Dean&Francis
ISSN 2959-6157

Research On Cryptocurrency

Wei Wang

Yew Chung International School of Shanghai, Shanghai, 200127, China
wei.wang2025@ycis.com

Abstract:

Cryptocurrency, a decentralized digital currency, has brought about significant social impacts. This essay explores its effects on crime rates, global economic integration, and the GPU market while also delving into the underlying technologies of blockchain and cryptography. The introduction introduces the concept of cryptocurrency as a decentralized, pseudo-anonymous digital currency. The historical journey and the impacts of cryptocurrency are discussed in section 2, focusing on its social implications. The technological underpinnings are further discussed in section 3. The paper concludes by addressing the core technologies: cryptography and blockchain. Cryptography ensures security and anonymity, with SHA-256 as a fundamental algorithm. Blockchain, a decentralized database, interlinks transaction blocks, making tampering difficult due to Proof-of-Work validation. In essence, cryptocurrency's social impacts and technological foundations intersect, offering insights into its intricate landscape.

Keywords: Cryptocurrency, decentralized, economic integration, blockchain.

1. INTRODUCTION

The fundamental concept of cryptocurrency, put into short words, is a type of decentralized, pseudo-anonymous digital currency that operates on a computer network. Decentralized means that they are not controlled and do not rely on a central authority. This is effectively achieved by blockchain technology, which will be covered later in this passage. Additionally, pseudo-anonymous means that it is not compulsory for users to identify themselves when a transaction occurs and that there would be no way to access one's account without their physical storage device and passcode. In a nutshell, cryptocurrency is essentially a special monetary system where the currencies are purely digital. The history of cryptocurrencies can be traced all the way back to 1989, when they were called "cyber-currencies." At the time, "cyber-currencies" were nothing more than a simple concept mentioned by some people. Then, after a few years, the American cryptographer David Chaum invented digital cash, which depended heavily on cryptography to ensure the validity and security of transactions, and thus came to the name "Cryptocurrency." Then, in October 2008, a paper by Satoshi Nakamoto titled "A Peer-to-Peer Electronic Cash System" outlined a system that can be used to set up a decentralized transaction environment [1]. This paper marked a new era for cryptocurrency and is one of the most important milestones in the history of cryptocurrencies. Later, in 2009, Nakamoto launched Bitcoin, and

ISSN 2959-6157

it quickly became popular among people who needed to send money across borders. Later that year came a famous payment: one person paid 10,000 Bitcoins for two pizzas delivered by Papa John's [2]. Note that 10,000 Bitcoins are worth nearly 1 billion USD in the present day. This payment marked the first ever Bitcoin payment used to purchase actual merchandise. After that, bitcoin rapidly developed and impacted our society in various ways that are discussed in this article. This article will discuss cryptocurrencies with regard to two different perspectives: their social and economic impact, including their effect on crime rates, their effect on the global economy, and their effect on the market prices of GPUs (Graphics Processing Units). Also, the technologies involved in modern-day cryptocurrency including blockchain and cryptography.

2. Impacts of Cryptocurrency

2.1 Increased Crime Rates

Cryptocurrency indirectly causes crime rates to rise and a higher overall amount of maliciously intended software on the internet. Here's why. Usually, when a transaction occurs, the central authority, typically a bank, would be the "middleman" transferring one's money to another's account. In this process, the authority would note down the transaction details, such as the amount of transaction, name, and location of sender and receiver, time the transaction took place etc. However, since all cryptocurrencies are decentralized, there will be no "middleman," and since it is pseudo-anonymous, the personal information of the sender and recipient would not be recorded, therefore creating a platform that allows anonymous transactions that are practically untraceable as there is no authority to review the transactions and organize transaction data. This leads to increased ransomware as the ransom asked by hackers couldn't ever be traced back to them. In fact, ransomware attacks increased by 435% in 2020, and in 2021, the FBI(Federal Bureau of Investigation) received 3,729 ransomware complaints with adjusted losses of more than $49.2 million, according to United States Homeland Security & Governmental Affairs[3]. Moreover, due to its inherent pseudo-anonymity, the presence of cryptocurrencies has made it a significant challenge for law enforcement agencies to monitor money laundering behavior. Consequently, it has been the prime option for criminal organizations such as drug cartels to launder their money. all the criminals need to do is ask their clients to pay in cryptocurrency or use the fiat governmental currency to purchase crypto currencies, and it would be extremely difficult to discover and trace down. A blockchain data company recorded that in 2021, an estimated amount of $14 billion was being transferred to criminals, and $8.6 billion was being laundered through crypto currency, according to [4].

2.2 Economically Integrate the global society

Since cryptocurrencies are virtual and decentralized, it does not represent any governmental organization or have any national elements in the transaction process, meaning it does not divide the world into different areas that use different currencies. As a result, it has the potential to revolutionize the current global monetary system and change it into one where everyone around the world uses the same type of money, thereby integrating the global society from an economic perspective. Apparently, billionaire Elon Musk believes in the future of cryptocurrencies and contributed to pushing the global use of Bitcoin. In February 2021, Musk Purchased $1.5 billion worth of Bitcoin and tweeted, "You can now buy a Tesla with Bitcoin." Experts expect more and more transactions via Bitcoin in the coming years. However, there is a huge problem regarding the daily and practical usage of cryptocurrencies like Bitcoin. They are extremely volatile, meaning their prices often change drastically, and since there is no central authority, it is difficult to predict the price trends for Bitcoin, nor is it possible to minimize change. Thus, portraying an almost spontaneous fluctuation in the price of Bitcoin [5]. This level of instability would never be acceptable for the average citizen to use in daily life. To effectively illustrate the level of volatility of bitcoin, here is a description of the value of bitcoin from 2009-2021: In 2009, BTC was worthless. In March 2010, a user could not sell a 10,000BTC auction for $50. On May 22, 2010, Bitcoin was first sold online at $0.0025—a historic purchase of Domino's pizza for 10,000 BTCs at $25. From July 12-17, the price rose 1000% from $0.008 to $0.08. In February 2011, the price became par with the US dollar. The price rose to $31.50 on June 8 and declined to $11.00 in July and $5.27 at the end of December 2011. In 2012, the price started at $5.27 and grew to $7.38 by January 9, crashed later to $3.80, and then gained about 154% in December. In March 2013, Bitcoin's value moved above $500. BTC hit $770 in January 2014 but fell to $314 in December 2014 and to $434 at the end of 2015. In 2016, the price spiked to $998, then increased up to $2800 in August 2017. The price protruded over 1350% to a peak of $19,783.06 on December 17, 2017. Then, the unprecedented spike decreased by about 45% to begin at $13,412.44 on January 1, 2018. By November, it fell to $ 4,000. The BTC price steadily rose to $8721 by May 29 and later to $12,500 in July. In 2019, BTC price, which started at $3700, steadily rose and stood at $7200 by De-

cember 31. By November 2020, the price rallied above $18,000, gaining all losses from the previous peak. By 2021 July, the price has reached $40,000 [6].

2.3 Increased Prices for GPUs on the Market

One significant way of earning popular cryptocurrencies such as bitcoin is through "mining" (details of this process will be covered later in this article). That process is best performed using the best GPUs (Graphics Processing Unit). Therefore, it wouldn't be difficult to logically conclude that there is most likely a correlation between the price of bitcoin and the demand for high-performance GPUs. Consequently, as bitcoin's value radically spikes up, the cost of high-performance GPUs also rises significantly due to a sudden drastic increase in demand. This has happened three times in the history of Bitcoin: The first time was at the end of 2013 when the value of a single Bitcoin grew from 100 USD to around 1200 USD [7]. As a result, large amounts of people bought graphics cards to mine Bitcoin, increasing the market price for top-tier gaming GPUs by a noticeable amount and impacting regular users to a certain degree. The second time was in 2017, when the value of Bitcoin rose from around 1,000 USD to nearly 20,000 USD. At this point, the price of one of the most popular GPU choices, Nvidia GTX-1066, grew 50% from 2,000USD to 3,000USD [8]. It was more significant this time, but obtaining a GPU for daily usage was still accessible if you were willing to pay. The third spike in bitcoin value happened in 2020 when the value of bitcoin grew from around 3,000 USD to 50,000 USD [8]. However, this time was significantly different from the other times. At this point, there has already been a global shortage of microchips, meaning that the production of any electronic device with the ability to process information has been cut down and slowed down. This indicates that there is no possible way for manufacturers to increase supply in response to increased demand, therefore causing the demand-to-supply ratio to be huge.

Additionally, from the experience gained from the first two spikes of bitcoin value, more people viewed this as an opportunity to get rich, resulting in even big corporations getting involved in mass purchasing GPUs. This not only resulted in the price of the popular GPUs, Nvidia RTX-3090 and Nvidia RTX-3080, becoming 300% of its original price, increasing from 1,500 to 4,500USD, but more importantly, it became difficult to purchase a GPU, even with the prices being raised to 300%. That is because large corporations, personal miners, and many more legitimate users are trying to purchase the same GPUs. Due to the global shortage in supply explained above, it was understood by people that to buy a GPU successfully, one needed to pay 300% of the original price and sit at their computer at 00:00 am to wait for online shopping websites to refresh to be the first to place an order. Only then would one have a chance of being able to receive a GPU? Historically, this problem has been worth noticing. Still, it was far more significant in the bitcoin value spike of 2020 due to a global shortage of chips, causing the supply not to be able to rise together with the demand of customers, further increasing the price of each GPU.

3. The Technologies Involved in Cryptocurrency

3.1 Cryptography

As is apparent from the name, cryptography is a huge part of cryptocurrency, it is without a doubt the most fundamental technology of cryptocurrency. Throughout history cryptography has been an important part of information interchange. Over 2,000 years ago, Julius Caesar invented the Caesar shift cipher, which shifts the alphabet by a certain number of characters, that number is the key used to encrypt and decrypt the message, and would be decided and agreed upon by both the sender and receiver before the message is sent. This idea of having a mutually agreed way of operating with information develops to the enigma code used by the Nazis, then to the modern day internet protocols like SSL and TSL encryption, and the SHA-256 hashing algorithm which we are going to be talking about. SHA-256 is essentially an algorithm that takes an input of any length and transforms it into a unique string of 256bits(32bytes), this algorithm is carefully designed so that even the most minor change in the input would result in a significant difference in the cipher text. For example, one would be able to input the entire game of thrones series into the SHA-256 algorithm and get a string of characters of a fixed length, then if one were to change only one single letter, the SHA-256 algorithm would produce a wildly different output. Another characteristic of the SHA-256 encryption method is that it is irreversible, once encrypted, it would be impossible to reverse engineer the process. As a result, if one were to try to find out what the original input was, assuming they that this cipher text was encoded by SHA-256, they would need to brute-force the process. This is also know as the exhaustive algorithm, were one would literally have to try every single possible combination of characters, put them into the SHA-256 algorithm, trial-and-error until a match is found. So how does this algorithm work? Here is an example of applying SHA-256 on the string "Hello World".

3.1.1 PREPROCESSING

ISSN 2959-6157

Convert "Hello World" into binary, making it "01101000 01100101 01101100 01101100 01101111 00100000 01110111 01101111 01110010 01101100 01100100", then appending a single 1 and the end, so that it becomes "01101000 01100101 01101100 01101100 01101111 00100000 01110111 01101111 01110010 01101100 01100100 1".

Then, pad it with zeros until the data is a multiple of 512. "01101000 01100101 01101100 01101100 01101111 00100000 01110111 01101111 01110010 01101100 01100100 10000000 00000000"

3.1.2 INITIALIZING HASH VALUES

Now we create 8 hash values, which are constants that represent the first 32 bits of the fractional parts of the square roots of the first 8 prime numbers. Hash values are as follows:

h0 = 0x6a09e667
h1 = 0xbb67ae85
h2 = 0x3c6ef372
h3 = 0xa54ff53a
H4 = 0x510e527f
h5 = 0x9b05688c
h6 = 0x1f83d9ab
h7 = 0x5be0cd19

The follow steps are summarized not demonstrated due to its extreme complexity, for more information, see https://blog.boot.dev/crytography.how-sha-2-works-step-by-step-sha-256/ --------

3.1.3 INITIALIZE ROUND CONSTANTS

Create 64 constants, they are the first 32 bits of the fractional parts of the cube roots of the first 64 primes.

3.1.4 CHUNK LOOP

Chunk refers to each "chunk" of 512 bit of data. Due to the short length of "hello world" there is only one chunk in this case, so a loop or an iteration is not needed. But typically, we would be looping through the data and at each iteration of the loop, the hash values would change, and finally producing an output.

3.2 Blockchain

Blockchain technology is also a vital part of cryptocurrency. Blockchain technology is what allows it to be decentralized. Essentially, a blockchain is a decentralized database. It is used in all cryptocurrencies and acts as a ledger [9]. This technology is called blockchain because it is figuratively a chain of blocks connected. Each block contains information on one transaction. Every computer connected to this network will be able to view the contents of these blocks, meaning that transaction data is stored on all computers of this network. If one computer has a different chain record, the system compares the two versions of the ledger and majority rules. As a result, if a large number of users are connected to this network, it is very difficult to tamper with transaction data as one would need to alter the data stored in 50% of the computers.

Blocks connect to form a metaphorical chain by using the cryptography method SHA-256 we discussed previously, together with a mechanism called Proof-of-Work (PoW). The first block of the blockchain is known as the "Genisis Block." It contains transaction data such as the sender and recipient's name, the amount of money transferred, etc. It also has a Hash value based on the data it stores. That hash value is generated using SHA-256 and is thus unique and extremely sensitive to input. The second block of the chain will contain:

· Transaction data.
· The hash value of the previous block.
· Its hash value is generated based on transaction data combined with the last value hash.

This way, all the blocks in the chain are connected by using their hash values generated by SHA-256. Therefore, if one block were to be maliciously altered, its hash value would change, causing a break in the chain, meaning every block after that block would be invalid as the hash values no longer match up. However, there is a problem with this system; it would be possible, nay easy, for modern day computers to alter the information in all the blocks, causing no invalidity of hash values. This is prevented by PoW. PoW describes a mechanism where to add a new partnership or change transaction history, that action must be validified by "miners." Essentially, when a user adds a block to the system, "miners," who can be anyone in the network, do a series of verifications for that new value-added if it is proven to be valid, the miner gives the block a commission, and the miner also receive some reward in the form of cryptocurrency [10]. This prevents malicious hackers to change the entire chain of blocks because when trying to validify the block, a miner needs to repeatedly put a dataset that could only be obtained by downloading and running the entire chain through a mathematical function. The best way to do that is by trial-and-error, making this process time-consuming and demanding on calculation power. Thus, the miners

slow down the process of adding blocks, resolving the concern of hackers creating an entirely new chain. Additionally, miners compete to be the first to verify a block as only the first gets a reward, therefore causing people to massively purchase strong graphics cards to perform these calculations, which is the fundamental reason for the rise of graphics card prices that is discussed previously in this article.

4.Conclusion

Overall, after looking at the social and economic impacts of cryptocurrencies, this author does not believe cryptocurrencies to have the potential of being an effective alternative for the contemporary currencies used around the world. As we have illustrated in sections 2.2 and 2.3, the decentralized nature of cryptocurrencies will inevitably result in its volatility and instability of value. Therefore, discouraging the public to transform their life savings into this form of money. Civilians need a system that they can trust and rely on, people need to be able to believe that their money that's capable of purchasing a house today wouldn't decrease drastically in value so that it can barely purchase an iPhone the next day. From this we can conclude that if cryptocurrencies are implemented to full-on everyday use, it was most certainly causing social unrest, and if hyperinflation were to happen, it would be so extreme and devastating, it would probably inflate thousand times more than the infamous German Hyperinflation crisis of the 1920s because no central authority would be able to influence its value.

Additionally, the logistics of the usage of cryptocurrencies are not suited for daily usage. We have people accidentally transfer money to complete strangers every day, in that case, they call the bank and withdraw that transaction before it is complete. However, that would not work for any cryptocurrency system. Also, if someone gets hold of another's credit card or detailed on their bank account, the owner could call the bank anytime and freeze all money in their account to prevent loss, that cannot be done with cryptocurrency either. In a nutshell, this author holds the belief that cryptocurrencies will never be a part of the general public's daily life since it is practically impossible for people to build up the trust for cryptocurrencies and therefore would never willing use it over their national currency.

REFERENCES

[1] Nigeria, G. (2021). The idea and a brief history of cryptocurrencies. The Guardian Nigeria News - Nigeria and World News. https://guardian.ng/technology/tech/the-idea-and-a-brief-history-of-cryptocurrencies/

[2] History of Cryptocurrency: The idea, journey, and evolution.(n.d.). https://worldcoin.org/articles/history-of-cryptocurrency?forceLocale=true&_gl=1*16vkbf9*_gcl_au*MjEzMzEwNzk3Mi4xNzI0NDM2MjU4

[3] UnitedStatesSenateCommittee on HomelandSecurity & GovernmentalAffairs, & Peters, G. P. (n.d.). Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns. HSGAC, 2–6. https://www.hsgac.senate.gov/wp- content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report_Executive%20Summary.pdf#:~:text=The%20use%20of%20cryptocurrencies%20has%20further%20enabled%20ransomware,transactions%20and%20make%20them%20more%20difficult%20to%20track

[4] BBC News. (2022). Crypto money laundering rises 30%, report finds. BBC News. https://www.bbc.com/news/technology-60072195

[5] World Economic Forum. (2022). The macroeconomic impact of cryptocurrency and stablecoin economics.

[6] Gbadebo, A. D., Akande, J. O., Adedokun, W., Lukman, A. A., & Akande, J. O. (2021). BTC price volatility: Fundamentals versus information.

[7] CoinMarketCap. (n.d.). Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap. https://coinmarketcap.com/

[8] T. (2022). How much did cryptocurrency mining inflate GPU prices? Priceonomics. https://priceonomics.com/how-has-cryptocurrency-mining-influenced-gpu-prices/

[9] IBM (n.d.) What is blockchain? https://www.ibm.com/topics/blockchain

[10] Nevil, S. (2023). What is proof of work (POW) in blockchain? Investopedia. https://www.investopedia.com/terms/p/proof-work.asp#:~:text=Proof%20of%20work%20is%20the%20process%20of%20validating,close%20a%20block%2C%20and%20open%20a%20new%20one.