Alexandria Tanner
Spring 2021

CS 463
Course Project

Digital Currency

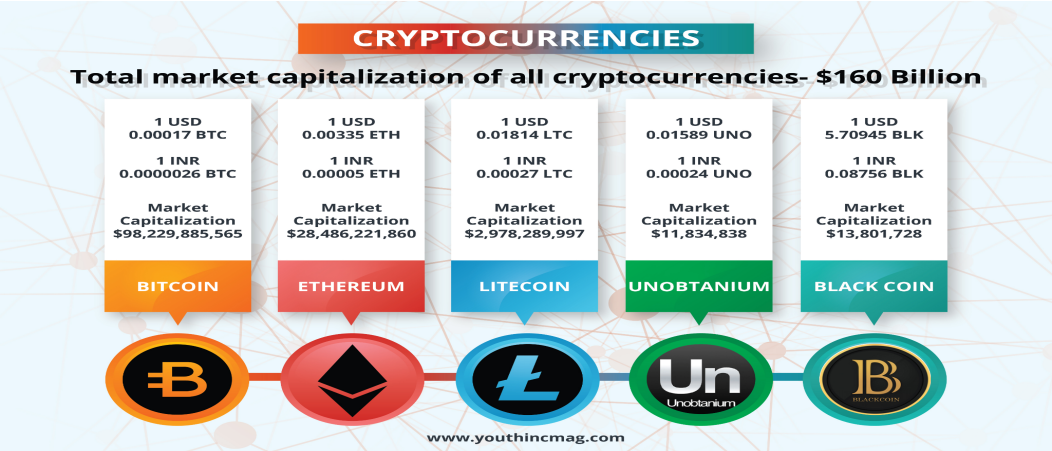
Cryptocurrency or crypto is a modern form of payment and may I say, the future of currency as we know it. Cryptocurrency is digital and possesses no physical form, but can still be used in the exchange of goods and services; the same as regular currency. The idea and/or the term 'cryptocurrency' was originally coined in 1998. "Crypto" meaning a secret or something that is kept concealed, in this case, the individual purchasing this kind of currency remains anonymous. It was in 2009 that the very first cryptocurrency was created, the infamous Bitcoin. Bitcoin is the oldest and the biggest digital asset globally and was created by an individual or individuals who wished to remain anonymous. We do know the creator or creators use the alias, *Satoshi Nakamoto*. There will be more about Bitcoin in a later section, for now, let us continue with more about crypto in detail.

Today, there are around 6,700 different cryptocurrencies that are traded publicly. The majority of crypto can be purchased with real currency, but some do require crypto to be exchanged with other cryptocurrencies. Many companies issue currencies of their own, known as 'tokens' that can be traded for goods and services provided by that company. As of February 18th, 2021, the total value of crypto reached $1.6 trillion. With its rise in popularity over the years, people are scrambling to buy before the value increases even more. With popularity on the rise, people will need to know if their digital currency is any more secure than the credit cards in their wallets.

Cryptocurrencies are more secure than traditional payments. This is mainly because crypto is secured by cryptography making it nearly impossible to double-spend or forge this type of payment. It uses online ledgers with strong cryptographic techniques to secure online transactions. Crypto also completely removes banks from managing their money supply so the value does not decrease due to inflation. It can be traded and purchased through many online brokerages, but not all online brokers offer the purchasing of all cryptocurrencies. Unfortunately, the buying and selling power is very limited depending on the platform. For example, the online brokerage *Robinhood* allows you to view the movement of hundreds of crypto but only allows the purchase of Bitcoin, Ethereum, Ethereum Classic, Dogecoin, Bitcoin Cash, Bitcoin SV, and Litecoin.

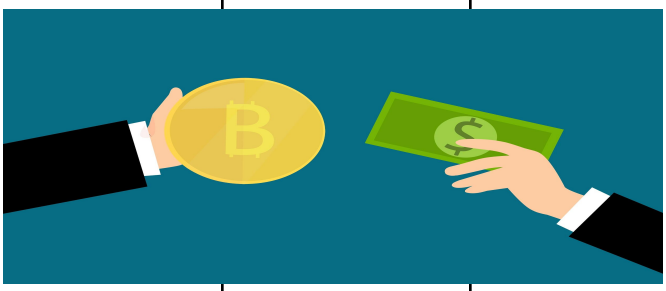
Types of Cryptocurrencies

As previously mentioned, there are around 6,700 openly traded cryptocurrencies. Bitcoin was the first and has grown to be the most popular over the years with the price increasing from only $1 to purchase in 2011 then $696 in 2016 to over $54,000 recently. *Satoshi Nakamoto, the* pseudonym of the person or group that created Bitcoin, also released a white paper in 2009. The white paper explained how Bitcoin ran on blockchain technology, which they referred to as a "triple-entry" bookkeeping system. Now all cryptocurrencies run on this technology, on blockchains.



Here is a list of Cryptocurrencies and the year of their release to the public:

Bitcoin - 2009	Litecoin - 2011	Namecoin - 2011
Peercoin - 2012	Dogecoin - 2013	Primecoin - 2013
Nxt - 2013	Gridcoin - 2013	Ripple -2013
Auracoin - 2014	Dash - 2014	Neo - 2014
Ethereum - 2015	Ethereum Classic - 2015	Zcash - 2016
Bitcoin Cash - 2017	EOS.IO - 2017	Cardano - 2017



Blockchain Technology

Cryptocurrency works using a decentralized technology called a blockchain. Blockchain technology operates across computer networks that manage and record crypto transactions. Part of the initial appeal of blockchain technology is its strong security factor. Blockchains are arguably the most essential part of cryptocurrencies. Their entire organizational method is to ensure the integrity of all transactional data. It is easy to think of blockchains as a database because they are; a special and very specific type of database due to how data is stored.

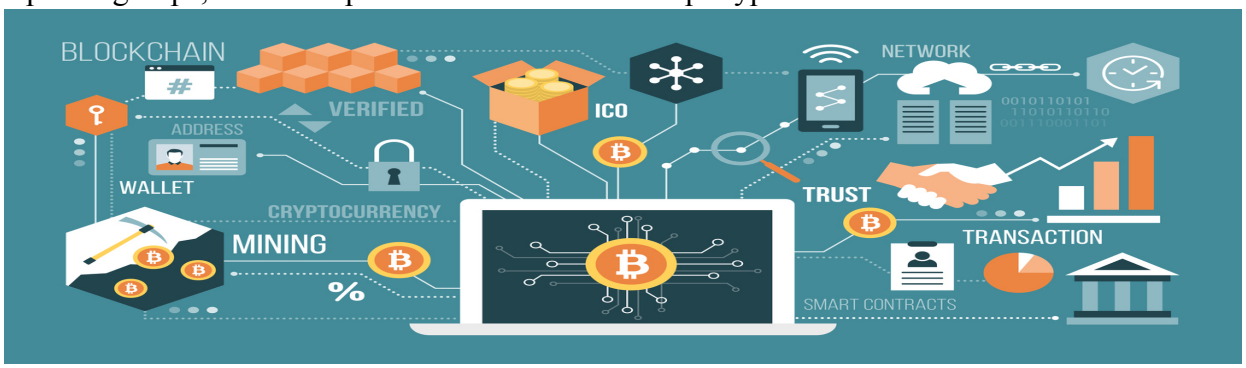
A database is a structured set of information stored and accessed on a CPU system. The information and/or data within a database is generally stored in a table format to allow for easy navigation when searching for specific data. Databases are designed to amass large amounts of information on servers to be filtered, accessed, and manipulated easily, but only by granted users. The key difference between a database and a blockchain is how the data is structured within them. Again, databases use tables to structure data while blockchains collect information in groups that are called 'blocks'. Making it so all blockchains are databases but not all databases can be a blockchain.

The main purpose of a blockchain is to store recorded cryptocurrency transaction history. The very first step in the process of creating a block is to fill it with data or in this case a transaction. When the block reaches its max storage capacity it is time-stamped then added to a chain of similar blocks of recorded transactions. After the transaction is entered it is then transmitted to a network of computers scattered across the globe. Once there the network of computers solves the equations needed to validate the transaction. Finally, the transaction should be confirmed, and clustered into its block. The block we just created with our crypto purchase will connect to the blockchain. As this process continues to happen with more and more purchases all the new information will be compiled into blocks and the blockchain will grow. There is no specific length that a blockchain is limited to but there is usually a fixed amount of crypto that can be purchased. For example, there are 21 million Bitcoins in total, and today just one Bitcoin cost over $54,000. The only limit is how much of a specific cryptocurrency is there to own and sometimes there is a daily or weekly spending limit depending on where you purchase your crypto.

The blockchains we are discussing need strong networks to back all the information being processed and at the same rate, it processes them. Luckily, blockchains do not run on a centralized network because they would not be able to securely support the crypto transactions it deals with. What a centralized network is a network built around a single server that handles the data processing, and storage for all the data and user information. The issue with a centralized network is that it has one server it runs on, and any failure can easily be exploited. Blockchains cannot afford to run on this type of network with the amount of sensitive information it keeps. However, blockchains do not have to worry because it runs on a decentralized network. This is the opposite of a centralized network because the network distributes information across multiple servers/devices rather than only one. Therefore if one server happened to crash there are multiple servers to rely on to provide data access to users, maintain the operation of the network, and its security.

Decentralized networks are easy to scale because you can simply add more servers to a network and increase the computing power. Thankfully maintenance does not warrant a full shutdown of the network whereas a centralized network might. Decentralized networks also perform at a faster rate with a greater degree of privacy but at a higher cost. It is expensive to run anything on this type of network but I believe the cost is worth it, especially when the data you

are trying to keep secure is meant to be confidential. These networks are types of databases but unlike most all the computer systems do not operate under one roof. Each group of computers is maintained by either an individual or a group of individuals. I would guess that how many administrators are needed is dependent on how many computers are being looked over at a time. Each set of computers holds its blockchain in different geographical locations all maintained by separate groups; these computer networks that makeup crypto networks are referred to as nodes.



What is a node? One could exclaim that *nodes* are the entire blockchain. A node can be any device, a laptop, CPU, or a large server, and that device is what forms a blockchain infrastructure. All nodes (servers/computers) that are a part of a blockchain are connected and exchange the latest data with each other around the clock so that all nodes remain up to date. Since they store, share, and maintain blockchains data, so convincingly blockchains exist on nodes. A full node is a device like a computer that contains a complete copy of the transaction history of that blockchain. Nodes also can accept or deny new blocks that are attempting to be added by *miners*. When a node has accepted a new block of transactions it stores and saves to the chain with the blocks previously stored.

A miner must run on a full node or else it will be unable to select valid transactions to form new blocks with. Without the full node, it cannot even determine if a transaction was valid or not because it has no access to the history of the blockchain. Thus, a miner is also always a full node; however, a node is not simultaneously a miner. A device is capable of running on a full node, much like a server without creating any new blocks. Nodes can also be either online or offline. Online nodes receive, save, and broadcast all the latest transactions to and from other nodes, while offline nodes do nothing. However, when offline nodes come back online they have to do a lot of catching up by downloading all the blocks that were added while it was offline.

Each node in a blockchain has a complete record of the data stored on that blockchain since the day it was created. Concerning cryptocurrency, the history of data would be of all made transactions. Nodes operate on a checks and balances system. If one node has an error it can refer to hundreds and thousands of other nodes to correct the error. The history of transactions per block remains irreversible this way and no single node can alter its information inside. If a node were to be tampered with in any way, all nodes would begin to cross-reference one another eventually establishing which node contains the incorrect information. With Bitcoin specifically, all transactions are transparent and can be viewed by almost anyone. All you need is a personal node or access to blockchain explorers. Blockchain explorer gives access to people who are interested in viewing transactions live. Each node possesses its copy of the chain and updates as new blocks are added, allowing people to track Bitcoin wherever it goes.

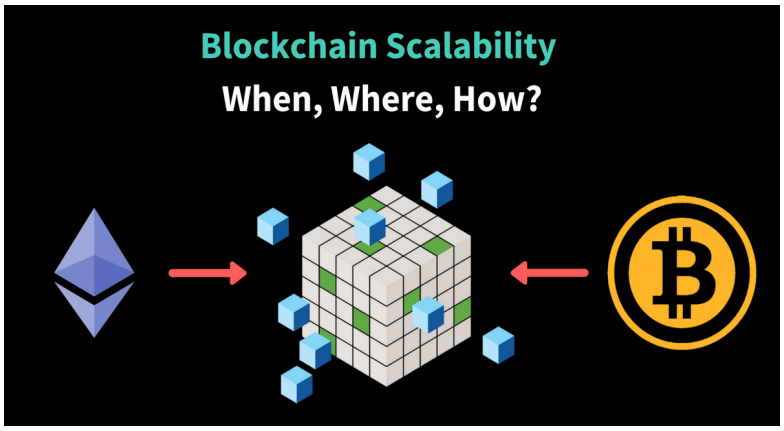
Back to our different types of networks. Although the decentralized network is the most secure network out of the two (centralized and decentralized), the network does have some coordination issues. What that means is sometimes servers will not sync up and communicate as

timely as they should. Luckily there are many servers, and the nodes run on a checks and balance system so this issue can be ironed out in the meantime.

There is another network, a distributed network that is most similar to a decentralized network. The biggest difference between the two is that a distributed network has multiple servers and multiple network owners. However, computational resources and data ownership are evenly shared across the board. Distributed servers are actually what adds blocks to their chains and they are immensely fault-tolerant due to their ability to rebalance computational workload if a node were to fail. You could argue that a blockchain is running on a decentralized distributed network. Distributed networks are also more scalable than both centralized and decentralized networks meaning the chains can be even longer.

Performance Implications

Speaking of scalability and long chains, let us dive into more possible performance implications of having a long blockchain. When a blockchain becomes too large, nodes running on a full client will need to extend their hard disk. In the context of blockchain, a client is a software connected to other clients/software in a peer-to-peer manner. All the "clients" communicate with one another to form a network where each client is a node.



Blockchain Disadvantages

When researching and learning about blockchain you generally see a trend of positive and informative information being spread about the technology. The reason being is that this technology is still fairly new to some people so the idea of it all is being sold to learners like myself, developers, etc. However, just like any other technology, there are pros and cons, advantages and disadvantages and unfortunately it is not all peaches and cream. Understanding the disadvantages of blockchain technology will only improve your knowledge about the topic.

This technology will change the world but before it does we have to know the ends and outs. Once that is learned and understood then solutions can be made to fix any possible disadvantages to this technology to make it as perfect as possible. One disadvantage of this technology is that the process can slow down if there are too many users on the network at a single time. These blockchains also consume a ton of energy, sometimes too much

energy which can lead to inefficiency and high costs. Another disadvantage is blockchain technology not offering interoperability, meaning: users cannot interact with users from another chain freely or without spending resources. Blockchain technology is fairly new and because of that it is not fully matured and has a long way to go before it matures and is standardized. Users also must maintain their wallets or else their access can be lost and this self-maintenance has proved to be negative. How they do this is with their private keys which they must keep track of and not share with anyone or their wallet could be at risk. The final disadvantages of blockchains are that they are immutable and hard to scale due to the consensus method.

I can think of solutions to a few of these issues. For instance, to improve the speed users should be evenly distributed across networks and/or increasing the size that way no single network runs slowly because it is supporting too many users. I believe in the future blockchain technology will be interoperable because allowing users to freely interact will draw in more users. Or they will not and make it so you can only interact if resources are spent to do so. Once blockchain technology becomes standardized I believe that many of these disadvantages will be solved as better and newer blockchain solutions challenge the first-generation technology.

Consistency

Consistency is important in all aspects of life, in business, learning, teaching, and even technology. Perfection is often unattainable but consistency is not. Maintaining consistency through work and business can affect your employees and how things operate. For example, employees need to be trained consistently therefore they are up to date on new programs, updates, network use, etc. So how does blockchain technology maintain its consistency? Blockchain consistency is maintained on a decentralized system by a peer-to-peer network. When a miner begins to mine a new block at the same time the network is deciding which will be the main block.

As we already know every node holds a copy of the chain and the network algorithmically approves newly mined blocks to be updated and verified. Combining public information with its checks and balances system helps maintain the integrity of blockchain and builds trust amongst users. There is a misconception about blockchain networks that like Bitcoin they are anonymous they are only confidential. When users make public transactions they are given a unique identifier called a public key and that is what is recorded onto the blockchain, not personal information.

Security

We reviewed specific disadvantages of blockchain technology; however, security is not one of them. Is one of the biggest advantages and what makes blockchain stand out. What evidence do I have may you ask? Believe it or not but blockchain had yet to be hacked until 2018. That has a lot to do with the use of public and private keys that secure blocks created on ledgers. When a transaction is first made your public key is converted into a private key which is then sent to whomever the transaction is meant for. This private key is a *hashed* (cryptographic technique) version of the currency that is sent to the receiver. It is imperative that this key remains secure and is not shared with anyone. Every single block created in the chain has a unique cryptographic key, so for a hacker to hack into any of the blocks they would have to hack into every single one on that ledger. Let us say a hacker were to hack into every block the system would show a warning and proceed to block any affected/changed blocks.

Many say the purpose of blockchain is for people who do not particularly trust one another to share valued data in a tamper-proof way. Two things make this system tamperproof; the first is the cryptographic fingerprint that is unique to each block. Fingerprint = Hash and a hash can take a lot of time and energy to generate initially. An example of this would be in Bitcoin, the hash and/or fingerprint serves as proof that the miner who added the block has earned the reward of the Bitcoin. Think of a hash as the final seal, because in order to alter the block or break that seal a new hash/fingerprint would need to be generated. The second tool that makes this system tamper proof is the consensus protocol. That is because all the nodes in a network must agree on a shared network.

Blockchain focuses on decentralizing a network, meaning there is no single owner, and everyone on the network stores a copy of the ledgers. By using blockchains the need for trusted authorities and middlemen has been eliminated. Thus making the completion of transactions easier because no one has to prove their identity before a transaction. Blockchain is a technology that increases the transparency of transactions as users on the network have a copy of the ledger.

Privacy is another feature of blockchain that makes the technology so notable. Privacy can be maintained as required data is published and can still rest assured that private information will not be misused. Users can create private networks where access is limited in order to keep transactions and their identities private. The basic security properties derive from both Bitcoin designs and executions, and cryptography advances.

Cryptography in Crypto

To reiterate, “crypto” means to keep something concealed or a secret. Cryptography methods use advanced mathematical codes to transmit and store data values in a concealed format ensuring whomever the transaction is meant for, can receive, read and process it. Cryptography methods also ensure the authenticity of transactions and participants, similar to identifying, say, a written signature. Cryptocurrencies emulate the concept of written signatures by using cryptography techniques and encryption keys. To explain in simpler terms, cryptography is a technique to send secure messages between two or more participants. The sender encrypts/hides the message using an algorithm and key, sends the encrypted message to the recipient for them to decrypt and generate the original message. Breeds of new cryptocurrencies like ZCash and Monero use various forms of cryptographic encryptions to keep transaction details secure and anonymous.

Here are examples of some cryptographic methods that are used in cryptocurrencies. The first method used is Symmetric Encryption Cryptography. It uses the same secret key to encrypt the raw message at the source, transmit the encrypted message, and decrypt at its destination. For example, letters of the alphabet can be represented by numbers ‘A’ is ‘01’, ‘B’ is ‘02’and so on and can encrypt a message this way with numbers.

A second method is Asymmetric Encryption Cryptography. This method uses two different keys - public and private- to encrypt and decrypt data. The public key can be circulated openly while the private key is known only by the owner. This method allows a user to encrypt a message using the receiver’s public key and allows the user to decrypt with their private key, the only private key. Asymmetric encryption achieves authentication and encryption for crypto transactions and that is an extremely important function of cryptography.

Last but not least, there is Hashing. Hashing is used to efficiently verify and maintain the integrity of data and transactions that take place on the network. Hashing maintains the blockchains structure and encodes users’ account addresses. Hashing is an indispensable part of encrypting transactions that occur between accounts and make mining blocks possible. Digital signatures complement various cryptographic processes by allowing participants to prove their identity to the network. I would not say digital signatures alone are cryptographic methods but are beneficial in maintaining authentication. Overall anonymity and concealment are key aspects of cryptocurrencies and there are various methods used through cryptographic techniques to ensure participants and their activities remain hidden on a network.

Digital Currency vs. Physical Currency

Why would or should an individual consider digital currency over the traditional, physical currency we are used to? What are some of the advantages digital currencies offer that traditional currencies may not? For starters, digital currencies are decentralized, borderless, safe, fast, and cheap. Crypto is on a network of distributed and anonymous users all in charge of the transaction process. A peer-to-peer mode of payment and as a result the need for a centralized government, banking system, or corporate board to control the supply of currency is eliminated. Cryptocurrencies are deflationary as well and this is largely due to the removal of the government and banking system. The number of available coins or currency is all predefined and no new units will be added. Due to the predefined amount of currency available the value will continue to increase because quantity is scarce. Governments can print traditional money arbitrarily which reduces the value.

There are also limitations to the amount of physical currency that can be carried across borders. Digital currencies eliminate this limitation since anyone can send and receive payments anywhere in the world so long as they have an internet connection and computer. Digital currencies are also much safer than traditional, physical currencies because they involve complex, encrypted networks. Digital currencies are difficult to breach, and the transactions are irreversible. Transactions can be nearly instantaneous compared to 24-48 hours or 1-3 business days it may take for traditional money transactions to process.

Blockchain Application Examples

Blockchain contracts have been rising in popularity in sectors such as government, healthcare, and real estate industries. I will go over a few examples of how companies are using blockchain technology to make ‘smart contracts’ and applications they have created to access them.

The first example is a company known as “BurstIQ”, in the healthcare industry. BurstIQ is a blockchain contract that helps patients and doctors securely transfer sensitive medical information. What the contract does is establish the parameters of what data can be shared and the blockchain aspect is the sensitive information of patients. Another is in the Music Industry and is known as “MediaChain”. MediaChain uses smart contracts to help musicians receive all the money they earn by entering into a decentralized but transparent contract. Artists can agree to higher royalties while getting paid on time and in full, MediaChain was acquired by Spotify in 2017. There is an application called Propy that is a global marketplace for real estate with a

decentralized title registry system. This online marketplace uses blockchain technology to make title issuances instantly as well as offering properties that can be purchased with crypto.

Many applications are in Crypto, Fintech and some are in the Gaming or Cybersecurity industry at the same time. OPSKINS is in the gaming, fintech, and cryptocurrency and allows gamers to purchase 'skins' with cryptocurrencies or exchange them for cash. CIRCLE is in the Fintech and Cryptocurrency industry, and what it does is oversees $2 billion /month in crypto investments and exchanges between friends. CIRCLE is an investment and transferring platform that currently features seven different currencies. CHAINALYSIS is also in the Fintech, crypto, and cyber industry. This application assists governments and financial institutions monitor the exchange of currencies. Detecting fraudulent transactions, laundering, and more.

Conclusion

In conclusion, I believe digital currencies are the future of payment as we know it. Eventually, we will begin to see the takeover, and the traditional, physical currency we know today will no longer circulate as heavily. I think that the advantages of digital currencies overall outweigh the bad. In my eyes, it is only a few kinks and that is because digital currencies have not completely matured. Users can comfortably and confidently finalize transactions and exchange their crypto because of the blockchain technology it runs on. Users can also confidently rely on the cryptography methods used to maintain the integrity, authenticity, and security of their personal information on these networks.

I love how different industries are experimenting with blockchain technology and implementing it within their own companies. More of this inclusion will boost popularity among the public and other businesses while standardizing the technology as a whole. With how technology is so present in our everyday lives it only makes sense to make the switch from physical currency to digital completely, down the road.