Bitcoin: Critical Analysis of a Decentralized Monetary System

Rano Marufova

Department of Computer Science and Math and Department of Business, Washington College

Senior Capstone Experience

Dr. Kyle Wilson (Computer Science) and Dr. Maria Vich (Business Management)

December 4, 2023

Acknowledgements

I am endlessly grateful for my family who have always been with me and supported me although we were physically 6500 miles away. Their belief in my abilities and love has been making me move forward.

I am also thankful for my advisors Dr. Kyle Wilson and Dr. Maria Vich, who have led me through the process of my college education and completion of my SCE project. Their insightful feedback and mentorship have been instrumental in shaping this work.

Table of Contents

Introduction.

Money has always been a very important element in the history of mankind. While early civilizations had economics based on bartering – the direct exchange of goods and services, it had many flaws that complicated the exchange process. That has led to money being invented all around the world in all the places where people formed communities. The fact that it was invented in isolation in different parts of the world implies that it's directly connected to the very idea of civilization.

Bitcoin as money is a very new concept that is the result of a long chain of changes in the way people perceive and use money. Money has taken many shapes and forms across human history. The shift from metal coins to paper can be classified as one of those crucial shifts, which would solve issues such as the storage and transportation of money. A bigger revolution was brought by debit and credit cards, turning paper into numbers that we see on our screens or ATMs when we check our accounts. Card payments have saved people from the problem of transferring money all around the world and dealing with small changes. Each time the new form of currency would solve the issues of the previous one and therefore was quickly accepted by the public. However, as the system was updated, new problems would come to the surface, that caused inconvenience for some while did not bother others.

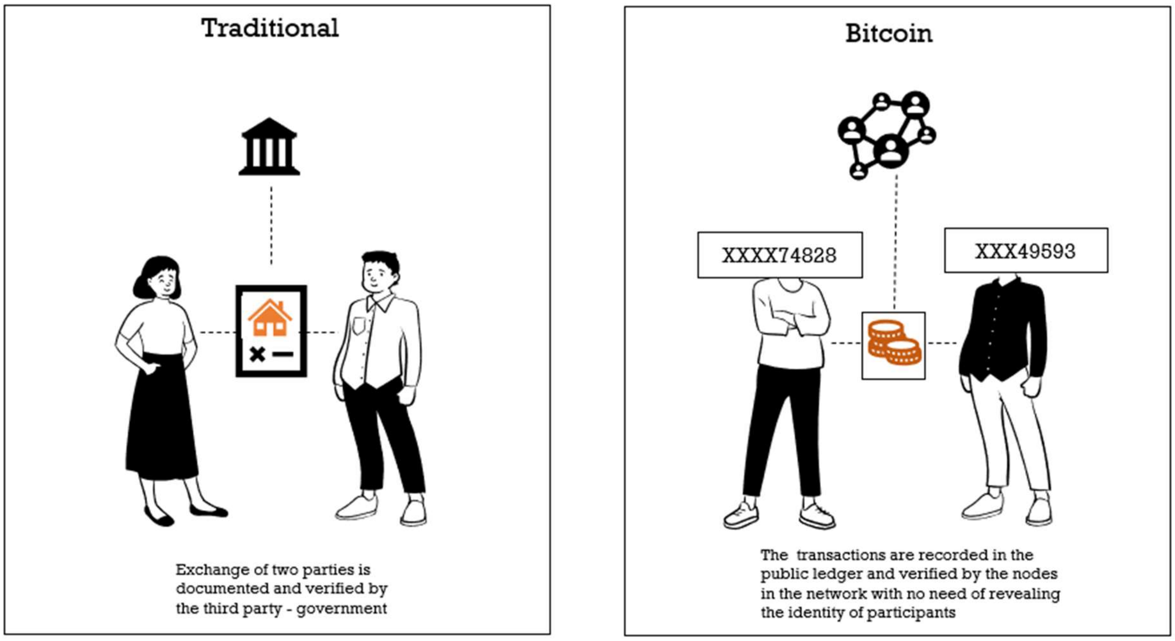
Bitcoin (BTC) was designed to be a form of money free from the control of any government or institution. Governments have always served as a form of authority over the production and circulation of money. While earlier people saw this oversight as a form of protection from fraud and economic instability, in the modern days some people began to see it as a restriction of personal freedom. Unlike traditional transactions where the exchange parties can be easily traced, Bitcoin operates on a decentralized system, offering a level of financial autonomy not subject to government authority. Bitcoin's innovation lies in its blockchain technology, which enables peer-to-peer transactions without the need for intermediaries like banks or governments. This decentralized nature offers users a level of financial autonomy and privacy that traditional systems struggle to match. Bitcoin transactions are recorded on a public ledger, the blockchain, but the identities of the parties involved remain pseudonymous. This pseudonymity, combined with cryptographic security, provides a solution to the perceived limitations of traditional financial systems (Nakamoto, 2008).

However, the main reason for the current popularity of Bitcoin is something else – the possibility to rapidly increase the value of the investment. The rapid growth of the value of Bitcoin attracted people to buy the currency and save it as an investment rather than a payment.

Chapter I. Bitcoin Overview

The white paper which defines Bitcoin, titled "Bitcoin: A Peer-to-Peer Electronic Cash System", was published in 2008, by a person or group of people under the name of Satoshi Nakamoto on Bitcoin.org (Nakamoto, 2008). The pseudonymous author also provided an accompanying open-source software implementation. The paper's primary objective was to present the core idea behind cryptocurrency and how it could potentially revolutionize the landscape of financial transactions, particularly by addressing the inherent privacy concerns associated with traditional fiat currency, issued and regulated by governments. One of the biggest differences is that the participants of the transactions are fully anonymous, under pseudonyms that they use as their addresses. People on either side of the transaction are unaware of the identity of one another (Nakamoto, 2008).

One of the most distinguishing features outlined in the white paper is the concept of fully anonymous transactions within the Bitcoin network (Nakamoto, 2008). Unlike conventional financial systems where personal identities are often tied to transactions, Bitcoin transactions are pseudonymous. They are recorded on an immutable public ledger, known as the blockchain, but without direct links to individuals' real-world identities. This key innovation of pseudonymity, while not complete anonymity, offers a level of privacy that was previously absent from the world of digital financial transactions. It allows users to conduct peer-to-peer transactions without divulging their personal information (See Figure 1), thus addressing concerns about privacy and security in financial exchanges.



Traditional

Exchange of two parties is documented and verified by the third party - government

Bitcoin

The transactions are recorded in the public ledger and verified by the nodes in the network with no need of revealing the identity of participants

Figure 1. Traditional Exchange of Property vs. Bitcoin Exchange. The traditional exchange entails connecting one's name to a transaction while Bitcoin allows using pseudonyms that are not connected to a person's identity in any way.

At its core, Bitcoin challenges the conventional understanding of money. Unlike physical currencies, such as banknotes or coins, Bitcoin is intangible and only exists as lines of code stored on a decentralized network. These digital coins are stored in the users' digital wallet, which serves as a repository for Bitcoin holdings. This wallet can be managed through a multitude of methods and platforms, each offering unique features and degrees of control. Bitcoins can be received into the wallet in one of two ways - receiving the Bitcoin from another person's wallet address or participating in on the Proof-of-Work process as a miner and reviewing a block reward of Bitcoins. These management techniques will be explored in depth in Section 2 of Chapter II.

Chapter II. Market Analysis

Section 1. Bitcoin Price

Price History.

The price of Bitcoin is one of the most important things that creates its value. It cannot be used for anything else since it does not possess a fundamental value.

The first Bitcoins that were created were nominally priced at $0 and obtained through mining, since that is the only to create new Bitcoins. Bitcoin's mining mechanism, which will be explained in detail in Chapter IV, operates in the way that new units are generated and validated in blocks. The initial block, mined by Bitcoin's creator Satoshi Nakamoto, contained 50 BTC. It is considered to be the first supply of Bitcoin. These coins were essentially obtained for free. However, as Bitcoin gained traction, its value experienced a gradual ascent. In the early days, the price of Bitcoin saw a modest increase, but it wasn't until February 2011 that it reached a notable milestone, hitting $1 for the first time. Subsequently, the cryptocurrency's value demonstrated remarkable volatility, surging to $10 and $30 in the following months. However, by the end of 2011, the price had dipped to under $5 (Edwards, 2023).

The first recorded purchase of goods and services using Bitcoin is a well-known story dating back to 2009. According to Wallace (2011) and other sources, the purchase was two pizzas. They were bought at the cost of 10,000 bitcoins, which were initially purchased for the price of $50. Notably, the pizza company didn't directly accept bitcoins as payment. Instead, a third-party intermediary was involved. This intermediary agreed to use a credit card (a traditional currency) to pay for the pizzas and, in exchange, received the 10,000 bitcoins. The intermediary person bought those pizzas and send them to the agreed address (Yermack, 2013). To put this into perspective, at recent Bitcoin prices, those 10,000 bitcoins would be worth over 250 million dollars after 14 years in September of 2023 (note that price for a single Bitcoin has ranged between $10,000 - $37,000 in 2023). This shows how the value of Bitcoin is now increased many times.

It's important to note that the current high price is observed after many fluctuations in the process. Since its inception, it has witnessed both substantial gains and periodic declines. Notably, its value surged over the years, reaching a pinnacle at $68,789.63 in November of 2021. For a comprehensive overview of Bitcoin's price evolution, refer to Figure 2, which illustrates the fluctuating of exchange rate of BTC to USD over the years. Dramatic increases in the value of the coin, have usually been followed by big drops right after.

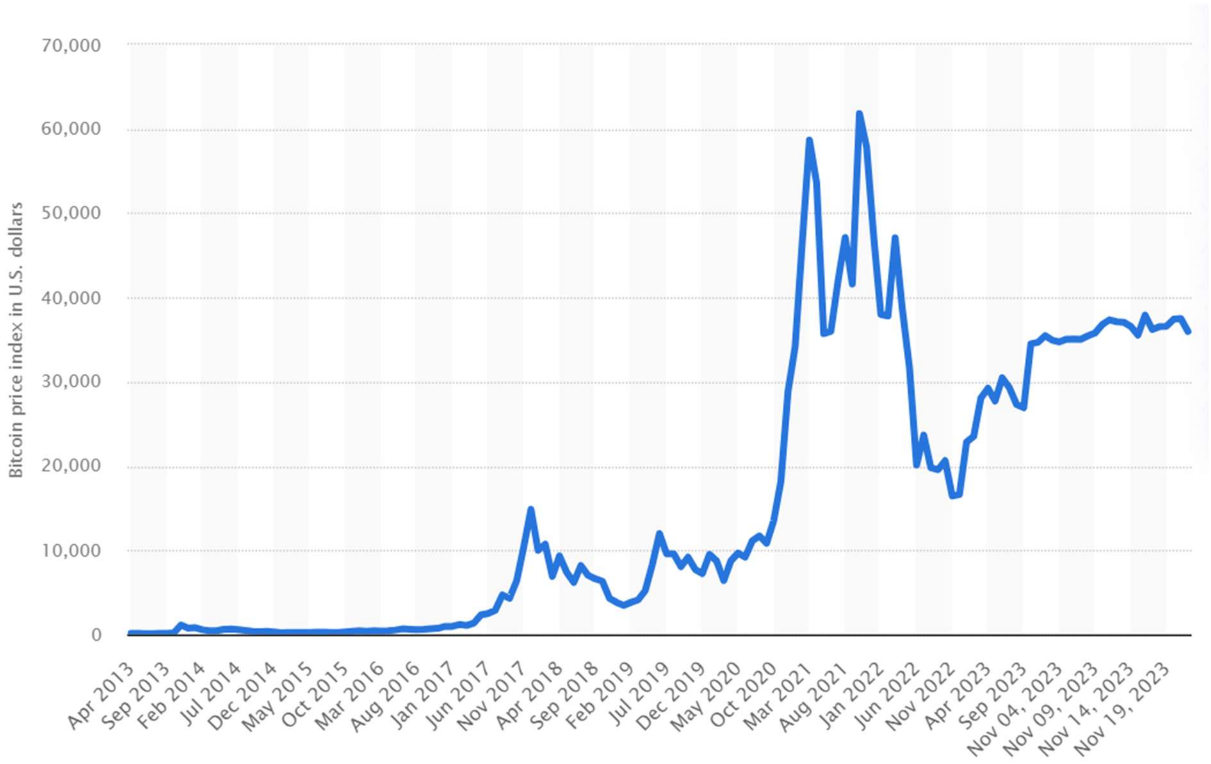


Figure 2. Bitcoin USD exchange rate (2013-2023). Source: Statista.com

As of September 2023,[1], a single BTC costs $26,274. The market value of Bitcoin is $512.10B and there are 19,000,000 Bitcoins in circulating supply. There are many factors that influence the price of Bitcoin, which makes it extremely challenging to predict.

Market Volatility

The data shows that Bitcoin has a very high market volatility[2], which indicates that the price tends to experience significant fluctuations over short periods.The Figure 3, shows the comparison of Bitcoin's volatility to other popular investment assets. Bitcoin tends to have a

[1] For the purpose of this paper, we will be using the prices from September of 2023, because of the fast changing nature of Bitcoin's price

[2] In finance, volatility usually refers to the rate at which a financial variable, such as stock price, moves up or down over time. Volatility is measured by the standard deviation or, sometimes, by the variance. The (absolute) empirical volatility of a stock price is usually calculated as the annualized standard deviation of daily change in price. A measure of the volatility of a stock relative to the market is its beta coefficient (Hashimzade, 2017).

visibly large volatility, sometimes it being 10 times bigger than for other assets. According to Zimmerman (2019), the reason for Bitcoin’s high volatility is partially because of the unique characteristics of the currency.

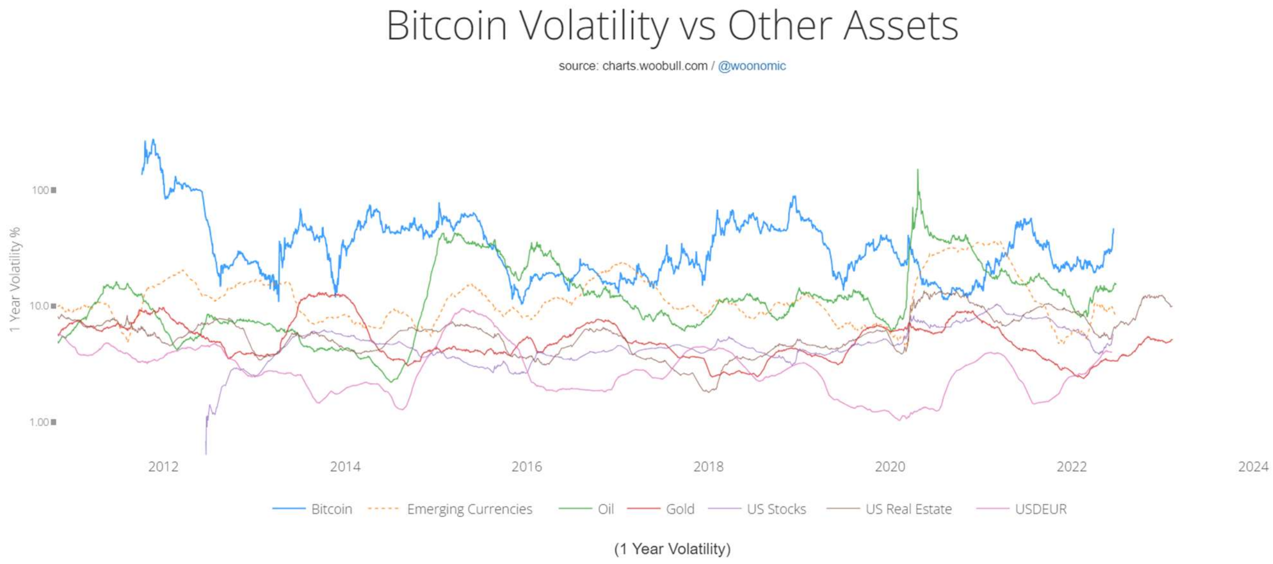


Figure 3. Price Volatility Comparison of Bitcoin to other Assets (Logarithmic scale). The graph shows that Bitcoin has historically had more volatility than the other assets, sometimes it being 10x higher. Source: charts.woobull.com

The analyses that have been conducted on the market suggest that there are two key drivers of Bitcoin's demand: transactional and speculative demand. Transactional demand comes from those who use Bitcoin for everyday payments, while speculative demand is driven by investors hoping to profit from price fluctuations (Nguyen, 2018).

Bitcoin's demand is on the rise due to its increasing scarcity, as the limited supply becomes a driving force. Wealthier investors tend to hold onto their Bitcoin for the long term, limiting the exposure of those with fewer assets. According to the National Bureau of Economic Research, a significant concentration of one-third of all Bitcoins was in the hands of the top 10,000 investors by the end of 2020 (Reiff, 2023).

The speculative demand results to crowding out. The phenomenon of crowding out, where increased participation diminishes the cryptocurrency's utility as a means of payment, leads the market maker to lower her expectations about the cryptocurrency's value, resulting in a lower market price—this is known as the pecuniary effect. The demand curve for cryptocurrencies can exhibit a local upward slope due to the potential impact of buy-side speculation on reducing prices, making price formation distinctly different from traditional assets. This pecuniary effect contributes to price volatility. When crowding out occurs, the market maker, anticipating a lower cryptocurrency value, adjusts the price more significantly if there is a positive order flow observed later. This heightened sensitivity to order flow contributes to the intrinsic feature of high price volatility in any monetary asset settled on a blockchain. Notably, a cryptocurrency with lower blockchain capacity tends to experience greater volatility (Zimmerman 2019).

Market sentiment plays a significant role in Bitcoin's price movements. Positive news in the media and optimism can drive up prices, while negative sentiment can lead to price drops. These factors are considered unconventional indicators, since they suggest that the prices are dependent on the sentiment rather than the practical qualities of the currency (Nguyen, 2018).

Risk of Liquefying

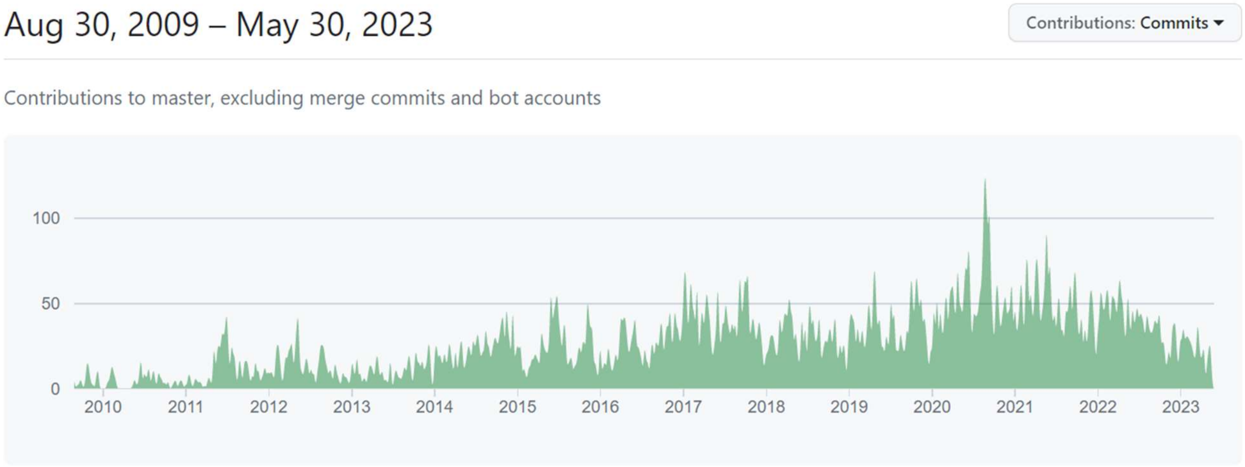
Individuals owning more than 10 million BTC — known as whales — hold outsized influence on Bitcoin’s volatility. The manner in which these whales could liquidate their substantial positions into fiat currency without causing a significant impact on Bitcoin's market price remains unclear. A sudden sell-off by these whales could trigger panic among other investors, resulting in a sharp decline in prices, which would negatively impact the Bitcoin whales on the bigger scale than other players in the market (Reiff, 2023).

To manage the potential impact of large-scale liquidation, most exchanges impose daily limits, typically around $50,000. For investors holding thousands of Bitcoins, this limitation could pose challenges in liquidating their assets quickly enough to prevent substantial losses. In a scenario where Bitcoin prices hover around $50,000, a larger investor might only be able to liquidate one coin per day. This slow pace of liquidation could lead to a cascade effect, with other investors selling and causing prices to plummet rapidly, resulting in significant and sudden losses (Reiff, 2023)

Section 2. Bitcoin Exchange and Use

Bitcoin Core is the default software for exchanging coins within the network. It was developed by Satoshi Nakamoto, the creator of Bitcoin, to serve as a reference implementation for Bitcoin transactions. It was first published on GitHub.com[3]. The code is available for public download and contribution. Since the launch, the software has been constantly updated by the many voluntary contributors and the scale of those contributions over the years can be observed on Figure 4. Those updates have been consistent over the years, and they are still ongoing.

[3] GitHub.com – is an online platform used for software development and version control.



Aug 30, 2009 – May 30, 2023

Contributions to master, excluding merge commits and bot accounts

Figure 4. The graph of contributions to Bitcoin Software on GitHub.com over the years (2009-2023). The graph includes the bug fixes and improvements made by developers. The x-axis of the graph represents the years, and the y-axis shows the number of commits – the changes that were made by the developers.

However, those improvements did not focus on user-friendly software. Saving the keys, finding the buyers and managing funds might be challenging for a person who is not familiar with the use of such technology. Therefore, many people start off by using Crypto Apps and Exchanges (Forbes, 2023). Despite the decentralized nature of Bitcoin, most transactions happen in centralized exchanges. Those exchanges are enabled through the Bitcoin Trading Software provided by different companies. The main reason for this is that the decentralized exchange is not user-friendly. In those platforms, users treat Bitcoins and other cryptocurrencies as an alternative to stocks rather than a tool for anonymous money exchange.

The user's approach to Bitcoin in centralized exchanges stated above is not unreasonable. Trading Bitcoin operates in a manner similar to trading stocks, particularly on a limit order book market. In both cases, participants can place orders to buy or sell assets. Unlike some traditional stock markets where market makers facilitate trades by providing liquidity, Bitcoin trading platforms do not act as market makers. Instead, traders themselves post market or limit orders.

The Bitcoin market is fully transparent about the total available volume and price of the offer. In the Bitcoin market, the minimum tick size [4]is 0.01 units of the base currency, which means that prices can change in increments of 0.01 (Dimpfl, 2017).

Wallet and Money Services

Bitcoin wallets serve as the secure repositories for the private keys necessary to access and manage bitcoin addresses. They come in various forms, including software wallets (desktop, mobile, and web-based), hardware wallets (physical devices designed for secure storage), and paper wallets (physical documents with printed keys). Each type has its advantages and trade-offs in terms of security and convenience.

Desktop Wallets. Desktop wallets, like Bitcoin Core and Armory, are software applications installed on personal computers. Bitcoin Core, for instance, serves as a full node, allowing users to relay transactions on the network, create bitcoin addresses, and store private keys. Armory, tailored for enhanced security, also falls into this category. These wallets offer users control over their keys and the ability to participate in the broader Bitcoin network (Ankalkoti et al., 2017).

Mobile Wallets. Mobile wallets, such as Mycelium, operate as applications on smartphones. Unlike full clients, they don't download the entire bitcoin blockchain, making them suitable for devices with limited memory. Mobile wallets often employ simplified payment verification (SPV), downloading a smaller subset of the blockchain and relying on trusted nodes for accurate information. They facilitate on-the-go access and even enable contactless payments via near-field communication (NFC) (Ankalkoti et al., 2017).

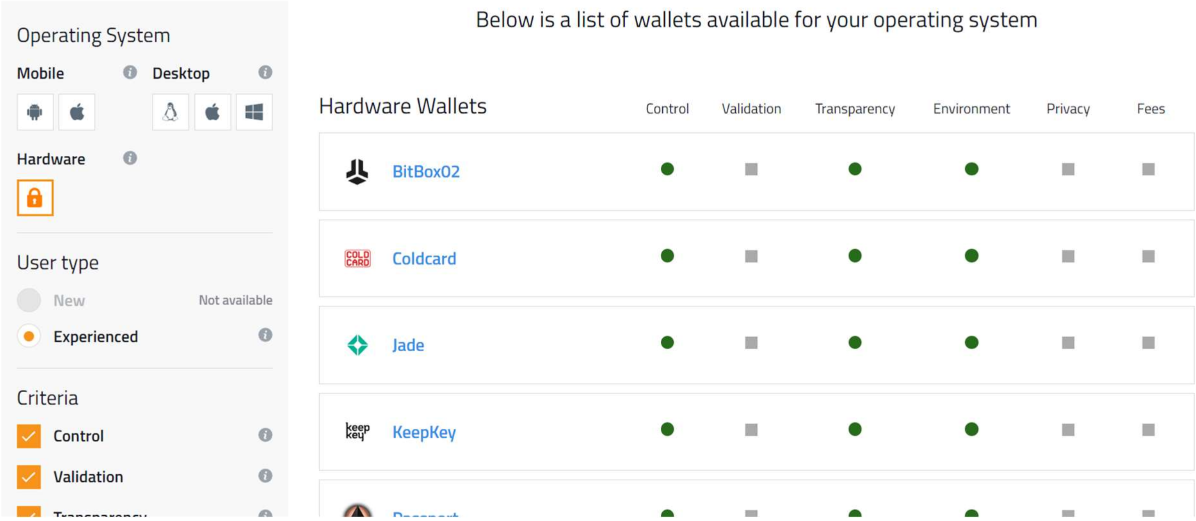
[4] Tick size is a minimum price movement of a trading instrument in a market.

Online Wallets. Online wallets store private keys on servers connected to the internet. Platforms like Coinbase, Blockchain, and Strongcoin fall into this category. While offering accessibility from any device, they introduce a trade-off as the organization running the website gains control over users' private keys. Despite this drawback, online wallets are convenient for users who prioritize accessibility and ease of use (Ankalkoti et al., 2017).

Hardware Wallets. Hardware wallets are physical devices designed to securely store private keys and facilitate bitcoin transactions. Examples include Trezor, Ledger, and KeepKey. These devices offer enhanced security, as private keys are stored offline, reducing vulnerability to cyber-attacks. Hardware wallets provide an attractive option for users with substantial bitcoin holdings seeking a balance between security and convenience (Ankalkoti et al., 2017).

Paper Wallets. Paper wallets are a cost-effective and secure means of storing bitcoins. Websites generate a bitcoin address along with QR codes for the public address and private key. The private keys are not stored digitally, providing resilience against cyber-attacks. Paper wallets are particularly favored for their simplicity and offline nature, making them immune to hardware failures or digital vulnerabilities (Ankalkoti et al., 2017).

Bitcoin.org provides a user's guide on the selection of Bitcoin Wallet software, by asking users questions about their preferences. On the Figure 5, you can see the users screen after answering the questions. The users can see their selections for the preference questions and the results based on those selections. These wallets are not issued by Bitcoin itself but offered by other independent companies.



Operating System

Mobile

Desktop

Hardware

User type

○ New Not available

● Experienced

Criteria

☑ Control

☑ Validation

☑ Transparency

Below is a list of wallets available for your operating system

Hardware Wallets	Control	Validation	Transparency	Environment	Privacy	Fees
BitBox02	●	■	●	●	■	■
Coldcard	●	■	●	●	■	■
Jade	●	■	●	●	■	■
KeepKey	●	■	●	●	■	■
Passport	●	■	●	●	■	■

Figure 5. Bitcoin.org Recommendations of Wallets. This current filter shows the Wallet recommendations selected for the experienced user who wants a hardware wallet, which fits the criteria of providing control, transparency, Environment and Validation to the user. Notably the user type "new" is not available for the users who want a hardware wallet.

Bitcoin has enabled the rise of many new businesses that use the coin as their foundation. More have taken advantage of Bitcoin to gain a bigger market by including Bitcoin exchange as their offerings. You can see a classification of companies connected to Bitcoin and Blockchain on Figure 6. This has led to Bitcoin being advertised by those companies and getting higher brand awareness. As mentioned earlier, the price of bitcoin and demand for Bitcoin are highly influenced by the media and it is in the best interest of those companies to promote Bitcoin.

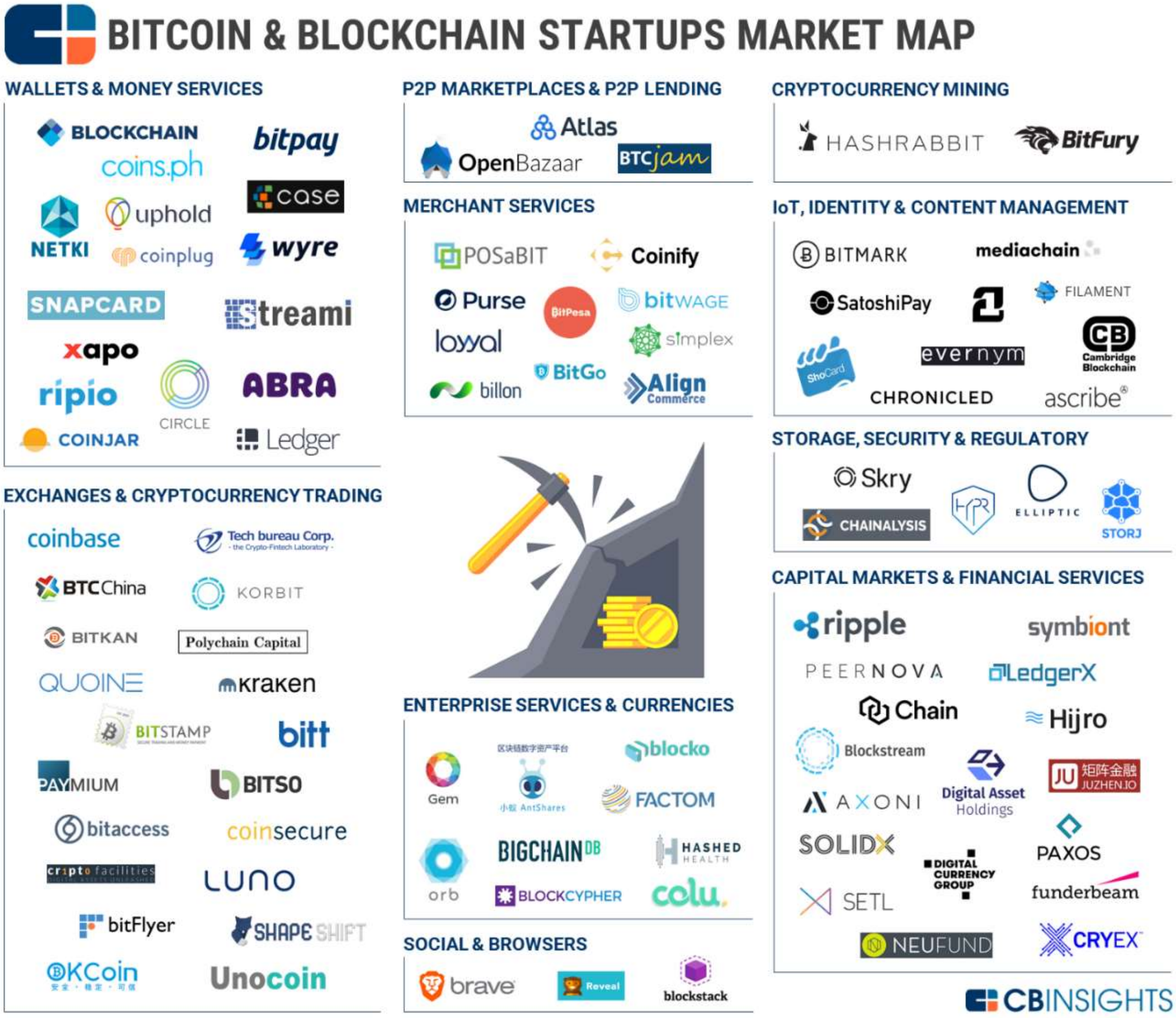


Figure 6. 95 Bitcoin & Blockchain Startups in One Market Map. Bitcoin companies offer products or services related to the trading, storing, or usage of bitcoin, while blockchain-based companies develop solutions that apply blockchain technology across sectors and verticals. Each of them is categorized by their primary area of service. Source: cbinsights.com

Chapter III. Blockchain

Section 1. What is Blockchain?

Basic concept of Blockchain

All the transaction handling processes involving Bitcoin occur only in a decentralized digital environment. This environment inherently has many potential security and trust concerns that Bitcoin has effectively mitigated.

To understand the challenges associated with digital assets, let's examine the transfer process of physical entities. In the regular system of ownership of assets, ownership is usually easy to verify. For instance, take a basic analogy of real estate property ownership transfer. In this transaction, one of the parties who is confirmed to own the property exchanges the ownership for a mutually agreed sum of money from the second party. This transaction is recorded on a legal document that lists the conditions of the transaction, signatures from both parties and a timestamp (See Figure 1). This exchange is only possible with the help of a trusted third party that ensures the validity of the exchange between these two parties participate in the trans in the transaction. The government usually operated as a third party that confirms that:

1. The property legally belongs to the first individual initiating the transaction.
2. The second person has given the money or agreed to give it within a set period of time.
3. The timestamp is valid, and ownership is transferred to a new party and cannot be sold to any other person by the previous owner.

After the transaction is completed, the government ensures that it is recorded in its system and can be located in the case of another transaction or ownership disagreement.

However, such a system of trust is seemingly unachievable with a decentralized currency, because there is no government or bank to validate transactions (Nofer, 2017).

Another problem that appears with the absence of central authority is the risk of people abusing the system by double-spending. The double spending problem in cryptocurrencies and digital cash schemes is when the same digital token is used multiple times. The problem is to ensure that the digital tokens cannot be easily duplicated or falsified. It is easy because sending a digital code to one individual does not inherently prevent someone from subsequently transmitting it to another party and attempting to claim payment from both parties. (Chohan, 2021).

Blockchain entered the financial market as a groundbreaking idea. It has effectively addressed one of the significant challenges of finance by creating a trusted shared digital ledger that is immutable. With blockchain two anonymous participants in a transaction can exchange Bitcoins without the need for mutual trust, but rather with the trust to the ledger that ensures the transaction is secure, and unalterable by of the neither of the participants nor any other parties.

Blockchain is a system of storing data in linked blocks. It is a type of digital ledger implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). The idea of blockchain and the need for such technology started in the late 1980s and early 1990s, but only in 2008 it reached its real-life implementation. It was revealed as a mathematical foundation behind Bitcoin in Satoshi Nakamoto's white paper *Bitcoin: A Peer-to-Peer Electronic Cash System*. Blockchain was a key feature of Bitcoin that has distinguished it from other cryptocurrencies attempted prior to it. Because of blockchain technology, Bitcoin has ensured security within the decentralized network and broke the political borders between transactions. After Bitcoin's success, the notion of employing blockchain technology became a blueprint for other cryptocurrencies to follow (Yaga el at., 2019).

The blockchain makes it computationally hard to falsify transactions by requiring each transaction to be confirmed by solving a challenging cryptographic problem. Instead of relying on a third party, blockchain verifies transactions by making the nodes on the network confirm or deny the transactions (Nofer, 2017). In this chapter we will gain understanding of how Bitcoin implements blockchain technology and how it ensures security of transactions in the network.

While blockchain technology offers a multitude of potential applications and uses, to this day it is predominantly used for cryptocurrencies. (Di Pierro, 2017). In this chapter we will learn about blockchain and its role in Bitcoin.

Section 2. Foundation of Blockchain.

User permissions within blockchains

Depending on the permission given to the users, uses of blockchain can be divided into two groups – permissioned and permissionless.

Permissionless blockchain networks are like digital ledgers. Anyone can read and write to them without the need for the approval of a central authority. That means anyone can download the software and use it, as well as add their own contribution to the public ledger in the form of new blocks. This creates a trust problem between users since anyone can enter false information into the ledger. To prevent this permissionless blockchains often use a multiparty agreement or ‘consensus’ system that requires users to expend or maintain resources when attempting to publish blocks. To encourage users to participate in peer-to-peer reviews to verify the transaction, Bitcoin rewards them with bitcoins. Therefore, we can classify Bitcoin as a permissionless blockchain.

In permissioned blockchain networks, only authorized users can create new blocks in the blockchain. This authority can be both centralized and decentralized. This means that access to read, and transaction privileges can be restricted to only those who are given permission (Yaga el at. 2019). One of the examples of is Ripple, currency exchange and remittance network that is open to financial institutions worldwide.

In some permissioned blockchain networks, all users must be authorized and identified – they are not anonymous. This discourages fraudulent behavior because bad actors can be identified and held accountable through legal means (Yaga el at., 2019). However, disclosing one's identity fully runs contrary to a core objective of Bitcoin.

A word about hashing

"Hashing" is a cryptographic technique at the heart of Bitcoin. We will describe it in detail in Section 3. For now, let it suffice that hashing is the process of using a particular complex formula to transform a chunk of data into a large number. Crucially, this operation is one-way: it is extraordinarily hard to recover the data given the output of hashing (Zola, 2021).

Components of a block

As mentioned above, blockchain consists of linked blocks. On Figure 7 you can see the visualization of such blocks.

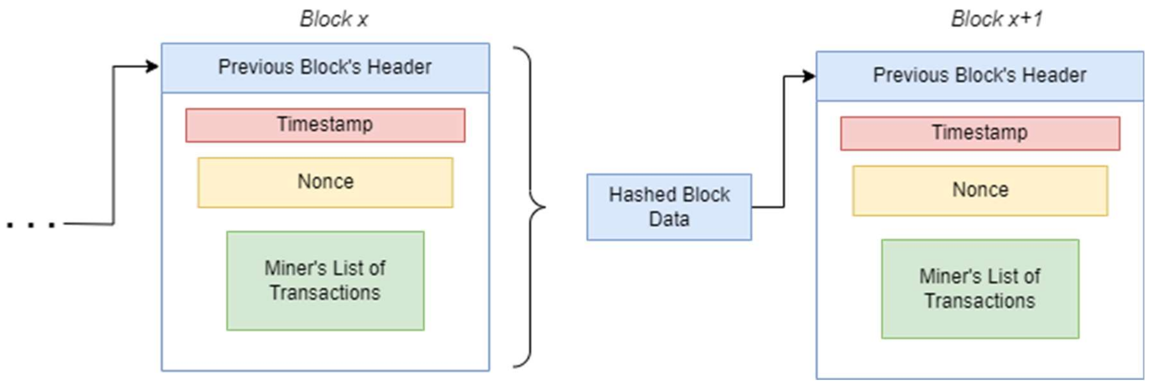


Figure 7. Block Structure. The block consists of the previous block's header which is all the information of the block hashed[5] together as one number, a timestamp, a nonce and a list of transactional data selected by the miner.

Each block consists of the hash value[6] of the following elements:

- *Prior Block's Hash Value* - a hash of previous block that is hashed to the block as a way of connecting two consecutive blocks.
- *Nonce* – a number that is an answer to the puzzle that enables the creation of the block.
- *Timestamp* - is the exact time in Unix time format when the block is created.
- *Hash of Block Data* – List of transactions, fees, messages etc.
- Each block contains many transactions that are included in the Block Data. Each of those transactions hold the following data:
- *Amount of Transaction* – exact value that is being transferred.
- *Address of a receiver* – A hashed code connected to the receiver's public key (wallet). This ensures anonymity, and the total funds of the receiver are secured.

[6] Hash Value - the result of applying a hashing function to a string of data

- *Transactional fee* – a reward given to the miner that includes the transaction in their block and ensures that it is recorded.
- *Cryptographic Signature* – The proof that the sender has access to the wallet and the funds in it.

Transaction Walkthrough.

To gain a deeper comprehension of how blockchain transactions work, let's look at the processes of the Bitcoin transaction.

Creating a Transaction. The process begins with the sender initiating a transaction from their Bitcoin wallet. Wallets are files that store cryptographic access keys for one or more Bitcoin user addresses (user IDs). To make a transaction a user must choose a wallet and create a new address using Bitcoin software. There is nothing preventing a user from creating many wallets and/or addresses. As shown on Figure 8, any user can have multiple wallets and each wallet can have multiple addresses directing to it.

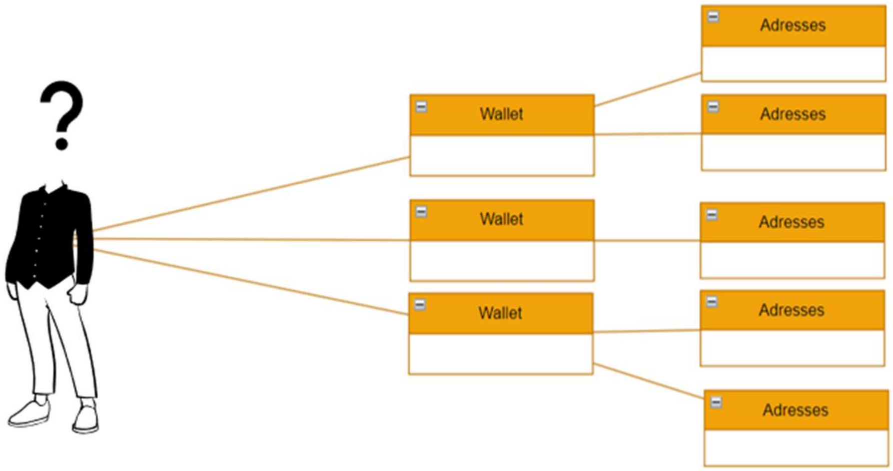


Figure 8. User Wallet Relationship. The user has a one-to-many relationship with wallet and the wallet has one-to-many relationship with addresses. There is no data that is stored about the user. A wallet has information about a private key. An address hash is generated from the master private key.

When the user wants to initiate a transaction, they send it to the address of the receiver. Bitcoin addresses serve as cryptographic representations derived from the user's public and private key pairs. These keys are at the core of the security and functionality of the Bitcoin network. When someone sends Bitcoin to an address, those funds get directed to the associated wallet. It's essential to note that every Bitcoin address is used only once. This enhances security and privacy by preventing reuse, as well as making it more challenging for outside observers to trace the transactions back to the sender or receiver (Zhao, 2015).

Signing the transaction. The sender creates a digital signature using their private key and transactional data. This digital signature is cryptographic proof that the sender possesses the authority to send the specified amount of Bitcoin from their wallet. It serves as a digital stamp, indicating that the transaction has been authorized by the rightful owner of the Bitcoin.

Broadcasting into the network. The transaction is then broadcasted to the entire network and distributed among the nodes for validation (See Figure 9).

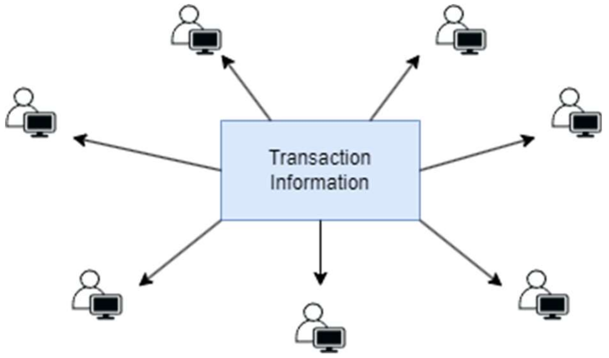


Figure 9. Broadcasting Transaction Information. Each node shares their ledger with other nodes in the network. All nodes download the transactional information contained in those ledgers by constantly updating theirs.

Each node that receives the transaction will independently validate it. This validation involves checking that the transaction follows the rules of the Bitcoin protocol, including verifying that the inputs are unspent (no double-spending) and that the digital signatures are valid. Additionally, the node checks the transaction against its own copy of the blockchain to ensure that the funds being spent are available. Then they broadcast the transaction to the nodes they are connected to.

Broadcast to miners. If the transaction passes these initial checks, it is added to the node's mempool. The transaction enters the mempool, which is a temporary pool where unconfirmed transactions wait to be picked up by miners. While transactions in the mempool have passed initial checks, they are not fully validated until they are included in a block. The recipients of these provisional transactions do not yet have ownership of their incoming funds.

Selection by Miners. Each node can have a different set of transactions in its mempool. The transactions in a mempool still need full validation. Miners are a subset of nodes that create a new proposed block (See Figure 10). Miners choose which transactions from the mempool to include in the blocks they mine based on various factors, including transaction fees.

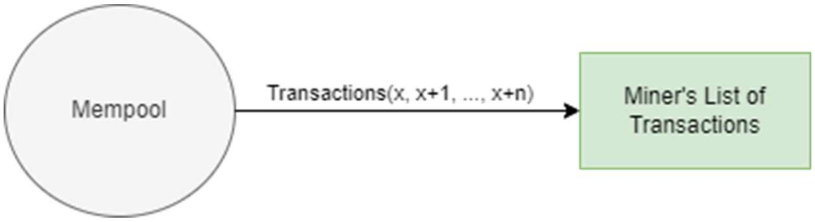


Figure 10. Selection of Transactions from Mempool. Miners select the set of transactions from the mempool to include in their block. It is in their best interest to include maximum amount of transactions to receive a higher transactional fee total.

Generating the Block. The miners use the transaction data, timestamp, and nonce to create a proposed block. The timestamp in a Bitcoin block header records the approximate time when the miner began working on the block. Nonce is a random value that a miner needs to use as a potential solution to the block puzzle (See Figure 11).

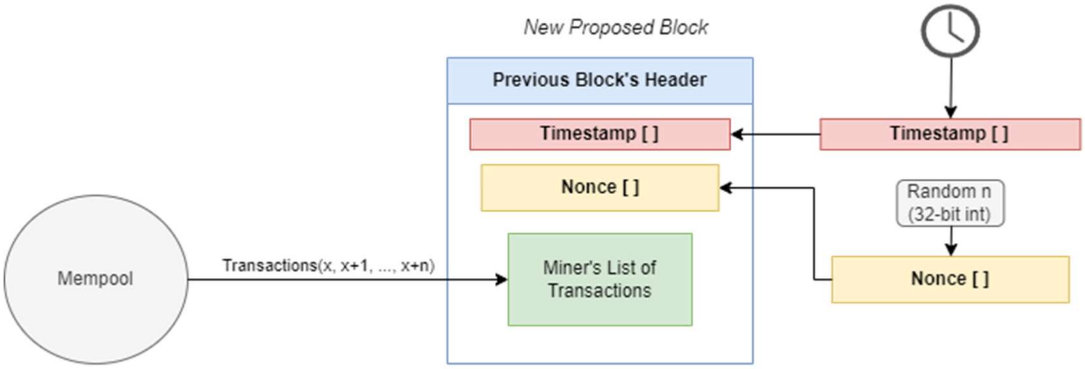


Figure 11. Adding Nonce and Timestamp to the block. Timestamp code is received from the actual time. The nonce is randomly generated. Both are added and hashed with the block information.

Hashing the proposed block. Miners combine all parameters, including the nonce, and then hash them using a cryptographic hash function, which in Bitcoin's case is the SHA-256d (Secure Hash Algorithm 256-bit)[7]. The result is a unique and seemingly random string of numbers and letters known as the block hash. Miners repeatedly change the nonce and rehash the block parameters until they find a block hash that is smaller (in numerical value) than the current target value. This process requires significant computational power and is essentially a game of trial and error. When the target value is met, the block will be verified by other nodes in the network who perform the same hash calculation. This process is called Poof-of-Work (PoW), which will be explained in depth on the next section. If PoW is approved, the miners who found the valid nonce are rewarded with a few newly created bitcoins (the block reward) and transaction fees (Gervais, 2016). The full process of block creation can be seen on Figure 12.

[7] SHA-256 and SHA-256d hashing algorithms are addressed in the Section 3. Security and Trust in Blockchain.

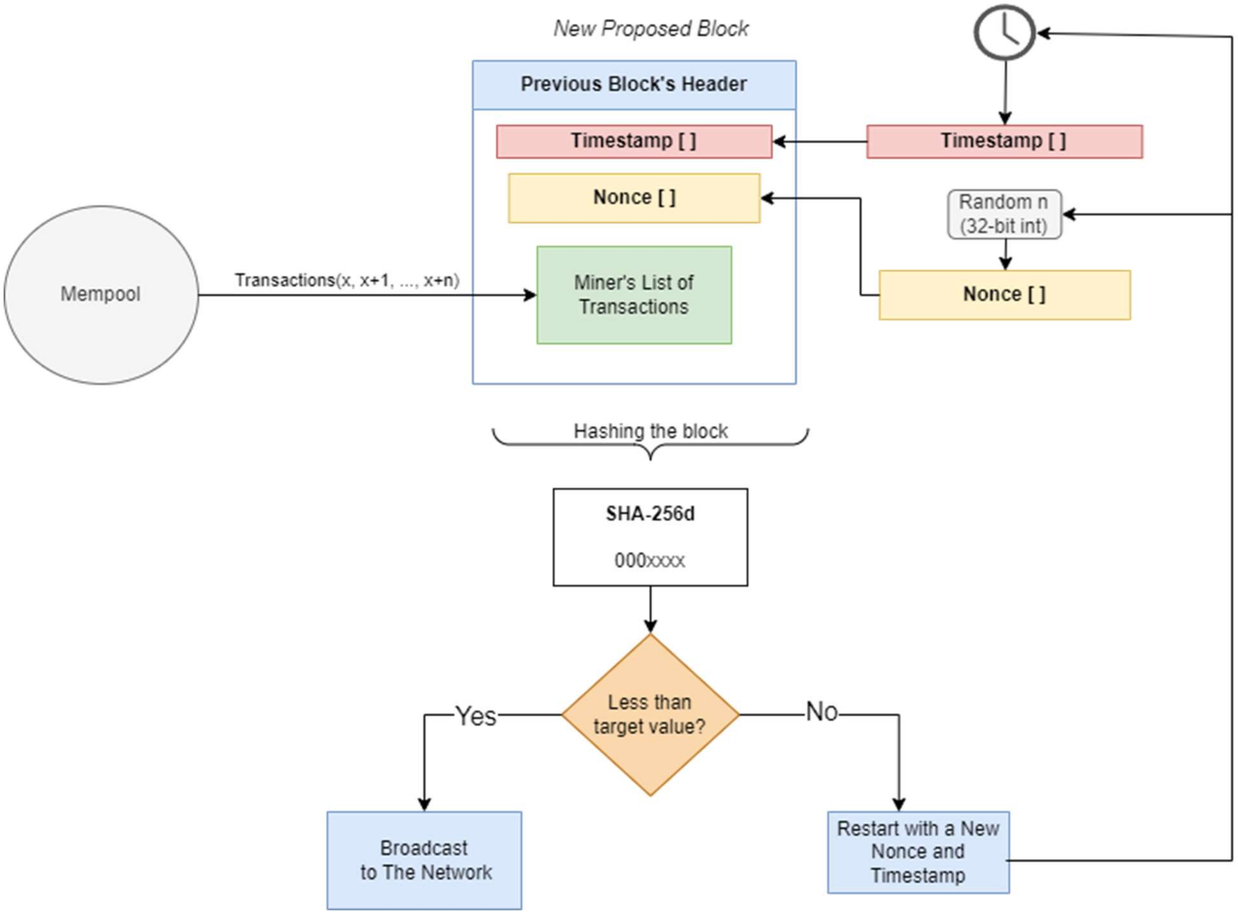


Figure 12. Block Creation Full Process. There is a loop that makes the miner make continuous guesses until the produced hash code is less than the target value.

Added to the Blockchain. If the newly mined block is valid and meets all the criteria, other nodes in the network accept it. After confirmation, the new block is appended to the blockchain (see Figure 13) and copies are held by all network participants. The transactions within this new block are regarded as validated. The miner can start working on the next block that would use the hash of this block in it.

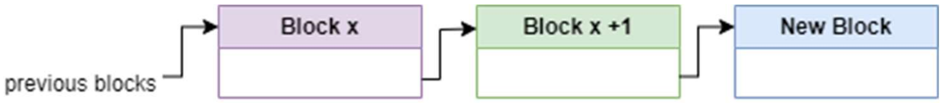


Figure 13. Linked blocks. The blocks are linked in a chain, and they are connected through having the header of the previous block encoded with the block data. Each block in the blockchain can be linked only to one block – the one that comes chronologically before itself.

Recipient's Wallet. Once the transaction with the transaction is posted on the published block, the wallet associated with the address updated with their new funds.

Proof-of-Work

Bitcoin relies on the Proof-of-Work (PoW) puzzle as a fundamental mechanism for securing its decentralized network and validating transactions, and additionally helping to maintain a consistent block creation rate (Nakamoto, 2008). POW is inspired by a simple question “What puzzle is mathematically hard to compute but easy to verify?”. Within the POW protocol, participating nodes engage in a competition to create the next block by solving a cryptographic puzzle involving finding the *nonce* value (Gupta, 2021). A valid nonce is one where when it is hashed with other data that goes into the block, their hashed value starts with a target number of zeros (Nakamoto 2008). The complexity of the puzzle to find nonce is modified every two weeks, and it has been generally increasing over time (Warmke, 2021).

The number of zeros in the PoW operation is determined by setting a target value. This is a specific number that the block hash must be less than for the block to be considered valid. The target value is adjusted by the network to control the rate at which new blocks are added to the blockchain. If the target value is lower, it's harder to find a valid block hash, and if it's higher, it's easier. The complexity of the puzzle is determined by the system based on the computational power of all the miners operating at that time. Bigger computational power results in an increase in the complexity of the puzzle, meaning more zeros should be in the hashed value (Gervais, 2016). This design guarantees that even as more miners join the network and the computing power spent on solving PoW puzzles increase, the rate of block confirmations remains roughly constant. The problems stay hard enough that no one miner has enough computing power to falsify the blockchain ledger.

Since Bitcoin is a universal currency and does not comply with any time zones, the timestamp of Bitcoin operates on different parameters. Timestamp is adjusted regularly to account for differences in time reported by various nodes on the blockchain network. The blockchain calculates the median of all the timestamps reported by different nodes. This helps eliminate outliers and provides a more accurate sense of time within the blockchain. One of the uses of timestamps is determining the time miners take to create an individual block. This information is later used to adjust the difficulty of puzzles to find nonces that miners work to solve (Fornell, 2019).

Section 3. Security and Trust in Blockchain

Role of PoW

When a Bitcoin user initiates a transaction, it needs to be included in a block before it's considered confirmed. Miners select and validate transactions, ensuring that they adhere to the network's rules. This includes verifying that the sender has the necessary funds, the transaction is properly formatted, and the digital signatures are valid (Nakamoto 2008).

PoW helps protect the network from Sybil attacks, where an attacker creates multiple fake nodes to take over the network (Douceur, 2002). The underlying mechanism of PoW is based on the principle that it's computationally expensive to solve the mathematical puzzle for block creation, but relatively easy to verify the solution. This ensures that miners cannot cheat or manipulate the blockchain. If a miner were to try to alter a transaction in a block, they would need to redo the PoW for that block and all subsequent blocks, which would be infeasible unless they had more computing power at their disposal than roughly the rest of the network combined (Nakamoto 2008).

SHA-256 Encoding

The Secure Hash Algorithm with a 256-bit output size, referred to as SHA-256 is one of the main hashing algorithms used by Bitcoin. In the Bitcoin system, SHA-256 is employed in the creation of a hash of the transaction data and the creation of block headers. The algorithm is favored for its speed and security. It produces a 256-bit (32-byte) hash value, which is often displayed as a 64-character hexadecimal string. That implies that there are $2^{256} \approx 10^{77}$combinations[8]. Refer to the Table 1 for the example of SHA-256 encryption. It can be observed that the produced hash codes do not have any visible connection to data that has been encrypted using the algorithm.

data	sha-256 encryption
a	ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb
b	3e23e8160039594a33894f6564e1b1348bbd7a0088d42c4acb73eeaed59c009d
ab	fb8e20fc2e4c3f248c60c39bd652f3c1347298bb977b8b4d5903b85055620603
"Hello World!"	86933b0b147ac4c010266b99004158fa17937db89a03dd7bb2ca5ef7f43c325a

Table 1. SHA-256 Encryption Example. The table shows the strings being encrypted using SHA-256 hashing algorithm. The data is transformed into a long list of characters. This operation is irreversible.

The asymmetry between easy hashing and impossibly hard un-hashing is the basis for the PoW puzzle that secures the Bitcoin blockchain.

Public and private keys.

[8] In a 256-bit system, each bit can have one of two possible values: 0 or 1. When these bits are converted into a 10-digit numerical system, there are a total of 2^{256} (or 2 to the power of 256) possible combinations, which is equivalent to 10^{77}.

Along with hashing, Bitcoin uses another cryptographic technique. The Elliptic Curve Digital Signature Algorithm (ECDSA) is used to establish user identities using public and private key pairs. From the earlier sections we know that every bitcoin user possesses a pair of keys: the private key, which is kept confidential and not shared with anyone, and the public key, which is made available to the public. ECDSA acts as the core algorithm that uses of those keys to confirm identity.

The ECDSA algorithm utilizes the mathematical properties of elliptic curves to generate a public-private key pair. Only a person who has the private key can sign the transaction initiated from their wallet (Johnson, 2001). An example of such encoding is given on Table 2. Anyone can verify this signature (and hence the ownership of the Bitcoin) by comparing the signature (generated from the private key) to the user's public key via ECDSA.

Encrypting a transaction with the private key provides clear evidence that the individual initiating the transaction has access to the private key. The encryption verifies the ownership and authorization required for the transaction. Thus, private keys are used to digitally sign transactions in the Blockchain system (Yaga et al., 2019). Users utilize different methods to keep those keys secure, including trusting third parties.

Component	Description	Value
Private Key	The user's private key.	88051012944125723492210602794191238317182124148173305233870870918860728447037
Public Key	The user's corresponding public key.	41691000613068744292337172649073251398895718338908835460963671630706680358968, 50144780470411340824387811106794553728764392705978487601872958326142628799432
Message	The data to be signed.	"Hello, world!"
Hash Function	The hash function used to hash the message.	sha-256
ECDSA Signature	The final digital signature.	3029684359787303895548845241950570345161567056089231651601024311177113004 2151, 3786203983814267895138440985194100983947543719006125145610013161756802270 3519

Table 2. An example of signing a message with Elliptic Curve Digital Signature Algorithm (ECDSA). Generated using the code from GeeksforGeeks.org.

Common security concerns and potential vulnerabilities.

Challenge of User Key Management. The shift from traditional passwords to key-based authentication presents a significant challenge for users of Bitcoin. This transition gives rise to various issues, including the complexity of using one's digital assets across multiple devices. Users are compelled to copy and transfer the access keys for their wallets between devices, which entails saving them in some file on their device or in a hard copy (that would need to be typed in for every use). This process requires more time to initiate a transaction.

The challenge of key-based authentication extends further by creating security concerns for users, who must assume sole responsibility for securing their digital keys. In the conventional password system, unauthorized access can be reversed and protected by legal measures. Banks are perpetually engaged in the implementation of diverse measures aimed at preventing fraudulent activities in their clients' accounts. Bitcoin, on the other hand, lacks a definitive solution for addressing such an inevitable problem. Although Bitcoin transactions are traceable, they remain irreversible, which adds a layer of complexity and risk. Losing the key or getting it stolen by another person implies that the funds have been irreversibly lost. Bitcoin does not present any protocol to ensure the return of funds in case of the stolen key. (Eskandari, 2018).

The only way to stop a transaction is to initiate a new transaction with the funds in the wallet to transfer them to a new address while the previous transaction is still in the mempool. If the new transaction has a higher transaction fee than the previous one, then it has a higher chance of being picked up sooner to be recorded in the blockchain. If the other transaction gets included in a block later it would constitute double spending, and it will eventually get invalidated by the network (Zimmerman, 2019).

Limited Number of Transactions. Blockchain relies on a broad network to validate transactions, which makes it much slower than other systems. In comparison, Bitcoin can only handle 4.6 transactions per second worldwide, while Visa can process 1,700 per second. Moreover, when there are lots of transactions, it can slow down the network. So, scalability remains a challenge on the way to future popularization of the coin (Rodeck, 2022).

Additionally, the transfer of the ownership of bitcoin is finalized only after a new block is made. This means it will also depend on the miner of the block. Each block has a limited capacity for the transactions that can be stored in it. The miner decides which transactions to give priority, and this encourages the initiators of transaction to offer some kind of fee. The transactions that offer a fee for a miner receive priority while others might take a long time to be processed (Zimmerman, 2019).

Cyberattacks. While Bitcoin is generally considered secure, it is not immune to all threats. There is an ongoing long list of attacks that have caused the loss of millions of dollars' worth of Bitcoins by different companies. Thefts and shutdowns highlight the urgent requirement for better oversight and rules to reassure investors (Chohan, 2018).

In case of cyberattacks and other reasons that might cause collapse of the cryptocurrency, regardless of the wallet used by the users of the cryptocurrency, they are unlikely to get refunds. The latest example of such collapses was the fall of FTX, one of the largest. cryptocurrency exchange platforms.

FTX account holders are facing grim prospects of recovering their funds as the cryptocurrency exchange goes through bankruptcy proceedings. FTX claimed it was hacked, indicating a substantial loss of assets. Legal and banking experts suggest that the likelihood of users getting their money back is low. FTX owes $102 million to customers and at least $3.1 billion to around 1 million creditors. Investigations by regulatory bodies focus on whether FTX improperly moved customers' assets to Alameda Research, a crypto hedge fund owned by FTX founder Sam Bankman-Fried (Popli, 2023).

The cryptocurrency industry, which has faced increased scrutiny, is undergoing a reckoning, with FTX's collapse amplifying concerns about the risks associated with unregulated platforms. The lack of a clear understanding of FTX's remaining assets and their location further complicates the prospects of account holders recovering their lost funds. Legal experts suggest that FTX customers may face a lengthy wait to recover their funds, with some expressing doubt that any funds will be returned (Popli, 2023).

Section 4. Summary of Blockchain.

In conclusion, Bitcoin's underlying technology is blockchain. It has enabled the system of decentralized trust within the network. By introducing a decentralized, transparent, and secure ledger, blockchain technology has addressed the long-standing issue of trust in online transactions. It has facilitated anonymous transactions which is one of the competitive advantages of Bitcoin over traditional money. However, those innovative ideas are not without flaws. Those flaws have not been addressed by the developers and they can slow down the further adaptation of the Bitcoin by the public.

Chapter IV. Mining

Section 1. Purpose of Mining

The nodes that participate in the creation of blocks in the blockchain are referred to as miners. Miners are the only recipients of newly minted Bitcoins. They compete to solve simple cryptographic problems. When they find a solution, they are rewarded with a certain number of Bitcoins. This reward is known as the block reward, which serves as a fundamental incentive for miners. It gets added to their wallet after the block has been accepted by the network. It is important to note that while many miners compete to mine a block, only one miner succeeds and gains the block reward. These block rewards are how new coins enter the market (Kroll, 2013).

The reward system for miners is structured around a fixed number of coins contained within each block. This reward undergoes a process known as "halving" every four years. During each halving event, the fixed reward is precisely divided by two, introducing a deliberate scarcity element into the Bitcoin issuance mechanism. As described in Chapter 1, the initial block reward of Bitcoin was 50BTC. As it stands today after 14 years, miners receive 6.25 bitcoins for successfully mining a block. So, while miners receive bitcoins as a reward for successfully mining a block, the mining process itself revolves around creating new blocks and adding them to the blockchain (Kroll, 2013).

Section 2. Mining Hardware

When Bitcoin was first launched, mining did not require powerful hardware. Anyone with a computer could participate in the mining process by running free software on their computer. They used standard computer hardware to participate in the network and earned rewards in the form of newly created Bitcoins. The competition, however, grew at the same rate as the popularity of the coin, completely changing the dynamics of mining processes. Over time, Bitcoin mining has transitioned from being a hobbyist activity to a professional and corporate one (Taylor, 2017).

Computer hardware that is used for mining is referred to as a mining rig. It can be as simple as a cloud computing option or as complicated as a highly customized system costing thousands of dollars. Bitcoin requires mining rigs to be working non-stop to achieve cost efficiency. This comes with more cost since the hardware requires a cooling system (Rodeck, 2023).

Today a single computer is no longer able to compete for Bitcoin. As the competition rose miners started improving their systems. In November of 2010, miners started grouping in pools. Pooled mining involves miners coming together and combining their computational power to collectively solve the complex mathematical puzzles required to mine Bitcoin blocks. Each miner in the pool contributes their computing resources to the group effort and the reward earned gets distributed respectively (Taylor, 2017).

To stay competitive, miners began using specialized hardware known as ASICs (Application-Specific Integrated Circuits) designed specifically for Bitcoin mining which was launched in January of 2013. These ASICs are highly efficient at solving the PoW puzzles required for mining (Taylor, 2017).

Nowadays, many mining operations are conducted in large data centers that are custom-built for mining purposes. Those operations are treated as corporate entities. Corporations invest in the maintenance and improvement of their hardware. Overall, the mining process requires a huge investment on property rent, computational and cooling equipment, as well as electricity and maintenance cost as fixed expenses. Thus, mining operations are often located in regions with favorable conditions for mining in order to increase profit. They look for low land and construction costs, cheap electricity, favorable taxation policies, and minimal regulation (Taylor, 2017). One of such places that enables favorable conditions for Bitcoin is Kazakhstan (See Figure 14).

a.

b.

Figure 14. The Ekibastuz mining facility located in Kazakhstan. The facility can host up to 50,000 mining rigs and handle as much electricity as needed to power 180,000 U.S. homes. Source. Reportedly those rigs were received from China after the country has shut down all of their mining operations Source (a): CoinDesk. Source (b): Yahoo Finance

Section 3. Supply and Demand in the Mining Market

It is important to mention that the mining process is a risky investment. The volatility of transactional fees arises from the intricate interplay between the expectations of miners and users and the actual market conditions. Oftentimes, the prevailing market circumstances do not align with the anticipated outcomes expected by the participants. This involves the electricity cost and the time that is required to create a single block. This discrepancy introduces a degree of uncertainty and unpredictability into the Bitcoin ecosystem, which can have implications for users and miners (Ilk, 2021).

It is worth highlighting that the lack of transparency in the fee calculation system which determines the reward received after successful mining, which complicates this situation further. The specific mechanisms employed to determine these fees remain obscure and ambiguous to the average user. As a result, individuals engaging in Bitcoin-related activities are left with limited means to accurately predict the associated costs. Consequently, they are forced to rely on speculation and estimation when making decisions concerning their Bitcoin transactions (Ilk, 2021).

In accordance with the fundamental principles of economics, supply naturally emerges in response to demand. Thus, mining business will exist as long as Bitcoins users are willing to participate in transactions and pay the associated transaction fees. However, the future of this business remains uncertain because of the challenge of accurately predicting shifts in demand over time.

Future of Mining.

Currently the block reward is considered the main incentive of mining. However, this is not expected to be the case in the future. The total supply of Bitcoin is capped at approximately 21 million. This is ensured by the halving process, and the anticipated mining of the last coin is projected to occur around the year 2140. Thus, the block reward, the incentive for miners, follows an exponential decrease as more blocks are created, eventually leading to the issuance of all available coins. Eventually, transaction fees will assume a more pivotal role (Zimmerman, 2023). Although there are many speculations on the influence of such a set-up on the mining operations, there is no certain outcome until that actually happens. The users of Bitcoin and miners would have to come to a consensus on transactional fees since one cannot operate without the other.

As the block reward decreases over time and the costs associated with mining continue to rise, it becomes evident that the mining business carries significant risks, particularly for existing mining operations, and poses even greater challenges for newcomers entering the industry. The combination of declining rewards and escalating operational expenses creates a scenario where both established and prospective miners face heightened uncertainties and potential financial vulnerabilities. The evolving dynamics of the cryptocurrency landscape necessitate careful consideration and strategic planning for those involved in or contemplating entry into the mining sector.

Chapter V. Ethical Issues Around Bitcoin

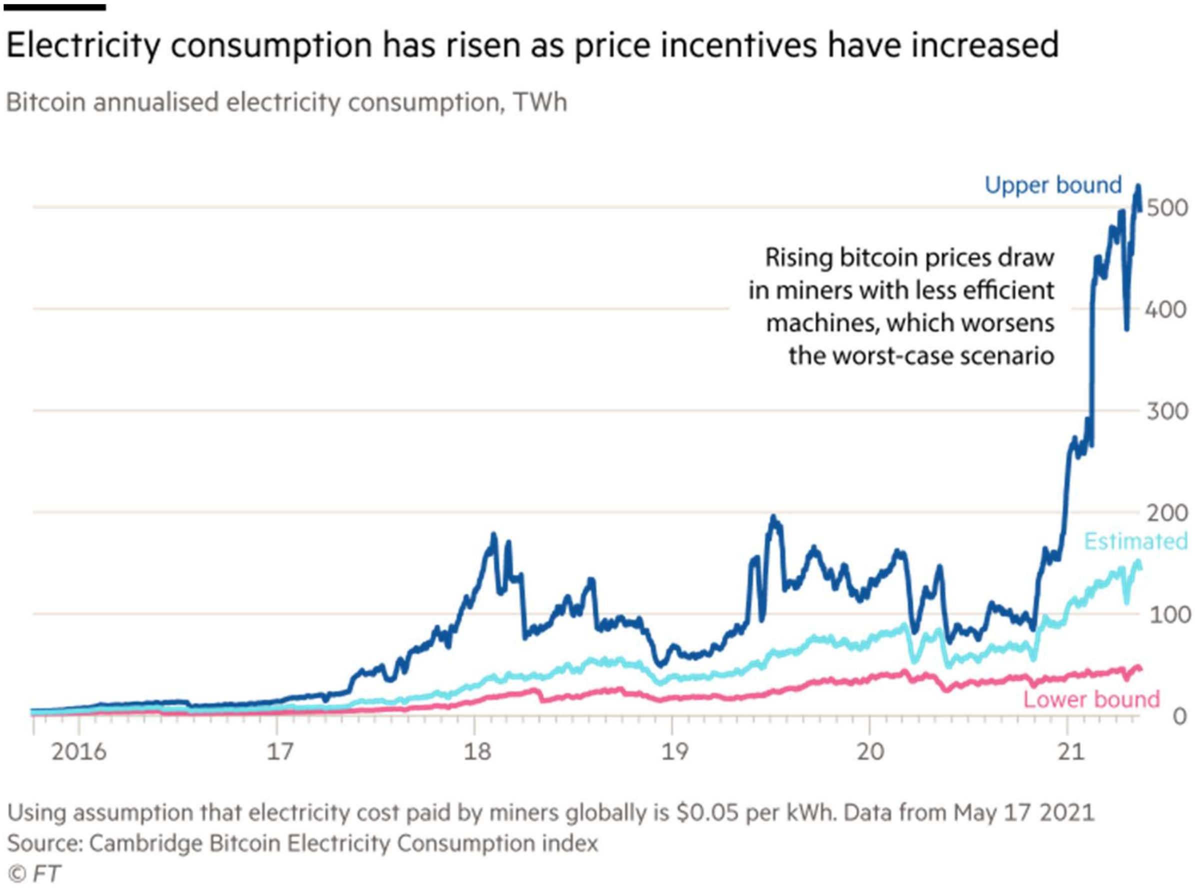
Corporate Social Responsibility (CSR) is a concept that encourages businesses to go beyond profit-making and consider their broader societal impact. It involves integrating ethical, social, and environmental considerations into a company's operations and decision-making processes. In the context of the Bitcoin industry, CSR takes on a unique set of challenges and responsibilities (Lindgreen, 2010).

The rise of Bitcoin has revealed many ethical issues that surround the usage of decentralized and pseudonymous digital assets.

Section 1. Environmental Impact of Bitcoin.

The Peer-to-Peer review feature, which grants Bitcoin its decentralization and independence from central authorities, also comes with a significant drawback: need for enormous amount of electricity. This is primarily due to the process of "mining," a fundamental aspect of how new Bitcoin transactions are verified and added to the blockchain (Badea, 2021).

As more miners joining the network to compete for solving the blockchain puzzle, the difficulty of the mining process increases to match. This means that electricity consumption has also increased over the years. You can see the Bitcoin's yearly consumption of electricity on Figure 15.



Electricity consumption has risen as price incentives have increased

Bitcoin annualised electricity consumption, TWh

Rising bitcoin prices draw in miners with less efficient machines, which worsens the worst-case scenario

Using assumption that electricity cost paid by miners globally is $0.05 per kWh. Data from May 17 2021
Source: Cambridge Bitcoin Electricity Consumption index
© FT

Figure 15. Bitcoin Yearly Electricity Consumption. Source: ft.com

This positive correlation between popularity and electricity consumption has led to concerns about the environmental impact of Bitcoin, especially when it is powered by fossil fuels. The energy consumption of Bitcoin has risen to the point that it can now compete with some countries on the level of consumption. You can see the comparison of the Bitcoin electricity consumption to some countries on Figure 16. According to the graph, Bitcoin is found to have an electricity consumption that is larger than countries such as United Arab Emirates, Argentina and Netherlands.

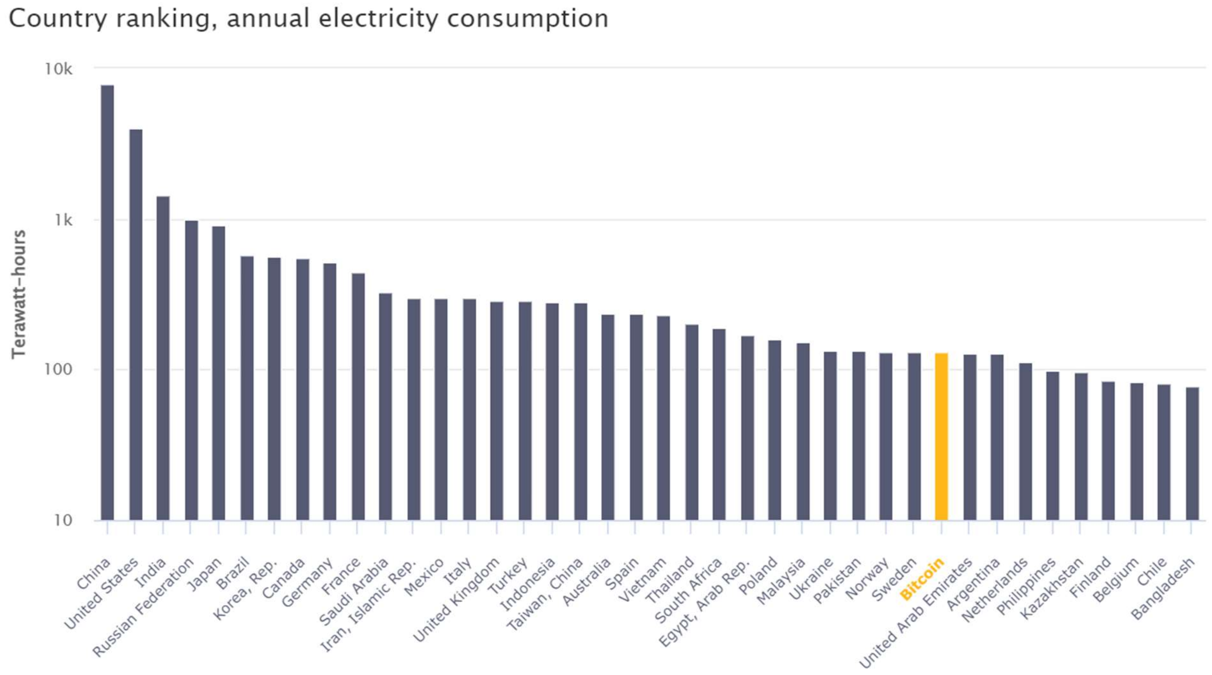


Figure 16. Energy Consumption of different Entities in Comparison to Bitcoin (Logarithmic scale). According to the graph, energy consumption of Bitcoin outweighs the list of countries. Data from 2023. Source: University of Cambridge

Section 2. Electricity Manipulation by Bitcoin Miners

It is a fact that Bitcoin consumes a large amount of electricity as seen in Figure16. Meanwhile, the tradeoff of the mining businesses having rows of computers, owned by mining companies, working on the puzzle is the regular people being left out in the darkness and cold with no electricity.

An example of such a case happened in Texas at the start of 2021. Due to Winter Storm Uri, many power plants were knocked out throughout the state. Many homes were left with no electricity, which reportedly caused the death of 40 people. At the same time, the Bitcoin company Bitdeer was still actively mining Bitcoin in its computer warehouses, consuming electricity in size big enough to operate a small city. Eventually the computers were shut down, but with a condition. The state had to pay compensation of $175,000 an hour to Bitdeer, bringing the company 18 million dollars in the span of four days. The company netted a big profit by not working at all (Dance, 2023).

This practice of shutting down the operations for compensation during blackouts is not new and is known as a way of getting revenue quickly. In some U.S. states, including New York, Pennsylvania, and Texas, Bitcoin mining operators generate revenue in a related way. In Texas, for instance, these companies are compensated by the grid operator for agreeing to quickly reduce their power consumption in case of potential blackouts. In practice, they rarely have to shut down, and they make extra money while continuing their Bitcoin mining operations. Since 2020, five such operations have collectively earned at least $60 million from this program. This is mostly enabled by the ability of such operations to shut down all the processes immediately, which is not possible for most businesses (Dance, 2023).

This situation shows the scale in which the electricity consumption of Bitcoin mining influences the lives of regular people. Not only does it pollute the environment for people who might not be the stakeholders of Bitcoin but also affects the communities around the areas where Bitcoin gets mined. Currently, there are 34 such Bitcoin mining operations identified across the

U.S., which makes it a global leader in the number of such operations. Each of those operations uses at least 30,000 times as much power as the average U.S. home. It is a debate if those companies should be allowed to operate in U.S. In fact, China has stopped all the ones in its territory, in part because of the electricity consumption (Dance, 2023).

Section 3. How Bitcoin Enables Crime

Separation from government regulations and absolute anonymity comes with major drawbacks for society's welfare. The system of anonymity enabled by Bitcoin is exploited by criminals for various illegal activities. Such activities include arms sales, drug dealing, human trafficking, murder-for-hire, money laundering, sale of child porn, and sanctions busting. It has the potential to grow on a scale that would be harmful to the security of the individual or group of countries (Engle, 2016).

One of the large illegal platforms that operated with the help of Bitcoin transactions was Silk Road. Silk Road was a secret online marketplace where illegal goods and services were available for purchase using Bitcoin as the currency. Operating on the Tor network to provide anonymity, users could hide their IP addresses and identities. The platform offered various illegal items, including drugs, firearms, fake IDs, pirated media, hacking services, and even contracts for murder. The site's founder, Ross Ulbricht, allegedly attempted to hire a hitman to eliminate a Silk Road employee who had been arrested and posed a threat to the network. Ulbricht faced charges related to narcotics trafficking, computer hacking, and money laundering. In addition to charges in the Southern District of New York (SDNY), he faced an indictment in Maryland for distributing controlled substances and attempted murder-for-hire. Silk Road reportedly generated approximately $1.2 billion in revenue and $80 million in commissions. Law enforcement authorities seized over $164 million worth of Bitcoin from the website. Despite the shutdown of Silk Road, illegal transactions using Bitcoin continued in other platforms (Engle, 2016).

Conclusion

Bitcoin stands as a first cryptocurrency, diverging significantly from conventional understandings of money. Its innovation lies in enabling a decentralized monetary system, a departure from centralized financial structures that require the presence of governmental control and involvement of banks. Unlike traditional currencies that often tie identities to transactions, Bitcoin offers a level of privacy that allows users to engage in financial activities without revealing personal details and having a pseudonym instead.

Bitcoin is an asset that has no fundamental value. Because of its unique characteristics, Bitcoin has a high volatility. Bitcoin's price history shows a lot of inconsistency, and big rises and falls of the value of the coin.

At the core of Bitcoin lies Blockchain technology, where transactions undergo validation by the users in the systems known as nodes before being added to a block. A block can store a finite amount of transactions. Then the blocks are linked with each other by including the hash code of the previous block. This interconnected chain of blocks provides resistance against the double-spending problem. Those blocks cannot be falsified because of their link to each other. Changing the block changes the hash code making it no longer connected to the block after.

The only supply of Bitcoin comes from mining. Miners are nodes in the network who participate in the validation of transactions and the creation of blocks, through the process of Proof-of-Work (PoW). PoW involves repeatedly hashing block data using SHA-256 algorithm and competing with other miners in the network to generate a hash code that meets the requirements of the bitcoin algorithm.

While Bitcoin is claimed to be an efficient currency for society by Satoshi Nakamoto, it has shown many flaws that make this debatable. The tradeoff of using Bitcoin is a contribution to environmental pollution, being a part of the system of exchange that enables the exchange of illegal goods and services and a risk of losing assets by because of the price fall or stolen keys.

References

Ankalkoti, P., & Santhosh, S. G. (2017). A relative study on bitcoin mining. Imperial Journal of Interdisciplinary Research (IJIR), 3(5), 1757-1761.

Badea, L., & Mungiu-Pupăzan, M. C. (2021). The economic and environmental impact of bitcoin. *IEEE Access, 9*, 48091-48104.

Baker, P. (2021a, September 14). *Bitcoin mining facility with room for 50,000 rigs set to launch in Kazakhstan*. CoinDesk Latest Headlines RSS. https://www.coindesk.com/markets/2020/08/21/bitcoin-mining-facility-with-room-for-50000-rigs-set-to-launch-in-kazakhstan/

Chohan, U. W. (2021). The double spending problem and cryptocurrencies. *Available at SSRN 3090174*.

Chohan, U. W. (2018). The problems of cryptocurrency thefts and exchange shutdowns. *Available at SSRN 3131702*.

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering, 19*(5), 92-95.

Dimpfl, T. (2017). Bitcoin market microstructure. *Available at SSRN 2949807*.

Douceur, J. R. (2002). The sybil attack. In proceedings of the first international workshop on peer-to-peer systems (IPTPS 02) (pp. 251-260). Cambridge, MA, USA.

Edwards, J. (2023, November 17). *Bitcoin's price history*. Investopedia. https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp

Engle, E. (2015). Is bitcoin rat poison: Cryptocurrency, crime, and counterfeiting (CCC). *J. High Tech. L.*, *16*, 340.

Eskandari, S., et al. (2018). A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351*.

Hashimzade, N., Myles, G., & Black, J. (2017). volatility. In A Dictionary of Economics. : Oxford University Press. Retrieved 26 Oct. 2023, from https://www.oxfordreference.com/view/10.1093/acref/9780198759430.001.0001/acref-9780198759430-e-3312.

Fornell, J. (2023). What Is Timestamp on Blockchain? *Bit2Me Academy*. Retrieved from URL. https://academy.bit2me.com/en/timestamp-blockchain/#:~:text=The%20timestamp%20or%20timestamp%20is,validated%20by%20the%20blockchain%20network

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International journal of information security, 1, 36-63.

Ilk, N., Shang, G., Fan, S., & Zhao, J. L. (2021). Stability of transaction fees in bitcoin: A supply and demand perspective.

Gabriel J.X. Dance. (2023, April 17). The real-world costs of the digital race for Bitcoin; Operations can lead to high public electricity bills, pollution. *Sarasota Herald-Tribune (FL)*.

Gervais, A., et al. (2016). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*.

Nguyen, T., de Bodisco, C., & Thaver, R. (2018). Factors Affecting Bitcoin Price in the Cryptocurrency Market: An Empirical Study. International Journal of Business & Economics Perspectives, 13(1), 106–125

Popli, N. (2022, November 25). *Why FTX account holders are unlikely to get their money back*. Time. https://time.com/6236610/ftx-account-holders-money-back/

Powell, F. (2023, September 30). *10 best crypto apps & exchanges of 2023*. Forbes. https://www.forbes.com/advisor/investing/cryptocurrency/best-crypto-exchanges/

Reiff, N. (2023, September 27). *Why is bitcoin volatile?*. Investopedia. https://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp#:~:text=Bitcoin's%20price%20fluctuates%20because%20it,together%20to%20create%20price%20volatility.

Rodeck, D. (2023, September 29). *Best bitcoin mining software of 2023*. Forbes. https://www.forbes.com/advisor/investing/cryptocurrency/best-bitcoin-mining-software/

Taylor, M. B. (2017). The evolution of bitcoin hardware. *Computer*, *50*(9), 58-66.

Wallace, B. (2011, November 23). *The rise and fall of Bitcoin*. Wired. https://www.wired.com/2011/11/mf-bitcoin/

Warmke, C. (2021). What is bitcoin? *Inquiry, 1*(1-43).

Yaga, D., et al. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*. https://arxiv.org/ftp/arxiv/papers/1906/1906.11078.pdf

Zimmerman, P. (2019, March 4). Blockchain structure and cryptocurrency prices.

Zhao, C., & Guan, Y. (2015). A graph-based investigation of bitcoin transactions. In *Advances in Digital Forensics XI: 11th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 26-28, 2015, Revised Selected Papers, 11*.

Zola, A. (2021, June 3). What is hashing and how does it work?. *Data Management.* https://www.techtarget.com/searchdatamanagement/definition/hashing