CS 463: Final Paper

Cryptocurrency

Kevin Durand, kdura002

Introduction

Cryptocurrency is the new trend on many people lips, it represents a new way of doing business that doesn't rely on banks or governments for value; by explaining and contrasting cryptocurrency to current methods, this paper will objectively determine the nature of cryptocurrency and its implications. Normally currency and financial interactions are determined by what is known as Fiat Currency, a method where the value of tender is determined by the success of a nation and the value the money is given by the bank for goods and services. Cryptocurrency seeks to do business beyond the need for countries and banks, the value of the cryptocurrency is agreed upon and carried out by encrypted databases full of cryptocurrency users. The meat of cryptocurrency is carried out using block-chains, a type of database technology that is distributed and administered by different users all connecting with identical copies of the same database, this is the basic structure of many things including cryptocurrency. Cryptocurrency transactions are carried out and stored in a long chain known as a blockchain, a blockchain is a distributed database that acts as a ledger for the cryptocurrency itself, storing the transactional history of the currency itself via the trading of its users. Bitcoin, of one the premier cryptocurrencies in use, works through the interactions of a bitcoin wallet, with the public block chain ledger; using an open-source block chain, users can buy and selling products for the currency, bitcoin. Cryptography is a key element of the blockchain itself, each user has a specific hash that allows them encrypted access to their copy of the shared ledger, in addition each transaction has an additional hash that keeps it encrypted from being changed, together those hashes for the secure nature of the cryptocurrency. As with anything radically different from normal methods of doing anything, cryptocurrency is a unique way to do financial interactions and carries with it a few advantages. Along with advantages, there are many disadvantages to cryptocurrency, a lot of interactions are unsupervised and can cause financial ruin to the person(s) involved. In my opinion for all the benefits that are received from cryptocurrency, it does not justify its use; there are a lot of protects in place because of the way fiat currency is done that makes it simply a better option for most people. Cryptocurrency is a very interesting idea that incorporates a lot of interesting and advanced ideas, the mechanisms are novel ideas, even if the end result is not without its issues.

Fiat Currency Overview

In modern times, the most widely used system of currency is known as the "Fiat Currency", where the value of money is based on the value it is given by the government that issues it. In the early days of economies and currency, currency represented the amount of gold and silver the person in question owned; instead of lugging around ounces of gold and silver bills and notes were given out the represent some weight of gold or silver. The current way of currency is based on the economic and trade stability of a nation, instead of basing the amount that a country owned the money in a country is based on the success of the nation issuing it. Normally financial interactions are represented by the trading of goods and services for money bills, this form of tender is generated and printed by banks that oversee the value of that money unit. [1] Defines the relationship between the two economies by saying, in the fiat money system, the value given to any currency in that system is based on the success of the nation involved; the value directly

depends on the supply and demand strength of the nation's economy and the stability of the nation printing that money, not the amount of commodity a nation possesses. in this case commodities are silver and gold. [2] Lays out the basic operations of this economy by giving a broad example of how the money is used and the expectations of the holder of that money. The medium for exchange, as [2] puts it, represents the money note that is given value by the government or bank that over sees it, storing up those money notes give the holder a financial value equivalent to the number of units, and that items being purchased also have value based on the money unit system. Defining the money unit itself [2] lists several things that must be satisfied. First a money unit must be durable, that same unit should be easy to be carried around by a person, the larger the bill the more expectation there is for the bill to represent many smaller bills of equal value, all bills printed are uniform in how they look, and lastly there needs to be a limited accessibility to the bill age in order to ensure its value. Having a good understanding of this basic money system that is normally followed is needed in order to explain what makes cryptocurrency so different.

Cryptocurrency Overview

Cryptocurrency is a digital form of currency, where instead of trading based on monetary bills, financial interactions are based on the trading of digital assets. In the original concept of money, the trade of goods or services for money meant that Bank A loses a certain amount of dollars from one person's account, whereas Bank B gains that same amount of money in the other persons account to show that the transaction has gone through. Cryptocurrency works a bit differently, when User A sells a service or product to User B, the value of each user is determined by the database all the other users share; during a transaction, the database record for the users is changed, showing the loss of cryptocurrency on User A's records and the gain of that same amount on User B's records. What makes this process so different between the two, is the crypto currency records are updated for everyone on the same database, while a normal financial interaction is simply between two different bank accounts. [3] Puts this in slightly more specific terms, "Cryptocurrencies run on a distributed public ledger called blockchain, a record of all transactions updated and held by currency holders.", in this case the blockchain is the type of database they use and that is where the value of each user is show and changed. In plain English every user in a specific cryptocurrency has access to the ledger in that they each own a copy of the ledger; using cryptography each ledger is distinctly separate from each other ledger in how you reach it, but all the ledgers match the same information. In order to complete a transaction, all the users must show the same ledger changes, that is that an individual user can not conflate or change the value of their cryptocurrency by simply changing their own ledger records, when that change is synced up to the other ledgers the change is evident, and the value does not agree with other records. When a service or good is rendered, all the members of the ledger will see the interaction between two users and the ledger will reflect that change, when the ledgers all agree then the value is pushed. The way to gain access to a cryptocurrency is gaining currency in the system, you can gain the currency either through the purchasing of coins with normal currency, or by supplying the cryptocurrency ledger with computing power for an amount of bitcoin. After purchasing or gaining bitcoins, as used by the cryptocurrency "bitcoin", the user then has a copy of the ledger itself and can start buying products or buying other products with that amount of bitcoin. The main push for cryptocurrency is that it doesn't rely on banks or other financial institutions, the values of the

currency along with the interactions occur from person to person across a encrypted network, without the use of middle men or fees of the financial institutions. Cryptocurrency represents a digital response to the traditional Fiat Currency, replacing bank records with publicly owned and controlled ledgers, and paper money with value based on the community that supports the currency.

Blockchains

Cryptocurrency is carried out functionally by ledgers that are comprised of encrypted segments of data know as blockchains, blockchains represent the different elements of a cryptocurrency system and are the key to the functionality of the cryptocurrencies in use today. A blockchain is a distributed database as discussed by [4], meaning that the blockchain is a system comprised of many different files working together across a network between multiple different computers, that work together to maintain a database comprised of the transaction data of the cryptocurrency it represents. Blockchains are also used in many different applications outside of cryptocurrency itself as well. [12] Shows a number of different industries that work in tandem with blockchain technology. Chainalysis is a company that uses blockchain technology to keep an eye on the interactions between different cryptocurrencies, Google uses blockchain to help in the processing of data science initiatives, and HYPR uses blockchain technology to help validate computers to networks between IoT operations, just to name a few. In cryptocurrency Blockchains are essentially bank records of all the transactions via all the users of a specific currency, each record contains at least the number of bitcoins used on any transaction, as well as the timestamp and encryption data of the previous transaction on the register. By providing the previous encryption data, explained further in the next section "Encryption", all other users can verify the validity of the user and that user's data. A good way to think about this is a train of car each either the same number of cans of oil, where the number of cans of oil are easily visible on the side and the train cars are all connected by color to the car before them; let's say at the same time each train is mirror by multiple trains on either side of that first train. As people trade the oil in each car for some amount of money, the side of the train is changed to a different color and number of cans painted on the side, which is in turn mirrored by the cars in one row from first to last train line. If someone tries to change the value on the train independently, everyone else can see that the train is a different color than theirs and show a value of oil cans different from their own, letting them know that that train car has been altered without consent from the rest of the train car users. [4] puts the train analogy together well by saying "a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed." An overview of the key elements of the block chain is given by [5] a block chain must be a distributed ledger, immutable records, and be comprised of smart contracts. The first element described by [5] is discussed earlier when the blockchain is defined as a distributed database, according to them it defined as having as allowing access to the ledger from any of the networks users, in this case anyone who has Bitcoin blockchain access should have undisputed access to those records. Next [5] determines a blockchain to be an immutable record if transaction records can only be changed by a group effort, not by an amount of users smaller than the whole group, after a transaction has been completed this is determined by the encryption information, discussed later, of the specific block of information. Lastly all elements of the blockchain must be detailed by smart contracts,

[5] describes the process of smart contracts as specific rules regarding the specific transaction that block is an example of. The overall process of the blockchain interaction with the cryptocurrency is quite interesting and happens in a specific set of steps. When someone does a transaction with the blockchain, a record is made of that transaction, containing the information about the transaction. The transaction block that is created is then attached to another block before that one, which copies its own specific information to the chain that existed right before that transaction on the ledger. After completing that process, the next transaction on the chain then goes through the same process, adding its unique information to the transaction that just happened before it. After a chain of transactions are carried out, they are attached in a long secure chain, this is where the name blockchain comes from. The main idea after those series of transactions is that the information can not be changed because it each block is connected to the block before and after it by a unique identifier, making the whole process a secure transaction. Each transaction of a cryptocurrency is contained in a block of data, as more transactions happen more blocks are added forming what is known as a blockchain, the structural element of a cryptocurrency.

Bitcoin

Bitcoin is one of the most popular versions of cryptocurrency and is a good introduction to how the whole crypto process works. Bitcoin, as any other cryptocurrency, is a process carried out in the blockchain, detailed in the previous section. [6] Gives a good overview of getting started as a user on the blockchain with bitcoin, which is explained over the next few sentences. The first step in getting involved in bitcoin is to obtain a Ledger wallet, this is how the user will interact with the ledger that the blockchain is created on. Next, after obtaining the wallet, it will be prudent to install a software that will help you record and manage your token, it works by directly interacting with the blockchain itself. With the ledger program installed, the next step is just to get registered on the ledger itself. Now that everything is set up to be involved in the blockchain ledger, the user now must obtain bitcoins. According to [7] There are two main ways of obtaining bitcoins, the user can straight out buy bitcoins for normal legal tender, or they can mine to help in the processing of transactions on the ledger itself. Buying bitcoins is straightforward, bitcoin would have a market value, and to obtain a bitcoin you spend that market value to obtain it. The next way, explained further by [7], is to help the ledger parse transactions and earn bitcoin. Each bitcoin transaction between users requires several cryptography-based operations that require computing effort to parse out, when a user can solve the correct cryptographic equations to let the transaction go through, they make bitcoin in reward for that. By solving the cryptographic equations, the currency system can keep things secure and moving. When a transaction is carried out, it is added to the blockchain (as explained in the previous section) with a secure value that cannot be altered. This transaction process can be done due to the peer-to-peer nature of the interaction between users. Bitcoin is one of the more popular cryptocurrencies out on the market and is a good example of how users and transactions interact on the blockchain ledger.

[this space left intentionally blank]

Security of Bitcoin

Through a mixture of a few encryption schemes, bitcoin can allow secure connection to the ledger, while making every transaction and bitcoin record immutable. The beginning of the security of bitcoin is a bit surprising, the ledger itself is actually open source distributed database technology, it's the interaction between users and their transactions that are secure. One of the security features of the bitcoin process starts with the wallet of the individual user, as explained by [8], an individual's wallet is secured using a private key and advanced encryption standard or AES. AES is a, described by [9] a symmetric key block cipher, which involves several permutations and substitutions depending on the size of the block being encrypted. [9] breaks down the process in 4 parts, byte substitution, shifting blocks, mixing columns of blocks, and doing bitwise math based on a key. In byte substitution a prearranged table is used to interact with the data being encrypted, the blocks are logically substituted by the hexadecimal units found on the table. After substitutions have occurred, the resultant rows of the data are rearranged according to their structure on the table, according to [9] the first row is left unaltered, the second row is shift by one byte to the left, third row shifted two byte positions to the left, fourth row shifted three bytes to left. Another table is used on the now shifted blocks, again logically replacing values on the block using a premade table. Lastly the entire message is now XORed individually against a premade key that finalizes the encryption product. The generated value is known as the private key of the user for their wallet, but as the public key for the actual security of the transaction block itself. Using Elliptic Curve Multiplication [10] explains, the private key of the individual wallet is turned into a public key to be used to verify the users involved in a transaction. Elliptic Curve Multiplication, further detailed by [10], is a mapped-out equation based on a specific modulo value, this creates a chart of infinite points related to the equation that mapped out the Elliptic Curve. The message itself is encrypted based on the relative location of points to other points. P1 and P2 represent points on the curve, when the actual encryption is carried out a third point on the infinite graph is determined by the addition of the first two points. When an actual public key is generated, [10] designates this "K", the addition of points to the final point used is equal to a value of k*P (where "k" is the original wallets private key generated using AES), adding from point P_1 to P_k. K, the resultant public key is more straightforward [10] details that a little simpler by saying that G, which would be P_1 is multiplied by the random private key "k" to produce the Public key "K"; or K = k*G,P_1. Now that the user has an appropriate public key, that public key is used along with other information about the transaction to generate a hash function that is used as a digital signature on the ledger for that transaction. Returning to [10], it is explained that the process of creating the eventual transaction encrypted code is based on a double hashing encryption, a SHA256 hash applied to the public key, that is then sent through a RIPEMD160 hashing equation. Hashing, detailed by [11], uses a key that is used to encrypt data, it is a process that always creates a unique identifiable output that can be retraced to validate the users involved; by using the same hash on the same message both encryptors and decryptors are able to get a unique consistent message using the same hash functions. SHA-256, again explained by [11], is a process that turns any message into a 256 bit encrypted message, using the hash function as detailed by SHA-256, based on MD5. RIPEMD160, using the lesser MD4 encryption hash function, is then applied on top of the SHA-256 resulting in the digital signature of the seller. Before it was described that as blocks are added their hash values are added to the block that represents that specific transaction,

it also details how many bitcoins both parties have. When a new block is added the specific information, the hash function output, is updated on everyone's ledger in the distributed database, this means that a specific hash that is recreatable is cemented into the transaction and records. Further than that, the hash from the previous interaction is added to any new block being created, this means that all records have two forms of verification. While someone might be able to change the hash value on one transaction, it would be near impossible for someone to fake both sets of hash functions. Using stringent encryption and hash value verification through repeatability, bitcoin is able to make a very secure model.

Advantages of Cryptocurrency

Cryptocurrency is a unique idea that is very different from the standard way of doing economies or currency, and with that has a number of unique features that make it advantageous to use. One of the biggest things that cryptocurrency has going for it is a stability in value. From [1] it was discussed how volatile a market based on Fiat Currency can be; there are many different societal impacts that can cause inflation. Inflation is basically when the value of various products are raised, basically it means that the fiat currency is worth less than it was. This sort of market volatility can be very bad for consumers, making products and services harder to reach. With the free market features of cryptocurrency, the chances for inflation are greatly reduced. [14] details another great advantage of cryptocurrency, since the ledgers are updated by the individuals in a crypto group, the entire process of the money is self-managed. Instead of being controlled by a select group of individuals, the control of the currency is shared among all the different members of the group. Ideally the cryptocurrency would also be free of monopolization, since everyone can have free access to sources of bitcoins by helping hash transactions it makes it a lot harder for one person to gain more control and monopolize the currency. Lastly, as it is extensively detailed in the previous section, this method of payment is entirely secure, with many different checks and balances it is hard to tamper with any element of the blockchains.

Disadvantages of Bitcoin

With every new great invention there also come roadblocks, Bitcoin is no different, there are a lot of disadvantages to cryptocurrency as well. One of the first problems is involved in its greatest strength, this is a currency that is not tied to any financial institutions, this makes bitcoin an excellent source of illegal materials or services. The records that are left behind in a transaction go from one encrypted wallet to another, and only describe how many bitcoins were transferred between two users. By not being able to detect what bitcoins are being spent on, there is no oversight in keeping the interactions within any bounds of morals or laws. Another of the biggest issues is the power usage required to make cryptocurrency work. When any transaction is completed power consumption is required to carry out the cryptographic hashing functions that give crypto its secure nature. In the current world it is more important than ever to figure out how to limit our consumption of resources, especially when so many way of generating power are directly linked to the climate change threatening to destroy our ecosystem. It is already shown that bitcoin causes a lot of power problem, with the right amount of computer equipment these stations are causes overloads on power systems, especially in third world nations where power is already a scarce resource. Lastly, another large problem with cryptocurrency is linked to its open source

nature, along with its independence from financial institutions. There is no oversight when it comes to losing funds, there is no insurance that you will even get the product or service you purchased. In current times if a business swindles you on a credit card purchase, you can typically go to the bank and argue against that transaction and usually get your money back. With cryptocurrency there is no governmental or lawful body enforcing legal trading practices, when a user's bitcoin is gone there is little in the way of recourse that user can take. As with anything, while there are many advantages to be had from any new technology, there are also always going to be a host of problems from its use as well.

Personal Opinion

My understanding of the whole process and reason behind cryptocurrencies is to go around normal bank requiring financial interactions, and make a better more equitable form of currency, but I have found that the process is not that equitable or different from traditional sources. In the bitcoin section it was explained that there are two ways of obtaining bitcoins, through buying bitcoins and then through mining. To start with buying bitcoins, this means that ultimately this currency is not actually on its own legs, one of the basic properties of the currency is to not rely on traditional currency. If the whole currency needs to be purchased with fiat currency to even begin, then this is a system that is additional to a fiat currency system and not diverse from it. Ultimately, being able to purchase bitcoin with normal money, means that bitcoin has a fiat value, meaning it has a value that is directly tied to the very systems it seeks to be different than. The next method of gaining bitcoins is by mining, as explained previously you complete hashes for other transactions and if you can complete one you get a certain amount of bitcoin for that success. The issue becomes that how much original value you have plays into this. While explaining the bitcoin process [7] explains "When Bitcoin was first released, it was possible to mine it competitively on a personal computer; however, as it became more popular, more miners joined the network, which lowered the chances of being the one to solve the hash."; this means that its not really a free currency, the better your computer the better your chances of making bitcoin through mining. Typically, people would not have bitcoin they would use to purchase what they want, so any equipment used in bitcoin has to be purchased through the normal banking system (discounting crime) this further proves that bitcoin only works when its subsidized by a more established monetary system. Logically the best way to do bitcoin would be to establish a large number of powerful computers, meaning that you would have to own the location to do the bitcoin mining at, while demanding a lot of power for the right computing. The first decision on bitcoin is that its just another tool for people who are already wealthy to get wealthier, there is not some currency-based revolution, just another rich get richer, and poor stay poorer system. [7] States why this is a bad idea even further, due to the volatility of the currency itself certain people have noticed the investment nature of the bitcoin itself. There are people that no longer use the currency as some new way of doing business, using the peer-to-peer interaction of the ledger, but instead use it as another way to make an investment. Purchase a bitcoin, let it rise or fall in price, and either sell or buy more bitcoin, eventually selling off your bitcoin to someone else when the price is on the rise to make a profit.

[this space left intentionally blank]

Conclusion

Cryptocurrency, without a doubt, is an interesting new way to do financial interactions, by investigating the elements of bitcoin, the viability of this new way of doing money is explained and judged. Fiat Currency, the modern way of most financial interactions, is a form of currency that is tied to a nation or financial institution, the value of the currency is based on the success or failures of that nation or institution. Cryptocurrency is an alternative to the traditional fiat currency model, but giving everyone equal access to this digital currency, a stable currency is created that exists outside the success of a nation. Blockchains represent the basic structure of a cryptocurrency, this distributed database network allows for the secure transactions of a cryptocurrency in a verified immutable ledger. Bitcoin is a good example of a successful cryptocurrency, as one of the most popular versions it offers a good overview of the specific elements of a cryptocurrency network. Based on hashing and encryption software, as well as some structural elements, bitcoin usage and ledgers offer a very secure way of doing business online. As with any new technology, there are a lot of great benefits to using Bitcoin, most of which come from the open secure nature of the blockchain bitcoin uses. With any new technology comes unseen disadvantages, bitcoin for all its goodness is still a victim of such disadvantages. Overall I think that cryptocurrency is a very interesting idea, but its disadvantages make it something I am not fully in support of.

Additional Remarks

1. Are these scalable? In other words, can the chains be as long as you wish them to be? What are the performance implications of having long chains?

Answer: Due to the nature of the ledger, as a distributed database, the only real constraint on size is over computing power of all the machines involved. Put bluntly, the larger the network of computers involved, the more of a constraint.

This is somewhat explained in the basic operation of a distributed database.

2. What has puzzle solving to do with cryptography? Why have they become popular in cryptocurrencies?

Answer: Puzzle solving is the basics of cryptography, in bitcoin especially, the ability to obtain bitcoin is directly linked to solving hashing equations to help solve transactions.

This is explained in the section on bitcoin and then the security of bitcoin.

References

1. J. Chen. (2023, March 28) "Fiat Money: What It Is, How It Works, Example, Pros & Cons" Investopedia.com https://www.investopedia.com/terms/f/fiatmoney.asp (accessed April 13, 2023)
2. "What is Fiat Currency" gemini.com https://www.gemini.com/cryptopedia/what-is-fiat-money-examples (accessed April 13, 2023).
3. "What is Cryptocurrency and How Does It Work?" Kaspersky.com https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency (accessed April 13, 2023)
4. A. Hayes. (2022, September 27) "Blockchain Facts: What is it, How it Works, and How it can be used" Investopedia.com https://www.investopedia.com/terms/b/blockchain.asp (Accessed April 13, 2023)
5. "What is blockchain technology?" (accessed April 13, 2023) IBM.com https://www.ibm.com/topics/blockchain
6. "The Best Wallet for you bitcoin coins" (accessed April 14, 2023) ledger.com https://www.ledger.com/coin/wallet/bitcoin
7. J. Frankenfield. (2023, April 05) "What is Bitcoin? How to Mine, Buy, and Use It" Investopedia.com https://www.investopedia.com/terms/b/bitcoin.asp (accessed April 14, 2023)
8. "How Bitcoin Uses Cryptography" (accessed April 14, 2023) river.com https://river.com/learn/how-bitcoin-uses-cryptography/
9. "Advanced Encryption Standard" (accessed April 14, 2023) tutorialspoint.com https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
10. Antonopoulos A. M. *Mastering Bitcoin* (2nd Edition). [Online]. Available: https://www.oreilly.com/library/view/mastering-bitcoin-2nd/9781491954379/ch04.html [April 14, 2023]
11. N-able (2019, September 12) "SHA-256 Algorithm Overview" n-able.com https://www.n-able.com/blog/sha-256-encryption (accessed April 14, 2023)
12. Daley S. "33 Blockchain Applications and Real-World Use Cases" builtin.com https://builtin.com/blockchain/blockchain-applications (accessed April 14, 2023)
13. "RIPEMD Hash Function" (Updated 2020, February 10) geeksforgeeks.com https://www.geeksforgeeks.org/ripemd-hash-function/# (accessed April 14, 2023)
14. "Pros and Cons of Using Cryptocurrency" (Accessed April 14, 2023) angelone.in https://www.angelone.in/knowledge-center/cryptocurrency/pros-and-cons-of-using-cryptocurrency