ISSN 2063-5346

ANALYSIS OF MINING DIFFICULTIES AS A SECURITY ATTRIBUTE IN BLOCKCHAIN TECHNOLOGY

Shruti Jain[1], Dr. Kanak Saxena[2], Sumeet Dhillon[3]

==

Article History: Received: 19.04.2023 Revised: 02.05.2023 Accepted: 10.06.2023

Abstract

Block-chain technology has the capability to revolutionize and enhance the global technological infrastructures connected to one another via Internet. The distributive nature of Block-chain technology makes it a suitable solution to improve the security challenges of device-to-device communication. Thus, it can create a database that is fully transparent and open to all, bringing transparency to all growing sectors. This achievement can be partially attributed to the secure reliability of Block-chain systems, which are largely dependent on the cryptographic advancements like hashing features and the digital signature. It also has concerns with the difficulty which controls the mining procedures and enables the devices to be updated as per the rising hashrates. This paper elaborates a comprehensive configuration and market analysis of Bitcoin's difficulty and its calculation to know how it reinforces the currency's security. Thus, it also proposes a system for emphasizing PoW and PoC Algorithm for enhancing Blockchains performance and efficiency.

Keywords: *Blockchain, Bitcoin, Mining Difficulty, Proof-of-Work, Proof-of-Contribution.*

[1,2,3] Department of Computer Science and Engineering, Samrat Ashok Technological Institute, Vidisha, India.

[1] shrutijain.3051998@gmail.com, [2] drkanak.cse@satiengg.in,

[3] sumeetdhillon.cse@satiengg.in

DOI: 10.48047/ecb/2023.12.si12.051

1. Introduction

Blockchain is a modernization to uphold the accuracy, secure data records and develop trust without the requirement of a trusted third party. A distributed repository as well as a ledger known as a Blockchain is accessible by every node present in a computer network. By creating a decentralized system, it removes the luxury of a central server and offers peer-to-peer interaction. As a database, Block-chain electronically stores information in digital form. The motivation of Block-chain is to store digital data which further gets distributed, but cannot be altered. Intrinsically, Block-chain is a foundation for recording data transactions or immutable ledgers those can't be modified/ changed, destroyed, nor deleted. Therefore, Block-chain is also referred to as Distributed Ledger Technology (DLT). Block-chain plays a key role in digital currency systems for example, Bitcoin, which are best known for maintaining a decentralized and secure record of transactions. Since, Bitcoin introduction in 2009, Bitcoin has evolved to become a part of the financial mainstream despite ongoing price swings. It is presently considered to be the most successful autonomous payment system and cryptocurrency in the modern era as compared to others.

Block-chain technology enables decentralized security and trust in numerous ways. Firstly, newer blocks are consistently cumulated linearly and chronologically. Thus, these are every time adjoined at the "end" of the Block-chain. Once a data block is appended at the end of Blockchain, it is extremely tough to return back and modify the data of these blocks until the majority of network agrees to do so. A mathematical function that transforms digital data into a set of strings combining letters and numbers produces a hash code. The hash value will get changed if the data is altered in any manner. So Block-chain is actually a reliable way to store data related to other sort of transactions.

The number of live Block-chains is increasing every day at an unprecedented rate. Today, as of 2023, there are over 10,000 other active Block-chain-based crypto-currency systems, plus hundreds of non-crypto Block-chains. Virtually tracking and trading anything of value on the Block-chain network, minimizing cost and reducing risk for everyone involved. Block-chain is not only used for financial transactions, as it continues to extend and become more user-friendly. It's secure and transparent nature allows this technology to meet interdisciplinary needs. Industries covering energy, education, logistics, and more are using Block-chain every day.

Blockchain technology and decentralized financing were made possible by Bitcoin. Bitcoin is defined as a Proof-of-Work system that necessitates the computing of a data set that defies logic and meets certain requirements [2]. Users must spend a lot of time and money on computations in order to generate such data, but users are rewarded for trying. The Proof-of-Work computation is done by generating random combination and is calculated through trial-and-error method. As a result, a user's ability to affect the network is not exclusively dependent on the quantity of network identities they possess. Hash Cash serves as the mining fundamental for Bitcoin and other PoW systems. The most popular PoW method, developed for the Bitcoin network, is SHA-256. Bitcoin mining is now a fiercely contested industry. Over $2 trillion has been invested in the Bitcoin system as a whole [3]. While bitcoin has a track record that investors should take into account that is 10 times longer compared to all other digital currencies combined. The most well-known among these cryptocurrencies is Bitcoin. With today's cutting-edge technologies and mining tools at one's disposal, mining, which refers to the process of synchronizing transactions in a computer network, can be profitable. The profit depends on the mining fee, which is rising with time, and the fluctuating value of the cryptocurrency.

Several researches claim that one of the most astounding cryptocurrencies to grow in 2023 will be bitcoin. The BTC price estimate for 2023 predicts a sharp climb in the second half of the year, perhaps attaining an average cost of $28,990.41, with a maximum potential range of $31,061.16 and a minimum potential range of $24848.93 [11]. This paper seeks to interpret the Bitcoin's mining difficulty by demonstrating its relation to the target, the value of the Bits, and how it enhances the security of the cryptocurrency. It offers some Python 3 scripts that can be employed to determine the mining difficulty and target as well as to validate the proof-of-work. Additionally, it proposes a system to maintain Block-chain security and employ PoC concept to emphasize blockchain performance and efficiency.

2. Block-Chain Architecture

In a Peer-2-Peer network, a block chain is a distributed and decentralized record of various types of transactions. It could be either private or public. Despite the fact that there are many devices in this network, the data cannot be altered without the consensus as a whole approving to it (each separate computer). The organizational structure of the block-chain technology is represented by a sequence of blocks comprising transactions in a determined directive. These records can be stored in a data file or a simple database (txt format). As mentioned in Figure 1, the fundamental elements of a blockledger are a node, a transaction, a block, a chain, miners, and a consensus process described in table 1.

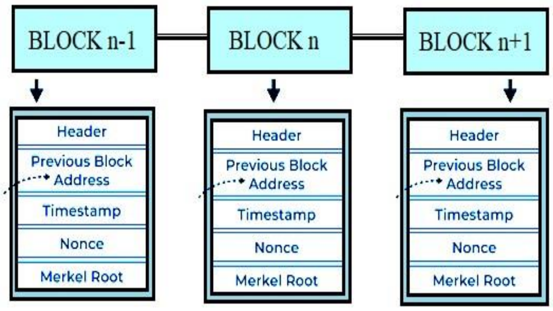


Figure 1: Blockchain Structure

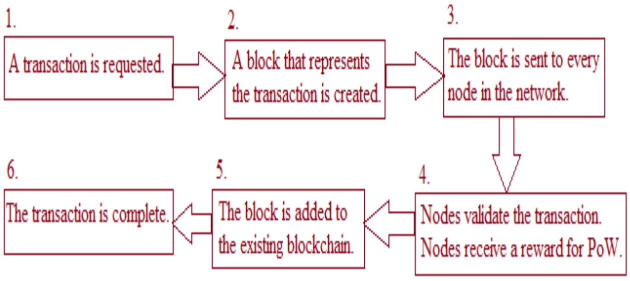

1.
A transaction is requested.
2.
A block that represents the transaction is created.
3.
The block is sent to every node in the network.
4.
Nodes validate the transaction. Nodes receive a reward for PoW.
5.
The block is added to the existing blockchain.
6.
The transaction is complete.

Figure 2: Blockchain Working

The process by which the distributed ledger is maintained among all nodes linked to a blockchain network is governed by a consensus mechanism. Participating nodes must all admit on these rules in order to continue adding data to the blockchain while protecting the integrity of the ledger. One well-known consensus protocol, identified as Proof-of-Work (or PoW), is the mechanism that adds new transactional blocks to a cryptocurrency's Block-chain [19]. Creating a hash (a lengthy string of characters) that corresponds to the required hash for the current block is the task under this scenario. The opportunity to do so allows the bitcoin miner to add that particular block as a reward to the blockchain. Every Blockchain block comprises of a specific amount of information, the block's hash, and the previous block hash. Each new transaction or record appended within the blockchain indicates the creation of a newer block. The legitimacy within each data records is then validated and signed digitally. The majority of the network's nodes should verify the newer block before it is joined to the network.

Table 1: Components of Blockchain

Blockchain Components	**Description and task done by each component of Block-chain**
NODE	A node within a Block-chain structure is termed as a user or machinery (all having an independent replica of the complete Block-chain chronicle).
BLOCK	Block is defined as data structure utilized for storing all accumulated transactions spread among network nodes.
CHAIN	A chain is a group of blocks sequenced in a particular arrangement.
TRANSACTION	A transaction is the smallest unit of a Block-chain structure (which contains records, information, etc.) and is what makes a Block-chain function.
CONSENSUS PROTOCOL	A set of guidelines and procedures to implement Block-chain is known as the consensus protocol.
MINERS	Miners are specialized nodes that verify blocks before introducing new information to the Block-chain system.

Figure 2 shows the process for requesting a transaction and adding a block to the blockchain network. The transactional record includes the digital signatures of all parties as well as a few other crucial elements of information. It is confirmed that the transaction is legitimate. This is a distributed process that happens among the different network nodes. Every block includes a hash value that encodes a code unique to each block. Although every block incorporates a hash of the preceding block as well as its own, users may frequently determine where a block ought to be in the blockchain. Once it has been successfully completed, the resultant block gets added to the ledger and may include several transactions. Its hash guarantees that information will be arranged in the proper chronological sequence.

Why Block-chain Matters: Businesses run on information. The outcomes are better the reception is quicker and more precise. Because it offers immediate, shareable, and transparent data that is compiled in an immutable ledger and can only be viewed by authorized network members, blockchain is perfect for disseminating information. Orders, accounts, payments, manufacturing, and more may all be tracked via blockchain networks. Additionally, members may witness every aspect of a transaction from beginning to end since they share a single version of the truth, which boosts trust while also creating new chances for efficiency.

3. Literature Review

The author in paper [1] offered a trustless electronic transactional system. Proceeding with the typical structure of digitally signed currencies provides adequate oversight of ownership but is limited in functionality since it lacks a mechanism to prohibit duplicate spending. To remedy this, the researcher developed a peer-to-peer network using proof-of-work to retain a public repository of transactions, considering trustworthy nodes holding the bulk of CPU power, which soon turns computationally challenging for an intruder to modify. The network is strong because it is unstructured and transparent. Nodes function when there is little simultaneous collaboration.

The paper [4] reviewed the principles and features like decentralization, non-modifiability, security, and stability, of Block-chain consensus mechanism. The consensus algorithms are vital part of Block-chain technology responsible for retaining Block-chain's efficiency and security. The author detailed the consensus algorithms namely PoW, D-PoS, PoS, and P-BFT also, explored the performance and applications of these consensus algorithms. According to author, the limitations to proof of work algorithm can be resource wastage, delay in verification of transaction and hard calculation of hashing power which can further be improved.

Since being first introduced in 2009, Bitcoins security has enticed the attention of several analysts from all over the globe. The Bitcoin system with chains of changing difficulty was proposed by 'AggelosKiayias, Juan Garay, and Nikos Leonardos' [5] as a means of thwarting any hostile attacker in control of a portion of miners possessing approximately 50% of the mining potentiality. The difficulty allows distinct blockchain instances to adjust their Proof-of-Work difficulty at varying rates with the aim to keep a consistent Block rate.

By design, Bitcoin is a safe cryptocurrency. The author in paper [10] suggested that modern cryptographic techniques like digital signatures and hashing are essential to its security. Since it controls the mining process, the Difficulty performs a significant part in ensuring Bitcoin's security. As a result, a newer block is often appended to the Blockchain in less than ten minutes. Additionally, its dynamic shift aids in preventing Block-chain takeover by miners with powerful computing equipment by keeping up with the rising hashing rate. Despite the advantages of difficulty, there is a significant problem that the Bitcoin organizations should address: the enormous energy used by Miners as they use their hashing equipment to overpower the difficulty.

The performance of the consensus algorithms of the Hyperledger Fabric and Ethereum in private Block-chain platforms is evaluated in the research paper [13]. The findings demonstrate that in terms of average delay and average throughput, the PBFT (Practical Byzantine Fault Tolerance) algorithm from Hyperledger surpasses the PoW method from Ethereum. Additionally, because security is typically exchanged for performance in consensus mechanisms, both Hyperledger Fabric and Ethereum experience performance limitations. The study [13] finding shows that when the numerous transactions rises, the performance gap between the two consensus algorithms widens. However, PBFT of Hyperledger Fabric regularly offers more throughput and lower latency. The research findings can aid Block-chain practitioners in fully comprehending the constraints imposed by Block-chain platforms and in making decisions regarding the best consensus mechanism.

The survey [14] defines Block-chain as a network of decentralized, distributed blocks used to record information secured using digital signatures. Transactions are very reliable and tamper-proof owing to the attributes of Block-chain, including decentralization, immutability, auditability, and transparency. Block-chain technology has applications outside of crypto-currencies, including risk management, financial, healthcare facilities, and social services. The paper [14] compares several consensus techniques namely PoW, PoS, DPoS, and PBFT, describes the categorization and structure of Block-chain, and covers complication such as scalability, privacy, energy consumption, interoperability, and regulatory issues.

Researchers and professionals in Block-chain sector have been paying close attention to the cutting-edge Block-chain technology recently [15]. Notably, the Bitcoin digital money is what makes Block-chain well-known. As of 2017, Block-chain has caused a 150-billion-dollar worldwide value disruption in several applications. The process by which all nodes in a Block-chain come to an agreement to acquire a new block is controlled by the consensus models. A crucial factor in maintaining Block-chain efficiency is the consensus model. The performance of Block-chain operations can be considerably improved by using the appropriate consensus model. Two groups of consensus models can be distinguished. The first category is the proof-based consensus model, where a Blockchain node must outperform other nodes by a sufficient amount to be the authority to link the next block to the chain. The voting-based strategy falls into the second group and requires nodes to share their findings in confirming a transaction of a new block before a decision is made. The properties of a few prominent consensus models are discussed in this study [15], along with some evaluations of how well they perform. Transaction throughput, network bandwidth, delay, and storage are the key topics of the reviews.

A distributed ledger of records known as blocks is a Block-chain. Cryptographic hash is used to connect these blocks. The primary layer of the Block-chain architecture is known as the consensus layer, where the consensus protocol is set up to control how new blocks are added to the Block-chain. The paper [16] offers theory and information that may be used to choose an appropriate consensus algorithm and aids scholars in their continued study of consensus in a private Blockchain context. Block-chain trust is resolved via the consensus algorithm. There are two categories in which consensus algorithms can be placed. Before adding a new transaction to the Block-chain, nodes in the first class of voting-based consensus must announce their findings from mining the new block or transaction. In order to prove that they are better qualified than the other nodes to perform the appending or mining activity, the nodes entering the Block-chain network must first solve a mathematical challenge. This is known as proof-based consensus. With the use of an appropriate consensus algorithm, Block-chain performance can be improved. However, there is minimum theory or data to support choosing a good consensus in a private Block-chain.

The three most well-known Block chain platforms, namely Bitcoin, Hyperledger fabric, and Ethereum, differ from one another in terms of permission, decentralization, and anonymity. Each platform also has its own implementation of a consensus process and a unique algorithm [17]. Computing complexity, fault tolerance, resiliency, durability, performance, and efficiency are different between them. In order to maximize strengths, minimize weaknesses, and increase effectiveness and performance, various consensus methods are paired with convergence and the application of a range of consensus algorithms.

Due to its unique characteristics, Bitcoin and Ethereum are the two most widely used Proof-of-Work (PoW)-based Block-chains. However, a Blockchains efficiency, user interface, and even security are significantly impacted by the BPT's unpredictability. The BPT's stability is controlled by mining difficulty. According to [18] first, the network hash rate cannot be tracked quickly enough by the difficulty control method. As a result, the BPT has a high variance and is unable to quickly approach to the targeted BPT (block produce time). The goal BPT can't be easily adjusted to a different value by changing the level of difficulty, which is the second issue. Thus, suggested a difficulty control approach based on a linear predictor to lessen these two issues. The prediction-based difficulty control algorithm provides considerably superior reliability and versatility of BPT using the correlation between the difficulty, hash rates, and BPT.

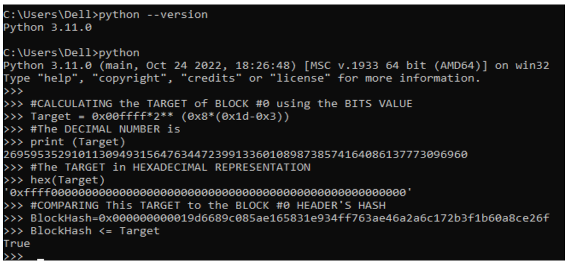
4. Bitcoin Blockchain

Bitcoin is referred as decentralized system, which means that no external or third entity is required to conduct transactions. All of the cooperating nodes are linked to the peer-to-peer Blockchain environment to attain and evaluate transactions. The blocks that include the validated and approved transactions are appended to the Blockchain. Since it makes use of several sophisticated cryptographic mechanisms, Bitcoin is regarded as a secure and trusted system [6]. For illustrate, the construction of Bitcoin addresses and keys is secure due to the one-way attribute of SHA-256 hashing algorithm, the randomness allowed to generate the private key, and the “Elliptic Curve Discrete” logarithmic, that can't be resolved with the extant computing power. The elliptic curve employed in Bitcoin is explicated by SECP256K1 Standards [4]. To fulfill the most important security goals, like confidentiality, integrity, and availability, security protocols were introduced to Bitcoins. These attributes include the Merkle tree that contributes to block integrity, the back linking of blocks, that enables to verify the consistency of the Blockchain, and the difficulty, that further guarantees system integrity by mandating miners to perform mining much harder for at a minimum of ten minutes to discover a ‘Proof-of-Work’ to gain newer mined blocks.

5. Bitcoin Mining Difficulty& Its Calculations

Mining produces bitcoins. The act of mining involves adding recently verified blocks to the blockchain in order to sustain it. The miners receive newly minted bitcoins and transaction fees in exchange for contributing their computational power to the network. High computer power miners are more likely to solve a block first, but as more blocks are solved, mining becomes increasingly challenging. According to the Bitcoin system, the incentive is divided in half every four years.

The difficulty is elaborated as a measurement of how challenging it is to locate a target's hash i.e. PoW. Every 2016 blocks, or roughly every two weeks, the Bitcoin network automatically sets this setting. The target and the Bits are two additional characteristics that are related to the difficulty [10]. The proof-of-work demonstrates that the miner put a lot of effort into locating the block's hash that meets all necessary criteria. The Proof-of-Work is difficult to locate but simple to validate. It entails determining a nonce value that produces a block's hash that is lesser than or equivalent to the difficulty target using the SHA-256 method (target). A field named "Bits," also referred to as "target Bits," is present in each block and consists of a four-byte value encoded in “hexadecimal floating-point” notation. The values of the bits are used to evaluate the difficulty target; those are needed for the mining algorithms.



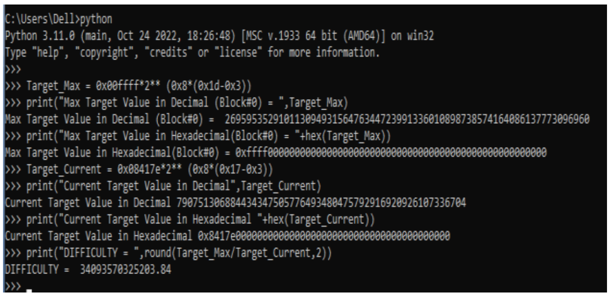
```
C:\Users\Dell>python --version
Python 3.11.0

C:\Users\Dell>python
Python 3.11.0 (main, Oct 24 2022, 18:26:48) [MSC v.1933 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> #CALCULATING the TARGET of BLOCK #0 using the BITS VALUE
>>> Target = 0x00ffff*2** (0x8*(0x1d-0x3))
>>> #The DECIMAL NUMBER is
>>> print (Target)
26959535291011309493156476344723991336010898738574164086137773096960
>>> #The TARGET in HEXADECIMAL REPRESENTATION
>>> hex(Target)
'0xffff0000000000000000000000000000000000000000000000000000'
>>> #COMPARING This TARGET to the BLOCK #0 HEADER'S HASH
>>> BlockHash=0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
>>> BlockHash <= Target
True
>>> _
```

Figure 3 Snapshot of Script for Comparing Block#0 Header Hash with calculated Target

1d00fff is the Bits field value of the Blockchain’s first block [8]. Conventionally, the target's total number of digits is represented by the starting 2 digits (1d) utilized as the exponent in the floating-point format. The remaining digits (00ffff) stand in for the coefficient. Now, to determine the target using Bits value, the formula preferred is: Target = Coefficient*2** (8*(Exponent-3)) explained in figure 3. The target condition determines how frequently newer proof-of-work are discovered. It also impacts how challenging a group of blocks will be. The target will change in accordance with the rapidly rising processing power where the Bitcoin mining network must maintain an average block creation time of 10 minutes. Each full node individually performs the dynamic retargeting for every 2016 block, when retargeting, Bitcoin's full nodes utilizes the following formula [9]: NewTarget = CurrentTarget*(Time on Minutes of Last 2016 Blocks)/20160 Minutes.

Employing, Python 3.11.0 for comparing the Block #0 hash target to the calculated target. The Block Hash is shown in the subsequent script (figure 4) to be less than or equal to the computed target, indicating the PoW to be legitimate.

The target difficulty is closely related with the targets and demonstrates how challenging it turns to discover a new block hash which attains the targeted criteria. A newer block is mined on an approximately average of every 10 minutes because its primary function is to supervise the mining procedure.



```
C:\Users\Dell>python
Python 3.11.0 (main, Oct 24 2022, 18:26:48) [MSC v.1933 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> Target_Max = 0x00ffff*2** (0x8*(0x1d-0x3))
>>> print("Max Target Value in Decimal (Block#0) = ",Target_Max)
Max Target Value in Decimal (Block#0) =  26959535291011309493156476344723991336010898738574164086137773096960
>>> print("Max Target Value in Hexadecimal(Block#0) = "+hex(Target_Max))
Max Target Value in Hexadecimal(Block#0) = 0xffff0000000000000000000000000000000000000000000000000000
>>> Target_Current = 0x08417e*2** (0x8*(0x17-0x3))
>>> print("Current Target Value in Decimal",Target_Current)
Current Target Value in Decimal 790751306884434347505776493480475792916920926107336704
>>> print("Current Target Value in Hexadecimal "+hex(Target_Current))
Current Target Value in Hexadecimal 0x8417e0000000000000000000000000000000000000000
>>> print("DIFFICULTY = ",round(Target_Max/Target_Current,2))
DIFFICULTY =  34093570325203.84
>>>
```

The formula [7] used to calculate the difficulty is given as: Difficulty = MaxTarget / CurrentTarget where Current Target denotes the latest block target (Block#770112) and MaxTarget denotes the target of initial (Genesis) block (Block#0).

Table 2: Block#770112 Details

Dificulty	34093570325203.84 - 34.09 TH
Bits	0x1708417e
Block Size(Bytes)	1,288,070 Bytes
Block Hash	00000000000000000000319ded5a8540f0c9e216427488927662ebee95c6a8d81
Block Height	770112
Merkle Root	91de2727b8b91ec7edd30cb503be43fca5e3429b13289fd094e438acdb79c8c5
Version	0x2809e000
Nonce	0x2619e45a
Next Block	770113

The outcomes of the script's execution are shown in Fig 4. The computed difficulty is consistent with the difficulty mentioned in the description of Block #770112 data [12]. (Refer table 2). The hashing rate and difficulty are closely related. Since the proof-of-work is rapidly produced as the hashing rate rises, the difficulty must also rise to maintain the average time for obtaining the proof-of-work at an average of 10 minutes. The complexity also lowers as the time required for proof-of-work discovery increases.

Table 3: Comparing Difficulty and Hashate of Blocks

Block Time and Date	Height	Bits	Difficulty	Mining Time	Average Hashrate
09:52:50 (2023-01-03)	770112	0x1708417e	34,093,570,325,203 - 34.09 T	09 min 04 s (+10.26 %)	243.66 EH/s
05:52:38 (2022-07-07)	743904	0x1709a7af	29,152,798,808,271 - 29.15 T	10 min 09 s (-1.41 %)	208.52 EH/s
13:15:37 (2022-01-08)	717696	0x170b8c8b	24,371,874,614,345 - 24.37 T	09 min 58 s (+0.41 %)	174.42 EH/s
12:04:06 (2021-07-03)	689472	0x171398ce	14,363,025,673,659 - 14.36 T	13 min 53 s (-27.94 %)	102.78 EH/s
20:54:37 (2021-01-09)	665280	0x170da8a1	20,607,418,304,385 - 20.61 T	09 min 02 s (+10.79 %)	147.46 EH/s

The significant relationship between hashing rate and difficulty [12] is mentioned in Table 3. Additionally, it demonstrates that the difficulty and hashrate have quadrupled over the previous years. Miscellaneous miners joining Btc network increases, thus security of these Bitcoin networks become stronger. The network's hashrate influences how difficult it is to attack the system. This is primarily a result of mining competitors. Any miner with significant hashing powers could control the Blockchain and alter it as they wanted without the difficulty. As a result, the difficulty has a significant contribution in securing the Bitcoin and its chain.

6. Market Analysis of Bitcoin Blockchain

The initiation of digital currencies took place at the end of the year 2008. Precisely Satoshi

Nakamoto was the first person to mine the initial block of Bitcoin Blockchain traditionally referred as Genesis Block, 50 BTC stepped into the marketplace at a cost of $0.00. Up to the initial halving occurrence in November 2012, 50 bitcoins per block produced about every ten minutes were in rotation. Fundamentally, it entails spontaneously reducing the quantity of newly created Bitcoin getting into the market for every 210,000 blocks, or roughly within every four years. The current Bitcoin reward for mining prevailing at present is 6.25 BTC.

Table 4 presents the data of BTC rewards and USD value on yearly basis.

Table 4: Yearly based Bitcoin Rewards & USD Value

	Dates & Year Duration	BTC Reward (Unit: Bitcoin)	USD Value (Unit: US Dollar)
1.	29 Dec 2008 – 26 Nov 2012	50.0 BTC	$0.00 - $440.21
2.	3 Dec 2012 – 4 July 2016	25.0 BTC	$328.89 - $15,344.89
3.	11 July 2016 – 11 May 2020	12.5 BTC	$8,275.52 - $115,321.48
4.	18 May 2020 – 3 July 2023	6.25 BTC	$58,947.63 – $192,929.34

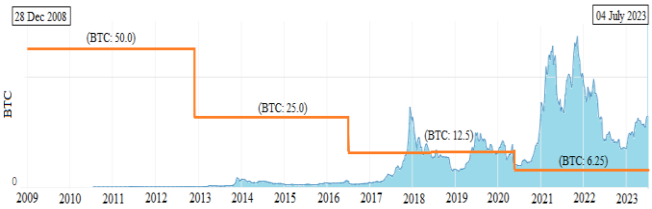


Figure 5: Bitcoin Market Value & Reward Halving from Year 2010 - 2023

According to "Coin Desks Digital Asset Classification Standard (DACS)", Bitcoin is categorized as a form of currency. The cost of bitcoin is notorious for having been extremely unpredictable, yet regardless of this, it has grown by an astounding 9,000,000% during the years 2010 to 2020 and has grown into the most successful currency of any type (such as equities, assets, and bonds) throughout the previous decade. The network is kept safe by the practice of compelling network participants to invest their energy resources and time in producing novel blocks. However, this security involves expenses.

As of the year 2023, the network of bitcoins will be consuming over 95.58 terawatt-hours (TWh) of electric power annually, which is roughly equivalent to the energy utilized by the 33th-largest nation across the globe. The graph in figure 5 depicts the entire history concerning Bitcoin's reward halves and its price increase as difficulty increases. The total market value of tokens is now $587,037,035,716.14 due to the recent fluctuations in the price of Bitcoin. Btc has changed by 83.58% to date 2023 or this year. The graph mentioned here in figure 6 shows the current history of price fluctuations in the Bitcoin market [20]. The total market value of tokens is now $587,037,035,716.14 due to the recent fluctuations in the price of Bitcoin. Btc has changed by 83.58% to date 2023 or this year. The graph mentioned here in figure 6 shows the current history of price fluctuations in the Bitcoin market [20].

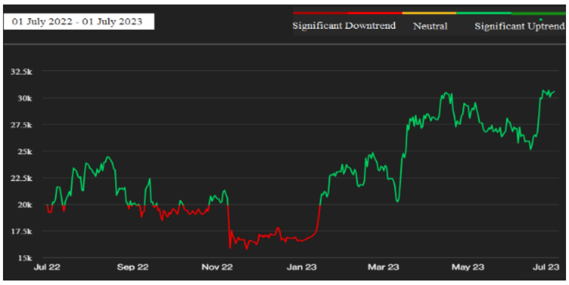


Figure 6: Graph Representing 2022-23 Record of Bitcoin Value Fluctuations

The difficulty of mining Bitcoin has increased as a result at block 797,707 the present Bitcoin difficulty is 50.65 T. The most recent Bitcoins difficulty target versus the difficulty target of Bitcoin periodically are plotted on the Bitcoin difficulty graph. Providing a historical information graph (shown in figure 7 and figure 8) that illustrates Bitcoin mining difficulty thus displays data showing Btc difficulty fluctuations and variations (that is, escalations and falls) for the period of 2010–2022[21] and during 6 months 2023 [22].

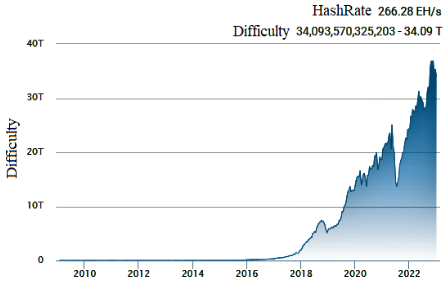


Figure 7: Increasing Difficulty Over Years 2010-2022

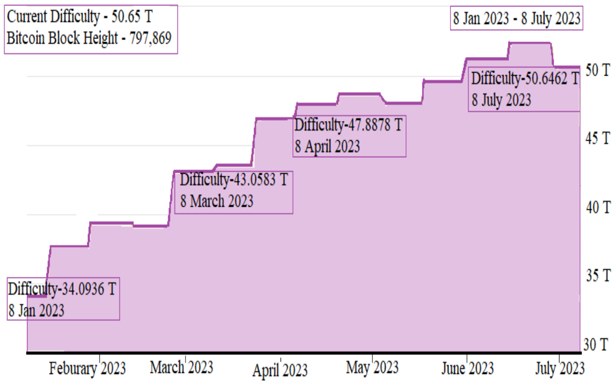


Figure 8: Increase in Difficulty from Jan 23-July 23

7. Proposed System

Bitcoin incorporates a Proof-of-Work consensus approach, which renders decentralization and an excellent secure network. In the PoW algorithm, a mathematical puzzle problem is provided to each miner, and then the participant who solves it earliest is going to upload that latest block within a blockchain thus earning rewards. The suggested structure demonstrates the way these classes interconnect and the manner in which each class component calls another class component in order to execute its function correctly.

Specifically, Blockchain, Block, Transaction, Wallet, Transaction-Pool, P2P Server, Chain, and Miners are the classes that constitute the system structure. The Class Blockchain basically constructs the chain of the latest blocks appended within the network ledger. In a blockchain, a block's architecture is developed using a Block Class. Both adding recently additional transactions and verifying the resultant transactions are done using transaction class. Moreover, it can be utilized in rewarding the miner for successfully mining blocks and upgrading the sender's account. A transaction is made with the help of the Wallet Class. The Transaction Pool maintains a record that includes all unmined transactions and determines if a transaction is legitimate or false. To establish several peers for the network which will serve as nodes for this decentralized ledger system, a peer-to-peer Server is necessary. This class pays attention to connections between peers, communicates the initial link across all associated sockets, synchronizes the local chains across every peer, broadcasts recently generated transactions to each node, and also transmits currently produced transactions to a pool of earlier produced transactions. Chain Class serves as a specialized class designed to create hashes of inputted data, key pairs (i.e. public plus private key), and distinctive transaction identifiers, to validate if the created signatures are accurate or inaccurate. Every transaction within a transaction pool is mined using the Miner Class, and the resulting block is subsequently uploaded to the distributed ledger. The complete interaction procedure is explained in figure 9.

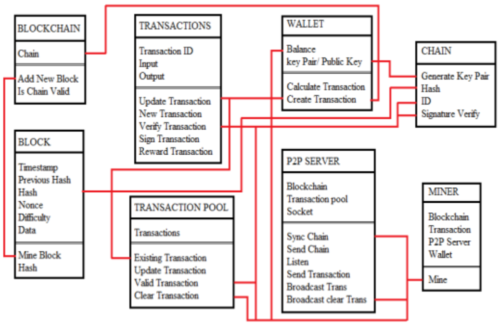


Figure 9: Blockchain Class Interaction Diagram

In case of data modification in any previous block, the miners use to work and create a new modified block since the block once added in the Blockchain can't be altered that is no changes in data because change in data will lead to hash change and give rise to further complexities. The modified block is further added to the network using PoW consensus and the majority of votes given by network nodes. Before this, it is important to know the urgency for modifying that block because this process is highly energy and resource consuming moreover too costly. Instead the new smaller Block-chain can be created linked to that particular block where the modifications needs to be done and in that smaller Block-chain the modified data blocks can be stored which are additionally secure , fast to access, and energy efficient. Based on the contribution of miners the priority to validate the blockchain should be given.

Suppose the block X of Blockchain needs to be modified for which a new smaller Block-chain is linked to block X containing modified data i.e. X'(shown in fig 10). This way the original Blockchain remains undisturbed. Now to validate the new Blockchain data the priority is given to the nodes with maximum contribution (depicted in fig 11). Assuming the network with limited miners where each miner joining the network at different difficulty level. Based on their overall contributed time, mining success rate and performance their total contribution (Ci) will be calculated (using formula 1& 2) and accordingly the miners and their votes will be prioritized.

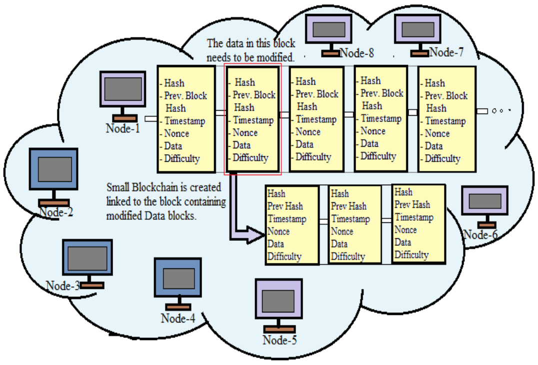


Figure 10: Block Data Modification by Linked a New Blockchain

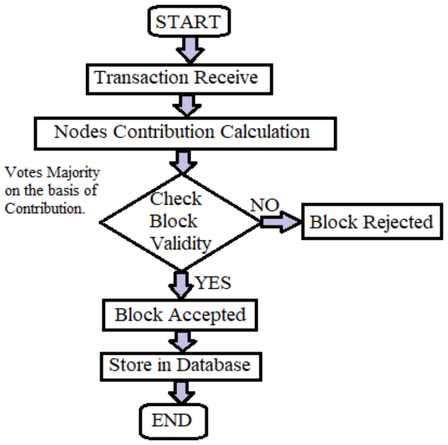


Figure 11: Flow Diagram to add Block using Contribution

SR stands for Success Rate that is total number of times the miner successfully added new block in the Block-chain Network (calculated in formula 1). Contribution (Ci) refers to the total number of times the miner participated in mining. The number of times miner couldn't successfully mine is referred to as unsuccessful attempts.

$$SR = \text{Ci (Contribution)} - \text{Unsuccessful Attempt}$$

Performance denoted by P is defined as the process of executing a task. The accuracy of performance is calculated as percentage result using SR and Ci as depicted in formula 2.

$$\text{Performance (\%)} = \frac{\text{Success Rate}}{\text{Contribution}}$$

Table 5: Contribution of Miners, their Success Rate & Performance

Users/Miner (U)	Contribution (Ci)	Unsuccessful Attempts	Success Rate (SR)	Performance (P)	Highest Contribution
U1	90	20	70	77.78%	C2
U2	100	80	20	20%	C5 (Lowest)
U3	110	60	50	54.54%	C3
U4	100	10	90	90%	C1 (Highest)
U5	85	55	30	37.5%	C4

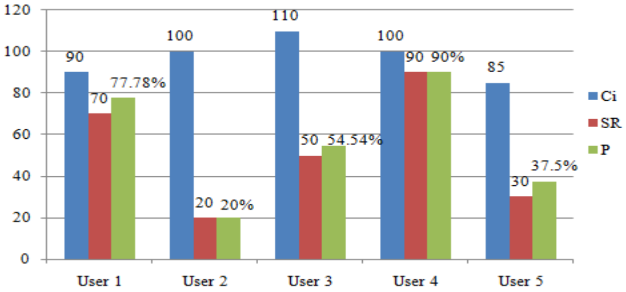


Figure 12: Graphical Data Results

The experimental data mentioned in table 5 is the complete record of experiment done to analyze the performance, success rate and contribution of miners. The graph depicted in figure 12 is the graph of record mentioned in table 5 showing the highest and least contribution of miner in the network. This graph will keep changing with the change in difficulty level, number of miners, and their contribution. With the increase in miner's success rate and performance their contribution will also increase which will result in change of their priority.

In accordance to all the above analysis and experiment done, the factors importantly performance, success rate, and efficiency are high in this proposed system as compared to PoW system (mentioned in table 6). The contribution of miners plays a crucial role in calculating and maintaining the competence of the mining. Whereas higher success rate will give rise to greater performance thus elevate the miner's contribution. This graph remains fluctuating with the up gradation and downfall in miner's success rate, performance and contribution.

Table 6: Factors Comparison on the Basis of Analysis

Factors-	Efficiency	Success Rate	Performance	Computation	Resource Usage	Cost
PoC	High	High	High	Less	Less	Low
PoW	Low	Low	Low	More	More	High

8. Conclusion & Future Work

The data structure of Block-chain technology has inherent security features because it is based on the principles of consensus, encryption and decentralization. Therefore, there is no reason for the error since its users can't modify transaction records. All above mentioned hypothesis indicates that Bitcoin is a robust and secure cryptocurrency by design. Modern cryptographic techniques like digital signatures and hashing are essential to its security. Since the Difficulty manages the mining procedure and ensures that novel data blocks are introduced to the Block-chain generally within 10 minutes, it performs a crucial role in securing the Bitcoins. Additionally, its continuous modification aids in preventing Blockchain takeover by miners with powerful computing power and by keeping up with the rising hashrate. Despite the numerous advantages of mining difficulty, there is a significant problem that the Bitcoin tech community should acknowledge and resolve: the enormous electricity used by Miners as they use their hashing devices to overcome the mining difficulty. The increase in difficulty level will lead to lessen the mining speed whereas if the difficulty level is low the mining speed will be elevated. Furthermore, the participants must uphold the Proof-of-Work principle while exploring the newer computational options and methods such as Proof-of-Stake/PoS or PBFT/Practical Byzantine Fault Tolerance algorithm those would make the hashing mechanism highly resourceful and energy-conscious with the hope to maintain Bitcoin security.

References

[1] Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf 4 (2008): 2.

[2] Mingxiao, Du, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. "A review on consensus algorithm of blockchain." In 2017 IEEE international conference on systems, man, and cybernetics (SMC), pp. 2567-2572, 2017.

[3] Coin market capitalization. https://coinmarketcap.com/currencies/bitcoin/

[4] Certicom Research. Standards for Efficient Cryptography. SEC 2: Recommended Elliptic Curve Domain Parameters. (n.d.). http://www.secg.org/sec2-v2.pdf.

[5] Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol with chains of variable difficulty. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017. Lecture Notes in Computer Science, vol. 10401. Springer, Cham (2017).

[6] Eyal, I., Gencer, A.E., Sirer, E.G., van Renesse, R.: Cornell University. Bitcoin-NG: A Scalable Blockchain Protocol. https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf.

[7] Bitcoin Difficulty. https://en.bitcoin.it/wiki/Difficulty.

[8] BlockExplorer.https://blockexplorer.com/block/00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

[9] Andreas, M.: Antonopoulos. Mastering Bitcoin: Programming the Open Blockchain, 2ndedn. (2017)

[10] Lamiri, Abdenaby, Kamal Gueraoui, and Gamal Zeggwagh. "Bitcoin difficulty, a security feature." In International Conference Europe Middle East & North Africa Information Systems and Technologies to Support Learning, pp. 367-372. Springer, Cham, 2018.

[11] Bitcoin difficulty. https://bitcoinwisdom.com/bitcoin/difficulty.

[12] Difficulty-BTC.com-https://btc.com/stats/diff.

[13] Hao, Yue, Yi Li, Xinghua Dong, Li Fang, and Ping Chen. "Performance analysis of consensus algorithm in private blockchain." In 2018 IEEE Intelligent Vehicles Symposium (IV), pp. 280-285. IEEE, 2018.

[14] Monrat, Ahmed Afif, OlovSchelén, and Karl Andersson. "A survey of blockchain from the perspectives of applications, challenges, and opportunities." IEEE Access 7 (2019): 117134-117151.

[15] Khan, Dodo, Low Tang Jung, Manzoor Ahmed Hashmani, and Ahmad Waqas. "A Critical Review of Blockchain Consensus Model." In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), pp. 1-6. IEEE, 2020.

[16] Pahlajani, Sunny, Avinash Kshirsagar, and Vinod Pachghare. "Survey on private blockchain consensus algorithms." In IEEE 1st International Conference on Innovations in Information and Communication Technology (ICIICT), 1-6.

[17] Zhu, Xingxiong. "Research on blockchain consensus mechanism and implementation." In IOP Conference Series: Materials Science and Engineering, vol. 569, no. 4, p. 042058. IOP Publishing, 2019.

[18] Zheng, Kaiwen, Shulai Zhang, and Xiaoli Ma. "Difficulty prediction for proof-of-work based blockchains." In 2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 1-5, 2020.

[19] Gupta C, Mahajan A. Evaluation of proof-of-work consensus algorithm for blockchain networks. In IEEE 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2020 Jul 1, 1-7.

[20] https://www.coindesk.com/price/bitcoin/

[21] https://btc.com/stats/diff

[22] https://www.coinwarz.com/mining/bitcoin/difficulty-chart