BITCOIN MINING TECHNOLOGIES AND THEIR EFFECT AS A FORM OF INVESTMENT

Habib Olaniyi Aliu & Dahiru Adamu
Department of Computer Engineering, Federal Polytechnic, Ilaro, Ogun State, Nigeria.
olaniyi.aliu@federalpolyilaro.edu.ng ; dahiru.adamu@federalpolyilaro.edu.ng

Abstract

Cryptocurrency is a peer-to-peer (P2P) programmable digital currency. They are virtual commodities designed as currencies without a centralized regulatory body. It is similar to fiat currency in that the users agree upon the value, giving it its market value. There is no centralized authority to regulate the price of the digital currency, so the price is volatile. Some common types of cryptocurrencies include Bitcoin, Litecoin, Ethereum, Ripple, Dogecoin, Tron, etc. To use cryptocurrencies, a digital infrastructure such as smartphones, computers, internet networks, and connectivity must be in place, which limits their easy accessibility and understanding by laymen. Since it is volatile, it is vulnerable to hackers and malware and is untraceable. Bitcoin is a digital currency that can be used to buy goods and services. It uses strong cryptography to secure online transactions. Since it's created in cyberspace, it does not require the existing banking system. Miners make use of their computers to solve complex algorithms and carry out tasks like mining, thereby getting rewards in the form of cryptocurrency, which are stored digitally and passed between buyers and sellers without the need for an intermediary. If cryptocurrency is adopted, it will allow a stream of easy digital transactions, thereby connecting the world to easy online transactions.

Keywords: Digital Currency, Blockchain, Cryptocurrency, Bitcoin Mining.

Introduction

Digital currency is a term for currencies that may be handled physically, just like traditional currency, but are used for online transactions. Digital currencies are fictitious, non-tangible money that, after being exchanged, acquire physical worth. Only digital devices like computers, tablets, and smartphones are used to transact with digital currency. Additionally, only digital wallets that are accessible online are used to store digital currencies. Unlike physical currencies like mint coins and notes, which can only be exchanged when a business is open, digital currency can be used anytime. A cryptocurrency is another type of digital money that is often employed in the creation of centralized currencies (Phillip *et al*, 2018).

The original creator of the Blockchain technology used in Bitcoin was Satoshi Nakamoto, which was invented in 2009.

Blockchain is a digital data storage system that uses encryption to save specific notes. The blockchain can be thought of as a linear chain or data chain because these records are uploaded to a database one at a time, creating an extremely lengthy succession of data (Wouda & Opdenakker, 2019). The data is then kept and cannot be altered or even removed once it has been entered into the database. All information submitted into the database will be kept on a network of computers made up of thousands of these nodes. Modern cryptocurrencies are built on the blockchain technology, which gives them their name due to the extensive use of cryptographic operations. In order to digitally sign and securely transact within the system, users use public and private keys. Users may solve puzzles using cryptographic hash functions for blockchain networks based on cryptocurrencies that involve mining in the hopes of being rewarded with a predetermined amount of the cryptocurrency.

How participants agree that a transaction is genuine is another crucial feature of blockchain technology. There are numerous techniques for doing this, each with advantages and disadvantages for specific business cases, and the process is known as "reaching consensus." It's critical to realize that a blockchain is only a component of the overall solution. Implementations of blockchain are frequently created with a particular goal or function in mind. Cryptocurrencies, smart contracts (software installed on a blockchain and performed by computers running that blockchain), and distributed ledger systems between companies are examples of such functions (Sinha & Chowdhury, 2021). The blockchain technology industry has seen a steady stream of advancements, with new platforms regularly being introduced as the landscape shifts. Permissionless and permissioned are the two broad, high-level categories that have been defined for blockchain methods. Anyone can read and write to the blockchain without permission in a permissionless blockchain network. Blockchain networks with permissions restrict participation to particular

individuals or groups and provide more precise controls. An organization can determine which subset of blockchain technologies would be appropriate to its needs by understanding the differences between these two groups.

Blockchain technology is used by cryptocurrency, one of which is digital money, electronic money, or virtual money that shares characteristics with real-world currency but does not have a physical form (Pavlovski, 2015). Every transaction that takes place will be extremely transparent thanks to the blockchain technology, and every piece of data that already exists will be related to one another and have a single user within the framework of the cryptocurrency system. This cryptocurrency idea was first introduced in a white paper by an anonymous inventor in 2008. He released it under an open-source license (Peng *et al*, 2018).

The Bitcoin (BTC) problem is referred to as mine and is worked on collaboratively in a network (Narayanan *et al*, 2016). Bitcoin's adoption was encouraged by the use of a blockchain, which made it possible to deploy electronic money in a distributed manner without a single user having control over it or a single point of failure. Its main advantage was the ability to conduct direct transactions between users without the use of a reliable intermediary. It also made it possible to issue fresh bitcoin in a specified way to users who are able to create new blocks and keep copies of the ledger; in the context of Bitcoin, these users are known as miners. The system's distributed management was made possible without the need for organization because of the miners' automated payments. A self-policing technique was developed using a blockchain and consensus-based maintenance to make sure that only legitimate transactions and blocks were added to the network.

2.0 Benefits of Bitcoin

- Bitcoin's decentralized nature : Each computer mining node is a part of this structure because cryptocurrency lacks a central authority and its networks are accessible to all users. This guarantees that the central government does not have the authority to impose regulations on cryptocurrency owners, making it safe and simple to use (Lee, 2019).
- Users' confidentiality: You can create an infinite number of wallets for cryptocurrency, regardless of your name, address, or other information. The account IDs are not anonymous, notwithstanding the anonymity of the users. Cryptocurrency uses a push method that enables users to send merchants or recipients exactly what they want without providing any more information (Sinha & Chowdhury, 2021).
- Elimination of third parties: In contrast to traditional asset transactions, which only allow for immediate payment between users, bitcoin contracts can be set up and performed to exclude or include third party permissions, compare extra information, or be carried out at a future date or time (Turner *et al*, 2019).
- Available and generally accepted:Cryptocurrency can be used internationally without issues because it is not constrained by exchange rates, interest rates, transaction fees, or other fees from any government. When compared to the centralized banking system, creating a cryptocurrency wallet is simple and causes less stress, making it widely accessible.
- Every transaction is open to the public: Every cryptocurrency transaction is recorded on the underlying Blockchain. The user-specified public data is visible to others.

Effect of Bitcoin As a Means of Investment

- Market Unpredictability : When compared to the current price in August 2022, which is $23,333 (#9,715,861), the price of bitcoin as of December 2021 was $47,192 (#26,616,383) (coinmarketcap, 2022). Since the exchange is always shifting, the market is unclear. Close market monitoring should be prioritized to prevent significant losses.
- Inability to Gain Access to Wallet: Due to insufficient recovery methods, you run the risk of losing your wallet if your hard drive (HDD) malfunctions or becomes infected with a virus.
- Usage Restriction: Some businesses and organizations accept bitcoin as payment. Many companies still do not accept bitcoin as a valid form of payment. The use of bitcoin as a viable payment method is decreasing due to bans from nations like China, Egypt, and others.
- Data Loss and Hacking: Malicious emails, click-bait, and other tactics can be used to target a specific individual's email, causing them to lose important data that could lead to the theft of their wallet.

3.0 Bitcoin Mining Technologies

Mining Hardware

Mining works in the protocol, carried out using software to control the currency. It secures the network by using the processing power to cover the previous transactions. Mining cross checks transactions by verifying the current one against the previous ones, making it safe from spending used or false currency. It makes use of a frequency that is targeted at an internet of 10 minutes to generate new blocks via a current defined by the new block reward. Cryptocurrency mining is the method of generating digital currencies like Bitcoin, Doge, Ethereum, etc., by solving difficult mathematical issues utilizing hardware. Those who execute this process are called miners. Hardware is needed for mining to occur. Different approaches using hardware have been used by miners. Mining is done by CPU but has evolved in recent times. It has changed to FPGA, GPU, and ASIC.

A GPU (graphics processing unit) is a complete chip. It provides images and graphics by executing rapid mathematical computations. Its use for simple operations like shading pixels and sketching triangles as much as possible per second makes it faster than the CPU.

An FPGA (field programmable gate array) is a highly programmable processor. It is more expensive than a CPU or GPU but uses less power.

Finding Valid Blocks

The procedure for finding a valid block requires the miner to develop a record of current transactions and compute a little outline information about the suggested block. The outline is integrated with an arbitrary number called nonce to develop a block herder. The block header hash is computed and evaluated to confirm if it can win at that particular difficulty, so the step is repeated by changing the nonce and the current hash is computed and tested. A Brute force search is used to produce a valid block. This process requires the miner to try one nonce at a time until it works.

Unless he gets lucky, the miner cannot tell which nonce works from the previous one. The fastest approach is to improve the speed at which you can execute with the nonces. The processing power determines how fast you can search. When an immediately valid block is created, it is distributed across the network to verify the other nodes in the network.

CPU Mining

Early phases of Bitcoin mining make use of CPUs. It searches with the aid of the code for nonces in a direct mode, then accesses SHA 256 in software to examine its authenticity in a block (Narayanan, 2016). CPU mining got outdated for a lot of reasons, including :

- Slow in processing.
- It has an average hash rate of 0.7 MH/sec.
- It consumes a lot of power.

SHA 256 is a cryptographic hash function majorly used in Bitcoin, basically because its hash function is secure and very efficient. (Naik & Courtois, 2013).

The hash rate is the unit for measuring processing power for any of the cryptocurrencies.

GPU Mining

GPU mining is the second generation of Bitcoin mining. It was created due to the low computation power of CPU mining. It processes faster than CPU mining, but on a long run it can't cope with the increases in difficulty rate. When mining, GPUs overheat and use a high level of hardware utilization.

FPGA Mining

FPGA (field programmable gate array) has higher computation power compared to GPU mining. It is the 3rd generation of Bitcoin mining. The number of miners using FPGA increases, thereby making it difficult for the network. Due to this, FPGA was unable to meet the projection..

ASIC Mining

An ASIC (application specific integrated circuit) is a chip designed to mine cryptocurrency. It consumes a lot of power. ASIC mining works on a particular algorithm. It operates faster than the CPU and GPU and performs better. Its hash rate is 14 TH/s.

When mining, miners are faced with the risk of high electricity consumption and excessive heat emission from the hardware. The best alternative to this problem is to use cloud mining (Golshan, 2007).

Mining Process

Miners use the processing power of hardware to solve difficult mathematical issues and validate the blocks. It's a way of adding log records to the public ledger. The log is valid when the sender signs it. As more miners join the network, mining becomes more difficult. Bitcoin mining has a flexible way of going about it. Its protocol is adjusted so that a block is verified and added to the blockchain network within 10 minutes. A valid block is one that has proof of work. Bitcoin is rewarded to miners for each block that has proof of work. Bitcoin is rewarded to miners for completed work after confirming the block.

Proof of Work

It is a consent algorithm used by Bitcoin and other cryptocurrencies. It comprises a difficult cryptographic mathematical puzzle. It searches for a nonce value. The nonce helps to determine the hash value of a block and also helps to meet the hash criteria. Miners mine blocks through the calculation of the hash of that block with a varying nonce, and it doesn't have a specific formula to vary the nonce. It varies randomly and give the expected result when the hash value is equal or lower than the given target value.

Target

The target is 256 bits in size and is shared by all miners. It has an effect directly on the difficulty of the Bitcoin network system. The lower it is, the harder it is for it to discover a block. Once a mining block reaches 2016, the target is calculated all over again, and it takes about 14 days to mine up to 2016 blocks.

Mining Reward

After 210,000 blocks of Bitcoin have been mined, the reward decreases by half, and the total number of Bitcoin that can be mined is 21 million. As more Bitcoins are mined, the reward for mining decreases. It takes up to 4 years to mine 210,000 blocks of Bitcoin. The reward drops over the years. The miners get a transaction fee for any addition of transactions in the blockchain (Stoll et al., 2019), which is 1% of the initial block reward. Table 1 below shows the drop in mining rewards over the years.

Table 1: Bitcoin Mining Rewards

Interval	BTC Reward
Jan 2009 - Nov 2012	50 BTC
Nov 2012 - Jul 2016	25 BTC
Jul 2016 - Feb 2020	12.5 BTC
Feb 2020 - Sep 2023	6.25 BTC

Mining Method

The two common method of mining Bitcoin is solo mining and pool mining.

Solo Mining

Just like the name implies, it is a mining method that involves an individual using its hardware resources to mine and work alone. Since it's done by an individual based on the hardware resources, he gets the reward for mining after solving the block problem. Its rewards for mining are determined majorly by how good its hardware resources are. It

actually takes a lot of time for solo miners to generate a valid block because of the limited hardware resources. When pool mining was introduced in 2011, all miners before then were solo miners (Wang & Liu, 2015).

Pool Mining

Pool mining is done by more than one miner. Each pool miner uses a unique ID to mine bitcoins (Narayanan, 2016). Miners combine their hardware resources to generate a valid block faster and have higher power than solo miners. The lower difficulty value is assigned to each member, making it easier for the miners to solve the hash problem and prove work. After it has been solved, each pool miner submits its work in hash value under the target value for verification. If the block is claimed by the pool, the reward is distributed to each pool miner. The distribution rate is determined by each pool miner's hash rate and time.

4.0 Conclusion

A new tool that could be useful for organizations is blockchain technology, which enables safe transactions without the need for a central system. Blockchain technology is used by Bitcoin, which strengthens its decentralized nature. Bitcoin's decentralized structure allows users to deal successfully without the assistance of a middleman because the system is not governed by a single central authority. Because bitcoin is so erratic, it has an impact on economic instability. Bitcoin mining is a continuous process that calls for the employment of CPU, GPU, or ASIC technology in order to identify a valid block and resolve the consensus issue with the transaction ledger. The economic value of the coin increases as more mining takes place. The continual use of bitcoin offers a simpler method for conducting international transactions and, if properly controlled, could assist future generations in overcoming obstacles in numerous types of financial transactions.

References

Wouda, H. P., & Opdenakker, R. (2019). Blockchain technology in commercial real estate transactions, *Journal of Property Investment and Finance*, vol. 37, no. 6, pp. 570– 579.

Phillip, A., Chan, J. & Peiris, S. (2018). A new look at cryptocurrencies, *Economics Letters* 163: pp. 6-9.

Sinha, D. & Chowdhury, S. R. (2021). Blockchain-based smart contract for international business–a framework, *J. Glob. Oper. Strateg. Sourc.*

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfede, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, *Princeton University Press.*

Pavlovski, C.J. (2015). Reference architecture for cryptocurrency in banking, *Information Technology in Industry* 3(3), pp. 74–80.

Peng, Y., Albuquerque, P.H.M., Camboim de Sa, J.M., Padula, A.J.A., & Montenegro, M.R. (2018). The best of Two Worlds: Forecasting High Frequency Volatility for Cryptocurrencies and Traditional Currencies With Support Vector Regression, *Expert Systems with Applications* 97: 177-192.

Lee, C. J. (2019). Crypto Liquidity: The Blockchain and Monetary Stability, *Journal of Entrepreneurship and Public Policy*, vol. 9, no.2, pp. 227–252.

Turner, A. B., McCombie, S. & Uhlmann, A. J. (2019). A Target-Centric Intelligence Approach to WannaCry 2.0, *J. Money Laund. Control*.

Arvind N. J. B. (2016). CPU mining, in Bitcoin and Cryptocurrency Technologies, *Princeton University Press*, pp. 136-142.

Naik, R. P. & Courtois, N.T. (2013). Optimising the SHA256 Hashing Algorithm for Faster a nd More Efficient Bitcoin Mining. *MSc Inf. Secur. Dep. Comput. Sci. UCL*, pp. 1–65.

Golshan, K. (2007). Physical Design Essentials: An ASIC Design Implementation Perspective. New York: *Springer*. ISBN 978-0-387-36642-5.

Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The Carbon Footprint of Bitcoin The Carbon Footprint of Bitcoin. *Joule*, 3, pp. 1– 15.

Wang L. & Liu, Y.(2015). Exploring Miner Evolution in Bitcoin Network, in Passive and Active Measurement. *Springer*, pp. 290–302.