Retrospective Study of Cryptocurrency Trends

Ravinder Singh Adhikari[1], Rohit Singh Aswal[1], Prabhjot Kaur[2]

[1]Student, [2]Supervisor
Department of computer science
Uttaranchal University
Dehradun, Uttarakhand

Abstract

This paper reviews the understanding of cryptocurrencies as well as the blockchain technology that led to the popularization of cryptocurrencies across the world. Cryptocurrency, as the name suggests, is a digital currency that uses a distributed peer-to-peer network and advanced encryption techniques called cryptography. This cryptocurrency is built upon the blockchain technology, which is a distributed ledger that contains the record of all the past transactions in a block. This is accomplished using mining. Mining includes the use of strong cryptographic algorithms that makes the transactions more secure and robust. This is done by miners to validate the transactions before it is added to the blockchain by solving the complex mathematical puzzle. Miners are then rewarded cryptocurrency coins for successfully mining the mathematical puzzle. This paper systematically reviews the types of cryptocurrencies used worldwide and also explicitly states the advantages and threats arising out of cryptocurrencies.

Keywords: Cryptocurrency, Blockchain, Mining

Introduction

The word cryptocurrency is formed by combining two words cryptography and currency. Cryptography means converting plain text into unreadable codes and vice versa. Currency means as a medium of exchanging goods and services. Cryptocurrency is also known as a digital currency that uses encryption techniques to prevent unauthorized access and fraudulent activity. The public key which is known as a shared key and private key which is known as secret key are used to share cryptocurrency peer to peer between individuals [1].Cryptocurrency uses a decentralized system in which there is no involvement of third party (central authority) instead, it uses a distributed public ledger technology, known as blockchain which acts as databases for all the transactions.

The Blockchain is a public ledger that contains information about all the transactions which are stored as blocks. Blockchain uses hash encryption and proof of work to secure transactions. Miners are responsible for the confirmations of transactions being done between two entities. We can say that cryptocurrencies are all about confirmation. Mining is an important part of cryptocurrencies where the job of miners is to take the transactions and then verify and confirm the transactions before the transactions are send across the network. This transactions are then to the block of every node that are part of the system. Once the transactions are confirmed they cannot be altered or modified. Miners are then rewarded with cryptocurrencies coins for their job. Proof-of-work and proof-of-stake are some mining techniques that miners use for adding the transactions in the blockchain. Miners use proof-of-work algorithm to verify and confirm the transactions and produce new blocks to the chain [2].

Bitcoin is the first and the most popular cryptocurrency invented by Satoshi Nakamoto in 2009. According to different web sources, there are over 1600 crypto currencies available on the internet as of 19 August 2018.Some of the mostly used crypto currencies are Bitcoin, Ripple, Ethereum, Tether etc. Bitcoin is the most popular used cryptocurrency with a market capitalization of $93,465,362,725 USD [3].The main feature of cryptocurrency is that it is not controlled by any central authority which makes the transactions easier and also with less transactions fee [4]. All these transactions take place on internet involving data flow via network traffic. There are various security issues that are needed to be taken care of while dealing with network traffic [26]. Various researchers proposed models and methodologies to take care of threats arising out of online networking and transactions [27].

At present-day, cryptocurrencies has become a new movement in the world of finance because of the benefits that cryptocurrencies provide to the investors. All of us have heard the word cryptocurrency but many of us do not know exactly about what is cryptocurrency. The purpose of this paper is to let readers know about cryptocurrency and also the technology behind its popularity, called blockchain. Well as the name suggest, cryptocurrency is also known as a virtual currency that is formed to work as a medium of exchange and uses cryptography for security. The reason behind cryptocurrency gaining attention in the market is because of the policies where there is no involvement of third party which reduces the transactions cost. Also, it provides the options for the transactions to be highly classified and be anonymous.

Literature Review

Mukhopadhyay, U., et al. [5] has concluded in their study that major cryptocurrencies mining use proof-of-work hashing algorithm which is resource intensive and proof-of-stake algorithms which cannot act independently. The study overall concludes that merging of both algorithms is found to be productive in cryptocurrencies mining.

Vranken, H., et al. [6] has concluded in their paper that proof-of-work algorithm in bitcoin mining is computer-intensive and energy consuming, but it helps to deal the problem of double-spending and security of the blockchain. The mining hardware has progressed from CPU, GPU and FPGA to ASCI resulting in performance increase and energy efficiency. Since bitcoin mining is becoming popular, it will also increase in the effort of bitcoin mining. The study also reveals that only those miners will survive who bid the most competitive mining hardware and have the advantage of low electricity cost.

D'Alfonso, A., et al. [7] has concluded in their study that bitcoin shows higher growth rate value than ethereum in the following next five years. The study overall reveals that 69% should be invested in bitcoin and 31% in ethereum in order to get maximum return in the next five years.

Seebacher, S., et al. [8] reveals in their study that blockchain technology creates a reliable environment through its translucent nature, making the information of transactions publicly to everyone throughout its entire network, while making sure that the information cannot be altered. Blockchain also provide security for privacy through various cryptographic algorithms.

The study overall reveals that blockchain technology can have a big impact in various aspects in the operation of service systems, such as facilitating co-creation value, ensuring accessible of information and offering mechanisms of collaboration.

Darlington III, J., et al. [9] reveals in his study that adoption of bitcoin helps in solving the problems of inflation, exchange, fraud prevention and accessibility. Also cryptocurrency can help struggling countries, as it can open a new door for economic transformation to occur and can help the individuals maintaining their own finances. The study overall reveals that cryptocurrency has changed the global economic topography forever. It also helps to prevent the problem of double-spending.

Shehhi, A. Al, et al. [10] has concluded in their study that majority participants in cryptocurrency mining are men (95.5%) who are of the ages between 26 and 35. Also study reveals the main factors behind picking a cryptocurrency to mine and use, the majority of the participants expressed mitigate of mining, having strong and large community, privacy, currency value and its popularity, easier to start mining, less complexity of use. Also half of the participants believed that the name and logo of the currency plays an important role in picking a coin to use.

Bunjaku, F., et al. [11] has concluded in their study that the prospective of cryptocurrencies can be resourceful if explicit situations can be met. Also cryptocurrencies can be the future of new form of payment taking over the old methods of payment. The study also reveals that banks should pay attention to the technology that cryptocurrencies use, as it can be a more productive way to transfer the ownership value in the future.

Vyas, C.A., et al. [12]has concluded in their study that the main hazard that bitcoin faces are its vulnerability in the process of mining and transactions and lack of security in storing the coins in the online pools. Also their study reveals that bitcoin have the attacks rate of 50% in the mining process. They also stated that in order to overcome this hazard, bitcoin framework needs to be changed with an advanced framework in the mining process.

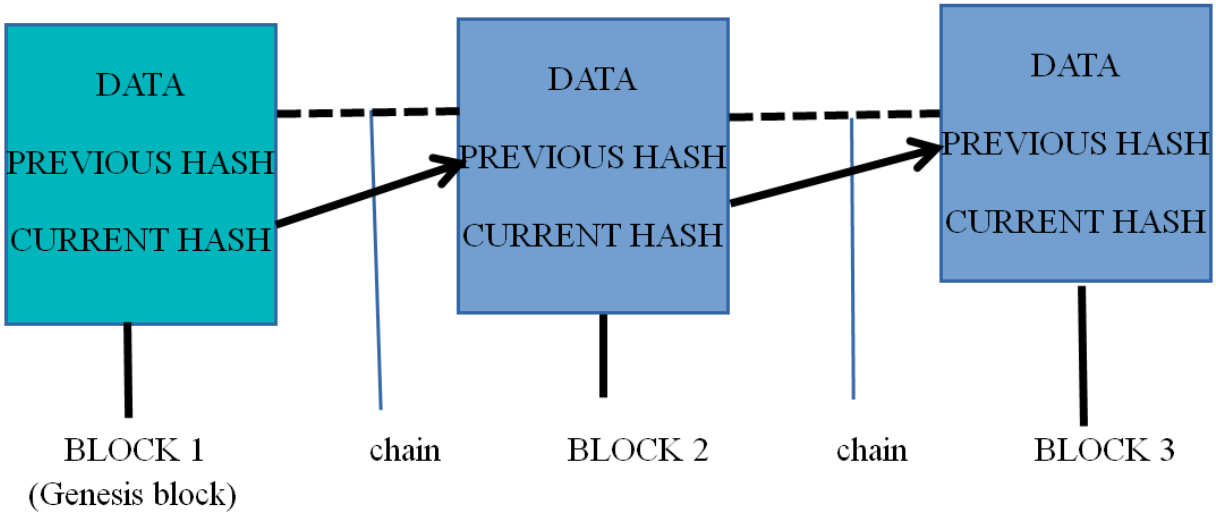
Harvic, C., [13] concluded that there is a prospect of security violation from the online domain. Shah Alam (2017) also reveals in his study that users of cryptocurrencies cannot recover their losses in the case of security violation because it does have a third party to oversee the security problems and also for new investors it requires of purchasing of technology and resources.

Blockchain in cryptocurrency

The blockchain is a distributed public ledger that contains information about transactions. It is a technology used in cryptocurrencies. Every time a transaction is done, it is stored in a block and a copy of a transaction is made and is distributed to every node that is part of the system. Every transaction which added to a blockchain is authenticated by the multiple nodes on the network. All nodes which are responsible for blockchain transactions create a network in which the files and resources are shared without any involvement of the third party, this network is also known as peer to peer network. Every node validates the transactions and added it to the blockchain [14].

In blockchain, there is no central authority rather it uses a peer-to-peer network. A cryptographic hash generated from previous block is used to link the new block added to a blockchain, ensuring the chain is never broken thereby recording the block permanently [14].

Figure 1: Simple Blockchain Scenario



In "**figure 1**" we can see Blockchain scenario, as its name suggests blockchain that is a chain of blocks. It is a distributed database, that has records and these records called blocks. If we assume bitcoin blockchain then it has data, hash and hash of the previous block. Data includes information about the amount that was sent and received by one block to another block. Hash also known as hash value is a unique identifier that identifies the block. Every block has its unique hash value, whenever a block created a hash value be calculated, changes in blocks result the changes in their hash value automatically. A block can also contain the hash of the previous block. All these things make it a blockchain. Other areas in which blockchain can be used are smart contracts, when certain condition are met. For non-financial purposes like Interplanetary File System (IFPS) block chain technology can be used to decentralize file storage by inter-linking them through internet [14].

Mining in cryptocurrency

Mining in cryptocurrency refers to the process of verifying the transactions of various forms of cryptocurrency and adding these transactions in the blockchain public ledger [15]. Whenever a transaction is made, a miner ensures that the transaction is valid and accordingly updates the blockchain. In order to mine cryptocurrency, a miner should have a computer with specialized hardware and internet connections. The mining process involves solving complex mathematical computations with cryptographic hash functions in a block that contains transaction data [15].

The miners are rewarded cryptocurrency coin in return for their services by the owner of the cryptocurrency. For example, the current reward for bitcoin mining is 12.5 coins. Mining in cryptocurrency is based on proof-of-work which requires an agreement to be reached and verification of transactions in the block chain public ledger [16].

Mining can also be done by forming a group, where miners forms a group together and integrate their computational resources to produce blocks faster, known as mining pool. In pool mining the rewards is usually distributed between miners based on their agreement and their contributions in mining including valid proof-of-work [17]. There are four types of cryptocurrency mining pools which are as follows:

1. Single coin pools: In this type of mining pool, the miners are only allowed to mine only one type of coins [18].

2. Multi Coin Pools: In this type of mining pool, the miners are allowed to mine multiple coins at the same time without affecting in its productivity [18].

3. Local Mining Pools: In this of mining pool, the miners have to purchase theirs own equipment like hardware, software, and the ASIC devices and has to setup this equipment [18].

4. Cloud Mining Pools: In this of mining pool, the miners need not purchase their hardware equipment rather it can bought through a contract where the miners needs to pay a fee for mining to happen and their fee will be debited from their mining reward [18].

Some of the biggest mining pools examples are listed below:

1. BTC.com: It is used to join and mines 15% of all blocks and it is a public mining pool [19].

2. Antpool: It is a china based mining pool and mines about 11% of all blocks [19].

3. Slush: It was first mining pool which mines 11% of all blocks [19].

4. F2pool: F2Pool is based in China. It has mined about 10% of all blocks over the past six months [19].

5. BTC.top: BTC.top is a private pool and cannot be joined. It mines about 7% of all blocks [19].

6. DPOOL: DPOOL is a Chinese pool and mines about 4% of all blocks [19].

Examples of cryptocurrency

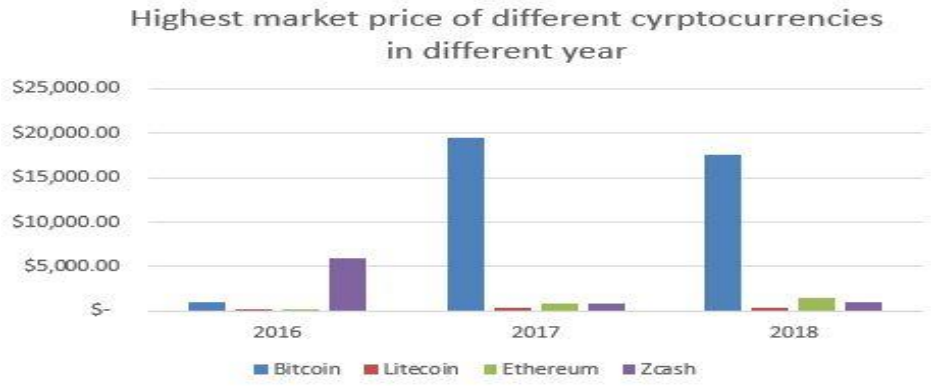
1. Bitcoin (BTC): Bitcoin is the first and most popular digital cryptocurrency launched in 2009 by Satoshi Nakamoto. Bitcoin is based on a peer-to-peer network that uses blockchain technology for storing the transactions detail that has ever happened. Bitcoin is a decentralized system in which there is no involvement of the third party which means transactions can be done directly between the sender and receiver. Bitcoin uses the hash cash proof-of-work algorithm to verify the transactions before it is added to the blockchain, this is done by the bitcoin miners. Currently, 12.5 bitcoins are rewarded to the bitcoin miners for successfully mining a block. Currently, Bitcoin market cap is **$93,465,362,725** USD and is the most popular cryptocurrency [3].

2. Litecoin (LTC): Litecoin is a digital cryptocurrency that is created by Charlie Lee, an MIT graduate, and former Google engineer. Litecoin is similar to bitcoin which is also known as silver cryptocurrency compared to bitcoin as gold [20]. Litecoin uses end to end encryption technique which eliminates the need of third party resulting in no transaction cost. Litecoin works on blockchain technology to store records of transaction and is made available to everyone who is part of this network instead of storing in a single database. Litecoin is based on proof-of-work but it uses script algorithm in its proof-of-work which makes the transaction faster and secure. Transaction in Litecoin is cheaper than other cryptocurrencies because of fewer transactions fees [20]. The market cap of Litecoin is $4,886,732,737 USD according to coin marketcap [21].

3. Ethereum (ETH): Ethereum was created by Vitalik Buterin, a programmer from Toronto, a platform that helps developers to build decentralized applications [22]. Ethereum is an open software platform [23] which works on a distributed network called blockchain, which is used to build and deploy decentralized applications [23]. In Ethereum, a blockchain mainly focuses on running the programming code of any decentralized applications [23]. Like Bitcoin miners, Ethereum miners also get rewards, a type of token, called ether for successfully mining in the Ethereum network. This token can also be used by application developers to pay transactions fee and other services on the Ethereum network [23]. There is also another type of token, called gas which can be used to pay the miners for adding their transactions in the block. In Ethereum block chain, smart contracts can also be built, a type of program that executes automatically when exact conditions are met [23]. The market cap of Ethereum is 16,409,762,599 USD which is ranked #2 after bitcoin [3].

4. Zcash (ZEC): Zcash was launched in October 2016 which was branched from Bitcoin. Zcash was formerly known as zerocoin. Zcash is a digital cryptocurrency that uses a peer-to-peer network like Bitcoin [24]. The only difference is that Zcash mainly focuses on private, anonymous, and fungible transactions that Bitcoin can't do [24]. Zcash uses ZK-SNARK protocol, a type of zero-knowledge proof protocol which helps to hide the sender and receiver information as well as the amount of transaction being done [24]. The market cap of Zcash, according to marketcoincap is $380,537,182 USD [3]. It has a total supply of 21 million of coins and is expected to be mined by 2032 [25].

Figure 2: Highest market price of Bitcoin, Litecoin, Ethereum, and Zcash in the year 2016-2018.



As we can see in "**figure 2**" that in 2016 market price of bitcoin was very low compared to zcash and the next year in 2017 suddenly the market price of bitcoin was extremely high, where zcash was gone down. In 2018 the market price of bitcoin was a little bit low compared to 2017, where Litecoin and Ethereum market price little bit growing every year.

Conclusion

In this paper, we narrated that the craze and growth of different cryptocurrency also known as digital currency. Cryptocurrency that uses blockchain technology makes cyrptocurrency highly secured and attractive. That is the reason peoples invest on cryptocurrency. Cryptocurrencies have become popular with the introduction of Bitcoin in 2009 encouraging various traders and merchants to invest in cryptocurrencies. There is also the main role of crptocurrency mining, without that it is impossible to use of block chain technology. Cyptocurrency mining is responsible for verifying and updating the transactions of different cyptocurrencies account holders. A miner has responsible for cryptocurrency mining process, as the result miners get reward from the cryptocurrency owner. A miners can use different type of mining pool which is suitable for them according to their budget. There are different type of cryptocurrency which used by the peoples for trading and other purposes. As we analyze that most of cryptocurrencies market price can be high and low every year. Few countries have already started to adopt these cryptocurrencies and are also been used by various companies for transactions.

References:

[1] "What is cryptocurrency?," *techopedia.com*, 2019. [Online]. Available: https://www.techopedia.com/definition/27531/cryptocurrency. [Accessed: 10-Apr-2019].

[2] "Proof-of-Work, Explained | Cointelegraph." [Online]. Available: https://cointelegraph.com/explained/proof-of-work-explained. [Accessed: 27-Apr-2019].

[3] "Cryptocurrency Market Capitalizations | CoinMarketCap," *coinmarketcap*, 2019. [Online]. Available: https://coinmarketcap.com/. [Accessed: 26-Apr-2019].

[4] "Read the Latest Cryptocurrency News | Cointelegraph." [Online]. Available: https://cointelegraph.com/tags/cryptocurrencies. [Accessed: 27-Apr-2019].

[5] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A Brief Survey of Cryptocurrency Systems."

[6] H. Vranken, "Sustainability of bitcoin and blockchains," *Curr. Opin. Environ. Sustain.*, vol. 28, pp. 1–9, 2017.

[7] A. D'Alfonso, P. Langer, and Z. Vandelis, "The Future of Cryptocurrency," *Int. Secur.*, vol. 7, no. 5, pp. 7–45, 2016.

[8] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: A structured literature review," *Lect. Notes Bus. Inf. Process.*, vol. 279, pp. 12–23, 2017.

[9] J. Darlington, "The Future of Bitcoin : Mapping the Global Adoption of World ' s Largest Cryptocurrency Through Benefit Analysis," *Univ. Tennessee Honor. Thesis Proj.*, pp. 1–21, 2014.

[10] A. Al Shehhi, M. Oudah, and Z. Aung, "Investigating factors behind choosing a cryptocurrency," *IEEE Int. Conf. Ind. Eng. Eng. Manag.*, vol. 2015-Janua, pp. 1443–1447, 2014.

[11] F. Miana, J. C. de Melo, C. N. Coelho, P. Nattrodt, and A. O. Fernandes, "Mixing Symbolic and Ternary Simulation Techniques for the Verification of Processor-Based Systems," pp. 31–39, 2004.

[12] M. Vyas, Lunagaria, "Security Concerns and Issues for Bitcoin," *Int. J. Comput. Appl.*, pp. 10–12, 2014.

[13] C. Harwick, "Cryptocurrency_and_the_problem.PDF," *Indep. Reveiw*, 2016.

[14] "Blockchain Definition," *Techterms*, 2018. [Online]. Available: https://techterms.com/definition/blockchain. [Accessed: 12-Apr-2019].

[15] Forrest Stroud, "What Is Cryptocurrency Mining? Webopedia Definition," *webopedia.com*, 2019. [Online]. Available: https://www.webopedia.com/TERM/C/cryptocurrency-mining.html. [Accessed: 12-Apr-2019].

[16] "All You Need to Know About Cryptocurrency Mining – UniversaBlockchain – Medium," *Universa*, 2018. [Online]. Available: https://medium.com/universablockchain/all-you-need-to-know-about-cryptocurrency-mining-d501fcae546a. [Accessed: 12-Apr-2019].

[17] "Mining Pool." [Online]. Available: https://www.investopedia.com/terms/m/mining-pool.asp. [Accessed: 27-Apr-2019].

[18] "What is Cryptocurrency Mining Pool? - CryptoGround." [Online]. Available: https://www.cryptoground.com/guide/cryptocurrency-mining-pool. [Accessed: 27-Apr-2019].

[19] "10 Best and Biggest Bitcoin Mining Pools 2019 (Comparison)." [Online]. Available: https://www.buybitcoinworldwide.com/mining/pools/. [Accessed: 27-Apr-2019].

[20] "What is Litecoin - An Ultimate Guide on LTC crypto," *coinwitch*, 2019. [Online]. Available: https://coinswitch.co/info/litecoin/what-is-litecoin. [Accessed: 26-Apr-2019].

[21] "Litecoin (LTC) price, charts, market cap, and other metrics | CoinMarketCap," *CoinMarketCap*. [Online]. Available: https://coinmarketcap.com/currencies/litecoin/. [Accessed: 26-Apr-2019].

[22] "Who Created Ethereum?," *coindesk*. [Online]. Available: https://www.coindesk.com/information/who-created-ethereum. [Accessed: 26-Apr-2019].

[23] "What is Ethereum? The Most Comprehensive Beginners Guide," *Blockgeeks*. [Online]. Available: https://blockgeeks.com/guides/ethereum/. [Accessed: 26-Apr-2019].

[24] "Zcash Cryptocurrency: Everything You Need To Know," *coinsutra*. [Online]. Available: https://coinsutra.com/zcash-cryptocurrency/. [Accessed: 26-Apr-2019].

[25] "Crypto 101: What is Zcash (ZEC)?," *coinelitist*. [Online]. Available: https://www.coinelitist.com/crypto-101-what-is-zcash-zec/. [Accessed: 26-Apr-2019].

[26] P. Kaur, A. Bijalwan, R. C. Joshi, and A. Awasthi, "Network forensic process model and framework: An alternative scenario," *Adv. Intell. Syst. Comput.*, vol. 624, pp. 493–502, 2018.

[27] P. Kaur, P. Chaudhary, and A. Bijalwan, "Advances in Computing and Data Sciences," vol. 905, pp. 208–217, 2018.