University of Louisville

Final Report

Cryptocurrency

Team 6; Regis Wilson, Kelsey Beeler, Mahendra Khanal, and Anthony Combs

CIS 481-01-4212

April 9, 2021

Table of Contents

Executive Summary

The goal of this paper is to define crypto currencies and outline their use & impact. Our team will provide examples of how the technology behind cryptocurrencies, blockchain, works to ensure a decentralized process of authentication. This leads to the true underlying value and attraction to cryptocurrencies such as Bitcoin.

The paper will provide examples of cryptocurrency platforms. This will start with a brief history of the original cryptocurrency, Bitcoin, and the evolution of alt-coins. This section will also detail the rise in value of individual platforms and the cryptocurrency market as a whole.

We will cover the obstacles in the way of further progress and implementation. This includes; valuation issues, social issues, and government oversight.

Once defined and understood, the paper will cover security issues. This section will include many examples of common attacks and the control in place to combat each specific attack. We will conclude will a brief overview and a glimpse into what's next for the Bitcoin and trading of cyrptos. We will also cover & review commonly asked question from our presentation.

Introduction

Defining blockchain

According to Dylan Yaga from the National Institute of Standards and Technology (Yaga, Dylan, et al. “Blockchain Technology Overview.”), Blockchains can be described at its simple level as distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision.

So essentially you can view a blockchain as a type of database, but it differs in many ways that makes it unique from a traditional one. A blockchain gathers information in groups or clusters that are known as “blocks” each one of these blocks has a certain storage capacity and once that capacity is reached a new block is formed. Each block is set in stone and given a timestamp when it was created and given a hash number that identifies it.

As more and more blocks are formed it becomes nearly impossible to modify previous blocks since each one is cryptographically linked to the next meaning that a change in one block would be easily found by comparing the previous hash in new blocks to the older ones. So, in order for a change to actually happen, each block must be gone through and modified individually which would consume an impossible amount of computing power to do.

What makes blockchain so enticing is in theory, it is completely decentralized way of storing things. For example, when all records are kept by a single entity changes can easily be made because they hold all the information about every transaction that has happened and are allowed too freely. A good example of this are banks. Before blockchain technologies, banks were the one centralized entity that kept track of all records of transactions. This means they hold all the power in changing these records. Using blockchains eliminates this possibility because all records of data are managed by a cluster of computers that is not owned by one single person (**https://blockgeeks.com/guides/what-is-blockchain-technology**/). This means anyone has access to these records. Not only this but each record is part of the "block" and the chain is what binds these records together. So anytime one part of the chain is changed another part must be changed to match up the records.

Explanation of Ledger Creation

To get a better understanding of how Blockchain and cryptocurrency tie together I'm going to explain how a transaction through bitcoin happens and how that ledger is put onto the blockchain.

Bitcoin works through the use of public and private key encryption for their transactions, each user has a public key which is their wallet ID that they can share and a private key which must be kept secret and used to unlock your bitcoin for spending. The information stored on bitcoins blockchain consist of mostly transactions.

So first a transaction is requested by a user. That transaction then becomes a block that represents the transaction. Each block header contains the hash of the previous and current block using SHA-256. As part of the decentralized nature, that block is then sent out to each node inside of that network. Since there is no central authority that manages and verifies each one of these transactions to be legit, the nodes inside of that network must work to verify it. These blocks are then verified through what we know was "bitcoin miners" who are the users who work to solve complex computational problems to work towards a target hash that verifies the transaction. The first person to solve this problem within the network is then rewarded with bitcoin the solution is then sent out to other nodes who then approve of that solution and the transaction is added on a new block and put onto the Blockchain.

History & Examples of Crypto Brands

The first cryptocurrency ever created was Bitcoin. The concept came from a Whitepaper written by a person under the pseudonym of Satoshi Nakamoto. The first block of Bitcoin was mined by Nakamoto on January 3, 2009. This first block is known as the genesis block or block number 0. The first transaction involving Bitcoin was two Papa John's pizzas for 10,000 Bitcoin.

Although Bitcoin remains the most prevalent and valuable cryptocurrency, over time there evolved several other platforms. These platforms became known as Alt-coins because they were considered an alternative to Bitcoin. Notable examples include: Litecoin, Dogecoin, Ethereum, and Orbs. Facebook, the social media & advertising juggernaut, is even developing their own cryptocurrency originally named Libra, now coined Diem. They plan on launching this altcoin late in 2021. This has raised concern with many regulators, as Facebook is already under the microscope for several other reasons. Many see a danger in Facebook wilding more power. Regulators are already in the process of pushing regulation to curb Facebook and other social media's ability to disseminate information and influence events. Having a company develop their own currency is just another red flag asking to be regulated.

Currently the second largest cryptocurrency behind Bitcoin is Ethereum or Ether as it's come to be called. In February 2021 this crypto reached a new high of $1,700. The platform also underwent a major upgrade to its system called Ethereum 2.0. This update aims to make their platform safer and faster. Bitcoin, Ethereum and other alt-coins have reached a total market value over $1 Trillion dollars in 2021 for the first time.

Roadblocks to Widespread Implementation

When considering the potential of a cryptocurrency's store of value, there are several issues. For one, there is very little that can purchased with it. Almost no major retailers, or marketplace will accept Bitcoin or altcoin as a form of payment. Tesla recently announced that they would begin accepting Bitcoin as a form of payment but have yet to complete a purchase this way. The inability to use the currency as an actual form of currency, say as you can a government backed currency, decreases its usefulness. Paypal has recently created a way for users to use Bitcoin on websites using their system. It uses real time values of Bitcoin at the time of purchase and translates that to dollars. They take your Bitcoin and pay the retailer, which they of course charge the user a fee for.

The price is also very volatile. It is not uncommon to have double-digit gains and double-digit losses all within the same month. Such volatility is not what many investors want in an investment. This is especially true for the average saver who can't afford to have a heavy loss. With that being said, it is true that long term holders of Bitcoin have experienced tremendous growth. With the coin originally being valued at around $.30 cents in 2010 to hitting over $60,000 in 2021. Bitcoin quadrupled its value over 2020 and has increased over 29% year to date in 2021.

There are also social roadblocks to the further use of Blockchain, the technology behind every cryptocurrency. One major issue that many young people have is the large carbon footprint generated by the constant mining and block checking. The decentralized oversight done by individual traders requires powerful computing devices. It is estimated that Bitcoin mining alone generates more electricity than the whole Czech Republic, a country of nearly 11 million people. Climate change is an important social issue that has gained political traction in the recent years. This social awareness towards climate change will become a larger problem for Bitcoin as people's understanding of how cryptocurrencies work increases.

Possible Government Oversight

Decentralization is part of the value and draw of cryptocurrencies. Should a government such as the U.S. decide to regulate a crypto such as Bitcoin, it could have significant ramifications on the value. The most recent Form 1040 used for 2020 taxes explicitly mentions Cryptocurrencies. Many see this as the first step toward eventual regulation within the U.S. The next logical step is to create a way for the government to require reporting for trades involving cryptocurrency. This would create a paper trail for them to use when measuring the taxable gains of investors and thus the taxes owed to the IRS. The only reason such reporting isn't clearly explained already is that Bitcoin has no central authority to comply or create such documents.

The government could even go so far as to make trading of Bitcoin illegal or make the use of Bitcoin as an exchange of value in a sale illegal. Ray Dallio, a well-known Wall Street insider, believes this to be very possible. He has also openly questioned the idea of Bitcoin as a store of value and pointed out similar issues alluded to earlier in this paper.

Security Concerns and Wallets/Common Targeted Attacks

Within the world or cryptocurrency and the threats that come with it, there is a plethora of attacks on people's property and assets gained through cryptocurrencies. And while all of these attacks are should be taken seriously in their own respect, there are a few of these attacks that are more common than others and should be addressed first. Starting things off we have Attacks on Wallet Software. There are client style applications that are known as wallets and just like a physical wallet, it is used to store and manage Bitcoin and other cryptocurrencies. The client would be able to either have a virtual or online wallet option, or the user can download that software to his or her node. Online wallets are more susceptible to attacks and for that reason there should be some type of offline backup encryption of said wallet. Distributed denials of service (DDoS) attacks are also some of the most formidable forms of this type of attack.

Next, we have timejacking attacks. This includes how the attacker would give out the incorrect time logging information when connecting to a node for a transaction. This way, the network and the counter of the node is changed and altered by the attacker and the node that has been affected by this has the potential to falsely accept an alternate blockchain than the one that was already in use. Reasons why this attack is one of the most dangerous attacks is because of the consequences that can arise because of it. Double-spending which is another type of attack is something that can result from it and become an even bigger problem than it already was, and the resources it would take during the mining process would essentially have been wasted which costs a lot of money and valuable time.

The '>50%' Attack is a major threat for in the cryptocurrency realm of things. This targets the mining process, and is when there is a user of some sort obtaining over 50% of all computing resources needed for the mining to begin. Once a user or users have access to this type of power and control, they can exclude, modify, self-reverse transactions, and even potentially prevent mining of blocks for their own personal benefit. Yet, it has been noted by researchers that even if the hackers have just around 40% of the computing resources, the attackers can still prove to be a formidable threat and have a 50% chance of success with their attack. To help reduce these types of attacks, is to establish a set in stone checkpoints so then if there are blocks before the checkpoint, they cannot be altered. Yet, if this attack in particular is successful, then the attacker(s) can do some serious damage to the whole system. A study conducted at Cornell University shows us that a '>50%' attack is very possible to happen because in a network in a single mining pool only control around 25%-33% of the overall mining power.

Double spending is also something that is a very serious threat for cryptocurrency transactions. This is when the attacker is able to make more than one transaction by using the same "coin" for multiple transactions; invalidating what an honest transaction should be. The most common way this attack would happen would be in a way of a quick payment mode. The attacker would be able take a specific coin and make a transaction at the same time that another transaction has been made using that same coin with a different address than the first one. By doing this and altering the timestamp, the illegal and false transaction can be made to be a real one. And through this type of attack, the original receiver would not be able to authenticate the transaction to confirm its truthfulness. Because of this type of attack ‘observers’ have been placed in the network to monitor this type of activity.

Lastly, to round out this list of harmful attacks, we have selfish mining. This deals with having a group of miners that spend their time and resources with respect to computing power to mine cryptocurrencies and then those uncovered blocks will not be added to the blockchain which would cause time and resources by other miners to be used wastefully but unknowingly. The group of miners who are forcing the honest miners to do this, will keep the blocks that they mined private to perform some type of divergence to the blockchain, while coincidingly keeping the honest miners using their resources to waste them. Essentially the greedy miner will work diligently to nullify the honest and truthful miners hard work.

Conclusion & Questions

Q: Does any group member own any Bitcoin or Cryptocurrency?

A: No, one group member does own NFTs, which are collectables that use blockchain.

Q: What is being done to stabilize the value of Bitcoin?

A: Nothing, the decentralization of Bitcoin makes it difficult for any one person or group to stabilize the price. The unstable price will most likely be a trait of Bitcoin for a long time. Getting more vendors to accept it as a currency may be one way to stabilize the price; but this is a double-edge issue as the instability is what keeps many vendors from accepting it in the first place.

Q: Has a blockchain ever been compromised?

A:

Q: What is an initial coin offering and is that a form of financial backing of a crypto currency?

A:

Q: Is Bitcoin the highest valued form of cryptocurrency?

A:

Q: How does the newer utility coins differ from traditional crypto currency?

A:

Q: Do you think cryptocurrencies will ever take over as a global currency, similar to how the U.S. dollar is today? And if you do think it will, what do you think the biggest security risk could be? For example, gold and silver was a currency, then came the dollar, then credit cards, which are ever evolving, what's next?

A:

Q: Does any of you have cryptocurrency? or would like to have?

A:

References

- “Blockchain Security Issues and Legislative Challenges.” *CoinCentral*, 30 Apr. 2019, coincentral.com/blockchain-security-issues/.
- Conway, Luke. “Blockchain Explained.” *Investopedia*, Investopedia, 18 Nov. 2020, www.investopedia.com/terms/b/blockchain.asp.
- Hong, Euny. “How Does Bitcoin Mining Work?” Investopedia, Investopedia, 10 Mar. 2021, www.investopedia.com/tech/how-does-bitcoin-mining-work/.
- “What Is Blockchain Technology? - IBM Blockchain.” *IBM*, www.ibm.com/blockchain/what-is-blockchain?p1=Search&p4=43700050370985721&p5=p&cm_mmc=Search_Bing-_-1S_1S-_-WW_NA-_-%2Bwhat+is+%2Bblockchain_p&cm_mmca7=71700000060890804&cm_mmca8=kwd-81638882113280%3Aloc-190&cm_mmca9=913f402a0e8513b3037520021bf70426&cm_mmca10=81638799805846&cm_mmca11=p&gclid=913f402a0e8513b3037520021bf70426&gclsrc=3p.ds&.
- “Redactable Blockchain – or – Rewriting History in Bitcoin and Friends.” *IEEE Xplore*, ieeexplore.ieee.org/abstract/document/7961975.
- Rosic, Ameer, and Blockgeeks. “What Is Blockchain Technology? A Step-by-Step Guide For Beginners.” *Blockgeeks*, 25 Nov. 2020, blockgeeks.com/guides/what-is-blockchain-technology/.
- Vyas, C. A., & Lunagaria, M. (2014). *Security Concerns and Issues for Bitcoin* [PDF]. Rajkot, Gujarat, India: International Journal of Computer Applications. Security Concerns and Issues for Bitcoin (psu.edu)
- Yaga, Dylan, et al. “Blockchain Technology Overview.” Blockchain Technology Overview, arxiv.org/abs/1906.11078.