Blockchain Layers of Security and Mining Difficulties Affecting Block Rewards for Miners of Bitcoin Cryptocurrency

[1]R. Anbazhagan, [2]Dr. K Saraswathi
[1]Part Time Ph.D Research Scholar, [2] Associate Professor
[1]Department of Computer Science,
[1]Government Arts College (Autonomous), Coimbatore-641018, Tamil Nadu, India.
[1]anbu.cs.lect@gmail.com ,[2]drsaraswathirajendran@gmail.com

ABSTRACT

Blockchain Technology is complex to understand but efforts can realise its benefits. Many countries and several States of India has implement blockchain technology in various fields. This research aims to understood the basics of block mining and validation of transaction process in bitcoin cryptocurrency. Elaborating layers contribution in terms of the activities involved in the process of security consensus of blockchain networking systems. Clarify the issues regarding mining difficulties which is adjustable depends upon the quantity of miners participating in the blockchain network. Genesis block of bitcoin was opened on 3rd January 2009, but as on 2nd December 2024 total number of bitcoin 19,790,325, which is already supplied in the universe, the remaining bitcoins will be circulate soon, It is anticipated that the main motivator for bitcoin miners would be transaction fees. Blocks can be Splitting Accidentally at the time of validation by the nodes of blockchain network and hackers may possible to split the block Intentionally to implement changes of the protocol, It causes the problem to getting the rewards of newly mined block. To transfer cryptocurrency from one wallet to another, the transaction must be register on the blockchain network along with the transaction fee by using public and private keys, but the registered transaction remains in a queue of unconfirmed until its validated by nodes, In this situation hackers may possible to hack the wallet.

KEYWORDS: **Block size, Block Rewards, Mempool, Difficulty Level, Fork, Layers.**

I. INTRODUCTION

Design and development of Bitcoin Cryptocurrency is implemented by using Blockchain technology by satoshi Nakamoto in 2009. A blockchain is a distributed, decentralized database with blocks that serve as storage units for data. To create a network chain, the blocks are appended to the preceding block, and each block needs to contain the prior block's hash address. At once the records are stored in blocks it cannot be altered or removed. **Bitcoin (BTC)** network block size is **1MB** its not sufficient space to store large number of transactions, so that miners are decided to increase the block size by upgrading their code to create a new blockchain as per their consensus mechanism **Bitcoin Cash (BCH)** cryptocurrency has been created with the block size to **8MB**, now it will be increased into **32MB [2].**

The Bitcoin blockchain network uses hashing to generate random hexadecimal numbers in an attempt to determine which one is closest to the network-set less than (or equal to) value. A new block is opened after the block solution has been located or verified. Once the network miners have verified, the winner is rewarded. Block time is the amount of time needed to solve the problem and produce a new block. Block construction takes an average of ten minutes, with around 144 blocks are mined daily, but now 900 blocks are mined daily. To limit the inflation, bitcoin creator designed only **21 million (2 crore and 10 lakhs)** Bitcoins released as specified by the ASCII Computer file [1]. The quantity of Bitcoins obtained upon successfully mining a new block is referred to as a block reward. Approximately every four years, or every 2,10,000 blocks, the incentive value is cut in half.

Each block reward in 2009 was valued at fifty bitcoins. The block reward was halved a third time, to 6.25 BTC, in May 2020. Around May 2140, the block reward is expected to drop to zero, but mining will no longer be profitable before then. In April 2039, approximately 99.6% of all bitcoins will have been issued, and the block reward will only be 0.19531250. Transaction fees are anticipated to eventually emerge as the main motivator for bitcoin miners.

II. LITERATURE REVIEW

The identity of Bitcoin's creator, Satoshi Nakamoto, is one of the cryptocurrency's most persistent mysteries. He is a person or group, and their identity is still not being proved.

In October 2008, Satoshi Nakamoto released a message to convey the creation of Bitcoin cryptocurrency within its white paper called **"Bitcoin: A Peer-to-Peer electronic cash system"[1].** He spent a few years working on the creation and development of cryptocurrencies as well as the advancement of blockchain technology in society. His final official statement regarding the Bitcoin convention was published in December 2010. Since April 2011, there have been unauthorized private messages. Because Satoshi Nakamoto hasn't been involved in the activities of design and development of bitcoin cryptocurrency since 2011, he or they

continue to be importance for blockchain Technology. Satoshi Nakamoto's wallets hold around **1 million** Bitcoin in **2011** but now the worth about **$67 billion** at current prices. But the creator's tokens haven't been moved in many years. In this situation mostly believe he is no more but digital world believes he is still alive. According to his 2012 Peer-to-Peer Foundation biography, Nakamoto stated that he was 37 years old, a resident of Japan, and that he was born on April 5, 1975.

In March 2014, Newsweek identified the bitcoin cryptocurrency creator as **Dorian Nakamoto** (July 1949). But Dorian Nakamoto continues to be declined that he is not a real Satoshi Nakamoto [5].

Wired Magazine claimed to have "**obtained the strongest evidence yet of Satoshi Nakamoto's true identity**" in a profile of **Craig Steven Wright** (October 1970) published in December 2015. According to Craig Steven Wright, a genuine Satoshi Nakamoto [6]. Vitalik Buterin, a co-founder of Ethereum, openly criticized Craig Steven Wright and called him a scammer. Since the blockchain's block records were backdated, there was evidence that Satoshi Nakamoto's public encryption keys were likewise backdated [7]. Judge James Mellor of the London High Court determined in March 2024 that Craig Steven Wright was not Satoshi Nakamoto [8].

In 2014, Dominic Frisby, the author of **Bitcoin: The Future of Money?,** proposed that Nick Szabo, born on April 5, 1964, was Satoshi Nakamoto [10]. After consulting with a specialist in stylometrics, Frisby came to the conclusion that Szabo's writing style was comparable to Satoshi's known works, both of which cited economist Carl Menger. Frisby also discovered that Szabo had been employed by DigiCash, an early effort to integrate encryption into digital payments.The first smart contract was developed by American computer scientist Nick Szabo in 1994, and it was envisioned as **"Bit gold"** a virtual currency, in 1998 [9]. But Nick Szabo denied Frisby thought.

In 2024 HBO documentary film **"Money Electric: The Bitcoin Mystery"** suggests **Peter Todd (**14 May 1985) is a Bitcoin creator by investigative filmmaker Cullen Hobak. But Peter Todd denied being Nakamoto and tweeted as **"exaggeration".**

Leung, a writer, wrote a thorough analysis on February 21, 2021, examining the likelihood that Len Sassaman (9 April 1980 – 3 July 2011) was Satoshi.

Throughout his life, Len Sassaman, one of the pioneers of cypherpunk, fought for privacy. He committed suicide on July 3, 2011, according to his wife, and **Black Hat Briefings** revealed that year that a memorial to Sassaman was incorporated into the Bitcoin network. Leung, the author who just released information that could link Satoshi and Sassaman, describes how the obituary is connected to the Bitcoin network.

The fact that Satoshi Nakamoto abandoned the Bitcoin project and the community two months prior to Sassaman's death serves as Leung's first piece of circumstantial evidence. Since May 11, 2020, when the well-known YouTube channel "**Barely Social**" released a video titled "**Unmasking Satoshi Nakamoto**," Adam Back has also been a suspect in the Satoshi Nakamoto enigma.

Sassaman joined the **Computer Security and Industrial Cryptography Research Group (COSIC)** as a researcher and Ph.D. candidate. Leung mentions that **David Chaum**, the "**father of digital currency**," served as Len's Ph.D. advisor at COSIC. Sassaman lived in Belgium when Bitcoin was being developed, which supports the theory that Satoshi was in Europe creating Bitcoin. According to recent research, Satoshi was developing the project in London.

"**He is considered as a strong Satoshi Nakamoto candidate**," reads the third sentence of Sassaman's Wikipedia biography. The Wikipedia editor's sentence is accompanied by a citation that points to Leung's research.

III. MINING PROCESS

Bitcoin Mining is hard, It's not necessarily hard to understand at a high level but it's hard to do. If you were attempt to mine a bitcoin, you must be toil away for years before discovering a block. Many blockchain networks employ Proof of Work (POW) as their consensus mechanism. It's a way of validating the transactions, adding new blocks into the blockchain and secure the network. The POW consensus mechanisms used in Bitcoin network with **Secure Hash Algorithm 256-bit**. This technique generates a fixed-sized output, known as the hash value, from an input, which is the transaction data. The network difficulty level sets a target value, and miners compete to find a hash value below that value. Because miners have to do a lot of calculations to find a hash value that satisfies the target requirements, this takes a lot of processing power [12]. A miner broadcasts the answer to the network and other nodes confirm it when they have solved the problem and found a hash value that satisfies the desired criteria. The miner receives a specific quantity of Bitcoin in exchange for a correct solution, and the block is appended to the Blockchain.

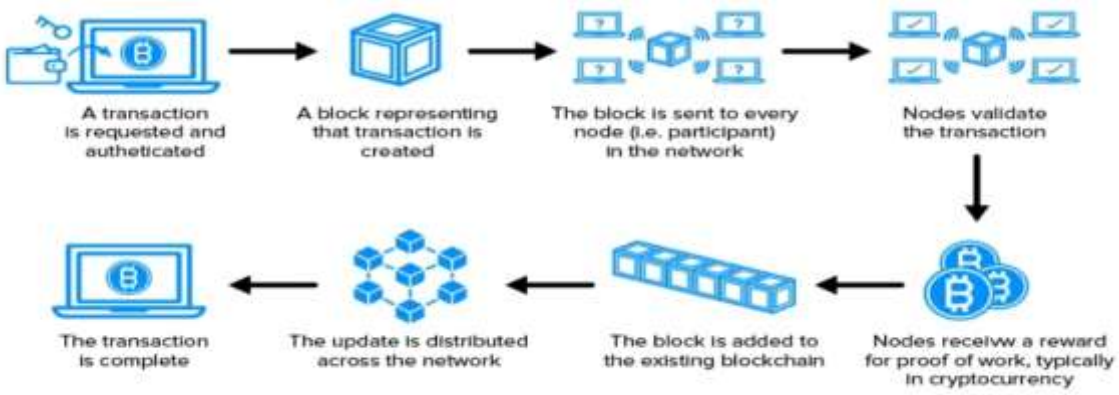

Figure 1: Process of Transaction added into Blockchain

Mining Difficulty

Finding a hash value that satisfies the desired criteria for adding a new block to the blockchain network is measured by mining difficulty. A high difficulty makes the network more resistant to attacks because it will require more processing power to mine the same number of blocks. Every 2016 blocks, or roughly every two weeks, the complexity is changed to maintain an average block time of ten minutes. The difficulty level will be raised if additional miners join the network in order to guarantee that the addition of new blocks occurs at a steady pace. Removing miners from the network lowers the difficulty level.

The profitability of the mining process is directly impacted by the degree of difficulty. Miners find it more difficult to locate new blocks and receive rewards as the difficulty level rises. This means that miners need more computing power to compete, which increases their costs. If the difficulty level decreases, mining becomes easier and more profitable. The difficulty level also affects the bitcoin owners in terms of the security of the network. As the difficulty level increases, it becomes more difficult for malicious actions to launch a 51% attack, which means that a single entity controls more than Half of the total mining power [13]. This is not possible it would require a significant amount of computational Power to successfully carry out such an attack. Mining difficulty is calculated by using a formula that takes into an account of the current block difficulty, the target block time is10 minutes and the total network hashing Power.

New difficulty = old difficulty * (2016 blocks/ time spent mining the previous 2016 blocks)

The time required to mine the most recent 2016 blocks is the average time required to mine each block during that time frame, and it is used to raise or lower the difficulty level.

The difficulty level is raised to make it more difficult to determine the hash value for new blocks if the average block time is less than ten minutes. The difficulty level is lowered to make it simpler to determine the hash value for the new blocks if the average block duration exceeds ten minutes. The difficulty level is only changed in accordance with the time required to mine the most recent 2016 blocks and the current difficulty level because the target block time of 10 minutes is constant.

The Mining difficulty formula has worked faithfully since it was first devised by Bitcoin creator Satoshi Nakamoto in 2009. To this day it remains a highly effective means of governing mining incentives. Regardless of total network Hash rate and the number of miners participate in mining, the difficulty formula keeps a Bitcoin is in the Goldilocks zone for mining such as **" Not too hard, Not too easy, but Just right".**

IV. CHAIN SPLITS

Another name for it is Forks. The technical phenomena known as a fork happens when a blockchain divides into two distinct branches. Up to the point of separation, the transaction histories of these two branches were shared. Following that, each branch operates autonomously under its own guidance. Forks in the blockchain can occur for a variety of reasons. There are two types of forks: **Accidental** and **Intentional**.

Accidental Fork

Thousands of miners compete to produce a new block at every moment. There is a lot of mining being performed at once in that scenario. An accidental fork occurs when two or more miners mine a new block simultaneously. The network abandons the shorter chain and keeps working on the longer one whenever new blocks are added. The blockchain network resolves unintentional forks [3].

Intentional Fork

The network precisely eliminates reconverge on an individual chain by partitioning the block. The blockchain developers employ this kind of fork to implement protocol modifications. An intentional fork can be used by developers to change the block consensus algorithm and increase block size. Intentional fork can be divided into Two categories.

i. **Hard Forks**
ii. **Soft Forks**

These Two categories different from each other in terms of Compatibility and their applications.

Hard Fork

It requires the network's nodes to update their software and introduces additional regulations. If you wish to extend the block size restriction so that it can contain up to 8MB of data, think about a blockchain with a 1MB block size limit. A new set of rules that raises the block size restriction from 1MB to 8MB must be put into place. It termed this approach "Hard Fork."

Users and miners in the community are forced to select a choice once a hard fork happens. They have the option of continuing to use the outdated software or updating their node and switching to the recently forked chain. In any case, they are the owners of cryptocurrency on both chains. They can claim the latest protocol's cryptocurrency on the newly created chain if they already have coins on the older chain. Any nodes that do not update to the revised consensus mechanism after a modification is implemented will be affected. As soon as the hard fork occurs, they are forced into a different chain. A blockchain that has been split by a hard fork that moves forward is inconsistent with the main chain since non-upgraded nodes are unable to execute the new consensus rules.

Soft Forks

Soft forks' modifications enable chains that move forward compatible. Blocks made with the new guidelines must also work with the old ones. Soft forks eliminate the need for node upgrades as a result. As transaction validators, they can continue to use the outdated software version while still taking part in the improved network. Users (**UASF, or User Activated Soft Fork**) or miners (**MASF, or Mine Activated Soft Fork**) can both activate soft forks.

V. BLOCKCHAIN LAYER ARCHITECTURE

Figure 2: Layers of Blockchain

Blockchain architecture can be divided into five layers, each of which serves a distinct function that is equally crucial for a decentralized network. Every blockchain layer fulfills a distinct function and enhances the network's overall security and functionality. Developers can build a more resilient and adaptable system that can change to meet evolving demands by dividing the technology into these discrete layers [11].

Infrastructure Layer: Another name for the infrastructure layer is the hardware layer. The blockchain network is supported by a number of hardware components found in the infrastructure layer. In a decentralized peer-to-peer (P2P) network, nodes are linked to one another and work together continuously to exchange transaction data. The hardware requirements for each blockchain vary based on the network's requirements. Because Bitcoin requires more processing power than other blockchains, its network will be more sophisticated and potent.

Data Layer: The data structure of block chain networks, which consists of blocks composed of Merkle trees that store transactions, is maintained and managed by the data layer. Each transaction in the block is secured by encryption and decryption techniques. A User can access the wallet in digitally signed transaction by using private key , and it is used to authorize a transaction, a public

key is used to verify who signed for the transaction. Digital signature is used to detect information manipulation. The identity of the sender is shielded by a digital signature.

Network Layer: Network layer establish a peer to peer connection between nodes and ensures that communication with other to synchronise the transactions and adding new blocks in the blockchain networks. it's also known as propagation layer.

Consensus Layer: Network participants create a defined set of rules known as consensus mechanism, which are effectively implemented to maintain network consistency. All Nodes must agree and ensures that transaction validation process to confirmation, adding only one block at a time in blockchain. It's a fundamental layer for creating decentralized networking between nodes.

Application Layer: Decentralized apps (DApps), chain codes, and smart contracts comprise the application layer. This layer partitioned into Application and Execution Layer. Application layer allows user can directly interact with the blockchain network with User Interface, Application Programming Interface. Application layer provide instructions to the execution layer to execute the smart contracts, consensus mechanism that ensures transaction validation.

VI. CATEGORIES OF LAYERS

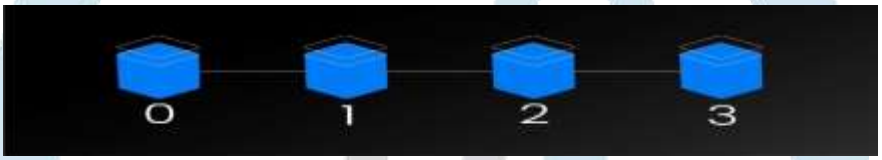

Figure 3: Categories of Layers

Each layer of the blockchain networks assuring the security, transparency, and efficiency of transactions. Different layers of blockchain works together to create a powerful and transformative technology that has potential revolution in various industries [4].

Layer 0: This layer is the fundamental layer which requires physical components to implement blockchain technology. Layer 0 provides the facility to interoperability between cross blockchain which allows to communicate and transfer the cryptocurrency tokens. The design and development of new tokens focus in the innovative features that supports customer needs.

Layer 1: Layer 1 blockchain networking system is also referred as Foundation layer or implementation layer. Every blockchain has a unique consensus mechanism to decide what information should be added into blocks and smart contracts are used to automatic execution when the prescribed conditions met between the parties, transactions are verified by the decentralized nodes in networks rather than centralized Authority. This Layer makes the functionality of the blockchain under the rule specified in the protocol.

Layer 2: Protocols of layer 2 to enhance scalability by eliminating certain interactions from the base layer 0 and Layer 1. Layer 2 blockchain is known as **scaling solution** because layer one creates the conditions, whereas layer two performs the actions. It is the most widely used method for resolving scale problems related to the Proof of Work consensus process. Although Layer 2 protocols are flexible in their capacity to increase transaction processing and total network throughput, they rely on the foundational Layer 1 blockchain for networking and security architecture. A state channel speeds up and increases the volume of transactions overall. For big transactions, a sidechain is an independent transactional chain that integrates with the blockchain.

The data transfer mechanism between side and main chains usually uses a utility token, and side chains have their own consensus algorithm that may be adjusted for scalability and speed. Layer 2 blockchain scaling alternatives include rollups, which involve doing transactions outside of the layer 1 network and transferring the generated data to the layer 2 blockchains.

Layer 3: It's also known as **Application Layer**. This layer is used to host dApps and other user-facing applications. DApps are software programs that offer a decentralized user experience and operate on a blockchain network. DApps are constructed on top of many blockchains, each of which has unique smart contract features and consensus mechanisms. The most widely used blockchain is Ethereum.

VII. CONCLUSION

Every 2016 blocks, the difficulty level of Bitcoin mining changes, requiring ten minutes to mine a block, nearly it will take 144 block creation on a day and its achieved completely within14 days but now Bitcoin miners mine 900 blocks on a day, so before involve in mining process, consider how many blocks created on a day and when the difficulty level is adjusted it will helpful for identifying the possibilities of finding the next difficulty level adjustment time. For a brief while, a parallel chain is created when two miners simultaneously create a block. The nodes on the networks agree on which versions of the blockchain is continued and which one is abandoned.

In that situation, a transaction is mined and validated by the abandoned block, the sender has to wait additional block confirmation in that blockchain. Because transactions on the Bitcoin blockchain are routed to a mempool and queued according to

the amount of transaction fees paid, transaction confirmation can take many hours. Every cryptocurrency exchange wallet has a limit on the number of confirmations it needs. Additionally, this figure varies depending on the particular blockchain network.

REFERENCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer electronic cash system”, 2008.
2. D. Konforty, Y. Adam, D.Estrada, and L.G Meredith, “Synereo: The decentralized and distributed social network”, 2015.
3. Atizhen, N.Z., & Svetinovic, D, “Security and Privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams”, IEEE Transactions on Dependable and Secure Computing, 2016.
4. Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A.hanif, Houbing Song and Yue Cao, “A survey on Blockchain Technology: Evolution, Architecture and Security” IEEE Access April 28,2021.
5. Newsweek. "The Face Behind Bitcoin", 2014.
6. Wired Magazine. "Is Bitcoin's Creator This Unknown Australian Genius? Probably Not (Updated)", 2015.
7. Vice. "Satoshi's PGP Keys Are Probably Backdated and Point To a Hoax." 2015.
8. Reuters. "Self-Proclaimed Bitcoin Inventor Is Not ‘Satoshi Nakamoto’, UK Judge Rules." 2024.
9. Nick Szabo. "Smart Contracts: Building Blocks for Digital Markets." 1998.
10. Dominic Frisby. "Bitcoin: The Future of Money?" Unbound Publishing, 2014.
11. A Beginner’s Guide to Understanding the Layers of Blockchain Technology, Blockchain Council, accessed on 13 December 2022.
12. J. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Indianapolis, IN, USA; Wiley, 2008
13. H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, ‘Blockchain challenges and opportunities: A survey,’’ Int. J. Web Grid Services, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS. 2018.10016848.