Cryptocurrency: Is it the Future of Payments?

Zachary Mineau, Dylan Hoffman, Jonathan Lor, and Nazim Choudhury

Abstract Cryptocurrency, which is built using blockchain technology, is one of the newest methods of doing secure transactions without a central authority. Due to the unregulated means in which cryptocurrency is transferred, it becomes incredibly hard to ensure the fairness and legitimacy of the transactions. This is to further explore the history, process, problems, competition, advantages, and the current future of cryptocurrency. Finally, the team built its cryptocurrency and blockchain similar in functionality to Bitcoin, which is currently the most popular cryptocurrency by sheer market capitalization of over $898 Billion. This allows people to track the flow of cryptocurrency in all its flaws, and its potential succession of other currencies. This chapter explore different aspects of the cryptocurrency which is a vital aspect of futuristic cyber smart cities. This chapter will serve as a reference for cyber smart city developers and other relevant stakeholders in designing futuristic cities.

1 Introduction

Currency is the fundamental essence of trade in the modern world. It is the legal tender for which people, businesses, and governments recognize and accept payment for various goods and services. With the advancement of fiat currencies, the value of the currency is not in the physical item, but rather the fundamental idea that the item is worth something more. This is the basis for all cryptocurrencies. It stands as a self-regulated virtual fiat currency that utilizes internet access. Therefore, it is important to understand the history, problems, competition, advantages, the future, and the process of how cryptocurrencies work.

The original cryptocurrency that struck out big was Bitcoin. Bitcoin was launched in 2009 by a user unknown. The only identification is a pseudonym, Satoshi Nakamoto. The promotional material for the new currency was that cryptocurrencies did not rely on trust of an organized banking system. Instead, it utilized "Crypto-

Z. Mineau · D. Hoffman · J. Lor · N. Choudhury (✉)
Department of Computer Science, University of Wisconsin Green Bay, Green Bay, USA
e-mail: choudhun@uwgb.edu

M. Ahmed and P. Haskell-Dowland (eds.), *Cybersecurity for Smart Cities*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-24946-4_12

graphic proof rather than trust" [1]. This prompted one of the greatest forms of tracking for online currency. Although Bitcoin was created and nuanced in 2008, it did not get worldwide attention until 2011.

Since Bitcoin utilizes proof of independent users, it led to many problems. One of these problems was that Bitcoin had no central authority. This meant that the ownership of Bitcoin had to be continuously monitored. A study in 2017 that showed the total mining revenue per year. The revenue gained by bitcoin mining is changing year to year. This is one of many reasons that people are hesitant to back bitcoin [2]. The revenue gained from mining is inconsistent at best. There is also a lack of immediate data from miners.

Another major problem is that cryptocurrencies, especially Bitcoin, are affected by the perception of the value that they hold. Data was collected on several cryptocurrencies to determine how each currency value rose or fell to outside effects and inside effects with each other. After several months it was shown that the overall pricing of the currencies was affected by the belief of the currency. As the media talked about a currency, the price of that currency would go up. When a negative story was published or no activity was published, the price would go down. It is suggested that it would be unlikely to sustain prices of cryptocurrencies as a financial asset if no one believed in its potential [3]. This poses a problem with any fiat currency.

Still, not all fiat currencies share all weaknesses. Cryptocurrencies are liable to DDos attacks. Some miners have shown that a DDoS attack can cause a system malfunction [4]. With every successful attack, the developers continue to update and perform bug fixes. However, there have been cases where a bug fix was not successfully updated at an exchange firm that led to an attack. The Magic the Gathering Online Exchange firm was hit when a hacker was able to rob them of approximately 460 million USD. It was found out that the CEO of the firm was not updating the systems regularly. Since the system was not updated, it ended up costing hundreds of millions of dollars [5]. This is a major concern to any company or government.

1.1 Chapter Roadmap

Rest of the chapter is organized as follows. Section 2 discusses the government recognition for cryptocurrency. Section 3 showcases the key concerns, Sect. 4 discusses the competition for the cryptocurrency, Sect. 5 highlights the advantages, Sect. 6 showcases the cryptocurrency processing and finally the chapter is concluded in Sect. 7.

2 Government Recognition

When a country does not recognize a currency, it causes numerous problems. The main restriction to adopting governmental backing is that the government must impose regulations upon the currency. With regulations, the currencies that are strug-

gling to obtain acceptance will gain greater legitimacy in the larger audience [6]. Inside Bitcoin, however, due to virtual currency being in the infancy stage, it is likely that many changes will occur before a nation backs any cryptocurrency.

If companies and countries begin to accept cryptocurrency as a legit currency, it will only ensure the reliability and sustainability of bitcoin. With the acceptance of the currency, many opportunities become available. It has been noted that bitcoin is great for international transactions. Although money can be wired to another country already, there are hurdles. Different countries have different values which means the money must be converted. Some transactions can elicit fees and even denial of service. If money needs to be transferred quickly to another country, having a unanimous currency that is unrestricted by governance is the way to go.

Some countries, like Canada, have already begun adopting virtual currency [7]. The system seeks to minimize the risks associated with cryptocurrencies by imposing the before mentioned regulations. This further benefits cryptocurrency as the Bank of Canada has acknowledged the developing virtual currency market. However, some countries like Russia are concerned with the emergence of virtual currency. The Bank of Russia has stated that it violates federal law stating that all currency must go through a central bank. Another concern from Russia is that the value of the coin fluctuates every day. It is nearly impossible to set a standard for the coin as it changes without proper regulation.

3 Major Concerns

This section discusses the major issues in adopting cryptocurrency in the futuristic context, such as smart city perspective.

3.1 Frauds and Scams

Even if all the bugs in the systems get patched and every country recognizes cryptocurrencies, there are always going to be problems. The ledger and block chain are public which allows for semi-anonymity [8]. A problem that can never be truly solved is scams. With the evolution of technology protection, the ways around that security also evolve. People are using scams, ransomware, Ponzi schemes, and most of these schemes can be traced to links associated with social media.

Scams have always been a part of society. If there has been coin and product to swindle, a swindler will appear. It is no different with cryptocurrencies. These scams tend to fall under two categories. The first is to convince the victim to transfer cryptocurrency to a blockchain address with a promise of returning more cryptocurrency. The old spend money to make money schemes. The second category revolves around the victim providing existing credentials that are required to access their private

cryptocurrency account with the promise of additional funds. Thankfully, as these scams get noticed, people warn others that it exists, and this means that the scammers resort to other tactics.

Another one of the tactics is ransomware. This is where a hacker gains access to a victim's computer system or other personal information. The hacker then threatens the victim with sharing, using, or even deleting all personal information accessible. A price is then set for an amount of a cryptocurrency to be sent to the hacker [9]. Cryptocurrency is great to have as a means of criminality as it is hard to trace where the account is and who truly owns that account. This is a problem because there is no central bank that runs all the accounts with a registered person behind each account. However, these are still able to be monitored by the blockchain.

The next tactic is simple Ponzi and pyramid schemes. These scams claim to be verified and trustworthy organizations that promote cryptocurrency. Some creators and influencers create their own version of a cryptocurrency. They hype it up to their audience and have them buy into the crypto. Once these initial people buy up the coins, the original creator leaves and the victims then must rely on selling the coin to someone else to regain what they lost [10]. Since the coin does not function as legal tender, and newcomers are slowly dwindling, those who bought the coin are without any reimbursement.

All these tactics are different, but they do have something in common. Most of the various versions of these tactics utilize social media to target and link each account to each other. It is common to see famous people like Elon Musk offering free cryptocurrency. However, these famous people are typically run by imposters [11]. This occurs when a user creates a fake Twitter or other social media account and pretends to be a well-known individual. Since people like Elon Musk are known for their technology savvy ways, people believe that the free cryptocurrency is real. The only real comfort comes in the way the scams are usually shut down quick. In fact, most of them that are recorded are no longer functioning [12]. When they click on the link they can easily fall into a scam.

3.2 Scalability Concerns

One problem of proof-of-work consensus is its scalability. Miners must verify each and every transaction on the network. As cryptocurrencies continue to gain popularity and more people join the network, the number of transactions increases as well. However, because every transaction must be validated sequentially, more steps are required for the transaction to be verified. It currently takes anywhere from 10 min to one hour to verify a Bitcoin transaction. Bitcoin verifies transactions at a max of seven transactions a second, but realistically verifies less than that. For reference, PayPal can verify around 193 transactions per second while Visa is able to verify around 1700 transactions a second. Ethereum also shares this scalability issue with Bitcoin. Ethereum on average processes around 20–25 transactions a second, way down from its theoretical 1000 transactions per second [13]. This is due to Ethereum's transaction

fees, also known as "gas", a fee determined by the "amount of computational effort required to execute specific operations on the Ethereum network". If Bitcoin or Ethereum are to become staples in the global economy, the relatively slow transaction verification becomes a big problem.

3.3 Energy Concerns

On March 24, 2021, Elon Musk, Tesla CEO tweeted, "You can now buy a Tesla with Bitcoin". Just 49 days later, on May 12, 2021, Elon Musk tweeted "Tesla & Bitcoin", alongside a statement that Tesla would be suspending vehicle purchases with Bitcoin [14]. Musk cited fossil fuel and energy consumption concerns regarding Bitcoin mining and transactions as the cause of the suspension. The statement also included praise for cryptocurrency in general and believes it has a promising future but was skeptical about the energy consumption of cryptocurrency. In a New York Times interactive article about Bitcoin, it's estimated that just Bitcoin itself consumes about 91 terawatt-hours of electricity annually, more than the country of Finland. Bitcoin's electricity usage has increased tenfold in about five years [15].

Proof-of-work is the most popular consensus protocol currently used in the cryptocurrency environment and a vast majority of cryptocurrencies use proof-of-work. Bitcoin and Ethereum, the two most popular cryptocurrencies both currently use proof-of-work consensus. Proof-of-work is a consensus mechanism wherein users or "miners" compete to solve an arbitrary math problem to become the first to validate the next block. The miner that solves the math problem first and validates the next block is awarded many coins. Miners, whether individuals or companies, compete to validate transactions to get coin rewards. The more computer power you have, the more likely you are to solve this arbitrary math problem and be rewarded with coins. As the price of cryptocurrencies rises, more and more miners are incentivized to join. As more miners participate in mining, the math problem becomes more difficult, requiring more and more energy to solve.

A study compared the US energy consumption to the trading volume of cryptocurrency, from 2014 to the end of 2017 [16]. The study found a positive correlation between the trading volume of cryptocurrency and energy consumption. As the trading volume of all cryptocurrencies went up, energy consumption in the US also went up. In regard to Bitcoin, the study concluded that the "trading of bitcoin appears to have a long-run positive influence on the production of energy" and that this energy consumption growth is a limitation of Bitcoin in terms of sustainability. As Bitcoin is the poster child of cryptocurrencies, Bitcoin's price and sentiment has a significant impact on the price and sentiment of other cryptocurrencies, which in turn incentivizes more miners to partake, thereby increasing energy consumption.

The rise of cryptocurrency prices over the decade has incentivized crypto miners to build data centers for the sole purpose of mining cryptocurrency. These data centers have a high demand for power, so miners are placing data centers in location with relatively cheap energy costs. The Greenburg and Bugden study [17] studied Chelan

County, Washington, where its abundance of cheap power attracted an influx of crypto mining to the community beginning in the early 2010s. This influx created an "energy consumption boomtown", and how the county is dealing with the increase in energy consumption over the years as Bitcoin and other cryptocurrencies grew.

In 2014, the county enacted a moratorium after receiving 34 power inquiries for the use of 220 MW of electricity, double the energy use for the entire county. In 2017, after another explosive Bitcoin price growth, Chelan County saw energy consumption considerably increase and enacted another moratorium on miners. In 2018, Wenatchee, the largest city in the county, banned crypto mining in residential and mixed-use areas for a year due to unauthorized miners overtaxing the power system. As Bitcoin and cryptocurrency continue to grow, increase in price, and gain popularity, more energy consumption boomtowns are likely to show up around the world.

4 Cryptocurrency Competition

After Bitcoin took off, it was not long before other people latched onto the cryptocurrency idea and changed it to how they would prefer it. This sparks competition between the cryptocurrencies. These competitors are called Altcoins [18]. All Altcoins take portions of Bitcoin and mimic it by creating slight differences in the structure. Since all cryptocurrencies utilize the blockchain model from Bitcoin, each cryptocurrency takes that section of code. Blockchain is the common statistic between them all. How that blockchain is used and monitored is where the differences come into play. As new currencies appear, new methods of reading the blockchain and monitoring transactions are created as well. This is the power of Altcoins.

4.1 Altcoins

Most Altcoins are like Bitcoin and build upon preexisting code. The best example of this is that most Altcoins use blockchain methods. To show this, an example of an Altcoin is Litecoin. A major promotion of Litecoin is that it can generate four times as many coins as well as add the transactions to the blockchain four times faster [19]. Another example of an altcoin making significant changes is Peercoin. Like how bitcoin utilizes blockchain and proof of work, Peercoin takes these efforts and improves upon them. Peercoin utilizes proof of stake alongside proof of work. With this, Peercoin can mitigate the need for powerful, and expensive computers for mining [20]. This makes it more acceptable to a common household family as a viable currency.

Bitcoin is the leading form of cryptocurrency. In 2017 the revenue of bitcoin was drastically higher than its competitors. Bitcoin made over $25 billion while other cryptocurrencies made just over $5 billion [21]. Litecoin and Peercoin are the

next leading options for cryptocurrency. Litecoin in 2011 and Peercoin in 2012. The purpose of the cryptocurrencies is not solely in competition, but to solve some of the inherent problems Bitcoin caused. As interest in cryptocurrency grows, so does the interest in creating a different currency. This is where the root of the competition begins.

5 Advantages of Cryptocurrency

The issues with the main system for doing payments of the internet i.e., giving our credit card information to a seller, is that people are exposing our identity as well as sensitive credit card information to the seller, let's say Amazon, and then that information is passed to another financial system, let's say MasterCard. Not only does this expose our financial information, but it also provides no anonymity when doing transitions online. One potential solution to this problem would be an intermediary between buyer and seller, such as PayPal. Here, both buyer and seller have an account with PayPal.

When a buyer wants to do a transaction with a seller, all they need to do is tell PayPal to charge the buyer for the transaction [22]. Since PayPal has both the seller's payment information and buyer's, they can just directly charge the buyer and they credit the seller without giving any of the payment details to the seller directly. While this is an improvement to previously giving our payment information directly to a seller, there is still the problem of anonymity that is not solved. A PayPal account is tied directly to a person that can be easily traced. Another problem with this system is there is a central authority, that is PayPal that is governing over the transactions, much like the banks do today.

Another failed system that predates Bitcoin was DigiCash. DigiCash, which was patented by David Chaum sought to seek out the challenges of creating a digital coin that deals with the classic double spend problem. Chaum's implementation uses what is called a "blind signature" where a central authority issues a coin, but you get to pick the serial number of it, then the central authority signs it, this way the coin is verifiable as being spent or not. DigiCash also relied on merchants to support it. With DigiCash, buyers are anonymous, but the merchants are not. When doing a transaction on a merchant's website, the DigiCash system would open a secure connection between the merchant and buyer so that the buyer can securely approve the transaction. While this system prevents double spending and is a form of anonymity, it still relies on a central authority to monitor transactions, such as a bank [22]. It ultimately failed due to these reasons as well as nobody wanted to adopt this system. Also note that DigiCash was primarily merchant-to-user transactions, there was no support for user-to-user transactions.

To propose another issue with previous ecash systems was minting new currency. With DigiCash, to acquire $100 of DigiCash, you needed to trade in $100 of real dollars to the bank. There are of course other failed implementations of minting a digital currency, such as e-Gold, which sought to back up the digital coin with a

vault of gold that was stored away. But with these implementations, the coin is still backed by some commodity or by a government. Bitcoin solves this minting and value problem by using a proof-of-work system. Here, miners use their computation resources to compete against other miners in order to obtain bitcoins in the form of a reward for solving a difficult puzzle. This difficult puzzle is the same computational puzzle as a Hashcash [23]. The reason for the difficult puzzle was security, but the reason for its success comes in the form of the reward for solving it.

The first main incentive for a node to be honest is by using a block reward [22]. The block reward is given (in bitcoin because this is currency!) to the miner who solves the Proof-of-work puzzle. The challenge here is that the transactions that the miner proposes as to be added to the blockchain must all be valid. When other miners perform their checks on the transactions, if they find that one of those transactions is invalid, those miners will choose not to extend that block onto the longest running blockchain, and thus the miner who mined that block will not get the reward. The other incentive is via transaction fees. A transaction fee is the implicit difference between the amount of the amounts and the total outputs. These transaction fees are paid to the miner who found the next block and is proposing said transactions. The transaction fee is paid by the person who is spending the bitcoins, and overtime has become an unofficial required fee. If no fee is paid, your transaction could take a long time to get into the block chain as miners will prioritize including transactions with fees.

Countries are starting to acknowledge Bitcoin as legal tender. The United States and various European countries are starting to accept bitcoin to be exchanged into green backed currency like the U.S. Dollar and Euro. However, it still stands that most of the countries still do not allow corporations to trade directly with one another via the Bitcoin system. This is where one country is starting to change.

5.1 Direct Trading

Bitcoin in El Salvador is striking controversy with its users and the World Bank. On June 8, 2021, President Nayib Bukele passed a law to make Bitcoin a legal tender. The goal of passing this law was to save on remittances from traditional money transfers. El Salvador's past with transactional fees, the hope that Bitcoin will stop the problem is high [24]. It is important to see how Bitcoin will affect the country by looking into the background of remittances, how people viewed bitcoin in the past, and how Bitcoin's remittance compares to traditional currency.

El Salvador relies on remittance payments for 20.93% of its GDP. Since the country relies on remittance payments, President Nayib Bukele is doing whatever he can to assist his people. When taking money from the World Bank, there are fees associated with those payments. Most firms charge between 3–4% per $200 and 1–2% per $500 payment. These fees add up quickly. These demanding fees is the direct reason stated by President Nayib Bukele. With that it was clear an alternative

method was needed. The option that was decided on in June 2021 was Bitcoin. It seemed like a promising new and improved form of currency. However, that was not always the case.

In 2019, the coastal town of El Zonte adopted Bitcoin. It was an incentive for shop owners to use Bitcoin as a means of payment, but a major problem occurred. There is a major obstacle that the government failed to realize. To access Bitcoin as payment over the internet, the people need access to the internet. Not all citizens of El Zonte have the internet which makes payments with Bitcoin impossible. 92% of respondents said they did not want a mandation of Bitcoin, and 93.5% said they did not want to receive salaries in Bitcoin. That is the most pressing matter, but it is not the only problem occurring. The other major issue is that fees of Bitcoin may be more than expected.

Since many stores still require greenback currency, Bitcoin must be exchanged at a Bitcoin ATM. These ATMs charge a fee. The fee is 5% for every transaction (https://athenabitcoin.com/). Noted above the average fee % on payments was only 3–4% on the average highest end. The virtual transaction of Bitcoin from one user to another is significantly less than greenback currency, the fees for using Bitcoin come out to be higher than the original fee of the greenback currency.

Even though Bitcoin is becoming a recognized currency in countries, it is still far away from becoming a major currency. Even with all the security risks involved with the currency, the fact that not everyone can obtain it is crucial. The problem of remittances, the history of rejection by civilians, and the alternative fees imposed on people continue to hold back the progress of Bitcoin. Only when all people can truly access it can Bitcoin become a viable option for civilians.

6 Processing of Cryptocurrency

All cryptocurrency transactions have a beginning. A transaction occurs when a payer sends currency to a payee. When a transaction takes place, the miner then checks the payer to ensure that they have the currency, and that the payer is not trying to double spend. The miner must perform Proof of Work where the result of the resource confirms the performance [25]. This is achieved when transactions are recorded by combining the digital signatures of each party's timestamp.

6.1 Signatures

Once done, the digital code is then broadcasted to all nodes on the network. Each node then agrees the transaction is correct and then the transaction legitimate. This puts integrity into the system, using blocks. With the bitcoin protocol, all transactions are collected into a block. A block is the item that gets broadcasted to all nodes connected on the network. The way each node verifies the block is by adding a nonce to it. This

way each node uses the SHA-256 hashing function to decipher the (block + nonce) algorithm [1]. It finally ends out with (block + nonce + hash). As only one block can only be verified at a time, the amount of CPU power expended can increase proportionally. Hence why CPUs are vital to bitcoin mining.

6.2 Proof of Work

This process is called Proof of Work. The purpose of this proof is to protect all miners' transactions as well as their mining. This proof functions as the fundamental security for all miners of Bitcoin. It is crucial for the proof to work as mining is how Bitcoin generates more coins for each miner which in turn increases the value that each coin is worth. With the Proof of Work, trying to cheat the system is significantly harder. Mining works in the following steps.

1. The miner selects transactions to verify
2. The transactions are then put into a Merkle Tree
3. It then extracts the root block has from the Merkle Tree
4. Then it adds a nonce or "hashes the block header"
5. The nonce and hash are incremented until the desired result is obtained
6. Once done, this is a form of Proof of Work.

However, Proof of Work is only one form of proof. Bitcoin uses Proof of Work, but there are others like Proof of Stake and Proof of Retrievability. Proof of Stake requires that the miner must show how much currency the miner already owns in the system [26]. This shows that a miner has the money to make the transactions with. Proof of Retrievability on the other hand has it where the miner is required to show that the data that was given has been stored intact and can be recovered as well [27]. This proof is set up that a miner cannot continue with a transaction until it is shown that the translation is fully complete. It also proposes that each proof relies on the fundamental aspect of the blockchain, and why every cryptocurrency utilizes it.

6.3 Proof-of-Stake

November 25, 2014, Vitalik Buterin, a co-founder of Ethereum, writes a blogpost [28] on the benefits of proof-of-stake as a consensus mechanism and addressing some arguments against proof-of-stake. On December 1, 2020, Ethereum ships "The Beacon Chain", Ethereum's phase 0 into the transition from proof-of-work consensus to proof-of-stake consensus, known as Ethereum 2.0. On the official Ethereum site, Ethereum 2.0s vision of moving from proof-of-work to proof-of-stake is to improve Ethereum's scalability, security, and sustainability. In early 2022, Ethereum plans to merge the Beacon Chain, a set of upgrades and the proof-of-stake consensus

mechanism, together with the main Ethereum chain, enabling staking for the rest of the network and phasing out proof-of-work.

While there are many consensus mechanisms, proof-of-work and proof-of-stake are the most prevalent. As the concerns of the proof-of-work consensus mechanism are brought to the forefront of the cryptocurrency sphere, Ethereum has had switching to proof-of-stake in its future since early in its development. Proof-of-stake is a consensus mechanism where instead of using computational power to add blocks to the blockchain, users must stake their own tokens in order to participate in the validation of new transactions and updating the blockchain which is overseen by the network. Benefits of proof-of-stake include better energy efficiency, lower barriers to entry with reduced hardware requirements, stronger immunity to centralization, and faster transaction confirmation speeds [29].

6.4 Hashcash

Hashcash is a mechanism for providing a difficult puzzle to solve to a client. By challenging a client to solve a difficult puzzle, it provides a way to show proof-of-work, i.e that a client performed some expensive computation where the work is done in cpu cycles. Upon solving the puzzle, the client is granted a token to which they can spend. The original implementation of Hashcash was to solve the problems of spam emails [30].

Hashcash provides an efficient way to block email spammers by offering this challenge to each email they would send. For a regular user, sending a few emails a day does not provide much delay in sending the emails. But for a spammer who may be sending thousands of emails per second, solving all these challenges becomes difficult thus providing a bottleneck.

Bitcoin has adapted this concept for its proof-of-work, where the miner needs to solve a difficult challenge in order to propose the next block for consensus. In Hashcash, a long string, which consists of a version, difficulty, timestamp, resource, and random string [30]. Once the string is generated, it is hashed with a nonce value that is "guessed" by the miner. If the hashed value begins with n number of zero bits (where n is the difficulty) then the puzzle is solved. If the value does not meet this requirement, another nonce is tried until the puzzle is solved.

Now to get into some of the properties of Hashcash that make it work. Hashcash is a cost-function. This means it is expensive to compute but easy to verify [23]. To verify, you just hash the challenge string with the nonce value, and if it meets the difficulty requirement then it's solved. Hashcash is hard to solve because the best way to solve the puzzle is with a deterministic algorithm [30]. What people mean by deterministic algorithm is that there is no efficient function or value to guess for the nonce, so the best method is by using random values. Finally, Hashcash is Trapdoor-free, meaning the server that is serving the challenges has no advantage of mining tokens [30].

6.5 Security

First off, Bitcoin accomplishes security in a variety of methods. Bitcoin employs block chain technology to be an append only, tamper proof ledger. The ledger is tamper proof because the data contained in the ledger undergoes cryptographic hashing. A cryptographic hash is a 1-way function that takes any data and produces a fixed-size output in an efficient calculation [22]. Secure hash functions provide a property called collision free. A collision free function says that nobody can feasibly find X and Y, such that X does not equal Y and the hash of X equals the hash of Y. Hash functions also need a hiding property. This hiding property states that given the hash of X, it is infeasible to find X. Since the input space is larger than the output space, the pigeonhole principle states that there exist at least two inputs that would hash to the same output value.

Finally, the hash function needs to have an avalanche effect, where any change in the input completely changes the output. If we have all three of these properties satisfied, then nobody will be able to (1) change any bit of data since the hash of it will change completely; (2) nobody will be able to produce another value Y where the hash of Y equals the hash of the data, thus the data cannot be altered this way; and (3) if we hash two values X and Y together, then we can easily verify if Y is the correct hash given X and the hash value.

To quickly ensure that each transaction is immutable, we will employ the concept of a Merkle Tree [1]. In Merkle Trees, each transaction will be added to a perfect binary tree. Then from the bottom up, two pairs of transactions are hashed together. This process continues until there is one node left called the Merkle Root which contains a cryptographically sound hash of the entire tree [31]. To ensure that not a single bit is changed in each block, we need to link them together with hash pointers. With hash pointers, each block contains a pointer to the previous block's hash, thus if a single bit is changed in the block, it will break the next block's previous hash pointer.

Now that we have hash functions to provide security in the form of immutability, we need a secure way of making payments to other entities. A couple of challenges that need to be solved with a digital currency include: how can someone that is sending the currency digitally sign-off on the transaction? Where exactly does, the currency get sent to? How can we detect/prevent other malicious entities from forging our payments to steal our currency? All these challenges can be solved with public and private keys [22].

Under a digital signature algorithm, such as the Elliptic Curve Digital Signature Algorithm, both the public and private keys are derived as a pair. The public key acts as a public address which is distributed to the public. Although Bitcoin is an anonymous currency, the public key is what acts as the identity. The private key is kept securely from everyone else and is used to digitally sign messages. Once the message is digitally signed with the private key, only given the private key will the message signature be valid. A message should be easily verifiable by anyone given the public key, the message, and the signature.

How does bitcoin achieve consensus between competing nodes in the network and how does the network ensure that nodes are incentivized to be honest? Both problems can be solved with proof-of-work [22]. As described earlier, Bitcoin uses Hashcash for its proof-of-work mechanism. Once a miner successfully solves a Hashcash puzzle, they are awarded Bitcoin and collect the transaction fees from all the transactions contained in the block. After the puzzle is solved, the block is also proposed to the rest of the network for consensus. During consensus, all other nodes check the block to ensure it is really solved and go through each transaction to verify they are valid transactions. If a miner finds a fault with a translation or the block, the miner will not extend the blockchain with the proposed block. If enough miners reject the proposed block, the block will not make it in the longest running blockchain called the consensus chain and therefore the miner who mined the block will not get the reward.

Finally, a transaction model is required to make cryptocurrency a fully-fledged currency. In traditional banking with fiat currency, an account-based model is used. With an account-based model, users have an account with a balance. To make transactions, their accounts are debited and or credited based on the transaction amount. Bitcoin does not use a transaction model. Instead, they employ a new model called the Unspent Transaction Output (UTXO) model. A Bitcoin transaction contains a list of transaction inputs and transaction outputs. The inputs contain hashes for the previous transaction, an output index from which the transaction originates, and the signature of the input. The output contains the public key of the recipient, and the value of the transaction. The UTXO then consists of the hash of the transaction, and the index of the output. Since we are given the hash of the transaction from which the UTXO originates, and we are given the output index of said transaction, we can get the output value and where the output goes to. Bitcoin maintains a pool of all the UTXO's which are available to be spent, and given an UTXO, a user can submit a new transaction.

7 Conclusions

Bitcoin has many distinct attributes that have proposed its longevity. It has lasted for years already and continues to improve and become recognized. The research of Bitcoins history, problems, competition, and advantages has suggested that Bitcoin has significant structure that continues to improve. With the simulation that was created, Bitcoin is going to stay for a while. It is impossible to know if Bitcoin will be the currency of the future, but the data suggests that it will become a common form of legal tender that is utilized by numerous countries and corporations.

References

1. Nakamoto S (2009) Bitcoin: a peer-to-peer electronic cash system, May 2009
2. Rauchs M, Hileman G (2017) Global cryptocurrency benchmarking study. Number 201704-gcbs in Cambridge Centre for Alternative Finance Reports. Cambridge Centre for Alternative Finance, Cambridge Judge Business School, University of Cambridge
3. Yermack D (2013) Is bitcoin a real currency? An economic appraisal. Working Paper 19747, National Bureau of Economic Research, Dec 2013
4. Ahmed M, Akhter A, Rashid A, Fahmideh M, Pathan A-S, Anwar A (2022) Blockchain meets secured microservice architecture: a trustworthy consensus algorithm. In: Proceedings of the 19th international conference on wireless networks and mobile systems—WINSYS. INSTICC, SciTePress, pp 53–60
5. McMillan R (2014) The inside story of Mt Gox, Bitcoin's $460 Million Disaster. https://www.wired.com/2014/03/bitcoin-exchange/
6. Fargo S (2015) Bitcoin.com. https://news.bitcoin.com/
7. Vásquez J, Voia M, Balutel D, Henry C (2021) Bitcoin adoption and beliefs in Canada. https://www.bankofcanada.ca/2021/11/staff-working-paper-2021-60/
8. Chan S, Chu J, Nadarajah S, Osterrieder J (2017) A statistical analysis of cryptocurrencies. J Risk Financ Manag 10(2)
9. Huang DY, Aliapoulios MM, Li VG, Invernizzi L, Bursztein E, McRoberts K, Levin J, Levchenko K, Snoeren AC, McCoy D (2018) Tracking ransomware end-to-end. In: Proceedings—2018 IEEE symposium on security and privacy, SP 2018. Institute of Electrical and Electronics Engineers Inc, July 2018, pp 618–631
10. Wood J (2022) Crypto Ponzi schemes: how to identify and protect yourself from these scams. https://www.coindesk.com/learn/crypto-ponzi-schemes-how-to-identify-and-protect-yourself-from-these-scams/
11. Wright J, Anise O (2018) Don't@ me: hunting twitter bots at scale. Blackhat USA
12. Phillips R, Wilder H (2020) Tracing cryptocurrency scams: clustering replicated advance-fee and phishing websites. In: 2020 IEEE international conference on blockchain and cryptocurrency (ICBC), pp 1–8 (2020)
13. Chauhan A, Malviya OP, Verma M, Mor TS (2018) Blockchain and scalability. In: 2018 IEEE international conference on software quality, reliability and security companion (QRS-C), pp 122–128
14. Musk E (2021) You can now buy a Tesla with bitcoin. https://twitter.com/elonmusk/status/1374617643446063105?
15. O'Neill C, Huang J, Tabuchi H (2021) Bitcoin uses more electricity than many countries. How is that possible? https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html
16. Schinckus C, Nguyen CP, Chong FHL (2020) Crypto-currencies trading and energy consumption. Int J Energy Econ Polic 10(3):355–364
17. Greenberg P, Bugden D (2019) Energy consumption boomtowns in the united states: community responses to a cryptocurrency boom. Energy Res Soc Sci 50:162–167
18. Farell R (2015) An analysis of the cryptocurrency industry
19. Gandal N, Halaburda H (2014) Competition in the cryptocurrency market. Technical report
20. Zhao W, Yang S, Luo X, Zhou J (2021) On peercoin proof of stake for blockchain consensus. In: 2021 The 3rd International Conference on Blockchain Technology, pp 129–134
21. Rauchs M, Hileman G (2017) Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance. Cambridge Judge Business School, University of Cambridge
22. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S (2016) Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press
23. Back A (2003) Hashcash—amortizable publicly auditable cost-functions, Dec 2003
24. Hanke S, Hanlon N, Chakravarthi M (2021) Bukele's bitcoin blunder. Studies in applied economics, vol 185. The Johns Hopkins Institute for Applied Economics, Global Health, and the Study of Business Enterprise, June 2021

25. Mukhopadhyay U, Skjellum A, Hambolu O, Oakley J, Yu L, Brooks R (2016) A brief survey of cryptocurrency systems. In: 2016 14th annual conference on privacy, security and trust (PST), pp 745–752
26. Nadal S, King S (2012) Ppcoin: peer-to-peer crypto-currency with proof-of-stake
27. Miller A, Juels A, Shi E, Parno B, Katz J (2014) Permacoin: repurposing bitcoin work for data preservation. In: 2014 IEEE symposium on security and privacy, pp 475–490
28. Buterin V (2014) Proof of stake: how i learned to love weak subjectivity. https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity
29. Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E (2019) Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access 7:85727–85745
30. Back A (2002) Hashcash-amortizable publicly auditable cost functions. Available http://www.hashcash.org/papers/amortizable.pdf
31. Merkle RC (1988) A digital signature based on a conventional encryption function. In: Advances in Cryptology—CRYPTO'87: Proceedings, vol 7. Springer, pp 369–378