish this feat with network consensus, a majority of the network’s computing power is needed (discussed further below as a “51% attack”).



In the case of the Bitcoin protocol, a hash of a block is required to contain a certain amount of leading zeros. The protocol is designed to regularly adjust the number of leading zeros required, in effect increasing or decreasing the difficulty of achieving a valid hash, to maintain the desired, approximate 10 minute block interval timing. When the first block was mined on the Bitcoin blockchain, 8 leading zeros were required.[10] Currently, the Bitcoin protocol requires 19 leading zeros for a block’s hash to be valid.

[10]“Block 1.” *Blockchain.com*, www.blockchain.com/btc/block/1.

Because hash functions are one-way functions, miners cannot work backwards with a valid hash to find a valid nonce. Instead, miners must take a “brute force” approach by repetitively guessing a nonce until a valid hash is found. Because miners must take this approach, the miner with the greatest computing power, and therefore the ability to perform the most guesses in a given amount of time, has the best chance of beating the rest of the miners to seal the block.

*** Practice the Material: For a hands-on tool to reinforce these concepts, visit andersbrownworth.com/blockchain/ [11] for self-guided practice on hashing, blocks, chaining, and distributed ledgers.*

Why Mine?

Decentralized blockchains that require miners to power the network need to provide incentives for mining. In exchange for the expense of valuable resources (electricity, hardware, etc.) and the network security provided, protocols have defined rewards for miners. In the Bitcoin blockchain, the first miner to successfully seal the block is given a reward paid in Bitcoin. The reward is currently 6.25 bitcoins per block. The block reward is reduced by half about every four years and the reward will eventually reach 0 bitcoin per block around the year 2140.

Senders of transactions incentivize miners to include their transactions in the upcoming block by providing a transaction fee. The transaction fee is typically paid in units of the native currency for the blockchain being used. For example, in addition to sending bitcoin, you will also spend bitcoin as a transaction fee for miners to process your transaction.

[11]Brownworth, Anders. “Blockchain Demo.” https://andersbrownworth.com/blockchain/.

There is not a set transaction fee across the network. Instead, average transaction fees increase and decrease over time depending on how many transactions need to be added to the chain, how much senders are willing to pay for their transactions to occur, and how soon senders want their transaction to be added to the chain. The transaction fees paid by senders for their transactions to be included in the block are also given to the miner that first seals the block. Under this design, users wanting fast transactions compete against each other to provide the greatest transaction fee so that miners prioritize their transactions.

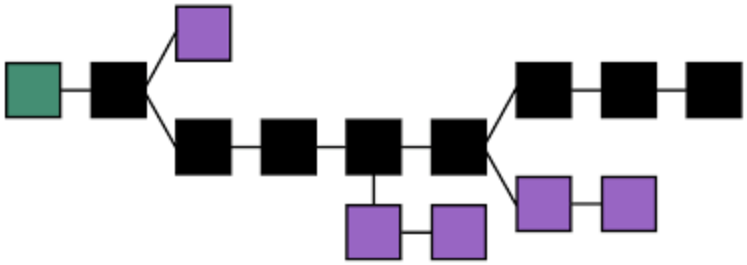
When the block reward eventually reaches 0 BTC in the case of the Bitcoin blockchain, only transaction fees of the block will be rewarded to the winning miner. The idea is that by the time the block rewards are substantially diminished/eliminated, the value of transaction fees alone will be adequate compensation for miners to continue contributing their computing power to the network.

Proof of Work Benefits

The proof of work system is utilized by the Bitcoin blockchain and many other blockchains due to the range of benefits that it provides. The incorporation of hashing functions makes it extremely difficult to generate a nonce that seals the block. However, it is easy for all other participants to validate the solution of the winning miner. Other participants can simply enter the nonce found by the winning miner and confirm that the hash is in line with what the protocol requires. The difficulty of computation can be adjusted as more computing power is introduced to the network, which helps to maintain the desired block timing. Increased computing power (incentivized by block rewards and transaction fees) helps to further secure the network. With greater computing power driving the network, the resources required to overtake the network increases. The Bitcoin blockchain has such a large amount of computing power that many regard the act of owning a majority of computing power on the network as theoretically impossible.

Longest Chain Wins

With many miners competing against each other in a system with multiple valid solutions for each block, disagreements can arise between the miners when multiple correct nonces are found. In this scenario, the “**longest chain**” will prevail and the miner proposing the corresponding nonce will receive the reward. The version of the chain with the most computing power behind it will continue on as the true chain of the network. This feature maintains that a single, “**Canonical**” chain operates as the Bitcoin blockchain.



It is possible for chains to be overcome by bad actors, especially chains with lesser computing power on the network. In this case, known as a **51% attack**, a bad actor or group of bad actors controls a majority of the computing power on the network and can therefore take control of the chain by only needing itself to reach consensus.

Putting It Together

Now that we have covered what goes into a block, let's look at an actual block of the Bitcoin blockchain. The following information comes from block 714,032 of the Bitcoin blockchain. It may be helpful to follow along on your own with this link[12] which will allow you to view the information outlined below in a formatted manner. This block happens to be special as it was the block which caused for 90% of all bitcoins to ever exist to be mined. Of the 21 million maximum supply, 18.9 million bitcoins existed after this block was mined.

The hash of the block is:
00000000000000000000194443d70e67a2b60aedf01913ee217833ca9a7e0b490

We see that this hash has 19 leading zeros, which is what the protocol of the Bitcoin blockchain required at the time (and currently) for a block's hash to be valid.

The nonce of the block is: 1,061,472,367

This nonce was the first value found to yield an acceptable block hash when combined with the other information of the block.

The block contains 2,079 transactions, with a total of 9,520.15386492 BTC transacted. The total transaction fees paid by the senders of these transactions was 0.12197489 BTC. The miner that solved the nonce shown above received these transaction fees plus the block reward of 6.25 BTC for a total reward of 6.37197489 BTC. This

[12]"Block 714032." *Blockchain.com*, https://www.blockchain.com/btc/block/714032.

transaction is shown as the latest transaction of the block, coming from the coinbase (this is where the company's name comes from).

The number of confirmations will depend on when you view the block. This number is the amount of times the block has been confirmed by the network. With each block containing a reference to the previous block, we can confirm the state of this particular block with every future block. This idea is represented by the fact that the amount of confirmations is the number of blocks since this block was added to the chain.

The block also contains some additional, interesting information. We can see the miner's address that found the accepted nonce. In this case the miner was AntPool, which is a mining pool where many people/firms pool their computing power to work together on solving the block and then split the rewards (more on this in the coming chapters). You can also see the full log of transactions that occurred in this block. We can also see the measure of difficulty to solve the block, which is the measure by which the protocol decides how many leading zeros to require in order to maintain the desired 10 minute average block time.

*** Practice the Material: Take some time to look through the linked block explorer or another block explorer of your choosing to see how these elements of a block appear in the blocks throughout the blockchain.*

Summary

The first blockchain, known as the "Nakamoto Blockchain," was created with the introduction of the Bitcoin blockchain. A blockchain is a subset of distributed ledger technology that is characterized by its unique approaches to the management of distributed databases such as how the data is stored, secured, added to the database, and how agreements between ledger participants are reached such as its decentralized structure. Furthermore, there are many different blockchain that exist, all with their own twist on the approach to these features.

Blockchain technology presents a solution to the double spent problem, which plagued prior attempts at creating decentralized digital currency. Blockchain technology combines antecedent technologies and concepts from cryptography, game theory, and software engineering.

Connected users that power a blockchain network are known as nodes. Verified transactions submitted by users are grouped into blocks. Blocks also contain a reference to the previous block, effectively "chaining" all blocks together. Blockchains are regarded as immutable because if any information in a prior block were to be altered

even slightly, the hash of that block and the hash of all successive blocks would be changed. The Nakamoto Blockchain uses proof of work consensus.

Review Questions

1. What type of “umbrella” technology is a blockchain?
2. What is the double spend problem?
3. What is a hash? What happens to the output of a hash function when the input is altered?
4. What does it mean by hash functions being a “one-way” function?
5. What are the cryptographic keys used in blockchain technology and what are their unique purposes and differences?
6. Describe one reason how actors in a blockchain network are incentivized to be good actors.
7. Where do new valid transactions go before they are included in a block to be added to the blockchain?
8. Describe the full process that a submitted transaction goes through on a blockchain network.
9. What are proof of work miners attempting to find?
10. What would a bad actor need to do in order to alter the information on a proof of work blockchain?

Chapter 3: Bitcoin: A History

What is Money?

Money can be anything that people in a society use to systematically represent value for the purpose of exchange. Money is commonly known to serve three functions: unit of account, medium of exchange, and store of value. As a unit of account, money allows people to quickly compare the value of different commodities. As a medium of exchange, money allows people to trade for commodities without the need for a barter system. As a store of value, money allows one to retain their purchasing power for use at a later time. Money is far more than the dollars and coins that we use today. At different times in human history, money that served these three functions has come in many different forms.

Evolution of Money

Before money became commonplace in society, exchange occurred as a barter system. While trade can occur with commodities, some arise which money is able to fix. In a barter system, sometimes a mutual exchange cannot occur due to the problem of commensurate needs. If one only has cows to trade, it can be difficult to reach a fair trade agreement for apples or shoes that meet the needs of both parties. Temporal issues can also arise in a barter system. A farmer that trades with the commodity of corn does not have the same access to his store of value during different seasons of the year. The functions of money discussed above work to address these problems of a barter system.

Money is a technology that has evolved alongside human society. Money first started as hard currency, which came in the form of practically every commodity available. Some commodities that have been used as hard currency throughout history are animal pelts, silk, shells, precious metals, and stamped coins. Governments first instituted society-wide currencies as claims on hard currency. Banks would issue notes that could be redeemed for the claimed hard currency at the bank. Currency in the United States has existed as claims on precious metals for the majority of the country's lifetime. It was not until 1971 that the United States dollar was taken off of a precious metal standard and converted to "fiat" money.

Fiat Money

The current medium of money is known as fiat money. Fiat money, money that is made "by decree," is instituted by a government with no intrinsic value. Instead of its

value being backed by a commodity, the value of fiat money is backed by the issuing government. Fiat dollars in the United States can take three different forms: central bank notes, central bank reserves, and commercial bank deposits. Fiat money must be accepted as legal tender to pay all debts.

Inflation and the 2008 Financial Crisis

The United States dollar saw a decade-long period of high inflation following its abandonment of the gold standard. From 1975 to 1979, the federal reserve frequently enacted monetary policy to change interest rates, sometimes with the intent of increasing rates to combat rising inflation and sometimes with the intent of decreasing rates to fight off a potential recession. The frequently changing interest rates caused confusion for many businesses, which in response elected to maintain high prices. Then, a severe recession occurred in the early 1980s.

Another recession pre-dated and occurred much closer to the creation of blockchain technology: the 2008 financial crisis. Many banking institutions were bailed out by the government and caused taxpayers to pick up the burden. The crisis brought rise to quantitative easing in the United States.

If not serving as the causation for the creation of a peer-to-peer digital cash system and subsequent blockchains, the fiat dollar system and these negative economic events at the very least served as catalysts for the work of blockchain pioneers.

The Bitcoin Timeline

Early Attempts

The idea of an “internet money” existed long before Bitcoin was created. In the decade leading up to Bitcoin’s emergence, various projects such as e-gold, Bit Gold, b-money, DigiCash, and Hashcash attempted to create a digital currency. While ultimately unsuccessful, projects like these contributed ideas and fundamentals that would be incorporated in the forthcoming Bitcoin blockchain.

The Beginning

In August of 2008, the domain name “bitcoin.org” was registered. Shortly after, a paper entitled “Bitcoin: A Peer-to-Peer Electronic Cash System” written by the unknown author Satoshi Nakamoto was published to the cypherpunk cryptography mailing list on October 31, 2008. In January of 2009, Nakamoto publicly released the Bitcoin software.

The genesis block was mined on January 3rd. In the genesis block, Nakamoto included the message “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks,”[13] which many people of the blockchain community see as a response to the events of the financial crisis.

Early Transactions and Growth

The first Bitcoin transaction occurred on January 21 2009 when Satoshi Nakamoto sent 10 bitcoins to Hal Finney, a fellow cypherpunk. Other cypherpunk members were creators of bitcoin predecessors, namely Wei Dai, the creator of b-money, and Nick Szabo, the creator of bit gold. Members of the cypherpunk group provided feedback on the proposed Bitcoin system.

The first exchange rate between bitcoin and the US Dollar was established on October 5, 2009 at a rate of $1 for 1,309.03 bitcoins, which was established with a calculation of the average cost to mine bitcoin in the United States at the time.[14] On May 22, 2010, the Bitcoin transaction that is perhaps the most famous Bitcoin transaction of all time took place. Two pizzas were successfully ordered for delivery in exchange for 10,000 bitcoins, serving as a proof of the ability for bitcoin to facilitate trade. This event garnered immense, continued news coverage of Bitcoin and the blockchain technology space as a whole.

Also in 2010, Satoshi Nakamoto handed control of the Bitcoin code repository to Gavin Andresen, who became the lead developer of the Bitcoin foundation. Satoshi Nakamoto soon began to step back from Bitcoin and eventually disappeared altogether.

Bitcoin saw continued growth in its use and vast price volatility in 2011, a lot of which is attributed to increased demand by users of Silk Road, an illicit goods online marketplace, which used bitcoin as the official currency of exchange. The price of bitcoin started the year of 2011 at 30 cents, increased to around $30 by June, fell to less than half of June’s peak price in July, fell to almost $2 toward the end of the year, and

[13]Redman, Jamie. “A Deep Dive into Satoshi's 11-Year Old Bitcoin Genesis Block – Featured Bitcoin News.” *Bitcoin News*, 3 Jan. 2020, https://news.bitcoin.com/a-deep-dive-into-satoshis-11-year-old-bitcoin-genesis-block/.

[14]Manly, Ronan. “Dawn of Bitcoin Price Discovery 2009 – 2011: The Very Early Bitcoin Exchanges.” *BullionStar*, 28 Jan. 2021, www.bullionstar.com/blogs/ronan-manly/dawn-of-bitcoin-price-discovery-2009-2011-the-very-early-bitcoin-exchanges/.

ended the year at $5.27.[15] The price of one bitcoin grew back to $13.30 in 2012, a year in which the growth was much calmer than that of the previous year.[16]

Growing Pains

Increased demand for Bitcoin increased the necessity for exchanges in the ecosystem. Mt. Gox became the exchange with the greatest trading volume and by 2014 it was handling a majority of bitcoin exchange transactions. In the same year, Mt. Gox suffered a severe hack/theft of its bitcoin holdings. Mt. Gox stated the magnitude of the theft to be around 850,000 bitcoins, which were worth over $450,000,000 at the time. Only around 200,000 bitcoins were ever recovered.

Increased adoption and demand for Bitcoin brought forth many scaling issues of the network. The network saw increased strain on the capacity of new blocks as transactions mounted, causing slowed transaction times. Two options were commonly considered as solutions to the issue: increasing the storage size of blocks and restructuring the data of blocks. Two main solutions were proposed to the network: SegWit and SegWit2x.

Proposed Solution #1: SegWit:

Segregated Witness, known as SegWit, was a proposal in 2015 to restructure the data in blocks to be more efficient in its use of block capacity. The proposed solution also would make use of the Lightning Network, a scaling solution that will be discussed in the coming weeks, on the Bitcoin blockchain. SegWit would also be only a soft fork of the Bitcoin blockchain, so it would be backwards compatible with all work previously done on the Bitcoin blockchain and the blockchain would be able to continue as it had since its creation.

Proposed Solution #2: SegWit2x:

SegWit2x, the product of an invite-only meeting of bitcoin developers, was announced as a competing proposal in May of 2017. The proposal would implement SegWit and double the capacity of blocks on the Bitcoin blockchain. Unlike the SegWit proposal, SegWit2x would be a hard fork of the Bitcoin blockchain, meaning that it would not be backwards compatible and a new chain would be started.

[15]"Bitcoin Price Today & History Chart." *Buy Bitcoin Worldwide*, www.buybitcoinworldwide.com/price/.

[16] Ibid.

SegWit was chosen, per network consensus, as the proposal to be implemented to the Bitcoin blockchain. SegWit went live on the Bitcoin blockchain in August of 2017. In the same month, a group of SegWit2x supporters decided to take principles of the SegWit2x proposal, such as the increased block size solution, and create a new blockchain, Bitcoin Cash, by hard forking the Bitcoin blockchain. Bitcoin Cash inherited the previous blocks of the Bitcoin blockchain, but became an independent chain going forward.

Highs and Lows

Towards the end of 2017, Bitcoin experienced a bull run that gathered mainstream attention at a magnitude never seen before in the blockchain space. In a year where bitcoin was trading for under $1,000 at the beginning, the price grew exponentially as the year drew to a close. In December of 2017, the price of one bitcoin peaked just shy of $20,000. Commonly regarded factors behind the rapid price growth of Bitcoin 2017 are Chinese capital controls that forced Chinese citizens to look for alternative methods to get capital out of China, a gold rush of alternative cryptocurrencies (ICO mania), the announcement of bitcoin futures by the Chicago Mercantile Exchange, and mass-FOMO as the price continued to climb.

Bitcoin then experienced a price crash of fervor equal to that of the bull run. The price of one bitcoin had crashed by nearly 50% within one week of reaching its all-time high. In February of 2018, China instituted a ban on the trading of Bitcoin and other cryptocurrencies. The price of bitcoin continued to fall, ending the year below $4,000. The crash gave way to a period, sometimes spanning years in length, known as “crypto winter” in the blockchain space, where price volatility and excitement in the space comes to a halt characteristic of an Ice Age.

Bitcoin Today

Facebook announced its plans in 2019 to create Libra, a stablecoin (a coin with a pegged value) which sparked further regulatory interest in the blockchain space. Intercontinental Exchange, the parent company of the New York Stock Exchange, began trading bitcoin futures in September of 2019.

Bitcoin suffered a price crash similar to that experienced by traditional financial markets in March of 2020 due to the COVID-19 pandemic. Bitcoin recovered throughout the year as more news surrounding Bitcoin adoption came out including the first Bitcoin ETFs in markets outside the United States and talks of creating Bitcoin ETFs in the United States.

Adoption news continued to flow as companies, such as MicroStrategy in 2020 and Tesla in 2021, added Bitcoin holdings to their balance sheets and traditional banking institutions began to offer Bitcoin opportunities to some clients. Publicly traded stocks such as Grayscale Bitcoin Trust allow everyday investors exposure to investment opportunities closely tied to Bitcoin, while still operating in the traditional finance system. Bitcoin's strengths as a deflationary, uncorrelated, and decentralized asset were also highlighted as governments around the globe started and continue to print additional currency in response to the pandemic. Bitcoin surpassed its previous all-time high of nearly $20,000 at the end of 2020 and continued its bull run to a price of over $60,000 in March and April of 2021. In September of 2021, El Salvador became the first country to adopt bitcoin as legal tender. In December of 2021, 90% of the 21 million bitcoins that will ever exist had been mined.

Bitcoin Properties

Bitcoin has many unique properties, compared to conventional mediums of money, that position it to serve as a potential alternative or future form of money and to serve as an asset that is uncorrelated from those of our traditional financial system.

Decentralized and Distributed

Because blockchains are a form of distributed ledger technology, the Bitcoin blockchain is inherently a distributed system. The network and its computation are spread across the group of participating nodes. The Bitcoin blockchain is also decentralized as there is no central party with authority over the system. Decisions are made by the majority rule of computational power provided by nodes of the system. Because the Bitcoin blockchain is decentralized and distributed, there is no single point of failure in the system. Unlike in centralized systems, there is no mass-gathering of value for someone to steal as it is dispersed across the network's nodes.

Public

Anyone with a computer and internet access can join the Bitcoin network and create an "account" or "wallet" which is an address with a public and private key pair. Everyone can see the full ledger of transactions and public key addresses. The public nature of the Bitcoin blockchain means that it is openly auditable for anyone that chooses to do so.

Immutable

Blockchains are **immutable**, meaning that the ledgers are **append-only**. The history of transactions cannot be altered. New transactions on the network are reflected

in the next block as an update to the ledger, but the history is still maintained. Previous blocks are time stamped so that all users know when a transaction occurred. The hashing functions utilized provide that if someone attempts to make changes to any blocks in the chain, it will be overtly apparent that the change was attempted and the consensus algorithm in place will not accept this attempt of a bad actor, assuming that the bad actor has not amassed a majority of the network's computing power.

A blockchain network using proof of work becomes more secure as more computational power behind the network increases. The network becomes more secure because as computational power increases, it becomes more difficult to overtake the network with the required majority of computational power. With scale, a blockchain can amass enough computational power that it becomes theoretically impossible to overtake.

Deflationary

Unlike the inflationary fiat money that we use today, Bitcoin is designed to be a deflationary asset in the long run. Only 21 million bitcoins will ever exist. Blockchain technology's solution to the double spend problem makes these 21 million bitcoins digitally scarce. If bitcoins are "lost," which can occur in ways such as sending bitcoin to an unowned address or losing key pairs, the bitcoins are gone forever, thus reducing the true circulating supply. While recent stories of lost bitcoins garner mass media attention due to the value appreciation the coin has experienced in recent years, most of the bitcoins that are presumed to be lost forever were lost in the early days of the network. A 2017 study performed by Chainalysis, a leading blockchain data company, posits that between 2.78 and 3.79 million bitcoins are likely to be gone forever.[17] If these bitcoins are truly gone forever, this has a significant impact on the true maximum circulating supply of bitcoin.

Additionally, the block reward given to miners decreases over time. The "halving" is an event that occurs approximately every four years where the block reward is cut in half. The block reward began at 50 bitcoins per block and now only sits at 6.25 bitcoins per block. Eventually, around the year 2140, the block reward will become 0 as the 21 millionth bitcoin is created. As block rewards continue until this time, the known schedule of block rewards gives users knowledge of the future supply of bitcoins for any given time.

[17]Roberts, Jeff John, and Nicolas Rapp. "Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says." *Fortune*, 25 Nov. 2017, https://fortune.com/2017/11/25/lost-bitcoins/.

Divisible

Modern currencies are divisible in nature and Bitcoin is no exception. One bitcoin is divisible down to the 100 millionth unit, known as a **satoshi**. This feature allows for transactions and prices of all sizes to be denominated in bitcoin, regardless of the purchasing power of one bitcoin.

Adaptive Difficulty

The Bitcoin protocol frequently adjusts the difficulty of solving a nonce to seal a block in order to maintain the intended block timing of 10 minutes. Block timings allow all network participants to keep pace with the ledger, prevent double spending, guard against bad actors with immense computing power, and maintain internal event scheduling such as halvings.

Trustless

Performing transactions on a blockchain makes the transactions “trustless.” You do not need to trust or even know the person on the other side of the transaction because the transaction is validated by the users of the network and the underlying computations of the protocol. By transacting on the blockchain, you can rest assured that the transacted amount is authentic and that you are receiving the true balance of the transaction once the network provides confirmation.

Censorship Resistant

As a decentralized, distributed blockchain, Bitcoin is censorship resistant. Central banks cannot manipulate the Bitcoin blockchain. The furthest that governments can go in an effort to go against Bitcoin is to regulate the actions of citizens regarding the use of the Bitcoin blockchain. Even in this case, paper wallets, self-storage of private keys, and local methods of using Bitcoin can allow users to continue using Bitcoin in the face of government regulation. Although no one can censor the blockchain, the addresses of bad actors can be “blacklisted” in regulated jurisdictions with “know your customer” (KYC) processes, effectively banning the use of that user’s bitcoins at reputable entities.

Bitcoin provides users pseudonymity in their transactions, and other blockchains have focused on features to improve user anonymity. Solutions such as mixers, which mix the bitcoins of many users to make tracing more difficult, bolster the anonymity of network participants. Even though Bitcoin transactions can be traced, it is far more difficult to track down a person on the Bitcoin blockchain than it is with our current financial system.

Bitcoin as a Bearer Instrument

Bitcoin transactions require possession of the private key that corresponds to the public address participating in the transaction. This makes Bitcoin a bearer instrument, meaning that the true owner of the bitcoin owned by a public address is whoever holds the paired private key. Common bearer instruments are paper stock certificates, bonds, and tickets to entertainment/sporting events.

The downside to the use of keys as proof of ownership is that if one misplaces or forgets their private key, then their bitcoin balance is not accessible and is effectively lost. Custodial accounts, offered by many popular cryptocurrency exchanges, replace the private key to a corresponding public key with a standard username and password (such as what is required to log into your email or bank account). With a custodial relationship, the exchange (or other custodial entity) is entrusted by the client with the management of the private key for the public address holding the assets.

Node Types

Participants on a blockchain network are known as nodes. However, there are different types of nodes that take on different functions in the ecosystem depending on how a user wants to interact with the blockchain. The Nakamoto Blockchain has four types of nodes: full, network routing, mining, and wallet. Full nodes hold a local copy and distribute copies of the entire blockchain ledger. Full nodes can authoritatively verify transactions without external references. Full nodes have complete freedom from any central authority. Network routing nodes validate and propagate transactions for insertion into the next block. Mining nodes perform the proof of work tasks required to add a new block to the chain and finalize the transactions of that block. Wallet nodes do not need to hold a full copy of the blockchain, but are still able to accept and send transactions on the blockchain. Wallet nodes are referred to as simplified payment verification (SPV) nodes.

Changing Bitcoin Narratives Over Time

As Bitcoin and blockchain technology have continued to evolve, so has the perception of Bitcoin's purpose. When Satoshi Nakamoto created Bitcoin, its purpose was to be a peer-to-peer electronic cash system. Bitcoin was also labeled, quite early on in its lifetime, to also serve the purpose of being a censorship-resistant asset, which has remained a constant function of Bitcoin to today. Many pioneers of the blockchain space were motivated by the monetary actions of governments to create a financial medium out of any government's reach.

Another narrative of Bitcoin's purpose which has persisted throughout most of its history is its ability to serve as a fast and low-cost payment network. Especially as Bitcoin began receiving increased adoption over time, many people have turned to Bitcoin for cross-border payments that have traditionally been slow and expensive. While Bitcoin fees are not nominal for lower-value transactions, Bitcoin, other cryptocurrencies, and available scaling solutions provide a strong alternative to contemporary payment method alternatives.

When the Silk Road site and its successors operated as high-volume online marketplaces for illicit goods, they caused increased demand for bitcoin, which created another use case for bitcoin: a currency for illicit, anonymous online transactions. After the dismantling of these sites by law enforcement agencies and the advent of blockchains which can provide better anonymity for users than Bitcoin does, this use case has all but disappeared as a leading use case for Bitcoin and other cryptocurrencies. However, the negative perception of Bitcoin as a form of "illegal dark-web money" has unfortunately persisted with the public, long after the near elimination of this use case relative to the volume of Bitcoin transacted.

Chainalysis conducts an annual study to investigate the use of cryptocurrencies in illicit transactions. While the total value of cryptocurrency-based illicit transactions reached an all time high in 2021, the share of all cryptocurrency transactions as illicit transactions reached an all time low of only 0.15% for the same year.[18] This strange relationship is largely a result of the heavily increased use of cryptocurrencies and blockchain-based applications. While any currency will have some use for illicit transactions, the share of transaction volume is the important metric to track when viewing how cryptocurrencies are separating from their former use case as a medium of exchange for illicit transactions.

As the blockchain space continued to develop and new blockchains were created each with their own coin(s), the use of Bitcoin as a reserve currency for cryptocurrency trading became more popular. While volatile itself, Bitcoin found a use case for itself as a "stable" trading partner and holding currency for the cryptocurrency market when considering the volatility of other cryptocurrencies. While still used today, this use case is not as relevant as before due to the increased use of stablecoins for trading in cryptocurrency markets.

[18]Chainalysis Team. "Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity." *Chainalysis*, 6 Jan. 2022, https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.

Finally, the narrative of Bitcoin as an independent, uncorrelated asset came about as adoption continued to occur and is considered by many to be the current primary use case for Bitcoin. This narrative has been helped by the COVID-19 pandemic where fiat currencies are continued to be mass-printed in response to the pandemic and by the collinear nature of traditional financial assets.

Summary

While the first to catch traction and remain in a prominent position today, Bitcoin was not the first attempt at creating an “internet money.” Bitcoin endured some tough times during its growth to where it stands today, facing its use as a means of transaction on illicit goods sites and a civil war among its community that still has a lasting result. In recent years, bitcoin has seen exuberant bull runs and dreary “crypto winters.” Along the way, adoption of Bitcoin has increased, finding itself traded on major international traditional financial exchanges, being held on the balance sheets of major corporations, and being adopted as legal tender in El Salvador.

Bitcoin possesses some unique properties that makes it stand out among other alternatives to money. Bitcoin exists on the Bitcoin blockchain where anyone can join and view the information of the network. The ledger maintained by the Bitcoin blockchain is immutable and maintained in a decentralized fashion. Bitcoin as a currency is a bearer asset, is deflationary in the long-run, and is divisible down to the 100-millionth unit. Users can transact in a trustless manner by only needing to trust the code of the Bitcoin blockchain and do not have to fear the censorship of a central party.

The perception of Bitcoin has changed quite frequently over its relatively short lifespan. Bitcoin was first created to be a peer-to-peer electronic cash system. It also picked up the label of being a censorship-resistant asset early on. The use of bitcoin as a form of payment on illicit goods sites created a narrative of bitcoin being a form of “illegal dark-web money” which has proven difficult to shake off. The rise of alternative cryptocurrencies gave rise to bitcoin’s use as a reserve currency for other cryptocurrencies. However, this use case has been outgrown in recent years due to the proliferation of stablecoins. Today, the perceptions of bitcoin as an independent, uncorrelated asset and as a type of “e-gold” largely dominate.

Review Questions

1. Describe the differences between the SegWit and SegWit2x proposals.
2. Describe unique properties of Bitcoin compared to other mediums of exchange. Explain their technical foundations.

3. What is the maximum number of bitcoins that will ever exist?
4. Approximately how often does the mining reward get reduced? By how much is the mining reward reduced at these times?
5. What is the smallest divisible unit of one bitcoin?
6. What is the approximate block timing of the Bitcoin blockchain? How does it maintain this block timing?
7. Is one able to recover their bitcoins if they lose their private key when self-custodying their bitcoins?

Chapter 4: Ethereum and Smart Contracts

Creating Ethereum

Today, the Bitcoin blockchain is focused nearly entirely on payments as it was initially proposed as a peer-to-peer digital cash payment system. Vitalik Buterin, an avid follower of Bitcoin and the editor of Bitcoin Magazine, saw potential in other compelling uses of blockchain technology beyond its use as a peer-to-peer payment system. In the early days of Bitcoin, some alternative blockchain uses began appearing. Built off of the Bitcoin Blockchain, projects such as NameCoin which aimed to be a decentralized domain registration system and Colored Coins which were Bitcoin-based tokens that had metadata associated with them provided early examples of how blockchain technology can be broadly used.

The Ethereum blockchain, a blockchain entirely independent from the Bitcoin blockchain, seeks to empower use cases of blockchain technology beyond peer-to-peer payments. The Ethereum blockchain was built to conduct logical operations on its own and allow for complex code to be processed on a blockchain, which greatly increases the range of possible use cases for blockchain technology. In his creation of Ethereum, Vitalik Buterin sought to develop a single blockchain platform where all other blockchain applications could be built, rather than requiring a different blockchain for every use case.

Ethereum: The World Computer

Bitcoin lacked a general purpose programming language that would allow for applications to be easily built on it. In recognition of this, Vitalik Buterin developed the **Solidity** programming language for all applications to use on Ethereum. Solidity is a “Turing complete” programming language, meaning that fully functioning applications can be created using the language. With its own Turing complete language, Ethereum functions as a development platform for others to build **decentralized applications** within a blockchain environment, known as “**dApps**.” Simply put, decentralized applications are computer programs that execute on a blockchain. Decentralized applications often employ “smart contracts” to execute their purpose. The **Ethereum Virtual Machine (EVM)** is the infrastructure for smart contracts on the Ethereum blockchain. The EVM is powered by the computers acting as participants of the Ethereum network. Ethereum is sometimes referred to as a “world computer” because any smart contract executed on the Ethereum blockchain is executed in the entire ecosystem of shared computing. With the creation of Ethereum, developers were given much more freedom to the bounds of what they were able to create on a blockchain.

Ethereum vs. Bitcoin

While Bitcoin and Ethereum are the two most prominent blockchains, the two function quite differently to achieve their respective goals. Both blockchains have a native currency: bitcoin (BTC) for the Bitcoin blockchain and ether (ETH) for the Ethereum blockchain. While Bitcoin's block time is approximately 10 minutes, Ethereum has a much shorter block time of approximately 15 seconds.

Bitcoin's block reward is currently 6.25 BTC plus transaction fees, while Ethereum's block reward is 2 ETH. Due to the shorter block timings, multiple "competing" solutions are more commonly found on the Ethereum blockchain than in the Bitcoin blockchain. In order to appropriately compensate and encourage miners to continue contributing computing power, miners are still rewarded for mining "orphan" blocks (blocks that have been correctly mined, but not added to the main chain due to delays in the network).

The Bitcoin blockchain typically processes about 4 transactions per second, while the Ethereum blockchain typically processes about 20 transactions per second. While Bitcoin has a maximum supply of 21 million BTC, Ethereum has an issuance cap of 18 million ETH per year. Bitcoin is divisible to the 100 millionth unit (0.00000001 BTC), known as a satoshi. Ether has greater divisibility, given that its smallest unit, known as a wei, is equal to one quintillionth of an ether (0.000000000000000001 ETH).

Ethereum Properties

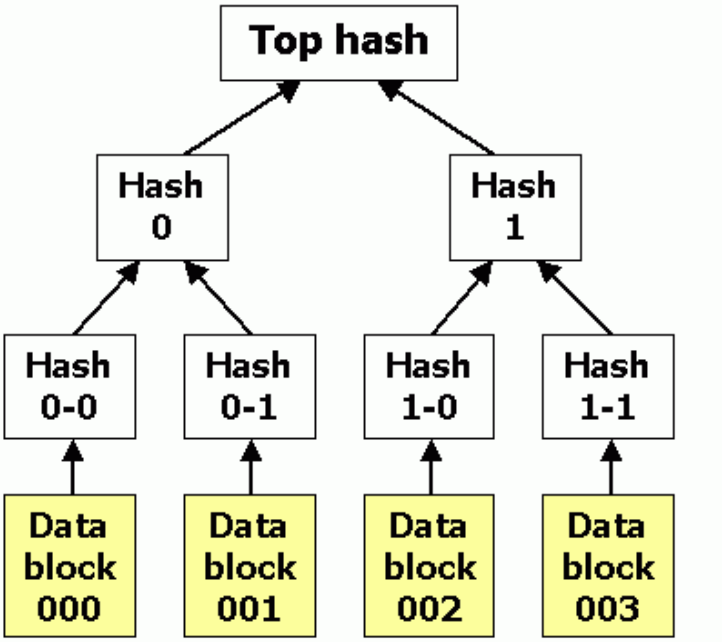
Underlying its different functions and purposes, compared to those of the Bitcoin blockchain, Ethereum is built with many aspects that are unique from those of Bitcoin.

Account Types

There are two kinds of accounts on the Ethereum blockchain: **externally owned accounts** and **contract accounts**. Externally owned accounts are accounts that are owned by the participants of the network, similar to the accounts of the Bitcoin blockchain. There is no additional code associated with these accounts. Externally owned accounts can initiate transactions on the blockchain with other externally owned accounts and with contract accounts. Contract accounts are accounts that are controlled by the computer code of a smart contract and are not directly owned by network participants. Contract accounts initiate transactions based on the predetermined instructions of its smart contract. Contract accounts can own other contract accounts and it is possible to create a "library" of associated smart contract-owned accounts.

Merkle Trees

A **merkle tree** is a data structure that leverages hash functions to create a verifiable state without the need to store all of the underlying data that created the current state. The image below provides a simple merkle tree structure.[19]



In a merkle tree, hashes propagate upward in a way that if data is altered on the bottom of the tree, the hashes above that data will be changed. For example from the diagram above, if the data in "Data block 000" is changed then "Hash 0-0" will be changed, as will "Hash 0," as will the "Top Hash." An upward ripple effect can be observed from the changing of data at the bottom of the tree.

The top of the merkle tree (titled "Top hash" in the diagram above) is known as the **merkle root**. A root node is dependent on the other data in its "branch" of the tree. If any data in the tree is altered, the merkle root hash will be changed, making obvious an attempted or accidental data change. The state of the entire merkle tree can be verified with merely the merkle root hash.

Merkle trees enable "light nodes" (or network routing nodes) to exist on a blockchain network, as these nodes can still perform their functions without needing the full copy of the ledger, but rather just the root hashes of the blocks. In a blockchain system where space is scarce/costly due to its distributed nature, data structures such as merkle trees are extremely helpful.

[19] Public Domain Image created by David Göthberg. Image has not been altered and may appear in original color or grayscale. Image is accessible at: https://commons.wikimedia.org/wiki/File:Hash_tree.png

GHOST Protocol

The "**GHOST** (Greedy Heaviest Observed Subtree) **protocol**" is an Ethereum feature that prevents multiple chains ("forks") by determining which chain is the Canonical chain. The GHOST protocol dictates that the main chain of the Ethereum blockchain is the one with the most computational power performed on it, shown by the amount of blocks that comprise each chain. Although Ethereum compensates miners for solving "orphan" blocks, only the main chain, as determined by the GHOST protocol, is continued.

Gas, Gas Price, Gas Limit, and Block Gas Limit

Transactions that involve more information, require more storage, and are more difficult to process should cost a user more to execute. **Gas** is the unit used to measure the required level of computation for a transaction in the Ethereum blockchain. The amount of gas required for a transaction is determined by the amount of computational power necessary to fulfill the transaction. A standard transaction on the Ethereum blockchain consumes 21,000 units of gas.

Gas price is the user-determined amount of ether that they are willing to spend on each unit of gas required for their transaction. Gas price is measured in "gwei," which is equal to 1,000,000,000 wei or 0.000000001 ETH. Users of the network looking to send transactions each submit their gas price "bids," effectively creating a market determined price floor for transactions to be executed. Users wanting their transaction to occur as soon as possible can incentivize miners to prioritize their transaction by offering a higher gas price than the rest of the market.

Gas limit is the maximum amount of gas that a user is willing to spend for a given transaction to be executed on the Ethereum blockchain. If a transaction exceeds the gas limit set by the transaction's originator, it will not execute. Gas limits prevent a transaction from executing that would incur a transaction fee greater than expected. Because there is no central entity to refund incidental transaction fee expenditures, once a user spends ether on a transaction fee (and any funds sent in a transaction for that matter), it is gone.

The **block gas limit** is the maximum amount of gas allowed in one block, which determines how many transactions and how much information can fit into the upcoming block. Miners decide which transactions will be included in the next block by maximizing the transaction fees to be collected. Because each block has a finite capacity, transactions with the highest gas price are typically the most appealing to miners.

Transaction fees

The maximum transaction fee is determined by the product of the gas limit for the transaction and the gas price. For example, if a user submits a gas limit of 50,000 and a gas price of 20 gwei, their maximum transaction fee will be 1,000,000,000,000,000 wei, or 0.001 ether.[20] The true transaction fee paid will be determined by the actual amount of gas consumed to complete the transaction. The actual transaction fee paid can be lower than the calculated max transaction fee, but will not exceed the maximum transaction fee.

Users must pay gas fees for the storing of information on the blockchain, as additional information stored on the blockchain creates a larger chain for all ledger-holders to keep a copy of. The greater the amount of information to be stored, the greater the gas fees will be for the transaction to execute.

EIP-1559: ETH Burn Mechanism

Ethereum Improvement Proposal (described below) 1559[21], instituted in Summer 2021, made a change to the way transaction fees were handled on the Ethereum blockchain. Previously, Ethereum transaction fees functioned similarly to that of the Bitcoin network. With the changes included in EIP-1559, the total transaction fee is split into two parts: a base fee and a priority fee. The base fee is adjusted by an algorithm of Ethereum's protocol which strives toward a gas target for blocks to reach. The priority fee is a fee which users adjust to get their transaction processed by miners before those of other users.

EIP-1559 stipulates that base fees are burned and that miners will only receive priority fees in addition to the 2 ETH block reward. This burning of base fees provides the Ethereum blockchain a mechanism to combat ether inflation while preserving block rewards for the future (unlike Bitcoin, Ethereum has no designated maximum supply). An average of 2 ETH burned per block makes ETH a deflationary currency. Many blocks burn 2+ ETH, with nearly 2 million ETH burned to date.[22]

---

[20]Kasireddy, Preethi. "How does Ethereum work, anyway?" *Preethi Kasireddy*, 13 Sept. 2017, https://www.preethikasireddy.com/post/how-does-ethereum-work-anyway.

[21] Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, Ian Norden, Abdelhamid Bakhta, "EIP-1559: Fee market change for ETH 1.0 chain," *Ethereum Improvement Proposals*, no. 1559, April 2019. [Online serial]. Available: https://eips.ethereum.org/EIPS/eip-1559.

[22]"Watch the Burn: EIP-1559 Real-Time Eth Burn Visualization for Ethereum." *Watch The Burn*, https://watchtheburn.com/.

Another motivation for this change is a desired movement away from the first price auction method of transaction fees. Up until now, we have described transaction fees to function as a first price auction where users submit their maximum transaction fee to miners. From here, miners will select the transactions of users willing to pay the most. This method causes large volatility and inefficiencies in transaction fees. By making this change, the Ethereum blockchain is positioning itself to provide more efficient transactions for its users, a front which many newer blockchains are challenging it head on.

Ethereum Request for Comment (ERC) Standards

In addition to the ether **coin** (an asset or "cryptocurrency" native to the blockchain, such as bitcoin for the Bitcoin blockchain) of the Ethereum blockchain, developers can also create **tokens** on the Ethereum blockchain. Tokens are assets that do not have their own blockchain network, but are rather built on top of another blockchain. Tokens of the Ethereum blockchain are processed by the same miners handling ether transactions. Transaction fees for transactions of tokens built on the Ethereum blockchain are paid in ether. Nearly all wallets that support ether also support the use of tokens built on Ethereum.

The Ethereum Request for Comment (ERC) system was created to provide common standards and information about protocol specifications and smart contract descriptions.[23] For example, many ERC standards provide information regarding tokens. The standards provide that all tokens of the same standard can be used the same. The standards allow for any Ethereum wallet to accept all tokens of the same standard once formatted to accept the standard in question.

The most commonly used Ethereum Request for Comment standard is ERC-20. ERC-20 tokens are **fungible**, meaning that every token of its kind is equal and interchangeable with the rest. Both bitcoin and ether are fungible coins. No one bitcoin, ether, or ERC-20 token is inherently different or more valuable than the rest of its kind. Any wallet address capable of receiving ERC-20 tokens can receive any token created under the ERC-20 standard.

[23]"ERC Token Standards." *EthHub*, https://docs.ethhub.io/built-on-ethereum/erc-token-standards/what-are-erc-tokens/#:~:text=ERCs%20.

Non-fungible tokens (NFTs) can also be created on Ethereum. A non-fungible token is a token that is inherently unique and has its own attributes, even compared to other tokens of its series. Non-fungible tokens are not interchangeable as these tokens fundamentally represent different objects. Non-fungible tokens are commonly used to represent digital collectibles and have also seen increased use as a tokenization method of real world assets. Anything from pieces of art to plots of real estate can be tokenized to create a unique, digital representation of an asset. The ERC-721 token standard and the newer ERC-1155 token standard are commonly used for non-fungible tokens on Ethereum.

Ethereum Improvement Proposals (EIPs)[24]

Ethereum has the ability to evolve and upgrade its features. Because there is no central entity of the decentralized Ethereum blockchain, another way of proposing and adopting changes to Ethereum is needed as compared to the typical decision-making structures found in centralized organizations. Potential upgrades, improvements, or new application standards are proposed in the Ethereum ecosystem as Ethereum Improvement Proposals (EIPs). Ethereum Improvement Proposals can cover a variety of topics, including protocol-level changes, ERCs, and smart contract standards. Any Ethereum participant can create an EIP.

Smart contracts

Contracts, in the traditional sense, are merely a series of “if this, then that statements.” A “smart contract” uses if-then statements as computer code. Smart contracts do not inherently serve as legal documents, despite what the name may cause one to presume. A **smart contract** is a program, made of pre-written computer code, that executes on a blockchain when predetermined conditions are met.

Smart contracts remove the need for a middleman in transactions. Smart contracts can automatically execute transactions based upon pre-defined rules written into the computer code. Trustless agreements can be reached between two parties through the use of smart contracts. Given this function, some refer to the blockchain and smart contract infrastructure as the “Court of the Internet.”

A real-world analogy for how a smart contract works is a vending machine. A vending machine has predefined rules for transacting. If the predetermined amount of

[24]“Introduction to Ethereum Improvement Proposals (EIPs).” *Ethereum.org*, 10 May 2022, https://ethereum.org/en/eips/.

money is entered, the vending machine will output a snack. If the customer does not input the predetermined amount of money, no snack will be given.

Decentralized Applications

Smart contracts are the foundation of most decentralized applications. Decentralized applications are applications which run in a distributed blockchain environment. By creating an application on the Ethereum blockchain, the application can easily inherit the decentralized aspect and benefits of the Ethereum network. When accessing the blockchain via a node, you and your application are connected to all of the other computing resources powering the network.

Just as with a decentralized blockchain, a decentralized application requires no central authority for it to run. For example, a common type of decentralized application present on the Ethereum blockchain is a decentralized exchange. A decentralized exchange enables users of the network to trade their cryptocurrency without a central entity processing trades or taking custody of user funds at any point in the transaction. Because decentralized applications are published on a public blockchain, users are able to fully examine the code they are interacting with, which increases transparency.

Protocols

Most of the applications that we use on the Internet today such as social media sites are platforms, not protocols. These platforms often operate independently and users typically experience difficulty in transferring their data between applications if they decide to switch to another or attempt to use multiple applications in conjunction.

With a common protocol, applications can be built that are interoperable by nature thanks to their shared set of predefined standards. Most decentralized applications assume a common protocol. Users can easily navigate applications of the same protocol and move their information between applications. Because of the ability to freely move personal information between applications, users maintain a stronger ownership of their own content and privacy when using decentralized applications of a shared protocol, compared to the use of siloed platforms.

The technology behind email (protocols such as POP3, SMTP, and IMAP) functions similarly to a blockchain protocol that hosts decentralized applications. Everyone is able to communicate with each other on the worldwide email system, despite there being many different email providers. If email providers acted as many online platforms do, users of an email provider’s platform would only be able to communicate with users that are registered with the same provider. The power and

interoperability of the worldwide email system we all use serves as an example of how we can imagine blockchain protocols for decentralized applications to function.

Smart Contract Use Cases

Smart contracts can be applied to manage many different forms of blockchain-based information and transactions. Sample fields and use cases of smart contracts include:

The Creation and Transfer of Digital Assets

One of the most prominent use cases of smart contracts, practically since the creation of Ethereum up until today, is the ability to create new digital assets without having to create a new blockchain. In later chapters, we will discuss in detail the different kinds of assets, referred to as tokens, that can be created on blockchains such as the Ethereum blockchain and what sets them apart from one another.

Tokenized assets can be created for anything from payment for cloud storage to representing ownership of digital art to the representation of real-world assets. Users can simply transact tokenized assets by using the underlying smart contract-enabled blockchain, similarly to how one would send ether, or the respective native coin of the blockchain being used, to another user.

The Ability to Embed Trust in a Transaction

Smart contracts allow for the creation of logical processes for the blockchain to execute when certain, specified conditions are met, without the need for further action by any involved party. Therefore, two parties are able to engage in a transaction without the need to trust each other to perform their respective obligations. Instead, the two parties only need to trust the published, viewable smart contract code governing the transaction that was agreed upon by both parties. In this application of smart contracts, an automatic enforcement of contractual agreements is made possible.

The Self-execution and Enforcement of Business Logic

Thanks to the ability to transact without counterparty trust, smart contracts provide an appealing application of business logic. Many business transactions and their contracts follow the same logic as the foundation of smart contracts: a series of if-then statements.

For example, let's look at a process where a purchaser is only entitled to receive their desired product once payment is made. Under traditional business conventions, the buyer must trust the vendor to deliver the product once payment is made. Additionally, the vendor often must trust in the validity of the payment made by the purchaser, or else the transaction will be faced with delays in waiting for the payment to clear. Today many of these transactions involve an intermediary, which helps to guarantee payment and receipt of the goods. However, both parties must trust the intermediary to perform its job correctly, both parties will be subjected to a lengthy process if a dispute is made, and intermediaries often command sizable fees for their role in the transaction.

Smart contracts offer a unique solution to this transaction in its only requirement being trust in the governing code agreed on by the involved parties. Rather than relying on another self-interested party and/or an intermediary to correctly perform their role in the transaction, the transaction can be self-executed by the smart contract. The purchaser can send the funds stipulated by the code and then the deliverable will be automatically sent to the purchaser. Of course there are limitations on what goods can currently be delivered by this process, but for example a transaction involving a business logo or banner design could easily be supported by smart contracts. Further extensions of this concept could be applied to more significant transactions such as the titles of cars or land. Smart contracts can be also applied to many other transactions such as financial asset trading, insurance services, trusts.

Timestamping events and proving rights/ownership

The sequential and immutable nature of block additions to a blockchain easily enable the ability to timestamp the occurrence of events, particularly in relation to other events. For example, if two parties are competing to acquire a certain asset, bids on the asset have a trusted, known occurrence in relation to one another, with precision down to the block time of the blockchain being used. Data can also be published to a blockchain, which will be stored in an immutable manner. This provides the ability to prove the existence of information at a certain time in the past, leading to applications such as intellectual property protection.

Selective transparency of information and user privacy

While many blockchains allow for most information to be publicly viewable, smart contracts can be used to restrict the view of specific

information to selected individuals. A digital signature by an approved individual could be required for access to information that appears as encrypted information to all other viewers. Selective transparency of information stored on a blockchain opens doors for many applications such as the storage and private sharing of sensitive information such as medical and education records.

The creation and maintenance of blockchain-based identities

Smart contracts can also be used to create digital identities. As with previous examples, the ability to prove who a user is with a simple digital signature is a powerful tool. A person can create an identity for themselves to use online, controlled by their private key, which can host encrypted personal information. Once the need arises to prove their identity, they can selectively reveal only the necessary personal information to the requesting entity.

The use cases of smart contracts go far beyond the facilitation of financial transactions. Smart contracts can be applied to almost anything, of any attached value, that changes state over time. The non-confined nature of smart contracts allow for new use cases to be created all the time. As we saw with these examples, many applications of smart contracts can be combined to create innovative and complex use cases for smart contracts.

Smart Contract Case Study: fizzy by AXA[25]

Fizzy was a parametric flight insurance product released by insurance giant AXA in September of 2017 that initially covered flights between Paris and the United States. At its peak, fizzy covered at least 80% of flights worldwide.[26] It was the first blockchain-based insurance offering by a major insurance group. Smart contracts deployed on the Ethereum blockchain powered fizzy. Fizzy offered flight insurance that was handled entirely by the smart contract.

The predetermined terms of the smart contract stated that in the event when a passenger's flight was delayed for more than 2 hours, the agreed upon insurance payout would be sent to the customer. In the event that one's flight was delayed by more than 2 hours, no claim filing was necessary as the smart contract would

[25]"AXA Goes Blockchain with fizzy." *AXA.com*, 13 Sept. 2017, www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy.

[26] CLEMENT, Alexandre. "fizzy by AXA: Ethereum Smart Contract in details." *Medium*, 24 May 2019, medium.com/@humanGamepad/fizzy-by-axa-ethereum-smart-contract-in-details-40e140a9c1c0.

automatically trigger a payout to the customer. The smart contract was constantly fed information from global air traffic databases so that it knew when a flight became delayed for more than two hours. Fizzy was discontinued in November of 2019, but it continues to serve as a real-world case study of applying smart contract and blockchain technology beyond the realm of peer-to-peer transactions.

Oracles

Computers are powerful tools that can achieve many feats far beyond the capabilities of humans. However, technology is only as good as the information given to it. If a computer is given incorrect input, then it will produce an incorrect output. Blockchain technology and smart contracts are no different in this regard. In fact, the decentralized nature of blockchain technology and many of the applications built on top of it requires an even greater reliance on a reliable third-party source of outside information.

An **oracle** is an off-chain data source from which smart contracts receive necessary data that is used to modify their behavior. For a long time in the world of blockchain technology, it has been a difficult task to get reliable “off-chain” from the real world and put it in an “on-chain” environment. Oracles are a crucial part to the working functionality of smart contracts, as smart contracts cannot fulfill their intended purpose without the correct information needed for their predetermined executions.

Oracle Case Study: Chainlink[27]

Chainlink is the market leader when it comes to oracles in the blockchain space. Chainlink is a decentralized oracle network that services many of the most popular dApps of the space. Chainlink’s core product is its network of market and data feed oracles. Decentralized finance applications, a major component of the blockchain space, cannot function without reliable, frequent price information. This reliable data is delivered through a process that can be summarized in three steps[28]:

1. Raw data is gathered by partnered data aggregators. In the case of market price data feeds, pricing data is collected from both centralized and decentralized exchanges and is prepared to be passed down to the next step.

2. Independent Chainlink nodes gather this raw, aggregate information and synthesize it into a market-representing aggregate value.

[27]“Blockchain Oracles for Hybrid Smart Contracts: Chainlink.” *Chainlink*, https://chain.link/.

[28]“Decentralized Data Feeds for Hybrid Smart Contracts: Chainlink.” *Chainlink*, https://chain.link/data-feeds.

3. Finally, many Chainlink nodes bring their results together to prepare an oracle report which is made available on-chain for smart contracts to use.

Another core service provided by Chainlink is its Verifiable Random Function (VRF). While it may appear as a simple idea, the need for a truly random function is critical to the success and fairness of many applications built on blockchain technology. Use cases include the randomization of traits in the minting of non-fungible tokens, gaming, and the random assignment of roles and picking of a population sample for consensus mechanisms.[29]

Decentralized Autonomous Organization(s)

Smart contracts can be deployed on Ethereum in ways that go far beyond the simple execution of a transaction based upon predetermined rules. With blockchain-based smart contracts, an entire organization can be constructed. A **decentralized autonomous organization** (DAO) is an organization owned by its community members that is created and managed by smart contracts. DAOs do not have a central authority. Instead, decisions are made by a vote of the organization's members on proposals written by community members. The concept of an organization running smoothly without any authority in the center of it can appear unconventional and even impossible to outsiders of the blockchain space. The following case studies about The DAO and MakerDAO will provide real-life examples of how DAOs function.

Decentralized Autonomous Organizations Case Study: The DAO

The DAO, founded in 2016, brought the concept of a decentralized autonomous organization to the mainstream blockchain community. The DAO was created and managed by a set of smart contracts existing on the Ethereum blockchain. The DAO sought to organize individual investors for venture capital investments, without the need for a central power in the group. Investment decisions would be decided by the owners of its native token: DAO. Anyone could propose a project to The DAO for investment and then its members would vote on whether or not to fund the project.[30]

The DAO raised more than 10 million ether through its massively successful crowdfunding efforts, which was worth more than $150 million at one point and

[29]"Introduction to Chainlink VRF: Chainlink Documentation." *Chainlink*, https://docs.chain.link/docs/chainlink-vrf/.

[30]Falkon, Samuel. "The Story of the Dao - Its History and Consequences." *Medium*, The Startup, 24 Dec. 2017, https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.

constituted ~14% of all ether in circulation at the time.[31] With initial indications pointing toward a successful future, The DAO quickly collapsed due to an issue with the smart contract which allowed for an exploit to drain The DAO of $60 million worth of Ether.[32]

The hack of The DAO highlighted an important feature of smart contracts. Smart contracts on the Ethereum blockchain (and other public blockchains) are fully viewable for all to see. The public nature of smart contract code requires for the smart contract publishers to be particularly diligent in ensuring that the code is not exploitable.

The DAO exploit also caused a pivotal moment in the history of Ethereum. In response to the hack which put a considerable amount of circulating ether at risk, the Ethereum Foundation and the Ethereum community decided to conduct a "hard fork" of the Ethereum blockchain to return the exploited funds to their owners before the exploit occurred, as denoted in the ledger. Members of The DAO were then able to reverse-exchange their DAO tokens for ether with their initial exchange rate used to join The DAO.[33] The controversial hard fork gave rise to Ethereum Classic which became a separate blockchain supported by Ethereum community members who opposed the hard fork. Ethereum Classic reflects the exploited funds and all prior blocks of the Ethereum blockchain, but has an entirely different ledger of transactions following the exploit.[34]

Decentralized Autonomous Organizations Case Study: MakerDAO

MakerDAO, established in 2014, is a decentralized autonomous organization on the Ethereum blockchain that presides over the Maker Protocol. The Maker Protocol primarily "allows users to generate Dai by leveraging collateral assets."[35] Dai holds an approximate (soft-peg) exchange rate of $1 USD with the deposited collateralized cryptocurrency assets.

---

[31]"The Dao of Accrue." *The Economist*, 19 May 2016, www.economist.com/finance-and-economics/2016/05/19/the-dao-of-accrue.

[32]Cryptopedia Staff. "What Was The DAO?" *Cryptopedia*, Gemini, 16 Mar. 2022, www.gemini.com/cryptopedia/the-dao-hack-makerdao.

[33]Castillo, Michael del. "Ethereum Executes Blockchain Hard Fork to Return DAO Funds." *CoinDesk*, 20 July 2016, www.coindesk.com/tech/2016/07/20/ethereum-executes-blockchain-hard-fork-to-return-dao-funds/.

[34]Cryptopedia Staff. "What Was The DAO?" *Cryptopedia*, Gemini, 16 Mar. 2022, www.gemini.com/cryptopedia/the-dao-hack-makerdao.

[35]"The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System." *MakerDAO*, https://makerdao.com/en/whitepaper/.

MakerDAO is governed by the owners of its native “governance token”: MKR. Members can “stake” their MKR tokens by locking them in a smart contract and gain voting rights in proportion to their staked MKR tokens.[36] Voting rights can be exercised in decisions regarding Maker Protocol parameters such as stability fees and allowed collateral types/rates.[37]

MakerDAO is responsible for over 10 billion Dai and more than $17 billion USD of collateralized assets.[38] The MKR governance token has a market capitalization peak of nearly $6 billion USD. MakerDAO has functioned as a central piece of blockchain-based financial infrastructure for several years without a central authority.

Summary

The Ethereum blockchain seeks to empower use cases of blockchain technology beyond peer-to-peer payments. The Ethereum blockchain was built to conduct logical operations on its own and allow for complex code to be processed on a blockchain, which greatly increases the range of possible use cases for blockchain technology. The Ethereum blockchain was developed to be a single blockchain platform where all other blockchain applications could be built, rather than requiring a different blockchain for every use case.

The Ethereum blockchain possesses distinctive qualities that allows it to expand on the use cases of blockchain technology. The native programming language of the Ethereum blockchain, Solidity, is a “Turing complete” programming language, meaning that fully functioning applications can be created using the language. Contract accounts are accounts that are controlled by the computer code of a smart contract that can initiate transactions based on the predetermined instructions of its smart contract. The Ethereum Request for Comment (ERC) system was created to provide common standards and information about protocol specifications and smart contract descriptions. A common application of the Ethereum Request for Comment standards is the creation of different types of tokens. Potential upgrades, improvements, or new application standards are proposed in the Ethereum ecosystem by community members as Ethereum Improvement Proposals (EIPs).

A smart contract is a program, made of pre-written computer code, that executes on a blockchain when predetermined conditions are met. Smart contracts can

[36] Ibid.

[37] Ibid.

[38] *Dai Stats*, https://daistats.com/.

automatically execute transactions based upon pre-defined rules written into the computer code. Smart contracts are the foundation of most decentralized applications. Decentralized applications are applications which run in a distributed blockchain environment. Smart contracts on a public blockchain can go beyond simple decentralized applications. With blockchain-based smart contracts, an entire organization can be constructed. A decentralized autonomous organization is an organization owned by its community members, with no central authority, that is created and managed by smart contracts.

Review Questions

1. What is a decentralized application?
2. What is the difference in the approximate block timings of the Bitcoin blockchain and the Ethereum blockchain?
3. What is the block reward of the Ethereum blockchain?
4. What is a merkle tree?
5. How are transaction fees calculated on the Ethereum blockchain?
6. What is the difference between a coin and a token?
7. Describe two different ERC standards.
8. What is a smart contract?
9. What role does an oracle play in a blockchain environment?
10. How are governing decisions made in a decentralized autonomous organization?

Chapter 5: Addressing Challenges

Although the decentralized nature of the blockchains we have discussed provide many benefits, there are also challenges which arise from not using a centralized system. This chapter discusses many of the main challenges faced by contemporary blockchains.

Centralized vs Decentralized Blockchains

Data stored on a blockchain is stored indefinitely. The append only nature of blockchain technology causes previously stored data to be immutable. A publicly accessible blockchain has an inherent tradeoff between lower transaction throughput and a higher degree of centralization. A decentralized blockchain accepts low transaction throughput in exchange for not having a central authority. Increased centralization of a blockchain provides increased efficiency, while increased decentralization of a blockchain provides more security.

As a blockchain network grows, the requirements for storage, bandwidth, and computing power increase. As of the beginning of 2022, the Bitcoin blockchain alone is about 400 GB of data.[39] This can cause for a public, permissionless blockchain that began with a high degree of centralization to become increasingly centralized as less and less users are able to keep up with the increasingly prohibitive requirements of participating in the network.

Mining and Asset Ownership Concentration

As the computing power and resource requirements needed to participate in the mining process continue to increase for the Bitcoin blockchain and many others, we observe an increase in the centralization of the computational power put towards these blockchains. Many miners have turned to mining pools which combine computing power and delegate the mining process to their members. In the event that the pool solves the block, the block reward is distributed to its members in proportion to their contributed computing power. Pooled mining increases the chance that a miner will receive a portion of a block reward. The four mining pools with the most pooled computing power consistently provide a majority of the Bitcoin network's entire computing power.[40]

[39]"Blockchain Size (MB)." *Blockchain.com*, www.blockchain.com/charts/blocks-size.

[40]"Pool Distribution." *BTC.com*, https://btc.com/stats/pool?pool_mode=day3.

Blockchain-based assets fall into a distribution that is similar to that of traditional financial assets. More than 85% of all bitcoins are owned by less than 0.5% of all Bitcoin addresses. The top 2% of Bitcoin addresses control nearly 95% of all bitcoins. The top 50% of Bitcoin addresses own more than 99.98% of all bitcoins.[41] Although these figures contain the addresses of some exchanges that custodially hold bitcoin for their clients, the point holds that a small portion of network participants control the overwhelming majority of the network's assets.

Scalability Issues

Decentralized blockchains, with the large amount of information that is required of them to store, suffer inherent scalability issues. We already investigated one attempt at solving scalability issues faced by Bitcoin: the contentious SegWit vs. SegWit2x event. The implemented SegWit proposal increased the effective capacity of a Bitcoin block from 1 MB to 2-4 MB by segregating block information into two distinct parts for faster processing. However, this improvement came only after a long, tumultuous discussion within the community and resulted in a divisive outcome.

Proof of Work Blockchain Challenges

Certain features of the decentralized proof of work system pose issues to the scalability of blockchain technology. The large number of nodes needed to maintain the transaction history of the blockchain and required to provide adequate decentralization of the system results in high storage costs of information held on a blockchain powered by proof of work. Each of these necessary nodes has to store a full copy of the information. Because there is no central entity, there is no central source of information that nodes can reference instead of having to store it themselves.

The intense computations inherent to a proof of work system brings rise to concerns regarding energy consumption and the environmental impact of running the network. Furthermore, the energy consumption of the network is fairly easy to view and estimate, which is a stark difference from other industries that warrant a similar level of scrutiny for their energy consumption and environmental impact.

Additionally, as computational intensity increases, specialized and expensive mining equipment becomes a necessary tool to participate in the network as a miner, which begins to price out individuals interested in mining. The intentional speed bump of block timings causes slow transaction times with limited room for improvement. Block

[41] "Top 100 Richest Bitcoin Addresses and Bitcoin Distribution." *BitInfoCharts*, https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html.

size capacities restrict the rate of transactions that can be processed in a given amount of time, yielding a maximum throughput that is quite low relative to contemporary payment networks. The open source nature of these blockchains give rise to the possibility of forks.

Blockchain Trilemma

The "**blockchain trilemma**" is a belief held by many in the blockchain technology space that blockchains are forced to make tradeoffs between decentralization, scalability, and security to where only two of the three can be achieved by a blockchain at any given time. Both Bitcoin and Ethereum are examples of blockchains that opt for decentralization and security rather than ease of scalability. If a blockchain were to want both security and scalability, it would need to sacrifice some amount of decentralization. If a blockchain wanted to be both decentralized and scalable, it would need to sacrifice some amount of network security.

Scalability Solutions

As blockchain technology continues to grow in use, the need for scalability solutions continues to become more apparent. There are many avenues of approach to expanding the scalability blockchains that are being considered by members of the blockchain community. We will dig deeper into four potential solutions to the scalability of blockchains.

Alternative Architectures

Blockchains are designed with architectures that help to best achieve their purpose. Blockchains intent on processing large-scale transaction volume can be designed with an architecture to support that goal. Additionally, blockchains can alter their architecture to better support its changing needs and goals. For example, the SegWit proposal presented a solution to the scalability of Bitcoin by altering the architecture of transactional information. Blockchain architectures that are permissioned or private can relax security features to allow for faster and more frequent transactions.

Proof of Stake (PoS)

Proof of stake is a consensus algorithm, different from the proof of work system that we have already covered, which replaces the intense computational work needed in proof of work with the staking of money inside the blockchain ecosystem.

Proof of stake drastically reduces the level of hardware required to reach consensus. While proof of work nowadays requires expensive, specialized equipment to

contribute meaningful computational power to have a chance at receiving a block reward, proof of stake can be run on a basic laptop as there is no longer a competition between network participants to seal the block first. The vast reduction of required equipment comes with a significant reduction in energy consumption to operate the blockchain. Proof of stake simplifies the block creation process and greatly reduces the amount of computational power needed to do so, allowing for greater scalability.

Sharding

As the amount of information stored in a database increases, searching the database becomes more challenging and the database becomes more difficult to properly manage. **Sharding** is a database management technique that logically breaks apart the data and stores it on different instances ("shards"). Under sharding, a database is split horizontally and handled simultaneously with these multiple instances.[42] Sharding effectively breaks apart a large database into smaller, sorted databases which makes the searching and management of data easier.

If sharding was applied to an email database, the single database containing all the information of the email users can be broken down into smaller databases ("shards") of continents from which users access the email service. Therefore, a search for an email user from North America can be performed only on the database of North American users rather than the whole database. The continent shards can be further broken down into country shards to improve the organization and searching of the entire database.

"Layer 2" Solutions

A "layer" can be built on top of a blockchain where transactions can occur in an off-chain payment channel without each transaction needing to be added to the main chain. Transactions that occur in an off-chain payment channel occur instantly, as there is no block time waiting period. Once transactions on the layer are finalized, the necessary information required to update the main chain can be processed and recorded. The main chain is used as a settlement layer that processes a final transaction that represents all of the transactions that occurred in the off-chain payment channel. Off-chain payment channels reduce the amount of transactions needed to be recorded on the main chain, which improves the scalability of a blockchain by increasing the effective number of transitions that can occur in a given period of time. The Lightning Network is a layer 2 off-chain payment channel built on the Bitcoin blockchain.

[42]"Shard Chains." *Ethereum.org*, 10 May 2022, https://ethereum.org/en/upgrades/shard-chains/.

In addition to transactions, off-chain layers can also host computation that would ordinarily be done on the main chain. Off-chain computation layers, such as Plasma for the Ethereum blockchain, perform the necessary, difficult computations of smart contracts and then update the main chain with the final state. Off-chain computation greatly reduces the computational burden placed on the main chain and improves the blockchain's potential for scalability.

Energy Consumption and Environmental Impact Concerns

The proof of work system and decentralized computing in general require a vast amount of computing power and therefore energy consumption. Concerns are often raised regarding the worthwhileness of energy consumption by blockchains and the subsequent environmental impact of the energy consumption. The University of Cambridge Bitcoin Electricity Consumption Index places Bitcoin's average annual energy consumption in the range of the 30th-40th most energy consuming countries.[43]

Energy Consumption and Environmental Impact Solutions

One avenue to reducing the environmental impact of blockchain technology is the use of renewable energy. Luckily, many miners are already drawn to renewable energy due to the low cost at which it can be acquired. At the right time and place, energy resources such as solar, hydroelectric, and wind can be used at far less cost than non-renewable sources of energy. Many mining operations in China have collocated with hydroelectric power facilities due to the cheap cost at which energy can be acquired. The 3rd Global Cryptoasset Benchmarking Study by the University of Cambridge, published in September 2020, found that 76% of miners use renewable energy as part of their energy use and 39% of total energy consumption used for mining is powered by renewable energy.[44]

Energy from the mining process can also be captured to serve as its own energy source. For example, a practice referred to as "hotmining" can be implemented where the heat expelled by mining equipment is captured and used to heat spaces that would otherwise consume electricity to do so.

---

[43]"Cambridge Bitcoin Electricity Consumption Index (CBECI) | Comparisons." *University of Cambridge Judge School of Business* | *Cambridge Centre for Alternative Finance*, https://ccaf.io/cbeci/index/comparisons.

[44]Blandin, Apolline, et al. "3rd Global Cryptoasset Benchmarking Study." *University of Cambridge Judge School of Business* | *Cambridge Centre for Alternative Finance*, Sept. 2020, www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf.

Privacy Concerns

Although many early adopters of Bitcoin thought that they were anonymous when using the network, it turns out that Bitcoin and other similar blockchains only provide a pseudonymous protection to its users. It is still possible to track transactions and link them to individuals. Federal agencies have long used Bitcoin transactions to track and apprehend criminals that chose Bitcoin as their medium of exchange. While once a fear of federal agencies, the blockchain has proven to be quite a nice tool in investigating the financial transactions of an individual.

Tracking individuals through pseudonymous blockchains is fairly simple once you can tie a person's identity to their public address. Due to the open nature of public blockchains, anyone can easily view every single transaction ever made involving a certain address. This is an extremely powerful tool, akin to (or even more powerful than) gaining access to someone's entire bank statement history. Unlike with bank accounts, no warrant or special is necessary to view one's public blockchain transaction history.

Tracking Through the Blockchain Case Study: Silk Road

As briefly mentioned in our discussion on the history of Bitcoin, Silk Road was an illicit goods online marketplace created by Ross Ulbricht that launched in early 2011. The site mainly hosted and facilitated transactions of illegal drugs, which represented about 70% of product listings.[45]

Silk Road operated as a website on the dark web. It was accessible by using the Tor browser, which aids a user in browsing the internet with greater anonymity by concealing IP addresses and user location.[46] The universal currency used for transactions on Silk Road was bitcoin. As covered in the changing use cases of Bitcoin, Silk Road had a piece of bitcoin transaction volume at the time, projected to be about 4% by some analysts[47], but more importantly the news coverage surrounding Silk Road has had a lasting impact on the public perception of Bitcoin and other cryptocurrencies. Ulbricht believed that the currency of bitcoin, which he perceived as a means to transact

[45]Ball, James. "Silk Road: The Online Drug Marketplace That Officials Seem Powerless to Stop." *The Guardian*, 22 Mar. 2013, www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace.

[46] Al Jawaheri, Hasam, et al. "Deanonymizing Tor hidden service users through Bitcoin transactions analysis." *Computers & Security*, vol. 9, 2020. https://www.sciencedirect.com/science/article/pii/S0167404818309908.

[47]Adler, David. "Silk Road: The Dark Side of Cryptocurrency." *Fordham Journal of Corporate and Financial Law*, Fordham Law School, 21 Feb. 2018, https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/#_edn51.

anonymously, would complement the identity protection offered by Tor in order to create a truly anonymous marketplace.[48]

The Silk Road site was ultimately shut down by authorities in 2013, along with the arrest of its creator, Ross Ulbricht. Ulbricht was discovered by the Federal Bureau of Investigation as the figure behind the site thanks to forum postings made by Ulbricht.[49] The FBI was then able to trace Ross Ulbricht's IP address, despite his usage of the Tor browser. Armed with Ulbicht's IP address, the Federal Bureau of Investigation was able to locate Ross Ulbricht and seize his laptop.[50] Once in possession of Ulbricht's laptop which contained access to both the site and his Bitcoin public and private keys used to facilitate trade on Silk road, the Federal Bureau of Investigation was able to trace all of Ulbricht's Bitcoin transactions, showing that the Bitcoin blockchain is not as quite anonymous as Ulbricht believed it to be.[51]

Ulbricht was convicted on seven charges: distributing narcotics, distributing narcotics by means of the Internet, conspiring to distribute narcotics, engaging in a continuing criminal enterprise, conspiring to commit computer hacking, conspiring to traffic in false identity documents, and conspiring to commit money laundering.[52] Ulbricht received a double life sentence plus 40 years[53] and has seen all his subsequent appeals be denied.

Ulbricht was also ordered to forfeit more than $183 million. The United States Marshals Service ultimately sold the 144,336 bitcoins seized from Ulbricht's computer for more than $48 million.[54] Just as when the Silk Road saga had gone cold, a new

---

[48]United States District Court, Southern District of New York. *United States of America v. Ross William Ulbricht*. https://antilop.cc/sr/trial/.

[49]Jackson, Joab. "Simple Google Search Outed Alleged Silk Road Founder." *Computerworld*, 27 Jan. 2015, www.computerworld.com/article/2875974/simple-google-search-outed-alleged-silk-road-founder.html.

[50]Lee, Dave. "Silk Road: How FBI closed in on suspect Ross Ulbricht." *BBC,* https://www.bbc.com/news/technology-24371894.

[51]Pagliery, Jose. "Bitcoin fallacy led to Silk Road founder's conviction." *CNN Business*, https://money.cnn.com/2015/02/05/technology/security/bitcoin-silk-road/.

[52]Ross Ulbricht, Aka Dread Pirate Roberts, Sentenced to Life in Federal Prison for Creating, Operating 'Silk Road' Website." *U.S. Department of Homeland Security | U.S. Immigration and Customs Enforcement*, 29 May 2015, www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating.

[53]Thielman, Sam. "Silk Road Operator Ross Ulbricht Sentenced to Life in Prison." *The Guardian*, 29 May 2015, www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced.

[54]"Acting Manhattan U.S. Attorney Announces Forfeiture of $48 Million from Sale of Silk Road Bitcoins." *The United States Department of Justice*, 29 Sept. 2017,

addition to the story came in November 2020 when nearly 70,000 bitcoins connected to Silk Road were recovered by the United States government. Through the use of blockchain analysis tools empowered by the public nature of the Bitcoin blockchain[55], the funds were traced all the way since the time they were taken from Silk Road by a hacker in 2012 or 2013.[56] The newly found bitcoins are planned to be sold by the United States government under forfeiture proceedings, totaling more than $1 billion at the time of seizure.[57]

The story of Silk Road and Ross Ulbricht shines a light on the power of tying a real-world identity to a public blockchain address and gives added understanding to what it means for blockchain-based identities to be pseudonymous. While one cannot directly extract a personal identity from a blockchain public key, it is possible to tie an individual's identity to a public key which is generally accomplished through analyzing the public blockchain transactions of the public key in question. Once a real-world identity is tied to the person's public key of a public blockchain, you have instant access to the person's entire financial transaction history. This feature is an immensely powerful tool for government agencies as it can often be extraordinarily cumbersome or outright impossible to obtain traditional financial statements of a person of interest.

Privacy Solutions

While the transparency of the most popular public blockchains such as Bitcoin and Ethereum provide many intended benefits, the use of these blockchains typically allows anyone else to view the entire transaction history of a given wallet address. Both services built to anonymize transactions on public blockchains and new blockchains focused specifically on privacy have been created in an attempt to provide increased privacy for transacting blockchain users.

---

www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-forfeiture-48-million-sale-silk-road-bitcoins.

[55]Chainalysis Team. "Chainalysis in Action: US Government Agencies Seize More than $1 Billion in Cryptocurrency Connected to Infamous Darknet Market Silk Road." *Chainalysis*, 5 Nov. 2020, https://blog.chainalysis.com/reports/silk-road-doj-seizure-november-2020/.

[56]Greenberg, Andy. "Feds Seized $1 Billion in Stolen Silk Road Bitcoins." *Wired*, 5 Nov. 2020, www.wired.com/story/feds-seize-billion-stolen-silk-road-bitcoin/#:~:text=According%20to%20the%20IRS%27s%20criminal,downfall%20in%20October%20of%202013.

[57]Whittaker, Zack. "DOJ Says It Seized over $1 Billion in Bitcoin from the Silk Road Drugs Marketplace." *TechCrunch*, 5 Nov. 2020, https://techcrunch.com/2020/11/05/justice-department-silk-road-billion-bitcoin/.

Mixers

One solution that has been used for a long time in the Bitcoin ecosystem (and has spread to other prominent public blockchains in recent years) to address the traceability of transactions is mixers. Mixers pool the bitcoins (or the asset being transacted) of many owners and then reapportion them in order to interfere with future efforts to trace one's transactions. If the assets of many people are sent to one address and then the one address sends out many transactions to the intended recipient (often in varying amounts or broken up into multiple transactions), it can be difficult to identify both the true, matched senders and recipients of the executed transactions. Mixers can take the form of centralized operations with agents of the entity receiving assets and then strategically sending assets back in exchange for a fee. Decentralized mixers have also been introduced to the market, where all transactions of the mixer are handled autonomously by code. Mixers use the power of multiple transacting users to add further obfuscation to the intended sender and recipient of a transaction. Mixers have recently come under regulatory scrutiny given the ability for mixers to lend easier facilitation to money laundering and illicit transactions. However, the ability for any future enforcements to be executed remains questionable given the unknown status of mixer facilitators or the decentralized nature of many mixers.

Privacy Coins

"Privacy coins" are another solution of the blockchain space to address the potential issues with the pseudonymous nature of Bitcoin and other public blockchains. Privacy coins are the native currency of new blockchains designed to provide greater anonymity to its users and their transactions. The independent blockchains built to facilitate transactions of increased user privacy are equipped with special features beyond those found in public blockchains.

Additional cryptography concepts are implemented to provide greater privacy to blockchain network users and transactions. Zero-knowledge proofs allow for one to prove that a set of underlying information exists without needing to actually know or see the information itself. Examples of privacy coins include Zcash and Monero. Beyond these special additions, these two blockchains are fairly similar to Bitcoin. For example, all three blockchains use proof of work consensus and all three currently exhibit decreasing block rewards.

Zcash

"zk-SNARK" (zero-knowledge Succinct Non-interactive ARgument of Knowledge) is a type of zero-knowlede proof, first implemented in Zcash, that allows someone to prove possession of a specific piece of

information such as a private key without requiring the person to reveal the information.[58]

Zcash allows for users to send both public and private transactions. Public transactions function similarly to transactions on public blockchain networks. Public transactions involve sending Zcash to a "transparent" address (t-address) where the transaction details can be viewed by others. Private transactions are sent to "shielded" addresses (z-address). Details of transactions sent to shielded addresses such as the involved addresses, amount transacted, and the memo field are not publicly viewable.[59] Private transactions are made possible by the use of zk-SNARKS.

The public transaction feature of Zcash likely provides the coin easier access to regulated exchanges, given that it is tradable on Coinbase, the largest centralized exchange in the United States, while coins such as Monero do not have a public transaction feature and are not listed on the exchange. Another interesting point is that Coinbase users are only allowed to send Zcash transactions to transparent addresses from their Coinbase wallet as the exchange does not currently support the ability to send transactions to shielded addresses.[60]

Monero

All transactions on Monero are private. Monero is structured in a way where each user is anonymous by default, rather than allowing users to opt into privacy for some transactions or not offering this benefit at all.[61] There are three core pieces of technology that enable Monero's private transactions: stealth addresses, ring signatures, and Ring Confidential Transactions ("RingCT").[62]

Stealth addresses are one-time public addresses that a sender must create on behalf of the recipient for each transaction that is initiated

[58]"What Are Zk-Snarks?" *Zcash*, https://z.cash/technology/zksnarks/.

[59]"How It Works." *Zcash*, https://z.cash/technology/.

[60]"Zcash (ZEC)." *Coinbase*, https://help.coinbase.com/en/coinbase/getting-started/crypto-education/zcash-zec-faq.

[61]"What Is Monero (XMR)?" *Monero*, www.getmonero.org/get-started/what-is-monero/.

[62] Ibid.

by using the public view key and public spend key of the recipient.[63] The transaction is published to the blockchain in a way that only identifies the recipient by the generated stealth address. The published information is not helpful to any other network participant viewing the information besides the sender and recipient. The recipient is able to identify that the transaction is theirs by using their private view key.[64] Once the transaction is identified, the recipient can generate a one-time private key to match the one-time public key of the transaction to receive their funds.[65] The use of stealth addresses keeps the recipient's real public address free of association with a transaction and provides anonymity from network users that were not parties in the transaction.

Ring signatures are a type of digital signature in which a group of network participants comes together to create a new, distinctive signature that can be used to authorize a transaction.[66] Transactions can be signed with a ring signature, which means it was performed by a member of the group, but it is impossible to know which person signed the transaction by looking at the ring signature.[67] While ring signatures work to anonymize the sender of a transaction, Ring Confidential Transactions work to anonymize the contents of the transaction including the amount being transacted.[68] The combination of ring signatures and RingCT create transactions on the Monero blockchain where one cannot view either the recipient or the transacted amount, yielding a blockchain for private transactions.

Government agencies have taken notice of these blockchains that seek to offer private, untraceable transactions. In an effort to gain tracing abilities of private transactions, the government has enlisted the help of firms that specialize in the analysis of blockchain data. For example, the Internal Revenue Service offered a

[63]"Moderopedia: Stealth Addresses." *Monero*, https://www.getmonero.org/resources/moneropedia/stealthaddress.html.

[64] Ibid.

[65] Ibid.

[66]"Moderopedia: Ring Signatures." *Monero*, https://www.getmonero.org/resources/moneropedia/ringsignatures.html.

[67] Ibid.

[68]"Moderopedia: Ring CT." *Monero*, https://www.getmonero.org/resources/moneropedia/ringCT.html.

bounty of up to $625,000 to any entity that could trace transactions on Monero and/or those of a few other blockchains.[69]

Security Concerns

The “bearer instrument” aspect of Bitcoin and many other blockchains creates concerns around the management of private keys. The ownership of a private key is effectively the ownership of the assets held by the account. Cryptocurrencies are most commonly stolen from exchanges and individuals through the theft of private keys.

Many exchanges offer custodial services where customers opt for exchanges to take custody of their blockchain-based assets in exchange for a standard username and password to access the exchange-based account. However, exchanges are still vulnerable to private key theft and are often targeted due to their large holdings. Custodial exchanges are also susceptible to social engineering hacks in which bad actors attempt to hijack common multi-factor authentication processes. This can be done in many ways including the contacting of exchanges to impersonate custodial clients and the practice of “SIM-swapping” where a bad actor attempts to have phone-based verification codes of an exchange client sent to a phone in their possession.

Security Solutions

One potential solution to the dangers of using an exchange is the use of a decentralized exchange. Users can execute trades on a decentralized exchange without the underlying exchange gaining custody of their assets. Decentralized exchanges conduct trades as peer-to-peer transactions, rather than having the assets flow through the hands of the exchange.

Other solutions to the dangers of cryptocurrency theft include the offline storage of assets, known as “cold storage.” Assets can be held on specialized hardware wallets not connected to the internet, or even held as printed copies of public and private keys, referred to as a “paper wallet.” Some companies even offer services to store offline cryptocurrency wallets in remote locations such as mountains, islands, and underground bunkers.

---

[69]Erb, Kelly Phillips. “IRS Will Pay up to $625,000 If You Can Crack Monero, Other Privacy Coins.” *Forbes*, 14 Sept. 2020, www.forbes.com/sites/kellyphillipserb/2020/09/14/irs-will-pay-up-to-625000-if-you-can-crack-monero-other-privacy-coins/?sh=19335c1f85cc.

Cold Storage Case Study: Ledger[70]

The market leader in the consumer cold storage market is Ledger. Ledger offers a line of affordable cold storage cryptocurrency wallet products, starting at $59 USD.[71] Ledger products are used by millions of consumers. Ledger wallet products offer a physical tool, resembling a standard flash drive, that allows a user to store their cryptocurrency offline.

Transactions processed from a non-compromised offline wallet requires the user to connect the device and manually approve transactions from the device. In order to use the wallet, a user will need to input the correct pin code for the device. If the wrong pin code is given, the device will reset to factory settings which will erase the private key from the memory of the device.[72] This is where another feature of the device comes into play: the recovery/seed phrase. If someone loses their device, forgets their pin code, or just desires to use another device, the wallet can be accessed with the corresponding 24 word recovery phrase. It is crucial to treat seed phrases with as much or more attention to security as one does to their physical cold storage device. If one loses their recovery phrase, they are at a risk of losing their funds if they proceed to lose their cold storage device.

Adoption Concerns

While offering heightened security, against many attack vectors and common ways of losing funds, user-friendly cold storage wallets can only go so far in addressing blockchain asset security concerns. If someone else gets access to one's seed phrase, the funds of a wallet can be compromised without even accessing the device. We also discussed the issues that can arise if one does not properly manage their device. These remaining concerns largely fall under the umbrella of human behavior and error, which derives from the full responsibility of an individual to bear their assets.

This gives rise to concerns regarding the mass adoption of blockchain technology. The risk in taking full ownership of one's funds, especially for those living in countries with a fairly strong financial system who enjoy benefits such as banks being trusted to hold onto the funds of customers and government insurance programs such

[70] *Ledger*, https://www.ledger.com/.

[71] "Ledger Nano X vs Ledger Nano S plus - Hardware Wallets Comparison." *Ledger*, https://shop.ledger.com/pages/hardware-wallets-comparison.

[72] "Forgot Your Pin Code? – Ledger Support." *Ledger*, 1 Apr. 2022, https://support.ledger.com/hc/en-us/articles/4405737674129-Forgot-your-PIN-code-?support=true.

as the FDIC, can be a daunting hurdle to overcome when deciding to dip one's toe into the world of blockchain technology.

Adoption Solutions

Great strides have been made in recent years to make blockchain technology and cryptocurrency more accessible to newcomers. However, this is still an area of the industry in which much work remains to be done.

User-Friendly Self-Custody Wallet Case Study: MetaMask

MetaMask, used by over 21 million people, is the most popular cryptocurrency wallet in the market[73] The wallet brings a user-friendly interface and experience to a piece of technology that has historically been fairly difficult to use and maintain, especially for those new to the space. While providing this ease of access, MetaMask also enables people to easily maintain the ownership of their private key.

MetaMask is primarily accessed through its browser plug-in and its mobile apps. Users can get a wallet set up in a few minutes through the use of an email account, then creating a password, and finally retrieving a seed phrase that can be used to restore the account on another device.

Thanks to the popularity of the product and its partnerships in the industry, MetaMask has become the standard means of interacting with dApps, which causes for many developers to specifically build to accommodate MetaMask users, furthering the ease of access provided by using MetaMask.

Non-Custodial Adoption Solutions

Other products and services go even further to make cryptocurrency more accessible to newcomers. However, these offerings are often controversial with the blockchain purist crowd. A common saying within the blockchain crowd is: "not your keys, not your crypto." Further developments in making cryptocurrency more accessible beyond the most accessible self-custody solutions require one to give up public-private key ownership of their blockchain-based assets. It is true that giving up custody of one's funds decreases one's control of their assets, but as we have observed from the quick rise in the popularity of centralized exchanges, many people are willing to do so. While controversial in some circles, these offerings have also greatly expanded the adoption and ownership of blockchain-based assets.

[73] *Metamask*, https://metamask.io/.

Many of the most popular cryptocurrency exchanges operate as a centralized exchange. These exchanges provide custodial services for their clients. When using one of these exchanges, users do hold the private key to a wallet holding their assets. However, users can still make transactions with their assets to send them to other blockchain addresses, including those for which the user controls the private keys.

Some of the most popular centralized exchanges have begun offering guarantees of held funds by purchasing insurance for funds held by the exchange in the event of hacks that have been a prominent feature of this industry for many years. However, these insurance policies generally only cover hacks of the funds held by the exchange and not of individual investor accounts[74] which could result in a hacker withdrawing the assets of a client from the custodial exchange. Exchanges work to mitigate the efforts and reward of hackers by holding an overwhelming majority of their funds in cold storage. For example, Coinbase holds 98% of customer funds offline.[75]

ETFs of cryptocurrency assets have started to become approved in countries around the world. The first Bitcoin ETF in Canada was approved in February of 2021 and the first Bitcoin futures ETF in the United States began trading in October 2021. Additionally, there are a number of companies in the blockchain technology and/or cryptocurrency industries or companies that hold cryptocurrency assets which are publicly traded companies. These products offer investment exposure to the space while allowing an investor to operate in their traditional finance zone of comfort and while not requiring the person to self-custody blockchain-based assets.

Volatility Concerns

High volatility is characteristic of cryptocurrencies. Rapid price swings of an asset make it difficult to use as a currency. It is difficult to price goods and services in terms of a highly volatile currency as prices would need to be constantly changed and both customers and merchants might feel reluctant to complete a transaction if the price could quickly move against them. Many Bitcoin users point to the famous purchase of two pizzas in exchange for 10,000 BTC as an example of why not to spend one's bitcoin holdings. Volatility in cryptocurrency markets is heightened by the widespread use of high leverage in trading positions and resulting liquidation events.

[74]"How Is Coinbase Insured?" *Coinbase*, https://help.coinbase.com/en/coinbase/other-topics/legal-policies/how-is-coinbase-insured.

[75]"Security." *Coinbase*, https://www.coinbase.com/security.

Similar to the reluctance of merchants and customers to transact in cryptocurrency, high volatility also increases the difficulty of institutional adoption. Financial institutions accustomed to the relatively low volatility of traditional financial markets may find the volatility of cryptocurrency markets to be too risky of an endeavor.

Volatility Solutions

One increasingly popular option to the volatility of cryptocurrencies is the use of **stablecoins**. Stablecoins are cryptocurrencies of stable value which is often achieved by assigning its value to that of a central bank's currency. The most commonly used stablecoins are pegged to the United States dollar, such as Tether, USDC, GUSD, and BUSD. The reserve currency of cryptocurrency markets has increasingly shifted from Bitcoin to the United States dollar, matching the state of many prominent financial markets around the world.

Another solution to the volatility of cryptocurrencies is the shifting of cryptocurrency use cases that has occurred over the years. When Bitcoin was first created, it was proposed as a peer-to-peer electronic cash transaction network, but in recent years it has increasingly been seen as more of an uncorrelated asset to be used as a store of value. Bitcoin's money function as a unit of exchange has been lessened in favor of its function as a store of value.

Forking Concerns and Solutions

The potential for a fork to happen in most blockchains is quite common. They can simply occur accidentally when multiple blocks are solved at the same time. Blockchains have internal protocols that help to prevent accidental forks and maintain the main chain, such as the GHOST protocol of Ethereum. Some blockchains and their consensus protocols such as Algorand prohibit forks altogether.

However, some forks occur on purpose. Intentional forks can occur for many reasons, such as the creation of an altered or improved chain to better accomplish a purpose or as a revolt against the direction of the original blockchain, known as an "ideological fork." Intentional forks can draw users away from the original blockchain if features of the new blockchain are more appealing.

Governance Concerns and Solutions

The lack of a central decision-making power in a decentralized blockchain creates issues in the governance of the network. In order to function without a central authority, decentralized blockchains use governance protocols which are predetermined

rules as to how improvements and changes to the system are proposed and implemented. Protocol upgrades and other proposed changes need to be voted on by the community of a decentralized blockchain. Network-wide decisions have been known to take a long time and to divide the community. It took roughly two years from the time it was initially proposed for SegWit to be implemented on the Bitcoin blockchain.

Interoperability Concerns and Solutions

Although blockchain protocols such as Ethereum provide a common standard for interoperable applications to be built, blockchains are still their own independent network. Fundamentally, blockchains fall into the same siloed nature of the platforms that we use today. While applications built on the same chain are capable of communicating with each other, applications built on different chains or different blockchains themselves cannot easily cross-communicate.

One solution to the interoperability problem faced by decentralized blockchains is the development of a common protocol for blockchains which will allow for interoperability. The idea expands on the common protocol that many blockchains provide for the applicants built on them. The inter-blockchain communication protocol (IBC) is an example of this solution which provides implementable standards that enable independent blockchains to communicate with each other.

Ethereum 2.0: Ethereum Upgrades

"Ethereum 2.0" is a long-anticipated upgrade of the Ethereum blockchain which will address many scaling challenges currently faced by the current state of the Ethereum blockchain. While originally referred to as Ethereum 2.0, the Ethereum Foundation has phased out the use of Ethereum 1.0 and Ethereum 2.0 in favor of the "execution layer" and the "consensus layer," respectively, which aims to relieve community confusion and scam attempts related to Ethereum 2.0 name.[76] The Ethereum upgrade functions around the "beacon chain" which is the main chain of the upgraded system and functions as a nexus for the network. The beacon chain is currently live and can be explored here.[77]

The upgrade changes the Ethereum consensus protocol from proof of work to proof of stake. In order to assume the role previously occupied by miners of the proof of

[76]Ethereum.org Team. "The Great Renaming: What Happened to eth2?" *Ethereum Foundation Blog*, 24 Jan. 2022, https://blog.ethereum.org/2022/01/24/the-great-eth2-renaming/.

[77]"The Official Etherscan Beacon Chain Ethereum 2.0 Explorer." *BeaconScan*, Etherscan, https://beaconscan.com/.

work system, a user will stake at least 32 ETH to become a “validator.” The beacon chain will randomly pick a validator, weighted by how much ETH each validator has staked, to create and propose a block, rather than it being the first miner to solve the nonce and resulting hash in proof of work. The other validators will attest the block, similar to how the other miners verify the block in a proof of work consensus mechanism. A block will continue if at least 128 validators, referred to as a “committee,” attest to the block. Finally, the beacon chain will accept and finalize the block and issue the block reward to the chosen validator.

Ethereum 2.0 also implements sharding by making shards of the beacon chain. With sharded chains, blocks are mined in parallel by multiple shards. The parallel mining of blocks allows for far greater transaction throughput. Shard chains will also have the ability to store and execute smart contract code.[78] The implementation of proof of stake and sharding greatly improves the scalability of Ethereum. These upgrades seek to scale Ethereum’s throughput capabilities from roughly 20 transactions per second to thousands of transactions per second.[79]

Another guiding purpose of these upgrades is to bolster the security of the Ethereum blockchain. In order to achieve the equivalent of a 51% attack for proof of work blockchain, a bad actor would need to accumulate enough ether to reliably gain enough required spots on the committee to attest to a false block. When practically applied, this would require hundreds of billions of dollars.

Another resulting improvement of forthcoming Ethereum upgrades is a drastic reduction in the use of energy to power the Ethereum blockchain. The upgrades will do away with a very large portion of the estimated 100 TWh consumed by the Ethereum blockchain annually.[80] Additionally, the hardware required for the network to process transactions will be far less than is required under the current proof of work consensus mechanism of the Ethereum blockchain.

Summary

While there are many benefits derived from the unique properties of blockchain technology, there are also many challenges that must be addressed. Data stored on a blockchain is stored indefinitely. A publicly accessible blockchain has an inherent

[78]“Shard Chains.” *Ethereum.org*, 10 May 2022, https://ethereum.org/en/upgrades/shard-chains/.

[79]“Ethereum Upgrades (Formerly 'eth2').” *Ethereum.org*, https://ethereum.org/en/upgrades/.

[80]“Ethereum Energy Consumption Index.” *Digiconomist*, https://digiconomist.net/ethereum-energy-consumption.

tradeoff between lower transaction throughput and a higher degree of centralization. A decentralized blockchain accepts low transaction throughput in exchange for not having a central authority. The “blockchain trilemma” is a belief held by many in the blockchain technology space that blockchains are forced to make tradeoffs between decentralization, scalability, and security to where only two of the three can be achieved by a blockchain at any given time. There are many proposed solutions to scalability issues faced by the blockchains of today, including proof of stake, sharding, and layer 2 solutions.

A high degree of centralization of mining computing power and assets of contemporary blockchains is prevalent. The proof of work system and decentralized computing in general also require a vast amount of computing power and therefore energy consumption. Potential solutions to the energy consumption of blockchains include the use of renewable and/or unused energy and less computationally intensive consensus mechanisms.

The public nature of contemporary blockchains allows for the public viewing of a network participant’s transaction history. The “bearer instrument” aspect of Bitcoin and many other blockchains creates concerns around the management of private keys. The ownership of a private key is effectively the ownership of the assets held by the account.

The novel aspect of blockchain technology and the risks associated with self-custodying one’s assets presents challenges to the mass adoption of blockchain technology. High volatility of blockchain-based assets also increases the difficulty of institutional adoption.

Review Questions

1. Describe a key tradeoff made between a decentralized and centralized blockchain infrastructure.
2. What are the three aspects of the blockchain trilemma for which it is believed that a blockchain must pick two in favor of the other aspect?
3. What is the database management technique of sharding?
4. How do layer 2 solutions help to ease the computational load placed on blockchains?
5. What is one common solution to privacy concerns of pseudonymous blockchains?

6. What is a stablecoin?
7. Which consensus mechanism will the Ethereum blockchain transition to in its forthcoming upgrades?

Chapter 6: A World of Chains

Introduction

While Bitcoin and Ethereum remain as the two most prominent blockchains, many new blockchains have been introduced in recent years. In a way, these chains seek to build upon the foundation created by Ethereum, just as Ethereum built upon the initial foundation created by Bitcoin. Some of these newer blockchains which boast innovative features include Solana, Polygon, and Cardano. However, there are many more blockchains in the industry that power the more than 19,000 unique cryptocurrencies.[81] With many chains available in the market, interoperability has become a feature focus of the blockchain space. Polkadot is one project that is working toward connecting the siloed blockchains of today.

"Ethereum Killers"

Much of Chapter 6 will focus on direct competitors of the Ethereum blockchain. Because Ethereum was the first to establish itself in the turing-complete, smart contract enabled blockchain space and did so with lasting success, new blockchains are often viewed as challengers of Ethereum. The term "**Ethereum killers**" commonly refers to the strongest programmable blockchains of today that offer similar functionality to Ethereum, which are believed to be viable long-term competitors that can amass and maintain meaningful market share in the space.

As you will see, many of these blockchains feature similar structures, even more so when considering where proposed improvements are leading these blockchains. These blockchains are primarily openly competing on the ability to reliably, cheaply, and quickly process transactions as well as the dApps and smart contract functionality these blockchains can offer to users and developers. It is still fairly early in the development of the blockchain space to make a determination as to how many blockchains the space will support with meaningful market share, but it is likely that many of the following blockchains will be around for the foreseeable future.

Solana

Solana, a newer competitor in the blockchain space, seeks to offer a blockchain that solves the main problem facing blockchains today: scalability. The Bitcoin blockchain and Ethereum blockchain currently cannot handle the demand for

[81] *CoinMarketCap*, https://coinmarketcap.com/.

transaction processing from its users, which has led to rampant growth in transaction fees and processing times in recent years. Solana uses proof of stake, the consensus mechanism that Ethereum plans to use as part of its long-anticipated upgrades, as its consensus mechanism. Solana's block time is only 400 milliseconds and transaction fees are a fraction of a penny.[82] The Solana blockchain processes thousands of transactions per second.[83]

Proof of History

The Solana blockchain also uses "**proof of history**" (PoH) in addition to its use of proof of stake to gain even greater scalability. Proof of history was first outlined in a whitepaper, published in November 2017, that was authored by Anatoly Yakovenko, who is also the creator of Solana.[84] Proof of history allows for "timestamping" of information in a blockchain and it allows for the "keeping [of] time between computers that do not trust each other."[85] When nodes can mutually agree on the time of events, they are able to place increased focus on processing transactions, which helps Solana to achieve its competitive advantage of transaction speed.

Criticisms

While offering improvements against its competitors, which has helped to cement itself in the pack of prominent contemporary blockchains, Solana does not come without its criticisms. The most common criticism of Solana is its lack of decentralization relative to competing blockchains. The previously discussed blockchain trilemma (where a blockchain can choose two attributes to possess between scalability, security, and decentralization) highlights this point. All prominent blockchains elect for security, so therefore Solana's election to focus on scalability causes it to diminish focus on decentralization. While the Bitcoin blockchain has over 14,000 reachable nodes[86] and the Ethereum blockchain has over 6,000 nodes,[87] Solana has around 1500 validator nodes.[88] It remains a topic of conversation in the blockchain space as to whether Solana is sufficiently decentralized or not.

---

[82] *Solana*, https://solana.com/.

[83] Ibid.

[84] "History." *Solana Documentation*, https://docs.solana.com/history.

[85] Ibid.

[86] "Reachable Bitcoin Nodes." *Bitnodes*, https://bitnodes.io/.

[87] "Ethereum Mainnet Statistics." *Ethernodes.org*, https://ethernodes.org/.

[88] *Solana*, https://solana.com/.

On its fast path to its current place in the center of the blockchain space, Solana has experienced many network-wide outages, with some lasting nearly a full day. During these outages, users were commonly unable to conduct any transactions. Critics also focus on these outages, with some relating it to the lack of decentralization compared to its competition, and point out the lack of network-wide outages experienced by competing blockchains such as Ethereum. Another common criticism of Solana is its concentrated token ownership. Less than 2% of Solana addresses control more than 98% of the SOL token (Solana's native token) circulating supply.[89] Although Solana has faced its share of challenges during its quick climb to the highest tier of contemporary blockchains, the Solana ecosystem has drawn in many users and is poised to be a strong competitor in the space for the foreseeable future.

Polygon

Polygon is another network looking to solve scalability issues currently facing the industry. In particular, Polygon is working to address the scalability of the Ethereum blockchain, for which its users have been eagerly awaiting the delayed Ethereum upgrades. Polygon is a layer 2 scaling platform for the Ethereum blockchain.[90] Polygon uses much of the same technology as the Ethereum blockchain, but it also makes its own improvements as well such as using proof of stake as its consensus mechanism.

No Need to Reinvent the Wheel

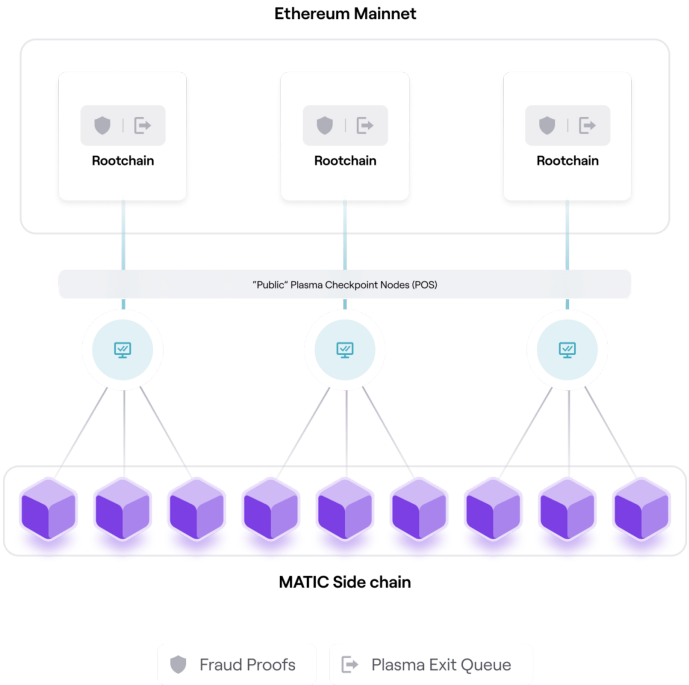
Unlike many other blockchains described in this chapter, Polygon does not seek to overthrow the Ethereum blockchain. Instead, it works to provide greater scalability to the Ethereum ecosystem by providing fast, low cost transactions and a familiar place for developers to build their dApps. Polygon is built to be compatible with the Ethereum Virtual Machine, meaning that smart contracts created for the Ethereum blockchain and its protocol are also able to be used on Polygon. This allows for a seamless transition of dApps from Ethereum to Polygon and has contributed to the rise in use of the network. The EVM-compatible nature of Polygon allows for a similar user experience to the Ethereum blockchain. Users of the Polygon network can use their same Ethereum address. For the popular MetaMask wallet, users can get their Ethereum wallet set up for Polygon in a few clicks.[91] Users can easily move many of their Ethereum-based

[89]"Network Supply." *Solana Beach*, https://solanabeach.io/supply.

[90]*Polygon*, https://polygon.technology/.

[91]"Add Polygon Network." *Polygon | Documentation*, https://docs.polygon.technology/docs/develop/metamask/config-polygon-on-metamask/.

assets to Polygon by using a **bridge**. A bridge is the pathway through which users can move their blockchain assets across blockchains.



The ease of use for users, many coming from the practically identical Ethereum blockchain, has contributed to the meteoric rise of Polygon. The network has processed over one billion transactions, has seen over 100 million unique wallets, hosts millions of monthly active users, and has over 7,000 dApps using its technology.[92]

Using Proof of Stake

Polygon's major improvement on the current technology of the Ethereum blockchain is its use of proof of stake. Polygon has over 13,000 **delegators**[93], which are network participants who are staking the network's native MATIC token with the more than 100 active **validators**[94], which are the nodes verifying the transaction under proof of stake consensus.[95] Validators receive the block reward and the non-burned

[92]"About Us." *Polygon*, https://polygon.technology/about/.

[93]"Who Is a Delegator." *Polygon* | *Documentation*, https://docs.polygon.technology/docs/maintain/polygon-basics/who-is-delegator.

[94]"Who is a Validator." *Polygon* | *Documentation*, https://docs.polygon.technology/docs/maintain/polygon-basics/who-is-validator.

[95]*Polygon*, https://polygon.technology/.

transaction fees (Polygon also has implemented EIP-1559) and give an agreed-upon "commission" to the delegator for their staked funds.[96] Proof of stake also drastically reduces the required hardware and electricity resources needed to power the network, compared to contemporary proof of work blockchains. While many of the largest proof of work blockchains consume about 35-140 TWh of electricity per year, Polygon only consumes about 0.00079TWh per year to power its network.[97]

Proof of stake, along with Polygon's other features, allow it to process thousands of transactions per second at its peak, with an average block time of around 2 seconds.[98] Transactions fees are only a fraction of a cent.

Polygon provides an insight into what we can expect of the Ethereum blockchain once the long anticipated upgrades occur. However, Polygon's improvements on the proof of work state of the Ethereum blockchain are only a piece of the many technological improvements coming to Ethereum.

Criticisms

Polygon's quick rise in popularity has caused immense growing pains for the network. Resemblant of the Ethereum blockchain since late 2017, Polygon has faced congestion issues as it experienced massive growth in transaction volume over a short period of time. This has led to network-wide outages, similar to those described above regarding Solana, that has caused network and bridge transactions to stall for hours or even days at certain times.

Another criticism derives from how similar and attached Polygon is to Ethereum: What does polygon do if Ethereum upgrades live up to the expectations? The proposed Ethereum upgrades include most of the distinguishing features of the current state of Polygon, plus much more such as sharding which carries immense scalability power on its own. However, many argue that there will always be a place in the ecosystem for scaling solutions. Polygon can continue to provide congestion relief for the main Ethereum chain and also serve as a place for new technologies to be implemented with testable volume before they are added to the Ethereum blockchain.

---

[96]"Rewards." *Polygon* | *Documentation*, https://docs.polygon.technology/docs/maintain/validator/rewards.

[97]Polygon Team. "The Eco-Friendly Blockchain Scaling Ethereum." *Polygon*, 28 Apr. 2021, https://blog.polygon.technology/polygon-the-eco-friendly-blockchain-scaling-ethereum-bbdd52201ad/.

[98]"Polygon PoS Chain Average Block Time Chart." *Polygonscan*, https://polygonscan.com/chart/blocktime.

Cardano

Cardano was created by Charles Hoskinson, who was also an early co-founder of Ethereum. Cardano was launched via an initial coin offering (discussed in the next chapter) in 2017 and since then the project has steadily maintained a high position in the blockchain/cryptocurrency space. Cardano is known to have one of the most devoted followings in the whole industry.

Branching Out From Ethereum

Given that Charles Hoskinson worked closely with Vitalik Buterin during the early days of the Ethereum blockchain, it is no surprise that Cardano is quite similar to Ethereum. The core of both blockchains is a turing-complete system for running smart contracts and developing decentralized applications that can run on the respective protocols.[99]

However, Cardano does possess distinguishing features that has allowed it to compete with the biggest blockchains of today. The biggest difference between Cardano and Ethereum is its consensus mechanism. While Ethereum still uses proof of work as its consensus mechanism (with plans to transition to proof stake with its upcoming upgrades), Cardano has used proof of stake since its launch in 2017.[100] Cardano also places heavy emphasis on research-based innovation and strategic partnerships.

Core Concepts

Cardano focuses on three core concepts that its team has identified as the most important for project success: scalability, interoperability, and sustainability.[101] As we continue to discuss contemporary blockchains, their unique aspects, and their challenges, it becomes clear that scalability is a primary focus of today's blockchains. Furthermore, this focus will likely not be going away anytime soon. For blockchains to live up to their potential, scalability needs to be unlocked so that ultimately tens of thousands of transactions can be reliably processed in a very short period of time. In addition to its proof of stake consensus mechanism, Cardano is implementing techniques such as data compression and multiple side chain functionality to achieve a higher level of throughput capability.[102]

---

[99]"Cardano vs Ethereum." *Kraken*, www.kraken.com/en-us/compare/cardano-vs-ethereum.

[100]"Proof of Stake." *Why Cardano*, https://why.cardano.org/en/introduction/proof-of-stake/.

[101]"Why use Cardano?" *Cardano Docs*, https://docs.cardano.org/new-to-cardano/why-use-cardano.

[102] Ibid.

While many blockchains are rapidly improving within their own ecosystems, much work remains to be done to enable the nodes of the many existing blockchains to communicate with each other and conduct cross-chain transactions. Cardano is developing its technology to support cross-chain transactions, multiple token types, and standard smart contract language and protocols of the blockchain space.[103]

The final core concept of Cardano is sustainability. Rather than the environmentally-concerned sustainability, which we already have described with the low electricity and hardware resource needs of the network, Cardano's core concept of sustainability refers to the ability of the network to be a long-term player in the space by becoming a self-sustainable ecosystem. Cardano primarily approaches this goal in a similar fashion to Ethereum's approach, which uses the Ethereum Improvement Proposals that we previously discussed, by allowing community members to propose and ultimately decide to implement improvements.[104] Cardano also has an established treasury that is controlled by the community. The community can elect to spend treasury funds on chosen proposals and the treasury fund is replenished by a share of network transaction fees and a share of new tokens issued.[105]

Criticisms

One common criticism of Cardano, and the other smart-contract enabled blockchains discussed in this chapter, is its future prospects if the Ethereum upgrades work as promised. It is still not clear as to how many blockchains the space will support with meaningful market share. While these Ethereum competitors currently offer scalability in a time when the Ethereum blockchain is overloaded with volume, it is unclear if decentralized applications and users will continue to operate on other chains once they can reliably perform fast and cheap transactions on the Ethereum mainnet.

Another criticism of Cardano is the slow nature of its rigorous academic approach. Compared to other competing blockchains, the process of innovation in the Cardano ecosystem is a more onerous task that churns out improvements more slowly. However, this time consuming process provides unique benefits as well such as more thorough/scientifically studied proposals and implemented improvements.

---

[103] Ibid.

[104] Ibid.

[105]"Cardano monetary policy." *Cardano Docs*, https://docs.cardano.org/explore-cardano/monetary-policy.

Polkadot

While the introduction of many new chains to the market has expanded options for users and pushed forward technological advancement, having many separate blockchains creates another problem. The nodes of a given modern-day blockchain are very good at communicating with each other, but nodes of different blockchains are not properly equipped to communicate with each other and handle cross-chain transactions. Solutions such as bridges and EVM-compatibility offer some relief for layer 2 chains and their layer 1 counterparts, but these solutions allow for nowhere near the end state of blockchain technology that can be achieved if all nodes of all blockchains are able to communicate with each other.

Polkadot, founded by Gavin Wood who was a co-founder and CTO of Ethereum (hopefully you are starting to see a trend here), aims to solve the lack of interoperability possessed by the siloed blockchains of today.

Polkadot: The "Layer 0"

We have already discussed the concept of blockchains serving as a "layer 1" with scaling solutions built "on top" of them as a secondary layer. Along the same lines, Polkadot is positioned to serve as a "layer 0" where layer 1 blockchains can connect and communicate with each other. Polkadot provides a central, standardized place for communication between chains which allows for the successful cross-chain transfer of information. Polkadot's approach allows for connection between "private and consortium chains, public and permissionless networks, oracles, and future technologies that are yet to be created."[106]

The Infrastructure[107]

The Relay Chain lies at the center of Polkadot. The function of Relay Chain is fairly similar to that of Ethereum's Beacon Chain which will be the heart of Ethereum once the planned upgrades occur. The Relay Chain is the base level of communication on the Polkadot network where information is transferred between independent blockchains connected to the Polkadot network.

---

[106]"About Polkadot, A Platform for Web3." *Polkadot*, https://polkadot.network/about/.

[107]"Technology: A Scalable, Interoperable & Secure Network Protocol for the Next Web." *Polkadot*, https://polkadot.network/technology/.

Connected to the Relay Chain are parachains, which are sharded, independent blockchains.[108] These sovereign blockchains can be optimized to fit the needs of its use case and network participants.[109] The sharded state of parachains allow for all transactions to be processed in parallel rather than sequentially, which provides increased scalability.[110] Parachains can pass along information through the Relay Chain if one parachain needs to communicate with another. The Cross-Consensus Messaging Format is a format for communicating via the Relay Chain which provides that messages sent between parachains can be understood by all parties.[111]

Parachain slot leases are auctioned on-chain to blockchain projects. In winning an auction for a parachain slot, the winning project locks up ("bonds") an amount of DOT tokens which is the native token of the Polkadot network.[112] Once the parachain lease ends, the DOT tokens become unlocked. A common approach for parachain auctions is the crowdfunding of DOT tokens by blockchain project supporters, which causes for community support of a project to be a vital piece of a successful parachain auction campaign.[113] Previous auctions have required millions of DOT committed to be locked up in order to win an available parachain slot.[114]

With DOT largely trading above $10 since January of 2021[115], this can be a rather large commitment of funds for new projects and can present a barrier to entry for projects with smaller communities. Parathreads present an opportunity for smaller projects that cannot compete in auctions against larger projects to access the benefits of Polkadot. Parathreads are sharded pieces of a parachain slot that allows projects to

[108]"Getting Started." *Polkadot*, https://wiki.polkadot.network/docs/getting-started.

[109]"Technology: A Scalable, Interoperable & Secure Network Protocol for the Next Web." *Polkadot*, https://polkadot.network/technology/.

[110]"Getting Started." *Polkadot*, https://wiki.polkadot.network/docs/getting-started.

[111]"Cross-Consensus Message Format (XCM)." *Polkadot*, https://wiki.polkadot.network/docs/learn-crosschain.

[112]"Parachain Slot Auctions." *Polkadot*, https://polkadot.network/auctions/.

[113]Ibid.

[114]"Making History, Again: Polkadot Auctions 1-5." *Polkadot*, https://polkadot.network/blog/making-history-again-polkadot-auctions-1-5/.

[115]"Polkadot." *CoinMarketCap*, https://coinmarketcap.com/currencies/polkadot-new/.

use the Polkadot network without needing a full parachain slot. Parathreads can be leased on a short term basis under a “pay-as-you-go” model.[116]

Bridges of the Polkadot network exist to connect external networks with parachains, which ultimately enables multiple connected, external networks to communicate with each other via the Relay Chain.[117]

*For more information on how the technology of the Polkadot network comes together to create a blockchain interoperability platform: you can view this video created by the organization.[118]

Consensus

The consensus mechanism of the Polkadot network is “nominated proof of stake.” Nominated proof of stake is a form of proof of stake consensus where token holders select a validator to represent their token ownership.[119] All network participants that own DOT tokens can participate in consensus as nominators. Nominators “bond” their staked DOT tokens to a selected validator to represent their DOT ownership share in the proof of stake consensus mechanism.[120] Nominators receive a portion of the rewards gained by their selected validator.

Validators of the Polkadot network take on the traditional validator role that we previously discussed with the Ethereum upgrades. Validators produce blocks on the Relay Chain when selected by the protocol.[121] Validators can gain increased weight in the validator pool by having increased support from nominators.

Due to the sharded aspect of the Polkadot network and the presence of multiple independent blockchains via parachains, there are a few additional actors needed to reach consensus and hold order on the network. Collators are network participants that run a full node on both a parachain and the Relay Chain. Collators collect transactions on a parachain and pass along proof of the parachain’s state to validators of the Relay

---

[116]“Technology: A Scalable, Interoperable & Secure Network Protocol for the Next Web.” *Polkadot*, https://polkadot.network/technology/.

[117]Ibid.

[118]“Polkadot: Are You Ready to Start Building?” *YouTube*, uploaded by Polkadot, 15 July 2020, https://www.youtube.com/watch?v=_-k0xkooSlA.

[119]“Polkadot Consensus: Nominated Proof of Stake.” *Polkadot*, https://wiki.polkadot.network/docs/learn-consensus#nominated-proof-of-stake.

[120]“Architecture.” *Polkadot*, https://wiki.polkadot.network/docs/learn-architecture.

[121]Ibid.

Chain.[122] Because all collators run a full node on the Relay Chain in addition to their respective parachains, collators can communicate with one another and can therefore facilitate cross-parachain communication.[123]

Summary

While Bitcoin and Ethereum remain as the two most prominent blockchains, many new blockchains have been introduced in recent years. Some of these newer blockchains which boast innovative features include Solana, Polygon, and Cardano. Solana implements proof of history and proof of stake to achieve high throughput, while having fast transaction times and cheap transaction fees. Polygon is working to address the scalability of the Ethereum blockchain, given it functions as a layer 2 scaling platform for the Ethereum blockchain. Polygon uses similar technology to that of Ethereum, which allows for the easy development and deployment of Ethereum-based applications on Polygon, while also implementing scalability improvements such as proof of stake. Cardano also makes use of proof of stake. Cardano also implements techniques such as data compression and multiple side chain functionality to achieve a higher level of throughput capability and compete in the contentious programmable blockchain space.

While the introduction of many new chains to the market has expanded options for users and pushed forward technological advancement, having many separate blockchains creates another problem. Polkadot aims to solve the lack of interoperability possessed by the siloed blockchains of today. Polkadot is positioned to serve as a “layer 0” where layer 1 blockchains can connect and communicate with each other.

Review Questions

1. What does the term “Ethereum killer” refer to?
2. What does proof of history allow a blockchain to do with stored information?
3. Which blockchain does Polygon primarily serve as a scaling solution for?
4. Describe one technology implemented on Cardano that contributes to its scalability efforts.
5. How is Polkadot positioned to add value to the blockchain technology industry?

[122]“Collator.” *Polkadot*, https://wiki.polkadot.network/docs/learn-collator.

[123]Ibid.

Chapter 7: Cryptocurrency and Initial Coin Offerings (ICOs)

Coins and Tokens

A **coin** is the native asset of a blockchain. We have already discussed the two most prominent coins in the blockchain space: bitcoin and ether. A **token** is similar to a coin, but it is not the native asset of a blockchain. Instead, tokens are built on an existing blockchain and are often a central component of a decentralized application. Both coins and tokens are commonly referred to as "cryptocurrencies."

Original Purpose of Coins

Coins primarily exist to power a blockchain by fulfilling two purposes: to reward the maintenance and/or securing of the network by providing computing power and to denominate transactions and the fees paid for transacting and computing on the network. Coins and their value incentivize network participants to participate in the proof of work system and provide a medium for exchange on the network. Bitcoin perfectly describes this theory of coin utility. Participants in the proof of work consensus mechanism are rewarded with bitcoins for securing the network. Users can transact over the network with bitcoins, denominating a particular value sent in the transaction. Additionally, users offer a transaction fee, paid in bitcoin, to the miners for processing and prioritizing their transaction.

Token Utilities

The creation of blockchain protocols, in which decentralized applications could be built, expanded the range of potential use cases for blockchain-based assets. In addition to serving as a medium of transaction ("money"), the four main categories of token utilities (and expanded use cases of coins) are:

> *Incentivized participation in the blockchain network or decentralized application:*
>
> This first utility has been around since the inception of blockchain technology. The Bitcoin blockchain is a prime example of how a coin can be used to incentivize participation in a blockchain network. By contributing one's computational power, good faith, and resource expenditure to the network, miners are rewarded with the blockchain's native coin.

Tokens can also be used to reward participation in a decentralized application. Compound, a decentralized application for the borrowing and lending of cryptocurrencies, distributes 2,880 COMP tokens[124] (its native token which also acts as the governance token (see below)) to users of the protocol. This daily distribution encourages users to join and continue participating.

Required ownership and/or redemption of a token/coin to use a service or to participate in the network:

Another utility for tokens is the use of a token to gain access to a service or to participate in a network. We have already covered a service which requires the use of a token in our discussion of Chainlink. Users of Chainlink oracle data feeds pay for this service with the native token: LINK. The consistent demand for these data feeds have built an economy for the LINK token that features a market capitalization in the billions of dollars.[125] The forthcoming Ethereum upgrades feature a similar added utility for ether. Network participants wanting to become a validator and receive rewards must put forth at least 32 ether, which provides further reason for network participants to obtain and hold ether.

Jumpstart a network/decentralized application with development funding:

The ICO craze (discussed below) featured many tokens that were released with the primary intention of providing funds for network/application development. As we will soon see, blockchain technology provides many benefits for new projects, chiefly among them is the relatively simple method to raise funding.

Governance decision-making on protocol upgrades/changes:

Tokens can also be used to distribute governance power between participants. The native token (MKR) of the previously discussed MakerDAO is a prime example of a token that features governance utility. MKR token ownership allows a person to gain voting rights in decisions regarding Maker Protocol parameters such as stability fees and allowed collateral types/rates.

---

[124]Dale, Brady. “Compound Changes Comp Distribution Rules Following 'Yield Farming' Frenzy.” *CoinDesk*, 30 June 2020, www.coindesk.com/tech/2020/06/30/compound-changes-comp-distribution-rules-following-yield-farming-frenzy/.

[125]“Chainlink.” *CoinMarketCap*, https://coinmarketcap.com/currencies/chainlink/.

Decentralized Exchanges (DEXs, to be discussed later in this text) commonly have a native governance token. Compared to centralized cryptocurrency exchanges which are governed by a central entity, decentralized exchanges are directed by protocols which are maintained by a vote of its users which is commonly measured by governance token ownership. Similar to MakerDAO, the governance token owners of DEXs can vote on changes to the underlying protocol to make decisions such as which chains/tokens are supported by the exchange, trading fee structures, and payouts to governance token owners.

Tokenomics

"Tokenomics" is an emerging field that studies the economics of cryptocurrency coins and tokens. Just as in the regular economics that we're all familiar with, the field fundamentally looks at the supply and demand of cryptocurrencies. There are three main pillars of tokenomics: what gives a token value, what value does the token have, and how a token's value is sustainable.

What Gives A Token Value

The value of a token is derived from its utility. While the list above provides common utilities assigned to tokens, the possibilities for valuable token utility are boundless. Multiple utilities can be used with one token, which would further give the token value in the hands of users. Alternatively, different utilities within an ecosystem can be spread out across multiple tokens to create a dynamic, multi-currency economy.

It is from the utility of a token that user demand is derived. In the following sections, we will observe how the utility-determined demand for a token, when paired with its supply, plays a role in the determination of a "real-world" value for the token and how a token is made sustainable for the long-term.

What Value Does A Token Have

This pillar is fairly similar to the one above. The main distinction between the two pillars is that the prior one is concerned with how the utility of the token creates any value for the token and this pillar is concerned with how much the token is actually worth (how much someone is willing to pay for the token with another currency).

This pillar is generally the easiest of the three to view a measurement for. One can simply look at an exchange where the token is traded with any meaningful volume (or one can turn to a Chainlink oracle market price data feed if so inclined) to discover how much people are willing to pay. You can then perform calculations with the

circulating supply of tokens and the fully diluted token supply to achieve a current market capitalization and a fully diluted market capitalization for the token, respectively.

Once the current price is established, you can turn to the information of the other two pillars to decide if the current price of the token is undervalued, fairly valued, or overvalued. This process is similar (depending on the token) to how one might value companies that are traded on a stock exchange. Alternatively for newly introduced coins, one might have to conduct internal modeling by using the information gained from the other two pillars of tokenomics to arrive at a valuation. This process is quite similar (depending on the token) to how one might go about assigning a value to a private company with no public exchange for its shares.

Just as with traditional assets, it is important to include liquidity considerations when looking at the value of a token. Without sufficient liquidity (the ease with which an asset can be converted into another asset without affecting the asset's market price), the stated market price of a token could be wildly different from its true value if sizable transaction volume is to follow.

How Is A Token's Value Sustainable

The final pillar of Tokenomics is concerned with how a token retains its value once its utility is established and the market assigns it a real-world value. Actions taken with regard to keeping a token's value sustainable address the long-term demand and/or long-term supply of the token.

Just as with the stock of companies, one critical action to maintaining the long-term value of a token is by maintaining a sustainable competitive advantage of the blockchain/platform it is used on. Sustainable competitive advantage fundamentally concerns itself with how the entity will maintain its unique and valuable offering for the market which is distinct from what competitors can offer. If there are 20 dApps all offering the same service to users with no plans or ability to break away from the pack, it can be hard to find a reason to justify why the token of the 13th dApp will retain value. This point is even more important of a consideration when concerned with blockchain-based applications because of the ability to easily fork public smart contract code. With a sustainable competitive advantage, users can be more confident in their continued demand for a token, which will help to support the token's long-term value.

Actions can, and should, also be taken on the supply-side of a token/coin to provide greater sustainability of its long-term value. While the tokenomics information of many projects focus on initial coin/token allotment and circulating supply curves, tokenomics and even just the supply-side of tokenomics is much deeper of a topic. One

of the biggest supply-side topics to address is coin/token circulating supply and inflation. Projects commonly address these issues with actions such as protocol-determined supply caps and distribution schedules, lock-up periods, and burning mechanisms.

Ever since the introduction of Bitcoin, protocol-determined supply caps and deflationary mechanisms of distribution have been a main focus of tokenomics. The Bitcoin protocol requires that there will only be 21 million tokens, with a deflationary schedule for the issuance of new bitcoins due to the decreasing block reward over time. With both a maximum supply and decreasing issuance over time, these mechanisms of the Bitcoin protocol set up strong supply-side forces to support long-term value.

Further actions can be taken to address the supply of a token which will help to support the token's long term value. One popular action is having determined "lock-up" periods for tokens. Lock up periods are commonly placed on the funds of early investors who receive a large portion of the network's tokens to mitigate mass-selling concerns. Lock-up periods are also commonly used in the funds received for "staking." Token lock-ups function similarly to the vesting of shares in traditional companies.

Burning mechanisms are also a common measure taken to balance the supply of a coin/token. The previously discussed EIP-1559 which instituted a burn of base transaction fees. Deflationary supply measures can help to promote long-term token value.

Initial Coin Offering (ICO)

An "**Initial Coin Offering**" (ICO) is a common practice where coins or tokens of a new network or decentralized application are first made publicly available for purchase. The Initial Coin Offering term is derived from the term "Initial Public Offering" (IPO) used in stock markets. Initial Coin Offerings, relative to comparables such as Initial Public Offerings, are a quick way to raise initial funding for a blockchain-based project and to help get the project's name in the market.

The ICO Process

A company with a new platform or decentralized application looking to hold an ICO will follow a process similar to the following common steps that have been observed in the newly released projects of recent years.

Whitepaper

Ever since Satoshi Nakamoto's public release of Bitcoin which was accompanied by a whitepaper, most new projects in the blockchain space continue to announce their offering with an accompanying whitepaper. The new project's team will create and publish the whitepaper: a document outlining the idea, tech, and team behind the network or decentralized application. This is where people will get most of the information regarding the project. Whitepapers vary greatly in length and detail, ranging from the eight pages of content in the Bitcoin whitepaper to over one hundred pages for other projects.

Community Building

The project's team will begin building a community to support the project. The team will identify and attract interested potential users and investors. It is extremely helpful to have your target user identified at this step in the ICO process. Early, dedicated community members can help to get the word out about the project and attract additional interested parties. Platforms such as Telegram and Discord are two of the most preferred gathering places for blockchain project community members.

Promotion

While continuing to build the community, the team will put forth concentrated marketing efforts to attract additional interested parties. The team will highlight important pieces of the technology, any recent developments in the project, and upcoming dates in the ICO process.

Pre-sale

Many companies hosting an ICO will opt to have a private, pre-sale open to large investors. Coins/tokens will typically be offered in large quantities at a discounted rate. Pre-sales help to gain community commitment early on in the lifetime of a project and serve as a way to reward early investors with greater asset appreciation if the coin/token performs well over time. Funds will be used to continue development and to serve as social proof to future ICO investors.

SAFT

Derived from the venture capital term "SAFE" (simple agreement for future equity), "SAFTs" (simple agreement for future tokens) became increasingly popular as the ICO scene continued to evolve. A SAFT provides an investment vehicle for venture investors that is similar to what they use in other investments. With a SAFT, a venture

investor gives an agreed upon sum of money to the project in exchange for a future apportionment of the coin or token that is being sold.

Whitelist Approved Participants

Projects that opt to forego a public sale due to regulatory reasons, along with many other potential reasons such as rewarding long-time community members, will often create a "whitelist" of approved participants who are the only ones allowed to participate in the sale. Smart contracts can be used to host an automated coin/token sale for only pre-approved investors in the event that the company wanted to only sell to accredited investors and/or require verifications based upon KYC (know your customer) and AML (anti-money laundering) regulations.

Exchange Listing

Once the ICO is completed or nearing completion, the team will look to get the coin/token listed on popular cryptocurrency exchanges to provide liquidity for initial investors and to increase accessibility to your token for new users of your network or decentralized application. The cryptocurrency market often places heavy weight on a project's ability to get listed on popular exchanges in its valuation of a project and its coin/token. This phenomenon is so prevalent in the cryptocurrency space that a name has been given price impact caused by a listing on Coinbase (a popular cryptocurrency trading app): the "Coinbase effect." Research regarding the Coinbase effect has shown that a listing on Coinbase is often immediately followed by an abnormal, quick price increase. With one sample, the average return on coins/tokens within five days of being listed on Coinbase was 91%.

ICO Benefits

The ICO model presents many benefits to the development team of new networks and decentralized applications. Coin and token sales are typically non-dilutive of company equity as coins and tokens are generally not tied to the ownership of the underlying company. ICOs allow new companies to raise meaningful capital without giving up ownership in the company. Along the same lines, ICOs give companies access to capital without the need to take on debt.

For a long time, ICOs have been "democratic" offerings, meaning that the offering was available to both accredited and non-accredited investors. This feature allowed companies to raise capital from a far larger audience of potential "investors," as well as avoiding the scrutinizing regulation of early-stage investing for the most part. ICOs also enable companies to raise capital in a fast manner, compared to the slower options of private equity/venture capital funding and stock market registration. An example of the

speed at which ICOs can raise capital is Brave which sold $35 million worth of its token, Basic Attention Token, in only 24 seconds.

The Token Network Effect

Perhaps the most important benefit to ICOs is the subsidizing of early adopters by providing a financial incentive. This benefit is referred to as the "token network effect" where users and creators are aligned in their desire for the network to grow in adoption and value. By having an asset in the hands of users that can increase in value as the network grows, users are incentivized to help.

ICO Challenges

While the ICO model presents many potential benefits for companies looking to raise capital, it also presents unique challenges to successfully funding the project. The first hurdle for a company to overcome in an ICO is to establish and maintain demand for the coin/token. If there is not adequate demand for the coin/token and its network/decentralized application, the company's ICO endeavor will almost certainly fail.

Although the ICO process is typically seen as faster than traditional funding alternatives, the process still places a heavy burden on the project's entire team. Successful ICOs require a team-wide effort, compared to traditional funding methods requiring mostly the work of the company's founders and executives. Questions concerning all aspects of the project can come in from potential investors all over the world, requiring the supportive, specialized effort of all team members.

The blockchain-based aspect of companies looking to raise capital via ICO causes difficulty in the implementation of modifications. While traditional startups are able to quickly pivot, companies that just completed an ICO based upon one direction for the network/decentralized application will struggle or be unable to change the direction of the project. Due to the open source-nature of decentralized blockchains, bugs in the publicly viewable code of the project can be exploited to create vulnerabilities by bad actors.

As the ICO space grew over time, governmental regulation became a greater overbearing force. Nowadays, projects are required, and severely punished if they fail to comply, to follow strict regulation. KYC (know your customer) and AML (anti-money laundering) checks must be made on ICO participants and many ICOs are now restricted to only accredited investors. Some projects elect to exclude residents of highly regulated jurisdictions such as the United States altogether.

The ICO process and blockchain-based aspect of these companies provide a tight window of how transparent about the features and functions of its project a company can be in its whitepaper and subsequent promotion. While companies must provide potential investors enough information to gain their trust, companies must also be wary about exposing their intellectual property to potential "copycat" companies. Even if intellectual property theft is staved off during the ICO process, the likely open-source nature of its software allows for anyone to easily fork the technology.

Finally, the relatively new and unique ICO model provides uncertainty for prospective venture capitalists. Venture capitalists can find the valuation of blockchain companies with a native asset in addition to company equity to be difficult. There can also be confusion surrounding whether the venture capitalist should receive the coin/token, equity in the underlying company, or some mixture of both in exchange for their investment. There is also not a universal understanding of how investors can participate in later rounds of funding, or if there will ever be another round after an ICO is completed. The legalities surrounding blockchain-based companies and ICOs are still being developed and can experience rapid change. With a native asset of the project floating around in an already new and not well understood business model, acquisitions of companies that held an ICO and maintain a native coin/token become more difficult.

ICO History

The first prominent Initial Coin Offering was held for the Ethereum blockchain in 2014. Ether was sold at a price of roughly 30 cents per coin, paid in bitcoin. By the end of the sale, Ethereum had raised more than $15 million.

ICOs exploded in popularity in 2017. Prior to the year, it is estimated that less than $300 million dollars had ever been raised through Initial Coin Offerings. In 2017 alone, the amount raised through ICOs is estimated to have been $10 billion and 2018 set a new record of an estimated $11.4 billion raised via ICOs, with a majority coming at the beginning of the year.[126] The largest ICO ever, which heavily contributed to the overall ICO funding figures of 2017 and 2018, was the block.one ICO of its EOS token. By the completion of the ICO, block.one had raised over $4 billion.

[126]Pozzi, Daniele. "Ico Market 2018 vs 2017: Trends, Capitalization, Localization, Industries, Success Rate." *Cointelegraph*, 5 Jan. 2019, https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate.

Crypto Gone Wild: Bitconnect

While many legitimate companies were able to fund promising networks and decentralized applications through ICOs, the allure of fast, substantial capital with minimal regulation also drew the attention of scam projects. One of the most infamous cryptocurrency scams was bitconnect. Bitconnect was a ponzi scheme cryptocurrency platform released in 2016. The project featured an anonymous team (at the time) and overt marketing strategies that highlighted its ponzi scheme-like features. At its peak the Bitconnect coin peaked at a market capitalization of nearly $3 billion.[127]

Bitconnect quickly collapsed at the beginning of 2018 as government entities began to take notice of the platform. Soon after, the anonymous team ran off with the funds of users. For years not much new information was released regarding this story, leaving many to believe that the funds were lost forever to the unknown perpetrators. In September 2021, the Securities and Exchange Commission charged Satish Kambhani, an Indian national and the exposed founder of Bitconnect, and others involved with orchestrating a ponzi scheme.[128] In February 2022, a federal grand jury in San Diego indicted Satish Kumbhani for orchestrating a global ponzi scheme that saw $2.4 billion taken from investors.[129] Satish Kumbhani, has since disappeared and is suspected by the SEC to be hiding in another country.[130] After years of a cold trail, these recent developments show signs of the Bitconnect saga having a few more acts for us before the curtain calls.

ICO Regulation

With the bypassing of intended regulations by many early ICOs and the increased occurrence of scams conducted via ICO, regulatory interest quickly found its way into the blockchain space. We will focus mainly on the regulation of ICOs and cryptocurrencies in the United States.

---

[127]"BitConnect." *CoinMarketCap*, https://coinmarketcap.com/currencies/bitconnect/.

[128]United States District Court, Southern District of New York. *Securities and Exchange Commission v. BitConnect*. https://www.sec.gov/litigation/complaints/2021/comp-pr2021-172.pdf.

[129]"BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme." *The United States Department of Justice*, 25 Feb. 2022, https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.

[130]"BitConnect's Indicted Founder Satish Kumbhani Has Disappeared, SEC Says." *The Economic Times*, The Times of India, 1 Mar. 2022, https://economictimes.indiatimes.com/tech/technology/bitconnects-indicted-founder-satish-kumbhani-has-disappeared-sec-says/articleshow/89916450.cms.

For a long time and only to a slightly lesser degree today, the regulatory climate in the United States has been fairly unclear regarding cryptocurrency. Multiple regulatory bodies have claimed some form of jurisdiction over cryptocurrencies, including the Securities and Exchange Commission which regulates securities, the Commodity Futures Trading Commission which regulates commodities, and the IRS which regulates property and taxation. Accounting practices for cryptocurrencies have also not been clearly defined. Many accounting questions still remain largely unanswered such as what constitutes a taxable event and which accounting method should be used (LIFO, FIFO, or weighted average). The increasing regulatory interest and the uncertainty of laws relevant to space has led many blockchain-based projects to leave the United States in favor of countries with more welcoming regulations.

When the SEC began implementing enforcement actions for ICOs, many projects made the argument that utility token sales were equivalent to “kickstarter” campaigns and that utility tokens were not securities. The SEC returned with arguments explaining the security nature of many coins and tokens. One argument was that the value of a coin/token serves as a proxy for the value of a project/protocol as a whole where if the network was successful then the coin/token would increase in value. The core of the argument was that the coin/token being sold was an investment in the future success of the project and therefore a security.

The Howey Test

The longstanding test for what is and what is not a security in the United States is the Howey Test. The Howey Test[131] outlines four necessary features of a security, all of which must be present:

1. An investment of money is being made
2. The money is invested in a common enterprise
3. There is an expectation of profits from the investment
4. Resulting profit is solely derived from the efforts of others

The Securities and Exchange Commission uses the Howey Test to decide and issue its enforcement actions against ICOs and other offerings of cryptocurrencies for the selling of unregistered securities. In many enforcement actions, the language and audience of marketing efforts of cryptocurrency sales are examined by the SEC to determine if a coin/token was or was not a security.

[131]Sykes, Jay B., “Securities Regulation and Initial Coin Offerings: A Legal Primer.” *Congressional Research Service*, 31 Aug. 2018, https://sgp.fas.org/crs/misc/R45301.pdf.

Regulatory Clarity

In recent years, regulatory bodies have issued rulings that have helped to some degree in the clarification of the law relevant to cryptocurrencies. One of the decisions made by the SEC regarding a blockchain-based project was its report on The DAO. As described previously, The DAO was a decentralized autonomous organization created for the purpose of crowdfunded venture investing. The SEC report included the decision that The DAO satisfied all components of the Howey Test and was a clear-cut case of what a cryptocurrency security looks like.

The Securities and Exchange Commission announced in 2018 that bitcoin and ether are not securities, citing sufficient decentralization of the networks and the lack of "a central third party whose efforts are a key determining factor in the enterprise."[132] This point raised by the SEC brought immense importance for cryptocurrencies to the final point of the Howey Test: resulting profit coming from the efforts of others.[133] Bitcoin and ether were deemed to not be securities as the sufficient decentralization of the networks eliminated a third party that could be pointed to as the party exerting effort that is resulting in profit for owners of a potential security. This component of the Howey Test provides an avenue for other decentralized blockchain networks to avoid being labeled as a security, given that all parts of the Howey Test must be satisfied.

However, the SEC noted that ether could have been deemed as a security around the time of its ICO when Ethereum was more centralized. Additionally, it was noted that even if certain digital assets are not inherently securities, they can still be used as a means of exchange in a security offering, which could bring enforcement action against the promoter.

In 2019, the SEC further clarified its position on non-security cryptocurrencies when it issued a no-action letter for TurnKey Jet. TurnKey Jet was a blockchain-based frequent-flier program that used a utility token which could not be transferred or increase in value. The letter cited aspects of the token sale such as the firm not using token sale proceeds to develop the platform, the existing functionality of the tokens to be used for booking air charter services, the restriction of user transactions to only TurnKey Jet wallets, a constant sale and consumption price of the tokens, and

[132]Hinman, William. "Digital Asset Transactions: When Howey Met Gary (Plastic)." *U.S. Securities and Exchange Commission*, 14 June 2018, https://www.sec.gov/news/speech/speech-hinman-061418.

[133]"Framework for "Investment Contract" Analysis of Digital Assets." *U.S. Securities and Exchange Commission*, 3 Apr. 2019, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

marketing by TurnKey Jet that emphasized the functionality of the token.[134] In weighing the collective nature of the token's aspects, the SEC determined that TurnKey Jet's token was not a security. Through these decisions, the SEC was likely attempting to lay a baseline for establishing under what circumstances a token is not a security, so that the agency could then pursue tokens it believes to be a security.

Around the end of 2019, the SEC began pursuing increased enforcement action against companies that were issuing non-registered securities as well as actions against heavily involved individuals. The SEC issued an order against Block.one, finding the firm to be in violation of registration provisions of the federal securities laws.[135] Block.one agreed to pay a $24 million settlement civil penalty for its ICO that raised over $4 billion. As part of the settlement, Block.one did not admit or deny the SEC's fundings. However, other companies received far greater fines relative to the amount raised. Sia was issued a settlement fine of approximately $225,000 for its sale of $120,000 worth of Siastock in 2014 which promised "guaranteed income proportional to the value of storage being rented from the Sia network."[136]

Other Initial Distribution Methods

In the wake of increased regulation and enforcement actions of cryptocurrency distributions via the classical ICO model, projects have started to distribute cryptocurrency in different ways in recent years. Additionally, blockchain technology and cryptocurrencies have been leveraged to host public offerings of securities.

Initial Exchange Offering (IEO)

While initial coin offerings are commonly managed independently by the entity responsible for the coin/token being sold, an **initial exchange offering** is a coin/token sale that occurs on a centralized exchange platform. The centralized exchange functions similarly to how a traditional financial intermediary would, with tasks such as approving participants, serving as an additional layer of trust on the offering, and managing funds during the offering period. However, initial exchange offerings likely do

[134]Ingram, Jonathan A., "Response of the Division of Corporation Finance, Re: TurnKey Jet, Inc." *U.S. Securities and Exchange Commission*, 2 Apr. 2019, https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.

[135]"SEC Orders Blockchain Company to Pay $24 Million Penalty for Unregistered ICO." *U.S. Securities and Exchange Commission*, 30 Sept. 2019, https://www.sec.gov/news/press-release/2019-202.

[136]"Order Instituting Cease-And-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, Making Findings, and Imposing a Cease-And-Desist Order in the Matter of Nebulous, Inc." *Securities and Exchange Commission*, 30 Sept. 2019, https://www.sec.gov/litigation/admin/2019/33-10715.pdf.

not free the entity responsible for the token from any regulatory concerns that we discussed with ICOs.

Initial Exchange Offering Case Study: Binance Launchpad

Even though not prominently used in the United States due to government regulation, Binance is the largest cryptocurrency exchange in the world. Binance regularly hosts daily transaction volume in the tens of billions of dollars.[137] Binance was one of the first exchanges to offer initial exchange offerings and has taken a center position in the space with its native initial exchange platform: Binance Launchpad. Binance launchpad has held token sales for over 60 projects, which raised over $100 million from more than 3 million unique participants.[138] Binance Launchpad offers many benefits such as advising, access to millions of platform users, and listing on the world's most popular exchange to prospective projects looking to host a token sale.[139]

Initial Decentralized Exchange Offering (IDO)

An **initial decentralized exchange offering** is similar to an initial exchange offering in that it is an exchange-based sale of coins/tokens, with the one difference being that the sale happens on a decentralized exchange. IDOs have become more popular as decentralized exchanges have improved to match the offerings of centralized exchanges. IDOs offer similar benefits to that of IEOs, without the additional scrutiny and hurdles of a centralized exchange. However, an entity hosting an IDO will likely not benefit as much from exchange-based marketing as it would from an IEO.

Security Token Offering (STO)

A **security token offering** is a type of public security offering where the security is tokenized as a cryptocurrency. As we will investigate in the next chapter during our discussion on decentralized finance, blockchain technology has many benefits to offer relative to traditional financial systems. For example, blockchain technology and its ability to easily automate many features through the use of smart contracts holds great potential in its ability to potentially reduce the costs associated with holding a security offering through traditional finance channels. Security tokens are registered with the relevant securities agencies (such as the U.S. Securities and Exchange Commission)

[137]"Top Cryptocurrency Spot Exchanges." *CoinMarketCap*, https://coinmarketcap.com/rankings/exchanges/.

[138]"Binance's Token Launch Platform." *Binance*, https://launchpad.binance.com/en.

[139] Ibid.

and thus provide increased regulatory certainty for cryptocurrency outsiders to more easily adopt the technology.

Airdrops

An **airdrop** is a free distribution of blockchain-based assets. Unlike initial coin offerings and the other initial distribution methods discussed above, airdrops do not collect payment for the asset. Airdrops provide a compelling advantage in the face of increased regulation and enforcement by government agencies. Airdrops have become increasingly more common in the past couple of years, especially for the tokens of decentralized finance applications and decentralized autonomous organizations.

While founding teams forfeit the possibility of immediately cashing out with a token sale, airdrops can serve as a way to reward a project's loyal users and help to set the project up for success in the long run. If project creators hold onto an allotment of tokens, which serves as an incentive mechanism for further project development and improvements, the creators can very possibly end up in a better financial position by distributing tokens via airdrop rather than by hosting a sale. The project will also likely avoid most of the possible regulatory consequences of holding a token sale based upon current enforcement actions, which enables projects to reside and operate in areas with heavy jurisdiction such as the United States.

Airdrop Case Study: Uniswap's UNI Governance Token

Uniswap, the most popular decentralized exchange (further discussed in the next chapter), is governed by a governance token. Today, the total market value of the UNI governance token is in the billions of dollars. Rather than sell the UNI token at initial release, the team behind the project elected for an airdrop. In September of 2020, at least 400 UNI tokens were sent to addresses that had previously used the product.[140] 150 million UNI tokens were set aside for the airdrop.[141] The value of 400 UNI at the time was around $1,200, which conveniently aligned with the current event discussions of stimulus checks at the time, yielding the airdrop and Uniswap additional press coverage.

[140]Shen, Muyao. "Uniswap Recaptures DeFi Buzz With UNI Token's Airdropped Debut." *CoinDesk*, 17 Sept. 2020, https://www.coindesk.com/markets/2020/09/17/uniswap-recaptures-defi-buzz-with-uni-tokens-airdropped-debut/.

[141]Dale, Brady. "Uniswap's Retroactive Airdrop Vote Put Free Money on the Campaign Trail." *CoinDesk*, 3 Nov. 2020, https://www.coindesk.com/business/2020/11/03/uniswaps-retroactive-airdrop-vote-put-free-money-on-the-campaign-trail/.

Airdrops: Free But Scot-Free

However, projects hosting token airdrops can still be and are actively pursued by the Securities and Exchange Commission for violation of securities laws. In the case of the enforcement action issued by the SEC against Tomahawk Exploration LLC's airdrop of free TOM tokens, the SEC found that even though the tokens are not sold, the promotional services required to receive the free TOM tokens sought to "advance the issuer's economic objectives or create a public market" for TOM tokens which were deemed to be a security.[142] Even though these tokens were distributed without necessary payment, Tomahawk Exploration LLC was still found to be in violation of securities laws.

Summary

A coin is the native asset of a blockchain. A token is a blockchain-based asset that is built on an existing blockchain and uses the existing blockchain to process its transactions and maintain its ledger. Coins primarily exist to power a blockchain by rewarding the maintenance and/or securing of the network by providing computing power and denominating transactions and the fees paid for transacting and computing on the network. Tokens are primarily used to incentivize participation in a blockchain-based network or decentralized application, redemption for services or the ability to participate in a network, jumpstart a network or decentralized application, and/or govern decision-making power on protocol upgrades/changes. Tokenomics is a new field of study that concerns what gives a token value, what value the token has, and how a token maintains its value over time.

An Initial Coin Offering is a historically common process by which new coins and tokens are introduced to the market. The ICO model provides many benefits to new projects looking to raise funds such as these sales typically being non-dilutive of company equity, broadening the field of potential investors, and the ability to raise large amounts of capital in a quick fashion. However, ICOs also present challenges to projects, including increased regulatory scrutiny and punishments for holding illegal security offerings. The Howey Test is commonly applied to see if a sale is classified as a security offering. Other coin and token distribution methods include initial exchange offerings, initial decentralized exchange offerings, security token offerings, and airdrops.

[142]"Order Instituting Administrative and Cease-And-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-And-Desist Order in the Matter of Tomahawk Exploration LLC and David Thompson Laurance." *Securities and Exchange Commission*, 14 Aug. 2018, https://www.sec.gov/litigation/admin/2018/33-10530.pdf.

Review Questions

1. What is the difference between a coin and a token?
2. What are the fundamental purposes of coins?
3. What are some of the most common token utilities?
4. What is tokenomics concerned with?
5. What is the first major step in hosting an Initial Coin Offering?
6. Describe two benefits of Initial Coin Offerings.
7. Describe two challenges of Initial Coin Offerings.
8. What was the first major Initial Coin Offering?
9. What are the core elements of the Howey Test that must all be satisfied for the designation of a security sale?
10. What is an airdrop and how is it different from other initial distribution methods?

Chapter 8: DeFi: Decentralized Finance

What is Decentralized Finance?

Decentralized finance, commonly referred to as "**DeFi**," is a decentralized take on the traditional financial system. Decentralized finance seeks to create an open financial system where financial services can be accessed by anyone connected to the Internet. Decentralized finance eliminates, or at least greatly reduces the influence of, a central authority commonly at the middle of financial transactions and agreements by incorporating blockchain technology. Decentralized finance is capable of or working towards providing many financial services such as savings, borrowing, lending, insurance, trading, and investing that can be accessed anywhere, at any time, and without the need for a strong central authority.

Smart Contract Use

Decentralized finance is implemented through the use of smart contracts. Smart contracts can be written with predefined terms to enforce the rules of finance. The predefined terms are agreed to by all transacting parties and cannot be cheated or changed. Smart contracts provide a high level of transparency due to the public nature of the code. With smart contracts, various components of the traditional finance system can be created in a decentralized manner. In most cases, smart contracts provide all the authority necessary to guide financial services and conduct transactions.

DeFi Characteristics

A successfully actualized decentralized finance system can be characterized by four general criteria:

Global access

In order for a decentralized finance system to align with the core tenants of blockchain technology, anyone should be able to access the decentralized system simply with a device connected to the Internet. The publicly accessible nature of blockchain technology and the decentralized applications built on top of it serves as a tool for economic equalization across the planet.

Permissionless

Building from the globally accessible nature of a decentralized finance system, anyone is able to create and/or participate in decentralized finance applications. There are no barriers to entry

instituted by central authorities when it comes to creating or using decentralized applications. Contrary to the requirements necessary to participate in the traditional financial system, a successfully created decentralized finance system offers equal access to all.

Flexibility

Another component of a decentralized finance system is flexibility for users. Users should be able to freely switch between decentralized applications to best fit their needs. Because users hold their assets and data, there are minimal switching costs and no central authority owns the information of users which prevents them from switching applications.

Composability

A final core component of a successfully created decentralized finance system is composability. Decentralized applications should be interoperable and multiple components of the decentralized finance system can be combined to create new services. New creators of decentralized applications can build on top of existing services, which lowers barriers to entry and allows for greater offerings to users.

Advantages of Blockchain for Finance

Blockchain technology provides many promising benefits to the evolution of the traditional finance system. At scale, blockchains can leverage its network effects of communities, infrastructure, and tooling. With these benefits, scaling solutions may allow decentralized blockchains to outpace the network-wide capabilities of centralized software. Three key advantages of blockchain technology use for financial services are:

Open Access

Blockchain technology provides a low barrier to entry. Only a device and internet connection is required to access public blockchain networks and the decentralized applications built on top of them. Anyone can join a public blockchain network and create a wallet in seconds. Additionally, anyone can create decentralized applications on the network. This feature allows a financial system built on blockchain technology to evolve at a far greater speed than traditional financial systems. The shared, transparent state of public blockchains help to garner strong user trust in the network.

Minimal Fees

Because blockchain-based financial systems operate on the internet rather than the brick-and-mortar and office structure of traditional financial institutions, the overhead costs to cover are much lower. The existing costs of maintaining the infrastructure are also shared among network participants, which further lowers the startup costs of building an application in a blockchain network. Lower costs translate to increased options and lower fees for users.

Novel Assets

Combining crypto assets, protocols, and smart contracts in new ways creates the potential for services that we have not seen before. Pieces of protocols and services can be picked and placed together to create a new service in a practice referred to as “money legos.” This practice stems from the goal of decentralized finance to be an interoperable system. Decentralized autonomous organizations can be built that perform the same functions as traditional financial institutions without a central power.

Incumbent Advantages

While decentralized finance applications enjoy many advantages by using blockchain technology, traditional financial institutions also have their own advantages in the battle for where customers choose to use financial services. Some of the many incumbent advantages are:

Head Start

While the oldest decentralized finance applications are only a few years old, many prominent banks have been operating for hundreds of years. These institutions have had an ample amount of time to smooth out their operations and to address problems. Unlike blockchain technology and decentralized finance applications, practically everyone has grown up surrounded by banks and their influence, along with being exposed to the concept of traditional banking very often starting at a young age.

User Data

Traditional financial institutions have accumulated tons of user data. With this abundance of data, banks can offer services such as automated fraud detection systems that new projects cannot compete with.

Community Trust

Throughout the hundreds of years that they have existed, financial institutions have gained the trust of their customers. Financial institutions commonly offer an in-person presence which the public has grown accustomed to. Given the nature of the business, trust is a major hurdle for decentralized finance applications.

Brand Recognition

Through their constant existence in history and the trust held in them by many members of the general public, traditional financial institutions are the top of mind choice for most people in need of financial services.

FDIC Insurance

Nearly all United States banks are covered by FDIC insurance which adds an additional layer of trust for customers. The insurance of $250,000 for one's deposited funds is an excellent provision afforded to customers. Investment firms hold similar insurance such as SIPC insurance. As of now, decentralized finance projects do not have the same access to government-backed insurance that many consumers associate with their trust of an institution.

Regulatory Certainty

Unlike the unknown nature of cryptocurrency and decentralized finance regulations, the regulations applicable to traditional financial institutions are well-known and understood. While there is much uncertainty encircling cryptocurrencies, especially for those unfamiliar with the technology, people are fairly certain about their expectations regarding traditional financial institutions.

Decentralized Exchanges

Decentralized exchanges are the decentralized finance improvement on the first generation of cryptocurrency exchanges. Centralized cryptocurrency exchanges, from the infamous Mt. Gox to modern-day titans such as Coinbase and Binance, have handled the majority of cryptocurrency trading volume practically since the inception of blockchain technology. However, decentralized exchanges are gaining meaningful traction, to a particularly large degree in recent years. Decentralized exchanges eliminate the central authority of exchanges and their custodianship of traded assets. In a transaction conducted on a decentralized exchange, users maintain full control of their private keys and non-transacted assets. The first decentralized exchanges enabled peer-to-peer trading guided by smart contracts and further developments have brought

decentralized exchange product offerings close to those offered by centralized exchanges.

Automated Market Makers

A central component to many contemporary decentralized finance applications is **automated market makers** (AMMs). An automated market maker functions as an algorithmic trading desk operated by smart contracts. Automated market makers require no designated counterparty for a trade to execute, unlike the first decentralized exchanges that paired peers for trading. Rather than peer-to-peer, transactions in automated market maker systems are “peer-to-contract.” The price at which trades are executed is set by an algorithm in the smart contract. Funds that a user trades for on an exchange powered by an automated market maker comes from a liquidity pool.

Liquidity

Liquidity is the ease with which an asset can be converted into another asset without affecting the asset’s market price. The first decentralized exchanges often ran into liquidity problems before the introduction of automated market makers. Automated market makers attempt to solve the liquidity problem faced by decentralized exchanges by maintaining **liquidity pools**. A liquidity pool is a collection of funds deposited by liquidity providers. Liquidity providers are incentivized to deposit and keep funds in the liquidity pool by receiving a liquidity provider fee (typically ~0.25%) of the transaction. Trades handled by AMMs are executed against the liquidity pool, preventing price slippage. AMMs can traverse several liquidity pools for a transaction to minimize end-user cost for the transaction.

Impermanent Loss

Impermanent loss is the loss in the value of assets provided to a liquidity pool. Transactions with the liquidity pool are done against the funds of liquidity providers, so the remaining funds of a liquidity provider may end up as less valuable than they were when initially provided due to the changing values of the two cryptocurrencies and the transactions executed against the pool.

For example, a pool might have experienced a large amount of transaction volume in one direction, leaving a liquidity provider’s share of the liquidity pool as lopsided toward one asset. If the resulting total value of the assets returned to a liquidity provider is less than what the liquidity provider would have if they had not contributed assets to the pool, then the liquidity provider has sustained impermanent loss. In order for

providing liquidity to return a profit, a liquidity provider is seeking for their share of transaction fees gained by the pool to outweigh the impermanent loss suffered by their provided funds.

Yield Farming

Yield farming, also known as liquidity mining, is a practice of staking or lending cryptocurrency for a reward.[143] Lending typically occurs in stablecoins due to the high volatility of cryptocurrencies. If the collateral that a borrower puts up falls below a specified threshold, then their collateral will be liquidated. Extreme examples of yield farming exist where one stacks multiple yield-earning accounts on top of each other in an attempt to gain increased rewards. However, the risk associated with this practice also increases heavily when stacking multiple yield-earning accounts.

DeFi in the Real World

As the potential for Decentralized Finance continues to grow, we have already seen some DeFi projects function at a high level with significant volume. The following projects are all examples of how Decentralized Finance concepts can be used to revolutionize more and more pieces of the traditional finance system.

Augur[144]

Augur was one of the earliest proposed decentralized finance platforms, hosting its ICO in 2015. Augur is a decentralized prediction market platform. Users are able to create prediction markets of their choosing that other users can partake in. Augur has no central authority that manages the prediction markets, results, payouts, and fees. Instead, smart contracts are used to conduct all steps from market creation to payout. An oracle is used to provide the smart contract with accurate information so that a winning side of the prediction market can be declared. Augur provides open prediction markets for users at fees far lower than centralized prediction markets.

Compound[145]

Compound is an autonomous decentralized lending platform that enables the peer-to-peer lending and borrowing of cryptocurrencies. All aspects of loans (principle, interest, collateral) are paid with cryptocurrency. The decentralized model cuts out the

[143]Vermaak, Werner. “What is Yield Farming?” *CoinMarketCap*, https://coinmarketcap.com/alexandria/article/what-is-yield-farming.

[144]*Augur*, https://augur.net/.

[145]*Compound*, https://compound.finance/.

traditional finance institutions typically at the middle of loans by getting the necessary authority through the use of smart contracts.

The Compound protocol has a native token: COMP. The COMP token is a governance token that is paid to liquidity providers as a reward for providing liquidity. COMP token holders can vote on protocol changes.

Aave[146]

Aave is a decentralized lending protocol that enables users to deposit cryptocurrency for yield and to borrow cryptocurrency from a variety of pools. The protocol offers fairly standard lending pools such as fixed rate pools and variable rate pools for a variety of cryptocurrencies. Aave also introduced the concept of **flash loans** to the Ethereum network. Contrary to the standard overcollateralized loans of many decentralized finance protocols, flash loans allow a user to borrow uncollateralized funds, use the funds to perform a transaction such as an arbitrage opportunity, and then return the funds to the lender with the addition of a small fee. Aave has issued billions of dollars in flash loans since their introduction to the Ethereum network in January 2020.[147]

Uniswap[148]

Uniswap is a decentralized exchange that utilizes automated market making and liquidity pools to execute trades. Uniswap is run by smart contracts with no central authority that takes custody of your cryptocurrency. Uniswap allows users to execute trades with near-zero price slippage and offers exchange fees as a reward for liquidity providers. Users have conducted nearly one trillion dollars of trade volume on the platform since its launch in 2018. Uniswap has a governance token, UNI, that enables holders to vote on platform changes. UNI tokens were initially distributed by giving a fixed amount to all previous users of Uniswap.

PoolTogether[149]

While some decentralized finance applications provide services similar to those we see offered by traditional financial institutions, decentralized finance has brought and

---

[146] *Aave*, https://aave.com/.

[147] Hamacher, Adriana. “What Are Flash Loans? The DeFi Lending Phenomenon Explained.” *Decrypt*, 28 June 2021, https://decrypt.co/resources/what-are-flash-loans-the-defi-lending-phenomenon-explained.

[148] *Uniswap*, https://uniswap.org/.

[149] *PoolTogether*, https://pooltogether.com/.

will continue to bring rise to new services that we do not ordinarily find in traditional financial institutions. PoolTogether offers a “lossless lottery” where users pool their money together into one interest-bearing account. At the end of the month, one user is chosen to receive the entire interest sum. All users are returned their initial deposit.

How Different is Decentralized Finance, Really?

Although decentralized finance and centralized finance systems are fundamentally different in their design, the two actually perform very similar functions in the real world. While they may take different approaches, both systems simply seek to provide the same financial services to their customers. In both systems you can find savings, borrowing, lending, insurance, trading, and investing opportunities. The theme of a select few making the majority of returns is readily apparent in both systems.

In its fullest form, decentralized finance improves on the current financial system by making it more efficient, while removing centralized powers that are no longer needed and returning power to the users. The true degree to which the financial system will be fundamentally changed by decentralized finance remains to be seen.

Summary

Decentralized finance, commonly referred to as “DeFi,” is a decentralized take on the traditional financial system. Decentralized finance seeks to create an open financial system where financial services can be accessed by anyone connected to the Internet, with a decreased reliance on central authorities. Decentralized finance makes use of smart contracts to develop autonomous, decentralized financial applications. Decentralized finance possesses a competitive advantage derived from its open access, minimal fees, and the ability to compound the services of multiple applications. However, decentralized finance is competing against an incumbent industry that has had centuries to develop a strong wall of defense.

Decentralized exchanges are a core component of DeFi. Decentralized exchanges allow network users to trade their cryptocurrencies without giving up custody of their assets to a central entity at any point in their transaction. Automated market makers typically perform trades against liquidity pools of user provided funds to complete trades on decentralized exchanges.

Decentralized finance is constantly expanding the services available to blockchain network participants. Examples of DeFi protocols include Augur which is a decentralized prediction market, Compound which is an autonomous decentralized lending platform, Aave which is a decentralized lending platform that introduced the

concept of flash loans to the Ethereum blockchain, Uniswap which is the most popular decentralized exchange, and PoolTogether which offers lossless lotteries.

Review Questions

1. What are some of the characteristics of a successful decentralized finance system?
2. Describe one inherent advantage of decentralized finance over traditional financial systems.
3. Describe one inherent advantage of traditional financial systems over decentralized finance.
4. What is the difference between a decentralized exchange and a centralized exchange?
5. How can automated market makers execute trades autonomously?
6. What is a liquidity pool?
7. Why do blockchain network participants contribute their funds to liquidity pools?

Chapter 9: Business of Bitcoin Mining

The valuable reward, currently 6.25 BTC per block, offered by the Bitcoin blockchain for the miner that solves the block occurring every 10 minutes and the intense resources required to do so has created a professionalized industry for proof of work mining. While Bitcoin is the most prominent blockchain that uses proof of work mining, plenty of other blockchains still use proof of work as their consensus mechanism and therefore also serve as a home to proof of work mining operations.

Mining in a Blockchain Ecosystem

Mining is a central component to a proof of work blockchain. The complex computations done by miners continue the blockchain and prevent double spending. The reward paid to miners and the real costs of running a mining operation incentivize miners to participate in the network and to be good actors. Mining secures the blockchain network and is the “price of trust” in a proof of work blockchain.

Components of a Mining Operation

Site

Large scale mining operations, necessary to operate as a full-time mining business, need specialized sites. Large mining operations need specialized access to large electricity flow, abundant space, and industrial cooling equipment to combat the excessive heat produced by the mining operation.

The location of a mining operation is perhaps the single most important decision when establishing a mining operation. As we will discuss in this chapter, electricity makes up a large portion of the costs associated with running a mining operation. Mining operations can set themselves up for future success by locating themselves in regions of low-cost electricity. Some mining operations even co-locate with electricity production operations such as hydroelectric power facilities.

Miner

A “miner” is a device specialized for the hashing requirement of proof of work mining. Miners are often specialized for a particular blockchain’s specific hashing algorithm and design. While many mining operations nowadays use these specialized pieces of equipment, you can also use a general purpose GPU as the entire function of the equipment

being used to mine is simply guessing a nonce that fits the requirements of the protocol via brute force. In fact, some blockchains (discussed later in the chapter) are built to remove any advantage to using specialized mining equipment.

Power

A reliable power source is required to feed the miners performing intense computation a large, consistent amount of electricity to power the mining process. Many mining locations are built in a given location because of the nearby power resource that will be used to power the operation. Many other mining operations create agreements with local energy suppliers to take on overproduced electricity for a cheaper price.

Software

Many mining operations are controlled by software systems. These systems can perform many management tasks such as alerting staff if a miner is not functioning properly and altering operations due to changes in electricity costs. Especially in areas with changing electricity prices, it is imperative that mining operations can be quickly terminated if electricity prices spike beyond a level that is profitable for the mining operation.

Pool

Almost all miners will join a mining pool to combine computational power given how many other miners are competing across the world to become the first to solve a block. Pooling computing resources increases the chance of the pool to earn a block reward compared to the efforts of one individual, which provides more stable mining revenue for a mining operation. Due to the constant electricity costs associated with mining, stable revenue is often required for a mining operation to remain functional. Additionally, the increased stability and predictability of mining revenue makes it easier for firms to raise capital for the expansion of operations.

Buyer

Given the consistent costs associated with proof of work mining, Mnmany mining operations need to consistently sell a sizable portion of their block reward proceeds. Miners will likely perform this transaction on an exchange as a standard transaction. If an operation is producing a large amount of cryptocurrency, then it could be directly partnered with

institutional firms or have a favorable deal in place with an exchange for a lowered transaction fee.

Turn-Key Mining Services

Due to the high startup costs of gathering the essential components described above, many companies offer a “turn-key” service to prospective miners in which the company will mine for the customer. In exchange for a fee, the customer will receive the mining proceeds gained by the mining company. Turn-key mining services also provide economies of scale benefits that prospective miners would not be able to achieve on their own. In this model, a prospective miner can earn mining revenue without establishing the infrastructure needed for an entire operation of their own.

Specialized Equipment

When the difficulty of Bitcoin mining was far less than it is today, common household technology was capable of participating as a miner on the network. Mining was first done by CPUs and then GPUs were used.

The increased difficulty of mining computations due to increased mining competition now requires highly specialized devices to mine on networks such as the Bitcoin blockchain. Contemporary miners are mostly ASIC (Application-Specific Integrated Circuit) machines. The chips of these machines are specifically designed for mining on the specified blockchain. Bitcoin ASIC miners are purely built to run the SHA-256 hashing algorithm.

Concerns about the evolution of mining equipment have become increasingly prevalent. While the efficiency of miners has historically followed a trend described by Moore’s law, some members of the tech community have begun to question the sustainability of Moore’s law. More recently, the global chip shortage has impacted the blockchain mining industry as well. Manufacturers of proof of work mining equipment are historically among the last to see their chip orders fulfilled.

Hash Rate

Hash rate is the measure of the total amount of computational power put toward the mining process of a proof of work blockchain. Hash rate is an important internal metric of blockchain networks. The difficulty of solving blocks in the Bitcoin blockchain is based upon the hash rate of the network, in order to maintain the approximate 10 minute block time. The greater the hash rate of a blockchain network, the more difficult it becomes to mine. Also, as the hash rate of a network increases, so does the security of the network.

Mining Pool Concentration

We have already touched on mining pool concentration as an issue facing blockchain technology. With a majority of Bitcoin's hash power coming from only four mining pools, there are concerns regarding the power that these mining pools own. With a majority ownership of Bitcoin's hash power, these four pools alone could reach consensus on decisions for the entire network. Although it is theoretically impossible for a single bad actor to carry out a 51% attack on the Bitcoin blockchain, the concentration of the network's hash rate among a select group of mining pools maintains the threat of a 51% attack carried out by a unified group of bad actors. Perhaps an even more plausible threat is the seizing of hash power by a nation's government to conduct a 51% attack.

Mining Costs and Revenues

In addition to the main cost source of electricity, there are also other factors to the total cost of running a proof of work mining operation. Other costs such as variable, fixed, pool, and exchange costs represent approximately 10-25% of the total cost to mine. Variable costs are any required labor to operate the mining equipment, software fees, and internet costs. Fixed costs of a mining operation include the miners, site lease/development, and infrastructure. Pools collect fees from the earnings of miners that join their pool, typically 2-4%. Exchange fees consist of the spread between bid and ask prices and exchange transaction fees.

The known block reward and block timing of bitcoin mining allows for one to easily forecast their future revenue with a few inputs. The simplified long-run daily mining profit can be calculated by the following equation:

$$\text{Daily Mining Profit (\$)} = 144 * 6.25 * (1-f) * (m/N) * P - 24 * m * e * E$$

- 144 is the amount of blocks mined per day
- 6.25 is the block reward, in BTC
- f is the pool fee (f = 0 if no pool)
- m is the miner's hash rate
- N is the network's total hash rate
- P is price at which the bitcoin is sold
- 24 is the number of hours in a day
- e is the miner's efficiency rate
- E is the cost of electricity

Energy, Electricity, and the Environment

Electricity costs are by far the greatest, recurring expense of blockchain mining. Many prospective miners will plan the entire business around where they plan on getting the most accessible, low-cost electricity possible. Other than increasing the amount of miners they are running, mining operations can often best increase profits by finding ways to reduce their electricity costs.

Renewable Energy

The large energy consumption has given rise to strong concern regarding the environmental impact of blockchain mining. Luckily, many miners are incentivized to seek out renewable energy sources, as they often have cheaper electricity prices. In our coverage of possible environmental impact solutions, we came across the statistic that 76% of miners use renewable energy as a part of their energy use.[150] Although this renewable energy use only accounted for 39% of the total blockchain mining energy consumption at the time, advances in renewable energy technologies will increase these percentages as more miners are incentivized to switch to low-cost renewable energy.

The Hydro Season

China already offers low electricity prices, but these prices can go even lower during the "hydro season." Between May and October, some southwestern Chinese provinces experience a period of heavy rainfall. Electricity prices from hydroelectric dams can fall below 1 cent per kilowatt-hour, compared to its usual price of about 3 cents per kilowatt-hour. During this time of increased mining profitability, greater mining activity has been historically observed in these provinces. These periods of ultra low-cost electricity highlight an opportunity for miners around the world to identify places and situations where electricity can be sourced for less than their competition. Given how much of a mining operation's cost is electricity expense, the sourcing of low-cost electricity is perhaps the most important action that can be taken to maximize profit.

Government Enforcement

While a government cannot control the Bitcoin blockchain, it can exert some control over the accessibility of a blockchain by its citizens. While once home to the majority of Bitcoin's hash power, China has banned Bitcoin mining and enforced its

[150]Blandin, Apolline, et al. "3rd Global Cryptoasset Benchmarking Study." *University of Cambridge Judge School of Business | Cambridge Centre for Alternative Finance*, Sept. 2020, www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf.

rulings enough in 2021 to where most Bitcoin mining activity has left the country. The United States is now the largest contributor to Bitcoin's total hash power.[151]

Government-Determined vs. Free Market Electricity Prices

Electricity prices are often fixed by a nation's government, including China where a majority of the Bitcoin network's hash power has historically resided. Fixed electricity prices make it easier on miners to determine profitability, as now it mostly relies on the price movement of Bitcoin. Because electricity is the main cost associated with proof of work mining, operational costs become far more stable and predictable with fixed electricity prices.

While average electricity costs in the United States are higher than those in many other countries, many mining companies still opt to mine in the United States. Some benefits that these companies derive from mining in the US are electricity prices not set by the government and the reliability of the grid. The free-market aspect of US electricity prices allow for opportunistic miners to source power at extremely low prices under unique circumstances such as the overproduction of electricity.

Mining Other Cryptocurrencies

While the Bitcoin blockchain is the most prominent blockchain using the proof of work consensus mechanism, there are plenty of other blockchains that also require proof of work mining to power the network.

As of now, the Ethereum blockchain still runs on a proof of work consensus mechanism. The mining aspect of the Ethereum blockchain is fairly similar to that of the Bitcoin blockchain, but there are some important differences. For one, Ethereum is an "ASIC-resistant" blockchain, which means that an ASIC miner does not provide an additional benefit over other non-specialized mining equipment such as a GPU of similar power due to inherent features of Ethereum's Keccak-256 hashing algorithm.

Other prominent blockchains that are currently using the proof of work consensus mechanism include Dogecoin, Litecoin, Bitcoin Cash, Ethereum Classic, Monero, and Zcash.

[151]"Cambridge Bitcoin Electricity Consumption Index (CBECI) | Bitcoin Mining Map." *University of Cambridge Judge School of Business* | *Cambridge Centre for Alternative Finance*, https://ccaf.io/cbeci/mining_map.

Is Mining Disappearing?

Many blockchains are now transitioning (as in the case of Ethereum) or initially launching with consensus mechanisms other than proof of work. Proof of stake and other consensus mechanisms don't use methods that require large capital expenditures on miners and electricity consumption, rendering the traditional "mining" concept largely obsolete. There is no longer a need for warehouses of miners across the world when a consensus mechanism only requires a regular laptop to fully participate in the consensus mechanism. The current transition away from proof of work begs the question: is mining disappearing for good?

While it is true that many blockchains are doing away with proof of work and its intense "mining" process, the outlook for miners is not entirely bleak. For one, it seems that the Bitcoin blockchain has no current or future plans to move away from proof of work. Bitcoin is home to a large portion of blockchain mining activity, so these miners can rest fairly assured that their ability to mine will not be disappearing anytime soon.

But as for those miners on blockchain such as Etheruem which has stated plans to imminently move away from proof of work: what happens to all the mining equipment? The future prospects for displaced mining equipment (beyond unemployment claims) largely depends on the equipment itself. More specialized equipment such as ASIC miners built for specific protocols will likely face the hardest times, being left to search for other protocols that the equipment can effectively run. However, more general mining equipment such as high-power GPUs will likely be able to be widely repurposed in most computing systems.

Summary

The valuable reward, currently 6.25 BTC per block, offered by the Bitcoin blockchain for the miner that solves the block occurring every 10 minutes and the intense resources required to do so has created a professionalized industry for proof of work mining. The major components of a cryptocurrency mining operation include the site of the operation, mining equipment, electricity, software, a mining pool, and a purchaser of the mined cryptocurrency.

Particular emphasis is placed on electricity given its share of a mining operation's cost and the dependence on a steady flow of electricity that meets the consumption demand of the operation. Before the outlawing of cryptocurrency mining by China's government, China was home to a large share of the Bitcoin blockchain's total hash rate largely due to the cheap, available access to electricity. Mining operations have also

found success in locations where electricity prices are a free market as opportunistic miners have a greater ability to locate advantageous arrangements.

Review Questions

1. What do large mining operations commonly seek to co-locate with?
2. What is a “miner”?
3. What is the benefit of joining a mining pool?
4. What is an ASIC machine and how does it provide an advantage to miners?
5. What does the term “hash rate” mean?
6. Which country became the largest contributor to Bitcoin’s total hash power after China outlawed cryptocurrency mining?
7. Besides Bitcoin and Ethereum, what is another blockchain that uses proof of work mining?

Chapter 10: Stablecoins and CBDCs

Stablecoins have surged in popularity and market capitalization over the past couple years. Many central governments have already created, tested, or looked into having their own national digital currency, known as CBDCs (Central Bank Digital Currencies).

Stablecoins

In our earlier discussion of cryptocurrency volatility solutions, we covered the use of stablecoins to fill the shortcomings of popular cryptocurrencies such as bitcoin in their use as money. Stablecoins are cryptocurrencies of stable value which is often achieved by assigning its value to that of a central bank's currency. The most commonly used stablecoins currently used in the blockchain space are pegged to the United States dollar. MakerDAO's DAI and Tether were among the first stablecoins. While the decentralized MakerDAO took a transparent collateralized approach, the centralized Tether took a more private approach to its issuance of USDT tokens. As criticisms arose regarding the accuracy of promised collateralization by Tether and the potential profit to be made from issuing a popular stablecoin was realized, many other stablecoins began to appear across the blockchain space.

Types of Stablecoins

While all stablecoins work towards the same goal of providing a cryptocurrency with a stable value, different approaches in the design of the stablecoin can be taken. Four of the most common types of stablecoins are fiat collateralized, cryptocurrency collateralized, commodity collateralized, and algorithmic.

Fiat Collateralized Stablecoins

The most popular type of stablecoin, by far, is fiat collateralized. Fiat collateralized stablecoins have a value that is "pegged" to an underlying fiat currency. Each unit of the stablecoins is, in theory, backed 1:1 with the fiat currency. For stablecoin issued, there is a corresponding fiat deposit made into a bank account. The backing of stablecoins with fiat currencies give users confidence in the current and future value of their stablecoin holdings.

The incumbent and market leader of the fiat collateralized stablecoin market is Tether. Launched in 2014, Tether has grown exponentially to have more than $80 billion

USD of stablecoins in circulation.[152] Nearly all of Tether's stablecoins come in the form of USDT which is a fiat collateralized stablecoin intended to represent one United States dollar. Currently, USDT ranks third in the market capitalization of cryptocurrencies, behind only bitcoin and ether.[153] Tether has come under immense scrutiny in the past regarding the validity of their claims to have all stablecoins fully collateralized, but has started to provide increased transparency[154] about their reserves.

Tether has likely become more transparent with their holdings in recent years due to the rise of strong competitors: chiefly among them being USD Coin ("USDC"). Introduced in 2018, USDC is a fiat collateralized stablecoin born out of a partnership between Circle and Coinbase. USDC has powered itself to a top five position in the rankings of cryptocurrency market capitalization, having around $50 billion in circulation at any given time.[155] USDC willingly opts into a large deal of regulatory oversight, likely aiming to be viewed as the most trustworthy stablecoin in the cryptocurrency market.

Commodity Collateralized Stablecoins

Commodity collateralized stablecoins function similarly to fiat collateralized stablecoins. The value of a commodity collateralized stablecoin is tied to that of the underlying commodity. Users can have confidence in the value of their stablecoin holdings due to the verifiable scarcity of the backing commodity. The value of commodity collateralized stablecoins can move with the value of the commodity, as opposed to the static, inflationary value of fiat collateralized stablecoins.

Cryptocurrency Collateralized Stablecoins

Cryptocurrency assets can also be used to create a stablecoin. The use of cryptocurrencies as the backing of the blockchain-based stablecoin allows for users to easily create their own stablecoins without a central authority. Cryptocurrency collateralized stablecoins usually maintain a "soft peg" to a fiat currency due to the volatility of cryptocurrency prices.

The previously discussed DAI stablecoin is backed by cryptocurrency. Users can generate DAI by depositing protocol-determined cryptocurrency assets such as ether,

---

[152]"Transparency." *Tether*, https://tether.to/en/transparency.

[153]*CoinMarketCap*, https://coinmarketcap.com/.

[154]"Transparency: Reports and Reserves." *Tether*, https://tether.to/en/transparency.

[155]"USD Coin (USDC) | Digital Dollars for Global Business." *Circle*, https://www.circle.com/en/usdc.

effectively borrowing against their own funds. The generated DAI can be returned to the protocol in exchange for the assets deposited by the user.

One drawback to the user-creation of stablecoins backed by volatile cryptocurrencies is the need for overcollateralization. DAI requires users to maintain 150% collateralization at all times, which inherently limits scalability.[156] If the deposited collateral falls below this threshold, the collateral is automatically sold by the Maker protocol to ensure the generated DAI is accounted for and the remaining funds are returned to the user, less an assessed liquidation penalty.[157]

Algorithmic Stablecoins

The newest type of stablecoin to be used at scale is the algorithmic stablecoin. Algorithmic stablecoins look to maintain a constant value over time, without the need for asset collateralization. Algorithmic stablecoins commonly make use of built-in algorithms that seek to balance stablecoin demand and price by automatically adjusting the supply of its stablecoin to maintain the intended value. Algorithmic stablecoins might also consider measures of real value such as the Consumer Price Index.

Algorithmic Stablecoin Blockchain Case Study: Terra

Terra is a public blockchain protocol that enables an ecosystem of algorithmic decentralized stablecoins.[158] While the most prominent stablecoins of today are centrally issued and managed, Terra seeks to provide the market with a stablecoin alternative with no central authority. Additionally, the current options in the marketplace are largely pegged to the United States dollar, while Terra seeks to provide stablecoin options for many currencies of the world.[159]

Because there is no central authority in the issuance of Terra-based stablecoins, an algorithm must take on this responsibility. An algorithm attempts to balance the demand and price of the stablecoins of Terra's ecosystem by buying and selling its governance token: LUNA. The Terra blockchain enables decentralized foreign exchange transactions by

[156]"Maker." *DeFi Pulse*, https://www.defipulse.com/projects/maker.

[157]"Liquidation." *MakerDAO*, https://makerdao.world/en/learn/vaults/liquidation/.

[158]"Terra | Programmable Money For The Internet." *Terra*, https://www.terra.money/.

[159]"Discover Terra | What are Terra stablecoins." *Terra*, https://www.terra.money/intro-to-terra.

providing the ability to easily swap between stablecoin currencies, which is an important feature in a worldwide Web3 economy.[160]

In May of 2022 Terra experienced a catastrophic decline of more than 99% in the value of its LUNA token after suffering a considerable decline in United States dollar stablecoin and rampant inflation of LUNA. The Terra blockchain was halted at times and exchanges halted some trading activity of the token. The rapid decline of a once top five market capitalization cryptocurrency shows how quickly things can change in this young and rapidly evolving industry.

Central Bank Digital Currencies (CBDCs)

The next evolution of stablecoins comes in the form of government issued currency. While stablecoins have traditionally been tied to the value of national fiat currencies, none of the previously discussed stablecoins are national currencies themselves. National treasuries have noticed the popularity and benefits of a digital currency and some have begun the process of implementing the technology in their currency systems.

Global State of CBDCs

Both established countries looking to remain ahead in their currency technology and developing countries looking to make a technological leap in their currency technology have expressed interest in the idea of central bank digital currency and the benefits it has to offer.

China has been developing its DCEP (Digital Currency Electronic Payment) system which uses the “digital yuan,” backed by the fiat yuan. The system has been live tested in some regions, with hopes for a nationwide release in the coming years. Both the United States and European Union have conducted internal research and testing of CBDC systems, but the technology has not found its way into the general public yet. One nation that has fully implemented a digital currency is The Bahamas. The Bahamas became the first country to officially distribute a nationwide CBDC with its Sand Dollar. The Sand Dollar is a digital version of the Bahamian dollar, which is pegged to the United States dollar. The largely uncertain status of global CBDCs should become clearer in the coming years as more central treasuries make definitive decisions regarding the use of CBDCs in their economies.

[160]Ibid.

The centralized aspect of national currencies has led many CBDC proposals to elect for a more centralized form of ledger technology, different from what we observe in classical blockchains, such as Bitcoin and Ethereum.

Summary

Stablecoins have surged in popularity and market capitalization over the past couple years. Stablecoins are cryptocurrencies of stable value which is often achieved by assigning its value to that of a central bank's currency. The most commonly used stablecoins currently used in the blockchain space are pegged to the United States dollar.

Four of the most common types of stablecoins are fiat collateralized, cryptocurrency collateralized, commodity collateralized, and algorithmic. The most popular type of stablecoin is fiat collateralized. Fiat collateralized stablecoins have a value that is "pegged" to an underlying fiat currency for which, in theory, one unit of fiat is held in reserve for every unit of the stablecoin in circulation. Tether and USDC are the two most popular fiat collateralized stablecoins. Commodity collateralized stablecoins are backed with reserves of a chosen commodity such as gold. Cryptocurrency collateralized stablecoins are backed by other cryptocurrencies. Cryptocurrency collateralized stablecoins usually maintain a "soft peg" to a fiat currency due to the volatility of cryptocurrency prices. DAI is the most popular cryptocurrency collateralized stablecoin. Finally, algorithmic stablecoins look to provide a stable value over time by employing algorithms used to balance supply and demand.

Central bank digital currencies are another hot topic within the blockchain space in recent years. Both established countries looking to remain ahead in their currency technology and developing countries looking to make a technological leap in their currency technology have expressed interest in the idea of central bank digital currency and the benefits it has to offer. CBDCs are digital currencies that are minted and managed by a nation's government. CBDCs make use of digital ledger technology to further provide scalability and ease of use. The Bahamas and China have respectively implemented and piloted CBDCs. Both the United States and European Union have conducted internal research and testing of CBDC systems, but the technology has not found its way into the general public yet.

Review Questions

1. What is the purpose of a stablecoin?
2. What is the most common type of stablecoin?

3. What are the two most prevalent stablecoins in the cryptocurrency market?
4. What type of asset is used to collateralize the DAI stablecoin?
5. How do algorithmic stablecoins attempt to maintain a stable value?
6. What is a central bank digital currency?
7. What is one country that has implemented a central bank digital currency?

Chapter 11: Non-Fungible Tokens (NFTs)

We learned earlier that non-fungible tokens are a type of token that can be created on an existing blockchain such as Etheruem. A non-fungible token is a token that is inherently unique and has its own attributes. Non-fungible tokens serve as an immutable digital certificate of asset ownership that is stored on a blockchain. NFTs have skyrocketed in popularity in recent years, which certainly warrants their own discussion.

NFT Properties

Non-fungible tokens are a distinctive component of a blockchain ecosystem. NFTs can serve in a range of use cases due to the following properties:

Indivisible

Unlike the fungible coins and tokens circulating in blockchain ecosystems, non-fungible tokens are typically indivisible in nature. There is one owner of the non-fungible token and what it represents. The single owner nature of non-fungible tokens introduce a variety of use cases where only a single individual may possess an asset. For example, an online identity can be generated for individuals in a unique, indivisible manner where only a single person can own the token of their identity.

Unique

While fungible tokens enable payment networks and many blockchain-based protocols to function, they lack the ability to effectively represent unique assets. Each non-fungible token is inherently unique from the rest, including those of a holistic series. Non-fungible tokens can be used to represent unique assets, which greatly expands the assets that can be represented on a blockchain. For example, it does not make sense to represent a collection of real estate plots with a fungible token. The inherent differences between plots such as location, size, and value prevent these plots from being interchangeable. However with the use of non-fungible tokens, you can generate a unique blockchain-based asset for each plot that encapsulates the unique aspects of each plot.

Ownership

The existence of non-fungible tokens on a blockchain provides the ease of individual custodianship of blockchain-based assets. Non-fungible tokens can typically be stored in the same cryptocurrency wallets that hold your fungible tokens of a given blockchain. The ease of self-custodianship and interaction with blockchain-enabled

applications makes it possible for users to maintain ownership of their assets: spanning from personal medical records to video game characters. Non-fungible tokens are not controlled or owned by the platform or company that created it once in the hands of the consumer/purchaser. Users are generally free to access, transfer, and sell their non-fungible tokens without the permission of another entity.

Verifiable

The blockchain-based aspect of non-fungible tokens also allow for simple verification of the asset's authenticity, ownership, and provenance. By assigning a non-fungible token to an asset, the authenticity of a given asset's blockchain-based representation can be easily verified. Non-fungible tokens can be used to provide simple verification of assets that are particularly difficult or risky to transport or display. Digital signatures can be used to easily verify ownership of an asset. Additionally, the public nature of many blockchains allow one to easily track the movement of an asset over its lifespan.

Programmable

The creation of non-fungible tokens on smart-contract enabled blockchains allow for the implementation of complex code with an asset. Creators can make non-fungible tokens with programmable aspects that allow for asset lifecycle controls. For example, creator royalties can be implemented on the future sale of an NFT. Creators can also use tools such as oracles to change the fundamental elements of an NFT over time.

NFT Use Cases

Non-fungible tokens can be used to assign a digital certificate of ownership for any asset imaginable. Some of the most common use cases for non-fungible tokens are digital collectibles, creative works, gaming, real world assets, and domain names.

Digital Collectibles

Digital collectibles were one of the first large scale use cases of non-fungible tokens and they still remain popular to this day. CryptoKitties was one of the first NFT projects which famously "clogged" the Ethereum network in late 2017. In CryptoKitties, users can own, trade, and breed virtual cats with unique and rare characteristics. CryptoPunks was another early NFT project, which has seen a recent resurgence in popularity. CryptoPunks is a collection of unique characters that possess properties of varying rarity.

Creative Works

Non-fungible tokens can also be used for creative work ownership such as art and music. The properties of NFTs provide many benefits to artists, particularly their ability to be programmable. Digital distribution is made simple for artists and it unlocks greater control over the art's lifespan for the artist. In addition to receiving payment on the initial sale of the piece in large NFT marketplaces with many prospective buyers, artists can institute a royalty percentage on subsequent sales of their pieces.

Gaming

Non-fungible tokens can be used to make more dynamic in-game assets and to further the bounds of what "gaming" can be. Traditionally, in-game assets are owned by the game creator rather than the users. Users often cannot transfer ownership of their in-game assets or can only do so with strong restrictions put in place by the game developer. Additionally, game developers and platforms often have authority over a player's account. Non-fungible tokens can be applied to in-game assets to provide true ownership to the player. With in-game assets represented by NFTs owned by the players, game creators and platforms have less authority over the player and their assets. Players can also trade or sell the asset to other players. The interoperable goal of blockchain systems and applications provides the potential for the same asset to be used in multiple digital gaming environments. In-game assets represented by non-fungible tokens can range from character outfits to athlete cards for sports games to digital parcels of land in a metaverse.

Gaming NFT Case Study: Axie Infinity

Axie Infinity is a game that has helped bring the "play-to-earn" gaming model into the public eye. Play-to-earn, as the name suggests, is a game design where players are compensated for playing the game. In Axie Infinity, players form teams of three "axies" to battle in player versus environment (PvE) or player versus player (PvP) combat. Players are rewarded for playing well with one of the native tokens of Axie Infinity: smooth love potion (SLP). Smooth love potion is a cryptocurrency with utility inside Axie Infinity, but it can also be sold on cryptocurrency exchanges to receive bitcoin, ether, or fiat currency.

Axies exist as non-fungible tokens owned by the controlling player, and can therefore be sold by the player. Players can use SLP along with AXS, Axie Infinity's primary native (governance) token, to breed axies. In breeding, players gain new axies that can then be used in combat, loaned out to another player, or sold on the marketplace. In its rise to stardom, Axie Infinity has seen more than

$3.6 billion of Axie Infinity NFTs traded on its marketplace, with the most expensive axie selling for a whopping $820,000.[161]

Axie Infinity has become a source of income for many players, many of which live in countries with unstable economies where workers earn wages below or comparable to the earning potential with play-to-earn games. Particularly during the height of the COVID-19 pandemic, many turned to Axie Infinity as a primary source of income to put food on the table at a time when their jobs/businesses went away or failed to provide adequate income. This fantastic, short documentary[162] provides an insight into people from the Philippines who turned to Axie Infinity during the COVID-19 pandemic as a means of providing for themselves and their families.

Real World Assets

Non-fungible tokens can also be used for real-world assets. The ability to create an immutable digital certificate of asset ownership and the easily verifiable nature of NFTs provide many benefits for real world assets. It can be much easier to prove and transfer ownership of an asset with an NFT rather than with the physical object that is often expensive or impossible to transport or travel to. Some of the real world asset use cases of NFTs are real estate, intellectual property, vehicles, memberships, access tickets (sports, concerts, etc), and collectibles.

Domain Names

NFTs can also be used as an alternative method of issuing and managing domain names. There are two main types of blockchain-based domain names: chain-specific and backwards compatible. Chain-specific names are built on blockchains which can be accessed by users through required browser extensions. The Ethereum Naming System (ENS) provides domains that end with ".eth" which can be used to represent the blockchain address of a user. Instead of having to use an incomprehensible string of letters and digits as an address for every transaction, users can obtain a chosen, unique name to represent their public key. Backwards compatible blockchain-based domain names can be used with the existing DNS, requiring no additional browser extensions for user access. Handshake is a backwards compatible decentralized naming protocol that allows anyone to more easily create namespaces and domains.

---

[161] *Axie Infinity*, https://axieinfinity.com/.

[162] "PLAY-TO-EARN | NFT Gaming in the Philippines | Subtitles" *YouTube*, uploaded by PLAY-TO-EARN, 13 May 2021, https://www.youtube.com/watch?v=Lg5C2EbYueo.

Summary

A non-fungible token is a token that is inherently unique and has its own attributes. Non-fungible tokens serve as an immutable digital certificate of asset ownership that is stored on a blockchain. NFTs have skyrocketed in popularity in recent years. Non-fungible tokens are indivisible, unique, provide assignable and verifiable ownership, and are programmable with access to governing smart contracts. Non-fungible tokens have a broad range of use cases given their ability to easily represent verifiable ownership of an asset. Common use cases for NFTs include digital collectibles, creative works, gaming, real world assets from real estate to intellectual property, and domain names.

Review Questions

1. What is the difference between a non-fungible token and the type of token created under the ERC-20 standard?
2. How many users are able to have ownership of a non-fungible token?
3. What technology can be used to make non-fungible tokens programmable and dynamic in nature?
4. What is one benefit that non-fungible tokens and blockchain technology provide to those producing creative works?
5. How do non-fungible tokens benefit those using digital assets such as those found in video games?
6. What kind of real world assets would be best represented by a non-fungible token?

Chapter 12: Blockchain Industry Use Cases

Emerging Use Cases: Blockchain Beyond Finance

While many of the initial use cases of blockchain technology were related to financial transactions, the use cases of blockchain technology have become more diverse as the technology has evolved. It is widely expected that this trend will continue. Blockchain technology's unique benefits have sparked interest in many industries, including supply chain management and logistics, energy, voting, healthcare, legal services, and digital identity verification.

Supply Chain Management and Logistics

One of the earliest industries commonly suggested as a candidate for blockchain technology adoption besides financial services was the supply chain/logistics industry. The pairing of logistics and blockchain technology seems to make perfect sense. Once one begins to imagine an immutable and verificable history that can be made to allow for public or private viewing, the potential benefits to be derived from blockchain technology become clear.

One major benefit of blockchain technology when applied to logistics is the ability to quickly trace the recorded history of a given object. For example, Walmart ran a series of experiments with blockchain technology provided by the Hyperledger Foundation. One experiment was designed to see how long it would take to trace the origin of mangos. Compared to the time of 7 days to trace the origin of a mango under Walmart's legacy system, it only took 2.2 seconds with the implementation of blockchain technology.[163] Today, Walmart uses blockchain technology to trace more than 25 products.[164]

Walmart also introduced the use of blockchain technology to its operations in China. Walmart China partnered with VeChain to improve its traceability and provenance efforts for a variety of products.[165] VeChain is a blockchain built to address the supply chain market. VeChain's suite of enterprise tools uses its native VeChainThor Blockchain which is specifically designed to make the benefits of blockchain technology

[163]"Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric." *Hyperledger Foundation*, https://www.hyperledger.org/learn/publications/walmart-case-study.

[164]Ibid.

[165] "Walmart China Takes on Food Safety with VeChainThor Blockchain Technology. " *VeChain Foundation*, Medium, 25 June 2019, https://medium.com/vechain-foundation/walmart-china-takes-on-food-safety-with-vechainthor-blockchain-technology-b1443e0e079c

as accessible to businesses as possible. VeChain's initial focus and still a large part of its offered services revolves around supply chain management and logistics. VeChain's services enable businesses to better track and trace their inventory.[166] The use of blockchain technology allows for businesses to extend the traceability of their products to customers in a trusting manner. Consumers can use an assigned QR code or identifying number of their product to establish legitimacy and provenance of the item.

Energy

The energy industry in most parts of the world has become centralized. Power generation is often governed by state-owned production facilities or large private companies. The level of energy production needed to meet energy demand during peak hours often causes excess energy to be created during non-peak hours. The current battery infrastructure of the energy industry is not capable of retaining all excess energy created. While energy production techniques have been nearly perfected, the storage issue of this energy serves as the limiting factor. While some municipalities offer to buy excess energy from residential solar producers, the long-term success of these initiatives are limited by storage capabilities.

Recent technological advancements have made the individual production of energy possible in an affordable way. These advancements have started a movement toward individual production of energy, such as residential solar panels and personal windmills. The increased production of energy by individuals and the storage concerns of the centralized energy model shows promise for the application of decentralized technology, including blockchain technology.

With blockchain technology, decentralized, peer-to-peer energy marketplaces can be created to link the energy production and consumption of communities. In a marketplace like this, residents producing excess energy can easily, or even automatically, sell their excess energy to others looking for energy to use or store. The decentralized model removes the need for energy to travel back through the grid system to arrive back in the same community, which improves the efficiency of energy transportation. Also, decentralized energy models encourage the use of renewable energy sources as individual energy producers almost exclusively use renewables.

[166]Cryptopedia Staff. "VeChain: Blockchain's Supply Chain Management Powerhouse." *Cryptopedia*, Gemini, 28 Jan. 2022, https://www.gemini.com/cryptopedia/vechain-crypto-blockchain-supply-chain-management.

Voting

While some voting systems across the globe have introduced electronic systems in recent years, many still use paper ballots. Paper-based voting systems carry inherent inefficiencies and many electronic voting systems are often criticized for their level of security. The citizen trust of voting systems and processes of nations vary wildly around the world. While some voting systems receive criticism for methods such as absentee ballots and identity laws, others are widely known to be outright corrupt.

Elements of blockchain technology provide solutions to many popular concerns and criticism of modern-day voting systems. The immutable nature of blockchains ensure that votes are counted as they were cast. Identity and credentialized concerns can be approached with the public/private key aspect of blockchain technology. The security of blockchain systems provides a digital voting option that could offer greater security than the digital voting methods used today.

Blockchain-based voting has been introduced through pilot programs for some important elections across the world. Voatz uses blockchain technology to enable citizens to cast their vote via mobile devices. The voting application aims to provide secure vote casting on internet-connected devices away from polling stations with a trusted tallying mechanism and public verification.[167] Voatz has been piloted in the states of West Virginia, Colorado, Oregon, and Utah with the pilot in Utah being the first United States presidential election where a blockchain-based mobile phone app was used to cast a vote.[168]

Healthcare

Electronic medical records of the current healthcare system are mostly fragmented datasets. The data is largely siloed in centralized databases. Medical record releases are often done in an “all-or-nothing” way. Patient information is mostly controlled and “owned” by the provider rather than the patient. It can be difficult to gain access to one’s records and to transfer records between healthcare providers.

The siloed nature of medical records is an intentional design of the system to protect the sensitive, private medical information of patients. However, blockchain

[167] *Voatz*, https://voatz.com/.

[168] Pressgrove, Jed. “Utah County Makes History With Presidential Blockchain Vote.” *Government Technology*, 20 Oct. 2020, https://www.govtech.com/products/utah-county-makes-history-with-presidential-blockchain-vote.html.

technology might be able to provide the same level of security while also expanding patient and alternative provider accessibility. The use of encryption and digital signatures could provide adequate security of sensitive information, while enabling patients to quickly access their information.

Blockchain-based medical records can return ownership of records to patients. With ownership of their personal medical records, patients would be more in control of what information gets released to new accessors, rather than the full set of records every time. Patients would also be able to quickly access new healthcare providers, without the need to request a transfer of records from another healthcare provider.

Legal

Legal systems, even today, are filled with large amounts of often repetitive documents. The problem is exacerbated by the levels of jurisdictions in legal systems and the non-continuous nature of legal systems when crossing borders. Legal systems are notorious for the amount of time it takes to get through them. If one has the time to go through the legal system, the high costs pose an additional barrier for most people.

Smart contracts are a component of blockchain technology that holds great potential for the legal industry. The terms of a contract can be entered into a smart contract which will automatically execute for the involved parties. Smart contracts can increase the efficiency of legal processes. More efficient legal systems make it easier and cheaper for members of the public to access and navigate them.

The record keeping ability of blockchains also provides upside to the legal industry. Blockchains can store immutable records in a way that is easy to access and verify, while also making the records tamperproof. Examples of records that could be kept on a blockchain include land titles and intellectual property records.

Identity

The method of personal identification required for many consequential activities is one's Social Security number. Because of this, one number is used to validate almost all of one's important accounts, creating further complications of identity theft. Another method of personal identification is government-issued IDs. When using either of these methods, people expose a large amount of information that does not have to be revealed in order for a certain subset of their identity to be verified.

Blockchain technology can be used to safeguard your identity with additional security protections. People can also choose which pieces of their personal information

are given out, rather than the full contents of what a drivers license provides and what a Social Security number can access. Digital IDs can be used to interact with online applications in an easier way, which will only become more prevalent as online applications continue to evolve.

Civic offers product solutions for blockchain-based digital identities. The flagship identity management product of Civic is Civic pass which enables "global blockchain identity verification, IP location checks for security, and permissioned DeFi access."[169] The pseudonymous nature of popular blockchains provides privacy benefits to its users, but some blockchain-based interactions require some level of identity verification, particularly with increased regulatory efforts in the space. Decentralized applications using Civic's products can perform checks to verify the user is a real person, the location of a user's IP address and their usage of a VPN, real-world identity document verification, age verification, and screenings for sanctions.[170] Necessary information can be selectively revealed to meet the verification needed to use an application, while keeping the rest of a person's information secure.

Summary

While many of the initial use cases of blockchain technology were related to financial transactions, the use cases of blockchain technology have become more diverse as the technology has evolved. Blockchain technology's unique benefits have sparked interest in many industries, including supply chain management and logistics, energy, voting, healthcare, legal services, and digital identity verification.

One of the earliest industries commonly suggested as a candidate for blockchain technology adoption besides financial services was the supply chain/logistics industry. Blockchain technology can improve the traceability and provenance of supply chain efforts. The centralized structure of the energy industry and the recent improvements in the ability for individuals to produce their own power present an opportunity for blockchain technology to be applied in the energy industry. With blockchain technology, decentralized, peer-to-peer energy marketplaces can be created to link the energy production and consumption of communities.

Blockchain technology also provides solutions to many popular concerns and criticism of modern-day voting systems. The immutable nature of blockchains ensure

[169]Hart, Chris. "Civic: Digital Identity Solutions for Web3." *Cryptopedia*, Gemini, 22 Mar. 2022, https://www.gemini.com/cryptopedia/civic-identity-cvc-crypto-civic-crypto-cvc-token#section-the-civic-solution-for-blockchain-based-digital-identity.

[170]"Civic Pass." *Civic*, https://www.civic.com/

that votes are counted as they were cast. Identity and credentialized concerns can be approached with the public/private key aspect of blockchain technology, enabling a secure digital voting alternative that could offer greater security than the digital voting methods used today.

The siloed nature of medical records is an intentional design of the system to protect the sensitive, private medical information of patients. Blockchain technology might be able to provide the same level of security while also expanding patient and alternative provider accessibility. The use of encryption and digital signatures could provide adequate security of sensitive information, while enabling patients to quickly access their information.

Similarly, the legal system is fraught with long, redundant, and inefficient processes. Smart contracts are a component of blockchain technology that holds great potential for the legal industry. The terms of a contract can be entered into a smart contract which will automatically execute for the involved parties. The record keeping ability of blockchains also provides upside to the legal industry. Blockchains can store immutable records in a way that is easy to access and verify, while also making the records tamperproof.

Blockchain technology can also be used to create and manage digital identities. Blockchain technology can be used to safeguard your identity with additional security protections. When verification of a certain portion of one's identity is necessary, that information can be selectively revealed while retaining the remaining unnecessary personal information.

Review Questions

1. How could blockchain technology be applied to the supply chain industry?
2. Which components of blockchain technology would be useful in creating a peer-to-peer energy marketplace?
3. What is one aspect of blockchain technology that could provide a benefit in its application to voting?
4. What aspects of blockchain technology could help to ensure the confidentiality of patient medical records in its application to healthcare?
5. How could smart contracts be applied to the legal industry to add efficiency?

6. What kinds of decentralized applications could benefit from the use of blockchain-based digital identities?

References

Aave, https://aave.com/.

“About Polkadot, A Platform for Web3.” *Polkadot*, https://polkadot.network/about/.

“About Us.” *Polygon*, https://polygon.technology/about/.

“Acting Manhattan U.S. Attorney Announces Forfeiture of $48 Million from Sale of Silk Road Bitcoins.” *The United States Department of Justice*, 29 Sept. 2017, www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-forfeiture-48-million-sale-silk-road-bitcoins.

“Add Polygon Network.” *Polygon* | *Documentation*, https://docs.polygon.technology/docs/develop/metamask/config-polygon-on-metamask/.

Adler, David. “Silk Road: The Dark Side of Cryptocurrency.” *Fordham Journal of Corporate and Financial Law*, Fordham Law School, 21 Feb. 2018, https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/#_edn51.

Al Jawaheri, Hasam, et al. “Deanonymizing Tor hidden service users through Bitcoin transactions analysis.” *Computers & Security*, vol. 9, 2020. https://www.sciencedirect.com/science/article/pii/S0167404818309908.

Anderson, Bruce M. “The Most In-Demand Hard and Soft Skills of 2020.” *LinkedIn*, 9 Jan. 2020, www.linkedin.com/business/talent/blog/talent-strategy/linkedin-most-in-demand-hard-and-soft-skills.

“Architecture.” *Polkadot*, https://wiki.polkadot.network/docs/learn-architecture.

Augur, https://augur.net/.

“AXA Goes Blockchain with fizzy.” *AXA.com*, 13 Sept. 2017, www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy.

Axie Infinity, https://axieinfinity.com/.

Ball, James. “Silk Road: The Online Drug Marketplace That Officials Seem Powerless to Stop.” *The Guardian*, 22 Mar. 2013, www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace.

Berners-Lee, Tim, et al. “The Semantic Web.” *Scientific American*, 17 May 2001, https://web.archive.org/web/20171010210556/https://pdfs.semanticscholar.org/566c/1c6bd366b4c9e07fc37eb372771690d5ba31.pdf.

“Binance’s Token Launch Platform.” *Binance*, https://launchpad.binance.com/en.

“Bitcoin Average Transactions Per Block.” *YCharts*, https://ycharts.com/indicators/bitcoin_average_transactions_per_block.

"Bitcoin Price Today & History Chart." *Buy Bitcoin Worldwide*, www.buybitcoinworldwide.com/price/.

"BitConnect." *CoinMarketCap*, https://coinmarketcap.com/currencies/bitconnect/.

"BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme." *The United States Department of Justice*, 25 Feb. 2022, https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.

"BitConnect's Indicted Founder Satish Kumbhani Has Disappeared, SEC Says." *The Economic Times*, The Times of India, 1 Mar. 2022, https://economictimes.indiatimes.com/tech/technology/bitconnects-indicted-founder-satish-kumbhani-has-disappeared-sec-says/articleshow/89916450.cms.

Blandin, Apolline, et al. "3rd Global Cryptoasset Benchmarking Study." *University of Cambridge Judge School of Business | Cambridge Centre for Alternative Finance*, Sept. 2020, www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf.

"Block 1." *Blockchain.com*, www.blockchain.com/btc/block/1.

"Block 714032." *Blockchain.com*, https://www.blockchain.com/btc/block/714032.

"Blockchain Oracles for Hybrid Smart Contracts: Chainlink." *Chainlink*, https://chain.link/.

"Blockchain Size (MB)." *Blockchain.com*, www.blockchain.com/charts/blocks-size.

Brownworth, Anders. "Blockchain Demo." https://andersbrownworth.com/blockchain/.

Buthein, Vitalik. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." *Ethereum*, 2014, https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_White_Paper_-_Buterin_2014.pdf.

"Cambridge Bitcoin Electricity Consumption Index (CBECI) | Bitcoin Mining Map." *University of Cambridge Judge School of Business | Cambridge Centre for Alternative Finance*, https://ccaf.io/cbeci/mining_map.

"Cambridge Bitcoin Electricity Consumption Index (CBECI) | Comparisons." *University of Cambridge Judge School of Business | Cambridge Centre for Alternative Finance*, https://ccaf.io/cbeci/index/comparisons.

"Cardano monetary policy." *Cardano Docs*, https://docs.cardano.org/explore-cardano/monetary-policy.

"Cardano vs Ethereum." *Kraken*, www.kraken.com/en-us/compare/cardano-vs-ethereum.

"Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric." *Hyperledger Foundation*, https://www.hyperledger.org/learn/publications/walmart-case-study.

Chainalysis Team. "Chainalysis in Action: US Government Agencies Seize More than $1 Billion in Cryptocurrency Connected to Infamous Darknet Market Silk Road." *Chainalysis*, 5 Nov. 2020, https://blog.chainalysis.com/reports/silk-road-doj-seizure-november-2020/.

Chainalysis Team. “Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity.” *Chainalysis*, 6 Jan. 2022, https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.

“Chainlink.” *CoinMarketCap*, https://coinmarketcap.com/currencies/chainlink/.

“Civic Pass.” *Civic*, https://www.civic.com/

CLEMENT, Alexandre. “fizzy by AXA: Ethereum Smart Contract in details.” *Medium*, 24 May 2019, medium.com/@humanGamepad/fizzy-by-axa-ethereum-smart-contract-in-details-40e140a9c1c0. “Collator.” *Polkadot*, https://wiki.polkadot.network/docs/learn-collator.

CoinMarketCap, https://coinmarketcap.com/.

Compound, https://compound.finance/.

“Cross-Consensus Message Format (XCM).” *Polkadot*, https://wiki.polkadot.network/docs/learn-crosschain.

Cryptopedia Staff. “VeChain: Blockchain's Supply Chain Management Powerhouse.” *Cryptopedia*, Gemini, 28 Jan. 2022, https://www.gemini.com/cryptopedia/vechain-crypto-blockchain-supply-chain-management.

Cryptopedia Staff. “What Was The DAO?” *Cryptopedia*, Gemini, 16 Mar. 2022, www.gemini.com/cryptopedia/the-dao-hack-makerdao.

Dai Stats, https://daistats.com/.

Dale, Brady. “Compound Changes Comp Distribution Rules Following 'Yield Farming' Frenzy.” *CoinDesk*, 30 June 2020, www.coindesk.com/tech/2020/06/30/compound-changes-comp-distribution-rules-following-yield-farming-frenzy/.

Dale, Brady. “Uniswap's Retroactive Airdrop Vote Put Free Money on the Campaign Trail.” *CoinDesk*, 3 Nov. 2020, https://www.coindesk.com/business/2020/11/03/uniswaps-retroactive-airdrop-vote-put-free-money-on-the-campaign-trail/.

“Decentralized Data Feeds for Hybrid Smart Contracts: Chainlink.” *Chainlink*, https://chain.link/data-feeds.

“Discover Terra | What are Terra stablecoins.” *Terra*, https://www.terra.money/intro-to-terra.

Edelman, Gilad. “What Is web3, Anyway?” *Wired*, 29 Nov. 2021, www.wired.com/story/web3-gavin-wood-interview/.

Erb, Kelly Phillips. “IRS Will Pay up to $625,000 If You Can Crack Monero, Other Privacy Coins.” *Forbes*, 14 Sept. 2020, www.forbes.com/sites/kellyphillipserb/2020/09/14/irs-will-pay-up-to-625000-if-you-can-crack-monero-other-privacy-coins/?sh=19335c1f85cc.

“ERC Token Standards.” *EthHub*, https://docs.ethhub.io/built-on-ethereum/erc-token-standards/what-are-erc-tokens/#:~:text=ERCs%20.

"Ethereum Energy Consumption Index." *Digiconomist*, https://digiconomist.net/ethereum-energy-consumption.

"Ethereum Mainnet Statistics." *Ethernodes.org*, https://ethernodes.org/.

"Ethereum Upgrades (Formerly 'eth2')." *Ethereum.org*, https://ethereum.org/en/upgrades/.

Ethereum.org Team. "The Great Renaming: What Happened to eth2?" *Ethereum Foundation Blog*, 24 Jan. 2022, https://blog.ethereum.org/2022/01/24/the-great-eth2-renaming/.

Falkon, Samuel. "The Story of the Dao - Its History and Consequences." *Medium*, The Startup, 24 Dec. 2017, https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.

"Forgot Your Pin Code? – Ledger Support." *Ledger*, 1 Apr. 2022, https://support.ledger.com/hc/en-us/articles/4405737674129-Forgot-your-PIN-code-?support=true .

"Framework for "Investment Contract" Analysis of Digital Assets." *U.S. Securities and Exchange Commission*, 3 Apr. 2019, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

"Getting Started." *Polkadot*, https://wiki.polkadot.network/docs/getting-started.

Göthberg, David. "Hash Tree.png." *Public Domain*, 20 Aug. 2005, https://commons.wikimedia.org/wiki/File:Hash_tree.png.

Greenberg, Andy. "Feds Seized $1 Billion in Stolen Silk Road Bitcoins." *Wired*, 5 Nov. 2020, www.wired.com/story/feds-seize-billion-stolen-silk-road-bitcoin/#:~:text=According%20to%20the%20IRS%27s%20criminal,downfall%20in%20October%20of%202013.

Hamacher, Adriana. "What Are Flash Loans? The DeFi Lending Phenomenon Explained." *Decrypt*, 28 June 2021, https://decrypt.co/resources/what-are-flash-loans-the-defi-lending-phenomenon-explained.

Hart, Chris. "Civic: Digital Identity Solutions for Web3." *Cryptopedia*, Gemini, 22 Mar. 2022, https://www.gemini.com/cryptopedia/civic-identity-cvc-crypto-civic-crypto-cvc-token#section-the-civic-solution-for-blockchain-based-digital-identity.

Hinman, William. "Digital Asset Transactions: When Howey Met Gary (Plastic)." *U.S. Securities and Exchange Commission*, 14 June 2018, https://www.sec.gov/news/speech/speech-hinman-061418.

"History." *Solana Documentation*, https://docs.solana.com/history.

"How Is Coinbase Insured?" *Coinbase*, https://help.coinbase.com/en/coinbase/other-topics/legal-policies/how-is-coinbase-insured.

"How It Works." *Zcash*, https://z.cash/technology/.

Ingram, Jonathan A., "Response of the Division of Corporation Finance, Re: TurnKey Jet, Inc." *U.S. Securities and Exchange Commission*, 2 Apr. 2019, https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.

"Introduction to Chainlink VRF: Chainlink Documentation." *Chainlink*, https://docs.chain.link/docs/chainlink-vrf/.

"Introduction to Ethereum Improvement Proposals (EIPs)." *Ethereum.org*, 10 May 2022, https://ethereum.org/en/eips/.

Jackson, Joab. "Simple Google Search Outed Alleged Silk Road Founder." *Computerworld*, 27 Jan. 2015, www.computerworld.com/article/2875974/simple-google-search-outed-alleged-silk-road-founder.html.

Kasireddy, Preethi. "How does Ethereum work, anyway?" *Preethi Kasireddy*, 13 Sept. 2017, https://www.preethikasireddy.com/post/how-does-ethereum-work-anyway.

Ledger, https://www.ledger.com/.

"Ledger Nano X vs Ledger Nano S plus - Hardware Wallets Comparison." *Ledger*, https://shop.ledger.com/pages/hardware-wallets-comparison.

Lee, Dave. "Silk Road: How FBI closed in on suspect Ross Ulbricht." *BBC,* https://www.bbc.com/news/technology-24371894.

"Liquidation." *MakerDAO*, https://makerdao.world/en/learn/vaults/liquidation/.

Polygon, https://polygon.technology/.

Polygon Team. "The Eco-Friendly Blockchain Scaling Ethereum." *Polygon*, 28 Apr. 2021, https://blog.polygon.technology/polygon-the-eco-friendly-blockchain-scaling-ethereum-bbdd52201ad/.

"Polygon PoS Chain Average Block Time Chart." *Polygonscan*, https://polygonscan.com/chart/blocktime.

"Proof of Stake." *Why Cardano*, https://why.cardano.org/en/introduction/proof-of-stake/.

"Maker." *DeFi Pulse*, https://www.defipulse.com/projects/maker.

"Making History, Again: Polkadot Auctions 1-5." *Polkadot*, https://polkadot.network/blog/making-history-again-polkadot-auctions-1-5/.

Manly, Ronan. "Dawn of Bitcoin Price Discovery 2009 – 2011: The Very Early Bitcoin Exchanges." *BullionStar*, 28 Jan. 2021, www.bullionstar.com/blogs/ronan-manly/dawn-of-bitcoin-price-discovery-2009-2011-the-very-early-bitcoin-exchanges/.

Metamask, https://metamask.io/.

"Moderopedia: Ring CT." *Monero*, https://www.getmonero.org/resources/moneropedia/ringCT.html.

"Moderopedia: Ring Signatures." *Monero*, https://www.getmonero.org/resources/moneropedia/ringsignatures.html.

"Moderopedia: Stealth Addresses." *Monero*, https://www.getmonero.org/resources/moneropedia/stealthaddress.html.

Mougayar, William. *The Business Blockchain.* Hoboken: John Wiley & Sons, 2016

"Network Supply." *Solana Beach*, https://solanabeach.io/supply.

"Order Instituting Administrative and Cease-And-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-And-Desist Order in the Matter of Tomahawk Exploration LLC and David Thompson Laurance." *Securities and Exchange Commission*, 14 Aug. 2018, https://www.sec.gov/litigation/admin/2018/33-10530.pdf.

"Order Instituting Cease-And-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, Making Findings, and Imposing a Cease-And-Desist Order in the Matter of Nebulous, Inc." *Securities and Exchange Commission*, 30 Sept. 2019, https://www.sec.gov/litigation/admin/2019/33-10715.pdf.

Pagliery, Jose. "Bitcoin fallacy led to Silk Road founder's conviction." *CNN Business*, https://money.cnn.com/2015/02/05/technology/security/bitcoin-silk-road/.

"Parachain Slot Auctions." *Polkadot*, https://polkadot.network/auctions/.

"PLAY-TO-EARN | NFT Gaming in the Philippines | Subtitles" *YouTube*, uploaded by PLAY-TO-EARN, 13 May 2021, https://www.youtube.com/watch?v=Lg5C2EbYueo.

"Polkadot." *CoinMarketCap*, https://coinmarketcap.com/currencies/polkadot-new/.

"Polkadot: Are You Ready to Start Building?" *YouTube*, uploaded by Polkadot, 15 July 2020, https://www.youtube.com/watch?v=_-k0xkooSlA.

"Polkadot Consensus: Nominated Proof of Stake." *Polkadot*, https://wiki.polkadot.network/docs/learn-consensus#nominated-proof-of-stake.

"Pool Distribution." *BTC.com*, https://btc.com/stats/pool?pool_mode=day3.

PoolTogether, https://pooltogether.com/.

Pozzi, Daniele. "Ico Market 2018 vs 2017: Trends, Capitalization, Localization, Industries, Success Rate." *Cointelegraph*, 5 Jan. 2019, https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate.

Pressgrove, Jed. "Utah County Makes History With Presidential Blockchain Vote." *Government Technology*, 20 Oct. 2020, https://www.govtech.com/products/utah-county-makes-history-with-presidential-blockchain-vote.html.

"Reachable Bitcoin Nodes." *Bitnodes*, https://bitnodes.io/.

Redman, Jamie. "A Deep Dive into Satoshi's 11-Year Old Bitcoin Genesis Block – Featured Bitcoin News." *Bitcoin News*, 3 Jan. 2020, https://news.bitcoin.com/a-deep-dive-into-satoshis-11-year-old-bitcoin-genesis-block/.

"Rewards." *Polygon* | *Documentation*, https://docs.polygon.technology/docs/maintain/validator/rewards.

Roberts, Jeff John, and Nicolas Rapp. “Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says.” *Fortune*, 25 Nov. 2017, https://fortune.com/2017/11/25/lost-bitcoins/.

“Ross Ulbricht, Aka Dread Pirate Roberts, Sentenced to Life in Federal Prison for Creating, Operating 'Silk Road' Website.” *U.S. Department of Homeland Security | U.S. Immigration and Customs Enforcement*, 29 May 2015, www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating.

“SEC Orders Blockchain Company to Pay $24 Million Penalty for Unregistered ICO.” *U.S. Securities and Exchange Commission*, 30 Sept. 2019, https://www.sec.gov/news/press-release/2019-202.

“Security.” *Coinbase*, https://www.coinbase.com/security.

Shannon, Victoria. “A 'More Revolutionary' Web.” *The New York Times*, 23 May 2006, www.nytimes.com/2006/05/23/technology/23iht-web.html.

“Shard Chains.” *Ethereum.org*, 10 May 2022, https://ethereum.org/en/upgrades/shard-chains/.

Sharma, Madhurkant. “Web 1.0, Web 2.0 and Web 3.0 with Their Difference.” *GeeksforGeeks*, 27 Jan. 2022, www.geeksforgeeks.org/web-1-0-web-2-0-and-web-3-0-with-their-difference/.

Shen, Muyao. “Uniswap Recaptures DeFi Buzz With UNI Token's Airdropped Debut.” *CoinDesk*, 17 Sept. 2020, https://www.coindesk.com/markets/2020/09/17/uniswap-recaptures-defi-buzz-with-uni-tokens-airdropped-debut/.

Solana, https://solana.com/.

Sykes, Jay B., “Securities Regulation and Initial Coin Offerings: A Legal Primer.” *Congressional Research Service*, 31 Aug. 2018, https://sgp.fas.org/crs/misc/R45301.pdf.

“Technology: A Scalable, Interoperable & Secure Network Protocol for the Next Web.” *Polkadot*, https://polkadot.network/technology/.

“Terra | Programmable Money For The Internet.” *Terra*, https://www.terra.money/.

“The Dao of Accrue.” *The Economist*, 19 May 2016, www.economist.com/finance-and-economics/2016/05/19/the-dao-of-accrue.

“The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System.” *MakerDAO*, https://makerdao.com/en/whitepaper/.

“The Official Etherscan Beacon Chain Ethereum 2.0 Explorer.” *BeaconScan*, Etherscan, https://beaconscan.com/.

Thielman, Sam. “Silk Road Operator Ross Ulbricht Sentenced to Life in Prison.” *The Guardian*, 29 May 2015, www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced.

“Top 100 Richest Bitcoin Addresses and Bitcoin Distribution.” *BitInfoCharts*, https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html.

“Top Cryptocurrency Spot Exchanges.” *CoinMarketCap*, https://coinmarketcap.com/rankings/exchanges/.

"Transparency." *Tether*, https://tether.to/en/transparency.

"Transparency: Reports and Reserves." *Tether*, https://tether.to/en/transparency.

Uniswap, https://uniswap.org/.

United States District Court, Southern District of New York. *Securities and Exchange Commission v. BitConnect*. https://www.sec.gov/litigation/complaints/2021/comp-pr2021-172.pdf.

United States District Court, Southern District of New York. *United States of America v. Ross William Ulbricht*. https://antilop.cc/sr/trial/.

"USD Coin (USDC) | Digital Dollars for Global Business." *Circle*, https://www.circle.com/en/usdc.

Vermaak, Werner. "What is Yield Farming?" *CoinMarketCap*, https://coinmarketcap.com/alexandria/article/what-is-yield-farming.

Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, Ian Norden, Abdelhamid Bakhta, "EIP-1559: Fee market change for ETH 1.0 chain," *Ethereum Improvement Proposals*, no. 1559, April 2019. [Online serial]. Available: https://eips.ethereum.org/EIPS/eip-1559.

Voatz, https://voatz.com/.

"Walmart China Takes on Food Safety with VeChainThor Blockchain Technology. " *VeChain Foundation*, Medium, 25 June 2019, https://medium.com/vechain-foundation/walmart-china-takes-on-food-safety-with-vechainthor-blockchain-technology-b1443e0e079c

"Watch the Burn: EIP-1559 Real-Time Eth Burn Visualization for Ethereum." *Watch The Burn*, https://watchtheburn.com/.

"What Are Zk-Snarks?" *Zcash*, https://z.cash/technology/zksnarks/.

"What Is Monero (XMR)?" *Monero*, www.getmonero.org/get-started/what-is-monero/.

Whittaker, Zack. "DOJ Says It Seized over $1 Billion in Bitcoin from the Silk Road Drugs Marketplace." *TechCrunch*, 5 Nov. 2020, https://techcrunch.com/2020/11/05/justice-department-silk-road-billion-bitcoin/.

"Who Is a Delegator." *Polygon* | *Documentation*, https://docs.polygon.technology/docs/maintain/polygon-basics/who-is-delegator.

"Who is a Validator." *Polygon* | *Documentation*, https://docs.polygon.technology/docs/maintain/polygon-basics/who-is-validator.

"Why use Cardano?" *Cardano Docs*, https://docs.cardano.org/new-to-cardano/why-use-cardano.

"Zcash (ZEC)." *Coinbase*, https://help.coinbase.com/en/coinbase/getting-started/crypto-education/zcash-zec-faq.