Cryptocurrency

Anthony Waterman

December 3rd, 2023

CS 463

Professor Zehra

Cryptocurrency

Cryptocurrency is a relatively new phenomenon that started with Bitcoin. With the invention of cryptocurrencies came the invention of blockchain technology. As blockchain technology evolved, so did cryptocurrencies themselves. We began to see new coins and a newly created token. Over time cryptocurrencies have become a means to pay for goods and services or an asset found on someone's investment portfolio. With the hype surrounding cryptocurrencies continually increasing, it is important that we know what they are and how they work. We understand that cryptocurrencies utilize blockchain technology, but what is blockchain technology? Is this technology scalable? Does this technology require continuous upkeep or is it fully automated? These are all important questions that we will answer in this paper. Before we discuss the blockchain and how it works, we must first begin our examination at the beginning with Bitcoin.

What are cryptocurrencies?

In the most simplistic terms, cryptocurrencies are digital forms of money that utilize cryptography when performing transactions. Cryptocurrency gets its name from the cryptographic encryption used for its security. The most important aspect, aside from cryptographic utilization, is that cryptocurrencies are not issued by any nation, group, or party. These digital assets are completely decentralized and can be stored in digital wallets. These digital wallets are akin to a thumb drive. Cryptocurrencies allow for peer-to-peer transactions with no regulatory body overseeing it. Since crypto utilizes peer-to-peer transactions, each transaction is recorded on a public ledger [1]. This public ledger is what's known as the blockchain [1]. A big difference between traditional currency and cryptocurrency is how its earned. Traditional currency is earned from working, the selling of goods or services, and much more. Cryptocurrency requires little effort from a person because all the work is done by a computer. The computer performs complex mathematical calculations that, over time, generate coins. This process is called mining. Many people around the world have dedicated computers that constantly mine cryptocurrencies. Mining can be done by almost anyone, however there are plenty of people that utilize mining farms. These are large buildings that house tons of graphics cards and processors that are dedicated to solving these mathematical equations for cryptocurrencies. Some examples of these cryptocurrencies are Bitcoin, Ethereum, Litecoin, and Ripple. Bitcoin was created in 2009 and was the first cryptocurrency available. The creator of Bitcoin also introduced blockchain technology which allows the rest of the cryptocurrencies to exist. The second most popular cryptocurrency is Ethereum. Unlike Bitcoin, Ethereum is known as a token. Coins and tokens utilize blockchain technology, but they are slightly different. Coins are native to the blockchain while tokens are built on an existing blockchain [2]. Now that we have a base understanding of cryptocurrency, its time we discuss the blockchain and everything it entails.

What is the blockchain?

The blockchain is a distributed database that's shared amongst different computers [3]. As stated in the previous paragraph, this database is used to maintain a record of all transactions that

is secured via cryptography. The blockchain is so secure that it makes all data within it immutable [3]. Because these blocks cannot be changed, the only point of trust in the system is when a user or program enters data [3]. Since there is only one point of trust in the system, it reduces the possibility of error provided by humans such as auditors [3]. An important aspect of the blockchain is that, because its decentralized, no one party can control it. Aside from the ledger, the blockchain also utilizes smart contracts, and public key cryptography [4]. Smart contracts are automated systems that are stored on the blockchain that complete transactions based on if-then checks [4]. Public key cryptography is utilized for accessing the ledger to view transactions. Each person who uses crypto has a private key. The public key is available to everyone on the network. This means, if two people proceeded with a transaction, they could access the transaction ledger to see if the transaction was completed [4]. If either party's private key was tampered with, the public key would not have been able to decrypt the transaction record [4]. The blockchain works via a four-step process. This process is as follows: transaction recording, gaining consensus, link blocks, share ledger [4]. This means for every transaction recorded, a majority of users must agree to have that transaction added to the ledger. Once this is done, new blocks are created and linked and then an updated ledger is sent out to all users [4]. The blockchain also offers different types of networks. These include a public network, private network, hybrid network, and a consortium network [4]. Now that we understand the blockchain itself, we need to understand what a block is. A block is a collection of recorded transactions that have not been permanently recorded to the blockchain [3]. Once these blocks are validated, they are closed and permanently stored on the chain [3]. Once a block is closed a new one is opened to continue recording transactions [3]. Each block houses different elements. These elements include magic number, blocksize, block header, transaction counter, transactions, version, previous block hash, hash Merkle root, time, bits, and nonce [3]. With all these elements, we create a block. These blocks are connected utilizing a couple different elements. These two elements are the Merkle Tree and the previous block hash [5]. The Merkle Tree is a data structure that encodes the blockchain itself [5]. The previous block hash is incorporated into the new block, so it's encoded in the correct location in the Merkle Tree when it gets validated [5]. Once a block is validated, a new block must be added to continue the recording of transactions. This responsibility falls on the shoulders of crypto miners. The miners are responsible for ensuring the accuracy of the data being recorded in the block prior to its validation [6]. This does not mean the miners are the ones maintaining the blockchain itself. Depending on the type of network, the systems maintaining the blockchain will vary. Public blockchains are maintained by everyone involved while private blockchains are maintained by a single entity [4]. With all of this in mind, we now must understand the size of these chains and how different sizes can affect performance amongst machines and the overall scalability of the blockchain.

Blockchain Scalability

For this section we will look at Bitcoins blockchain. When Bitcoin's blockchain was created, the creator set a block limit of 1 MB per block [7]. This was to ensure the blocks could be validated and a faster pace. The larger the amount of memory the longer it would take for the blockchain to update. Due to the drastic increase of transactions, the block size limit was increased to 4 MB in 2017 [8]. This change was to allow for more recorded transactions per

block. The reason the block limit is 4MB and not a larger value is to prevent security risks and prevent the loss of decentralization [7]. This discussion of scalability has been deemed the blockchain trilemma [8]. If the blockchain were to increase in scale, there would be more systems connected which results in a higher security risk. If the blockchain increases in scale and has robust security, the cost of maintaining the blockchain would go up which would result in the need to centralize [8]. These issues are related to the blockchain itself and the software surrounding it. The performance issues for systems brings a different set of problems. When scaling the blockchain, we must remember that each block holds multiple transactions. Each of these transactions require a computer to perform complex mathematical processes. The larger the scale of the blockchain, the more processes need to be performed. Computational hardware has limits, so scaling the blockchain would require a huge hardware requirement increase for all miners. The second performance issue is related to storage. Each miner must store a copy of the ledger on their systems [8]. As the scale of the blockchain increases, so does the storage requirements of the miners. More storage utilized results in slower computation rates. Aside from these issues related to scalability, we run into another possible issue. Even with scalability issues, the blockchain is being utilized for more than just cryptocurrency.

Applications using the blockchain

As it stands, cryptocurrencies are the largest utilizers of the blockchain. However, this technology has begun moving its way into different sectors. We previously discussed an application called smart contracts [4]. These contracts are utilized by businesses when it pertains to paying for different operating costs. An example of this would be a company receiving a shipment of goods from overseas. Once the shipment has been confirmed, the smart contract automatically approves the transaction and sends the payment to the shipping company. Blockchain technology has started to move into the banking industry as well. Banks can utilize the peer-to-peer system to reduce the cost of moving money [9]. A great example this is Cash App. Cash App utilizes the blockchain to provide peer-to-peer payments with no third-party authority involved. We can also store money in our cash app wallet in the same way crypto can be stored on a digital wallet. A new application for the blockchain is its utilization in the IoT [9]. This usage of the blockchain is directed at unsecure technology in the home. This can be a smart socket, smart thermostat, a smart bulb, or anything that is connected to the network without being encrypted. A great utilization of the blockchain is storing personal information. There are a few companies that have begun working on ledgers that allow for personal information encryption [9]. Utilizing the cryptographic structure of the blockchain for our personal information would reduce identity theft online. Logistic organizations also utilize blockchain technology for tracking and transparency [9]. Another popular use for the blockchain is for NFTs. NFTs are called Non-Fungible Tokens. These usually come in the form of digital art that is bought and sold. NFTs are digital assets that, for a short period, wanted to take the place of cryptocurrency. This was due to the talks about the government figuring out a way to tax and regulate coins and tokens. Because NFTs are digital assets and not a form of currency, they would be very hard to tax or regulate.

Security of cryptocurrencies

Cryptocurrencies utilization of the blockchain makes it heavily secure. This does not mean there are no weaknesses. There are many security issues that specifically target the crypto owners themselves. Phishing schemes are popular because they can trick people into revealing their wallet information. These schemes can also give an attacker the ability to infiltrate the user's computer and force it to mine crypto for them without the owner of the computer knowing. Another popular attack is a ransomware attack. These seemingly happen all the time. A person's computer gets hacked, and the hackers encrypt sensitive information. They then demand a payment of cryptocurrency, usually Bitcoin, in exchange for the decryption key. The reason why hackers target users instead of the crypto exchanges themselves are because of the security surrounding them. There is a specific standard called the Cryptocurrency Security Standard that is utilized for each exchange on the network [10]. The main reason why its so hard to hack into a crypto exchange is because of how the nodes work together. They offer a balance structure that prevents an attacker from altering anything within a specific node [10]. This is because each node has a copy of the database [10]. If a value is changed in one node, the other nodes will reject it because that value does not match what they have stored [10]. These nodes also utilize signatures for transactions. If one node authorizes a transaction, the other nodes need to authorize it as well with the signature that was provided to the initial node [10]. If the other nodes do not receive the signature, the transaction will be rejected [10]. There is the possibility of a double-spend attack to occur, however the overall security surrounding crypto exchanges makes these kinds of attacks very expensive [10]. As we can see, crypto exchanges are very secure, but there is an attack that poses a significant risk. This attack is known as a 51% attack [11]. This is when a miner controls more than 50% of the computing power used to validate transactions on the blockchain [11]. This means, the miner/miners would be able to dictate who gets awarded cryptocurrency after completing these computational transactions. This is highly unlikely to happen. This is why hackers target the user specifically rather than attempt to hack an exchange or become a miner and award themselves a large sum of crypto. Many different crypto exchanges offer security features to reduce attacks on the user. Some crypto exchanges offer two factor authentication via phone number. Having a code generator would be a better option for security since number porting is something that occurs. Many crypto investors utilize hardware wallets that they put all their crypto on. These wallets are very secure because they also use cryptographic encryption. They generally can only be opened with a password or a biometric input.

Puzzles in cryptography

When pertaining to puzzle in cryptography, we are referring to different encrypted messages or values. A message is encrypted using an encryption method and then someone must decrypt it with a specific cipher. A basic form of cryptographic puzzles are those utilizing the Caesar Cipher. This is a basic substitution cipher that substitutes a letter for another letter. To be more specific, the letter being substituted would shift two positions to a new letter. So, the letter A would be substituted for the letter C. We can also shift three or four positions to achieve the same result. These ciphers have evolved to become more complex. Newer encryption and decryption methods require computational power to solve the puzzle due to the number of calculations required to decrypt the message. DES and AES are examples of these methods.

These more advanced methods utilize larger block sizes that encompass far more than the alphabet. Depending on the encryption standard, there could be 64-bit blocks, 128-bit blocks, 256-bit blocks, and so on. Each block size results in a more secure encryption but increases the computational effort to decrypt the information. Many different websites utilize these types of encrypted connections. To provide more security, websites will utilize some form of key encryption standard. When we buy something online, the website will utilize asymmetric key encryption. This means that payment information is encrypted with a public key and the payment information can only be decrypted by the key the payment authority generates. In the way a hacker would attempt to decrypt the information that is encrypted via a key or cipher, miners try to solve puzzles with their computers to mine for cryptocurrency.

Translation of cryptographic puzzles to cryptocurrency

As previously stated, crypto miners utilize their computers to solve complex equations to mine for cryptocurrency. These equations can be looked at like puzzles. To be more specific, these puzzles come in the form of hashes. Hashes can vary in size, however depending on the size drastically increases the number of possible outcomes. We briefly highlighted the elements of a block in the blockchain. One of those elements is what the miners are trying to find. This element is called a nonce. The nonce is the solution the miner is looking for [12]. Each nonce is unique to each block and once a miner discovers the nonce, they are rewarded with cryptocurrency. Each cryptocurrency presents a different hash rate that's dependent on the miners and the type of cryptographic hash used. As it currently sits, Bitcoin miners process 190 quintillion hash functions per second [13]. This is because Bitcoin utilizes a SHA-256 bit hash function [13]. This means there are 256 characters that can be utilized in each puzzle. These hash rates are important for miners because they are in competition with one another [13]. The entire goal of a miner is to solve the cryptographic hash and get paid cryptocurrency for their work. This also accounts for greater security among the different networks. The more transactions being validated results in a higher difficulty for an attacker to successfully infiltrate the network [13] The large number of miners helping drive up the hash rate reduces the ability for a 51% attack to occur on a network [13] In more simplistic terms, the larger the payout helps increase the number of puzzles being solved which results in a more secure network.

Cryptographic techniques used for cryptocurrency

The blockchain utilizes a few different techniques we discussed in this class. The first being asymmetric key encryption. Asymmetric key encryption is when information is encrypted with a public key and is decrypted with a private key. We used an example of this earlier in this paper when we discussed transactions. For the blockchain, asymmetric key encryption allows for great security revolving around the transactions found in the blocks. If the either parties key has been tampered with, the encrypted data will not decrypt. This lets the user know the information has been tampered with without compromising their system. Another example of a technique we learned being utilized within the blockchain are digital signatures. These digital signatures are given to every node in the network as proof that they are legitimate and can begin mining [14]. We discussed this earlier in the paper as well. There is strong security surrounding the usage of digital signature. If we recall from the previous section on security, we know that all nodes must

authorize a new node via a signature. If the new node fails to provide signatures to all the nodes, the new node will not be allowed on the network. Hashes are also used in the blockchain. Hashes are utilized when trying to find a specific set of values through decryption. Hashes are utilized in cryptocurrency when it comes to mining and the placement of blocks. In the previous section, we discuss how miners are constantly trying to solve hashes by looking for the correct nonce for each transaction. In the previous section dedicated to understanding what a block is, we find that the previous hash is put in the newly created block. This ensures that, once the new block has been closed, it is placed in the correct location within the blockchain. These hashes do more than just provide great security for the blockchain. They also help reduce utilized bandwidth on the network, make the data immutable, and make verification easier for each transaction [14]. Cryptocurrencies provide many different advantages over traditional currency thanks to the robust security surrounding it.

Advantages of cryptocurrencies compared to traditional currency types

Traditional currency offers different mediums. We can utilize physical notes or debit/credit cards. Physical money offers the same benefit as a hardware wallet for cryptocurrency. The biggest disadvantage to physical money is theft. If someone were to steal physical notes, the thief would have access to the funds immediately. If someone were to steal a hardware wallet that is encrypted, they will not be able to cash out on the crypto in the wallet. Another disadvantage to physical notes is that everyone knows what physical notes look like. A physical crypto wallet looks like a thumb drive. This device is not likely to catch the attention of anyone wanting to steal money. When pertaining to credit/debit cards, cryptocurrency holds more advantages. Cards offer little protection against theft. Each card comes with a magnetic strip, chip, and usually NFC capabilities. The chip provides protection against something such as card skimming. The NFC capabilities and the magnetic strip are susceptible to card skimming. Some criminals will put card skimming devices on payment terminals in stores or gas pumps. Once we utilize our card with the magnetic strip, the card information is recorded and sent to the criminal. They can then make a copy of the card used. Another type of skimming involves the NFC capabilities built into the card. Some card skimmers will have NFC devices in a bag or some sort. They have to get close enough for your card to register on their device. Once they do that, they can capture the card information and clone it. We also utilize our cards online for reoccurring payments for bills or to purchase goods. If a company is involved in a breach, all our information could be exposed. An example of this would be the T-Mobile breach. Hackers were able to infiltrate their network and steal customers information. This information ranged from personal information to payment information. Having credit card information stolen while buying goods online is less likely to happen due to DES and AES, but it is still possible. There is also the possibility of physical theft. Cryptocurrency offers solutions to all those problems. Cryptocurrency is a digital asset that cannot be stolen like physical money. If its loaded on a physical wallet that wallet can be stolen. However, the cryptographic encryption on the wallet would prevent theft of that cryptocurrency. Crypto exchanges are also highly secure and is near impossible to infiltrate with hacking methods. The constant hashing prevents intrusions into the network while asymmetric key encryption prevents alterations to the data. No one can skim information from a physical crypto wallet. Due to the intense security surrounding crypto

exchanges and the blockchain, breaches are next to impossible to happen. The only point of failure that would allow any type of intrusion would be the failure of the user. If they do not properly secure their information or they fall for a phishing scheme, then their accounts can be taken over. This would result in the loss of their funds; however, these types of attacks would not result in an intrusion on the blockchain or crypto exchange itself. Cryptocurrency also provides other advantages not related to possible theft. With crypto being decentralized, its value cannot be dictated by market fluctuations or entities. Transaction fees are very low to the point where they are almost nonexistent [15]. This is due to the removal of third-party companies needed to process the transfer of money from the consumer to the merchant [15]. Cryptocurrency is also protected from inflation [15]. This is due to the cap of minted coins allowed [15]. Cryptocurrency also offers higher returns for individuals who invest. The protection against inflation coupled with it being decentralized are the reason why cryptocurrency has such impressive returns on investments. Cryptocurrency is far more accessible than traditional banks. Traditional banks have branches in certain parts of the country and may only offer benefits to certain people. An example of this would be Navy Federal Credit Union. Cryptocurrency only requires an internet connection and a crypto wallet of some kind [15]. Crypto wallets do not require any form of identification or background check [15]. Traditional banks require different forms of identification which can reduce the banks accessibility factor. Cryptocurrency provides, what seems like, a bountiful number of advantages. That is not always the case.

Disadvantages of cryptocurrencies

Cryptocurrencies offer their share of disadvantages. Cryptocurrencies are considered highly volatile assets [15]. Because cryptocurrencies are not governed by the traditional market attributes, investing in them can be risky. The cryptographic encryption associated with digital and physical crypto wallets are strong, however if one loses the private key to their wallets the crypto becomes impossible to gain access to. There can be a significant impact to the environment due to mining operations. The power consumption needed to power mining operations greatly increases electricity consumption which results in increased green house gasses to be emitted. Crypto farming can also have an impact on the consumer market as well. Large crypto operations require large graphical capabilities and processing capabilities. This means crypto farmers have to buy a large number of graphics cards and CPUs in order to farm crypto. This reduces the amount of these components available for the average person and forces the prices of these items to increase substantially. This also increases the price of the raw material needed to manufacture them.

Conclusion

Cryptocurrencies could potentially be the future for all of commerce. The blockchain provides the necessary security and accountability for users of the network while also providing robust security. Regulation should be put into place for cryptocurrency though. Regulation is necessary to ensure crypto exchanges are not being used for something that is law breaking. Taxing cryptocurrencies could also be beneficial to rebuilding infrastructure around the world. This is due to the profits being made on different coins and tokens every day. The most important aspects of cryptocurrency would be the blockchains security and its ability to scale. Although

decentralization is important, having a decently regulated crypto could help fix many different things. It could also help usher in a new generation of currency for the world. It would also greatly increase monetary access to many people. Through cryptocurrency and the blockchain, we can further evolve our understanding of security and accessibility for all.

Works Cited

[1]

Kaspersky, “What is cryptocurrency and how does it work?,” *usa.kaspersky.com*, May 03, 2023. https://usa.kaspersky.com/resource-center/definitions/what-is-cryptocurrency

[2]

“Crypto Tokens vs Coins — What’s the Difference?,” *crypto.com*. https://crypto.com/university/crypto-tokens-vs-coins-difference

[3]

A. Hayes, “Blockchain Facts: What Is It, How It Works, and How It Can Be Used,” *Investopedia*, Apr. 23, 2023. https://www.investopedia.com/terms/b/blockchain.asp

[4]

Amazon, “What is Blockchain Technology? - Blockchaining Explained - AWS,” *Amazon Web Services, Inc.*, 2023. https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

[5]

J. Frankenfield, “Merkle Tree in Blockchain: What it is and How it Works,” *Investopedia*, Jul. 26, 2021. https://www.investopedia.com/terms/m/merkle-tree.asp

[6]

C. Staff, “How a Block in the Bitcoin Blockchain Works,” *Gemini*, Mar. 24, 2022. https://www.gemini.com/cryptopedia/what-is-block-in-blockchain-bitcoin-block-size

[7]

J. Craig, “What Is The Size Of The Bitcoin Blockchain?,” *Phemex*, Nov. 02, 2022. https://phemex.com/blogs/bitcoin-blockchain-size

[8]

“Blockchain Scalability Approaches | Chainlink,” *chain.link*. https://chain.link/education-hub/blockchain-scalability

[9]

S. Daley, “25 blockchain applications & real-world use cases disrupting the status quo,” *Built In*, Dec. 05, 2018. https://builtin.com/blockchain/blockchain-applications

[10]

“Guide to Cryptocurrency Security,” *Arkose Labs*. https://www.arkoselabs.com/explained/guide-to-cryptocurrency-security/

[11]

J. Frankenfield, “Double-Spending,” *Investopedia*, 2019. https://www.investopedia.com/terms/d/doublespending.asp

[12]

A. Yanay, “Hash – The Puzzle of Bitcoin (What Are the Miner’s Mining?),” *vpnmentor*, Jul. 14, 2023. https://www.vpnmentor.com/blog/hash-puzzle-bitcoin/

[13]

R. Kavanagh, “Hash rate: A measure of the computing power on a cryptocurrency network that is a key security indicator,” *Business Insider*. https://www.businessinsider.com/personal-finance/hash-rate

[14]

“Cryptography in Blockchain,” *GeeksforGeeks*, May 07, 2022. https://www.geeksforgeeks.org/cryptography-in-blockchain/

[15]

K. Yasar, “Pros and cons of cryptocurrency,” *WhatIs.com*, Jul. 07, 2023. https://www.techtarget.com/whatis/feature/Pros-and-cons-of-cryptocurrency