I. J. Mathematical Sciences and Computing, **2023, 3, 46-57**
Published Online on August 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2023.03.04

Blockchain: A Comparative Study of Consensus Algorithms PoW, PoS, PoA, PoV

Shahriar Fahim
American International University- Bangladesh, Department of Computer Science, Dhaka-1229, Bangladesh
Email: 18-37534-1@student.aiub.edu
ORCID iD: https://orcid.org/0009-0009-0395-7856

SM Katibur Rahman
American International University- Bangladesh, Department of Computer Science, Dhaka-1229, Bangladesh
Email: 18-36922-1@student.aiub.edu
ORCID iD: https://orcid.org/0009-0008-0467-1983

Sharfuddin Mahmood*
American International University- Bangladesh, Department of Computer Science, Dhaka-1229, Bangladesh
E-mail: smahmood@aiub.edu
ORCID iD: https://orcid.org/0009-0009-1733-5564
*Corresponding Author

Received: 10 April, 2023; Revised: 31 May, 2023; Accepted: 23 June, 2023; Published: 08 August, 2023

Abstract: Since the inception of Blockchain, the computer database has been evolving into innovative technologies. Recent technologies emerge, the use of Blockchain is also flourishing. All the technologies from Blockchain use a mutual algorithm to operate. The consensus algorithm is the process that assures mutual agreements and stores information in the decentralized database of the network. Blockchain's biggest drawback is the exposure to scalability. However, using the correct consensus for the relevant work can ensure efficiency in data storage, transaction finality, and data integrity. In this paper, a comparison study has been made among the following consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), and Proof of Vote (PoV). This study aims to provide readers with elementary knowledge about blockchain, more specifically its consensus protocols. It covers their origins, how they operate, and their strengths and weaknesses. We have made a significant study of these consensus protocols and uncovered some of their advantages and disadvantages in relation to characteristics details such as security, energy efficiency, scalability, and IoT (Internet of Things) compatibility. This information will assist future researchers to understand the characteristics of our selected consensus algorithms.

Index Terms: Blockchain; Consensus algorithms; Blockchain Scalability

1. Introduction

Blockchain is a distributed ledger system that is open to anyone with access to the internet. In simple words, a blockchain is a chain of blocks that are used to store data. Once data is recorded in a block, it is immutable. A cryptographic function called hash is used to identify individual blocks. Each block contains distinct kinds of data (Sender, account details, receiver) including that block's hash plus the previous block's hash. After a block is created, a unique hash is generated for that block. If any changes occur in a block, the latest information is stored with a new hash. This uniqueness is what makes blockchain very secure.

In the modern era, Blockchain is a significant and hyped topic concerning data safety. Blockchain uses P2P (Peer to Peer) network. Blockchain is a decentralized data structure that represents a ledger. Blockchain is important for several reasons:

Distributed: Blockchain is distributed and decentralized. Supposedly in a centralized bank if a hacker succeeds at attacking the bank's database system the entire system can be corrupted and all data stored will be compromised. Since blockchain is a distributed system and uses strong cryptography, it is less likely that the blocks will be compromised. But even if it is compromised, the other blocks within the network will remain unaffected.

Security and immutability: The blockchain system remains secure by rejecting tampered information. This means that data cannot be changed. Therefore, if data is updated, a new block will be created.

In business and governance systems, blockchain can be incredibly significant for transparency, accessibility, high flexibility of usage, Internet of Things (IoT) functions, and privacy. Blockchain is not just a trend in modern science and technology. There are numerous alternatives to blockchain technology such as Centralized Databases, Cloud Storage, Distributed Databases, Decentralized Storage, and other Distributed Ledger Technologies. Blockchain's decentralized database provides high-end security and encryption for data that is immutable and difficult to disintegrate for hackers.

A centralized Database may be able to perform much faster transactions than a blockchain but since it is centralized, the network has a good chance that the data will be destroyed if a system failure occurs [26]. Blockchain does not face such issues as a backup of the data is encrypted and stored on multiple nodes known as blocks. Cloud storage may be a debated alternative to Blockchain, but there are solemn issues with Cloud Storage, especially when choosing the right Cloud Storage provider, as not all providers can provide the best security. The Lack of strategic accession and highly experienced security professional creates a security risk that is problematic among the providers [27]. Malicious files in the storage can affect any existing data on the same storage. Cloud Storage is also vulnerable to Ransomware attacks that are on the edge of the world [28]. The decentralization of Blockchain makes it a less appealing target for ransomware. Distributed Database has no data redundancy and there is a high possibility of data theft since it is based on multiple computers under a single network [29]. Alongside these alternatives, Blockchain already has vast implementations all around the world and has gained significant value in the field.

The working principle of blockchain is followed by a sophisticated process. When a transaction is initiated in a blockchain network it is promptly broadcasted to a Peer-to-Peer (P2P) network. A P2P network consists of miners and participants also known as peers. Therefore, it is a decentralized network architecture, where the participants share and access the resources directly without any involvement of central authorities. The initiated transaction is verified by the Miners, who are the active participants within the Blockchain's secure transaction. After a successful verification, a new block is created. This block contains a record of confirmed transactions from the previous block. Miners play a crucial role in maintaining and securing the network through consensus where the transaction validity is decided upon by their mutual agreements. After the consensus is archived finally, the new block is added to the network and linked together in chronological order.

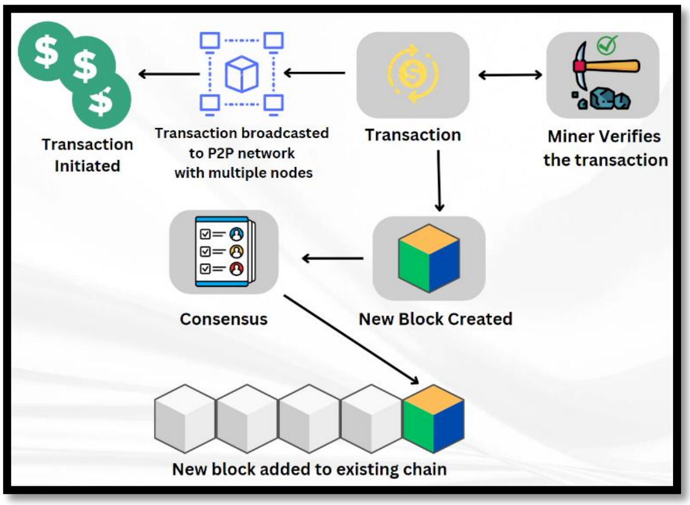
Transaction Initiated
Transaction broadcasted to P2P network with multiple nodes
Transaction
Miner Verifies the transaction
Consensus
New Block Created
New block added to existing chain

Fig. 1. Blockchain functional diagram [31]

The scalability issues in Blockchain may be a big problem that is constantly rising as more users join the network. However, using the correct consensus algorithms the scalability issues can be reduced to a sustainable level. Various consensus algorithms are known to exist such as Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-Of-Delegated-Participation (DPoS), Proof-Of-Activity (PoA), Proof-Of-Vote (PoV). Different consensus algorithms have various attributes that create a simple argument of which one is better in terms of what? Bitcoin, the most popular and leading cryptocurrency, first introduced the Proof-of-Work consensus algorithm [1,8]. It has its succession on both advantages and demerits like the other consensus algorithms. It is our objective to find out what they are. Being the most popular cryptocurrency in the world, bitcoin and its network have so much knowledge yet to be discovered. There are new consensus algorithms that are being developed every year. All the above factors significantly motivated us to work on this aspect of blockchain.

Since each Blockchain consensus has its limitations, there is no consensus that can be both energy-efficient and secure, provide the best scalability and support compatibility with an IoT network simultaneously. Although new consensus methods are proposed every year, there are no existing solutions for this problem. Therefore, from this paper researchers can decide on their plan of using a consensus algorithm according to their needs.

In this research study, our major objective will be on analyzing and determining utilized consensus algorithms in the realm of blockchain technology: Proof-of-Work (PoW), Proof-of-Activity (PoA), Proof-of-Stake (PoS), and Proof-of-Vote (PoV). Since no perfect consensus exists and each consensus has numerous advantages and drawbacks of its own. The intention will be to find the fitness of consensus algorithms in terms of Security, energy efficiency, scalability, and IoT (Internet of Things) Compatibility. Therefore, from this paper, researchers can gain knowledge on which consensus is suitable for a particular priority. For instance, if a researcher is concerned about an energy-efficient consensus, or a consensus that works best with IoT networks, this paper will give them a proper insight into which consensus might fit their criteria.

Proof-of-Work (PoW) is the best Blockchain Consensus. Compared to other consensus algorithms of blockchain, the security system of Proof-of-Work (PoW) is immensely high. Additionally, the implementation of Green- Proof-of-Work (PoW) can reduce energy consumption by 50% and improve the scalability system which is proven higher than any other blockchain consensus. However, it is disadvantageous in the framework of IoT (Internet of Things) Compatibility. Using PoW in an IoT Environment is ineffective due to its enormous power draw.

The authors strive to complete an in-depth comparison of four Blockchain consensus algorithms. They wish to aid the readers in deciding the trade-offs of the blockchain and making proper choices when choosing a consensus method for their own blockchain applications.

Chapter I of this research study contains the “Introduction” which exhibits the general knowledge about Blockchain and the motivation of this research study. In Chapter II, we present the “Description of Algorithms” where the details about the consensus are demonstrated. Chapter III consists of “Characteristics Details” that provides perspectives on Energy efficiency, Scalability, Security, and IoT Compatibility. In Chapter IV titled "Tables and Analysis," an examination of the findings is conducted. Subsequently, Chapter V: “Conclusion” will incorporate an analysis of the concluding part of this study.

2. Description of algorithms

A consensus algorithm is a mechanism that manages which participants in the network get to set the state of truth that everyone else follows and agrees on. In reference to how secure the agreement is, the algorithm applications include:

- Determining whether a database can execute a decentralized transaction.
- Designating a supervisor for A decentralized task.
- Coordinating and maintaining consistency amongst duplicates of automata.

Some of the popular consensus algorithms are Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Activity (PoA), Proof of Vote (PoV), Proof of ElapsedTime (PoET), Proof-of-Importance (PoI), Proof-of-Capacity (PoC), Proof-of-Burn (PoB). This paper will primarily focus on PoW, PoS, PoA, and PoV.

2.1 PoW

Proof of Work, in short PoW, was first developed in 1993 [1] to avoid denial-of-service assaults and misuse of other services. [20] The goal of a connection depletion attack is to overwhelm a server's resources and prevent it from responding to valid queries by submitting a significant amount of connection (or service) requests that are left unanswered. In the year 2009 [2,8], Bitcoin pioneered a revolutionary use of proof-of-work as a consensus mechanism, broadcasting new blocks to the blockchain and validating transactions. It then attracted attention and is now a frequent consensus algorithm in several cryptocurrencies. Bitcoin is a blockchain-based architecture that is supported by decentralized nodes working together. The miners among all these nodes oversee bringing additional blocks to the blockchain. Miners must attempt to guess a fictitious random number to accomplish this. The above number must generate a result that meets the requirements when concatenated with the block's data and runs through a hashing algorithm. When a relationship has been established, some other nodes will validate the effectiveness of the detection, and the mining node will receive a new block incentive. As a result, finding a valid nonce [nonce is a random 32-bit number that miners use as a base for their hash calculations] is a prerequisite for adding a block to the main chain. [3,8] This nonce provides the solutions to a particular block known as BLOCK-HASH. [9] It is named proof-of-work because each authenticated block contains a block hash that symbolizes the miner's labor. Proof-of-work helps defend the network against a variety of intrusions. [21] One problem with proof-of-work is that it necessitates expensive computer machinery that uses a lot of power, and while complex algorithm computations ensure network security, they cannot be used for anything else. Even though proof-of-work would not be the most effective approach, it is nevertheless one of the most widely used techniques for achieving consensus in blockchains. Alternative approaches and methodologies are being used to address the issues. However, time will only tell which solution will replace the proof-of-work strategy.

2.2 PoA

Proof of authority is an algorithm that provides an effective answer for blockchains, particularly private ones. [22] Gavin Wood is a co-founder of the Ethereum blockchain, and first used the word in 2017. In proof-of-authority, machines must pass a rigorous vetting procedure before they are allowed to create new blocks. Only trustworthy validation machines protect Poa blockchains. These system moderators are preapproved participants who check blocks and transactions. Transactions are grouped into blocks by preapproved validators using the software. Since the procedure is automated, the validators do not need to keep an eye on their computers all the time. The identity of a validator needs to be explicitly verified on the network with the capacity to cross-reference the data available in the public domain. The essence of the reputation mechanism is trust in the validator's identity. Making ensuring weak candidates are eliminated requires a complicated process. People with PoA have the motivation to hold onto the position they have attained since they must earn the privilege to be validators. By giving identities a reputation, validators are encouraged to defend the transaction process since they do not want their identities to be associated with a bad reputation. PoA consensus algorithm is less decentralized in comparison to other algorithms. The mechanism automatically filters out the non-active or non-committed validators, low energy consumption, and restricted number of actors. In Proof-of-Authority there is no technical rivalry between validators, unlike the Proof-of-Work system, occasionally known as mining. The operation of this consensus process takes almost no computational power, and consequently almost no electricity. The main advantage of the PoA consensus is that more transactions can be executed simultaneously [13]. An additional positive factor of the blockchain algorithm is that in PoA lesser computational resources are needed [11]. PoA consumes less time and energy compared to PoW and PoS. PoA guarantees defense against 51% of network attacks [10]. Therefore, PoA can be a significant initiative for private blockchain networks.

2.3 PoS

The Proof-of-stake method was first proposed in 2011 by an unknown user by the username Quantummechanic on the bitcointalk site [30]. The fundamental idea is that it serves no use to allow people to compete with one another in mining. Therefore, Proof-of-Stake employs an election procedure in which one node is selected at random to validate the following block. However, there is a subtle change in terminology: Proof-of-Stake uses "validators" instead of miners, [1,36] and new blocks are "minted" or "forged" rather than mined. The selection of validators is not entirely random. A node must stake a particular amount of coins into the network to become a validator. One may consider this to be a security deposit. The stake size determines the likelihood that a validator will be selected to forge the next block.

Rich individuals can benefit from the strength of economies of scale with PoW. The cost of their electricity and mining equipment does not increase linearly; rather, the more they purchase, the better pricing they can obtain. But returning to PoS, if a validator is selected to forge the following block, he will determine whether all of the transactions included therein are, in fact, valid. The costs connected with each transaction in this block go back to the validator as a reward.If they nonetheless allow fraudulent transactions, validators will lose a portion of their investment [2,36]. A validator can be relied on to perform their duties effectively as long as the stakes are higher than what they stand to gain from transaction fees. Otherwise, they will lose incentives instead of making it. It functions as a financial motivator and endures so long as the stake exceeds the total of all transaction fees. After a predetermined amount of time, if one node ceases to be a validator, his stake as well as all transaction fees received will be removed.

Since Proof-of-Stake prevents everyone from mining for new blocks, it consumes far less energy [1,14]. Moreover, it is more decentralized. "Mining pools" are a prospect that exists within the proof-of-work protocol. The pool refers to the individuals that are working together to raise their chances of mining a new block and thus obtaining rewards. However, these pools now have control over a sizable piece of the Bitcoin blockchain. They concentrate on the mining process, which is risky. The network would have had a majority share and could have started authorizing fake transactions if the three largest mining pools had united. PoS encourages more users to set up a node because no expensive mining equipment is required, which increases the network's decentralization and security. But even PoS has several drawbacks and is far from being a flawless mechanism.Anyone who purchases the majority of the network's shares will be able to effectively rule it and sanction fraudulent transactions. The 51% attacks, as it is known, were initially cited as a flaw in the Proof-of-Work method. If a single miner or group of miners can gather 51% of the hash power, they can effectively take over the Blockchain. On the other hand, Proof-of-Stake makes this approach exceedingly impractical because it depends on the value of a coin. If bitcoin were changed to PoS, it would cost an astounding amount of money to own 51% of all coins. Therefore, Proof-of-Stake reduces the likelihood of a 51% attack.

The process through which PoS mechanisms choose the subsequent validators must be heedful. Since the stake size must be taken into account, it cannot be chosen at random. However, the stake alone is insufficient because it will favor wealthy individuals, who will be selected more frequently, receive more incentives and become wealthier, increasing their chances of being selected as validators even further. There are several solutions to the coin age selection problem. Another potential issue is when the network selects the following validator but he fails to show up to perform his duties. By selecting a large number of backup validators as a fallback, this might be readily resolved. When compared to PoW, Proof-of-Stake entails more hazards, and much research is required to comprehend these dangers and mitigate them.Peercoin, Lisk, and Nxt are a few examples of coins that use Proof-of-Stake, but more are expected to follow in the future. For instance, the "Casper" Proof-of-Stake system is being implemented. Casper is a consensus mechanism in which the PoW/PoS collaborate [3,36]. It is actively being developed and is now available on the Ethereum test net. Additionally, the Ouroboros Proof-of-Stake is being developed to preserve the fair leader election process that guarantees the security of the protocol [37].

2.4 PoV

Proof of Vote (PoV) is a proposed consensus model based on the features of consortium blockchain. It has been proposed in 2017 by Kejiao, L, Hui, L. Hanxu, H. Kedan, L. and Yongle Chen in their research paper: “Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain.” The proposed PoV model works on the general idea of voting. A valid block that is final and unique will be generated through the voting method, and the result is a high throughput of the system and confirmation time. The four roles in the network model, Commissioner, Butler, Butler candidate, and Ordinary users are responsible for recording specific business transactions and operations [1,5]. The Commissioner reserves the right to vote, assess, recommend the butlers, and verify each transaction [2,5]. Commissioners can also recommend themselves to become butler candidates. The Butler team is selected to create blocks. Every block they create is submitted for voting and validation. Butler can be considered a miner. However, Butlers are not bound to waste computing power to produce blocks. A Butler is randomly selected to produce a block. Butler’s candidate becomes butler after being voted by the commissioner. Candidates can wait in queue for the next election if they lose the current election. To become a butler, a butler candidate is required to register a user account in the system and submit a relevant application. Candidates also require a recommendation letter from the commissioner using secret key encryption. Candidates need to submit the deposit to become a butler. Ordinary user consists of arbitrary behavior as they join or exit the network anytime without needing authorization. Ordinary users can join the process of block generation only with proper authorization. Without authorization, they can only take part in the distribution and message forwarding. While doing so, they can view the whole consensus process. The system can handle less than 50% of key nodes being attacked. The Generation of an Ordinary Valid Block and a special valid block in this model consists of separate steps (S). The model proves that Blockchains will never bifurcate [3,5]. Therefore, PoV can guarantee a secure, efficient, and never bifurcating blockchain network.

3. Characteristics Details

3.1 Security

The cryptography of blockchain is known to be a strong factor for this decentralized system. It is maintained by multiple network participants responsible for securing the data. Blockchain was predominantly designed to be immutable. But since several types of blockchain contain varied implications for participation privileges and data access, blockchain’s security is exceedingly subject to the type of blockchain that is being used. There are two conjugations of blockchain: (1) public and (2) private. Any user can join the public blockchain, which maintains the participant’s anonymity. Contrarily, only well-known organizations are permitted to participate in a private blockchain, therefore membership and access rights depend on identity. Blockchain certainly appears secure with its cryptographic security as well as the guarantee that no one may change data without the consent of the other participants, and blockchain can provide a tamper-proof account of interactions. However, this does not imply that blockchain is immune to security risks and online threats. Moreover, contemporary trends and security measures in blockchain technology can be advanced by technological developments like AI-based solutions for infrastructures, transactions, and code analysis.

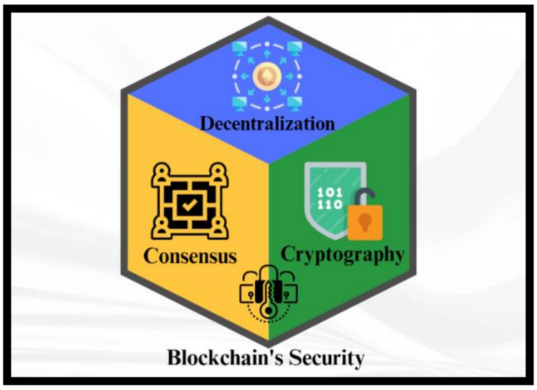

Fig. 2. Security Principles of Blockchain Technology

3.2 Energy Efficiency

The word blockchain has become synonymous with inefficiency and excessive energy use in recent years. These assertions frequently focus on only one technological element, the consensus method. The energy use of blockchains is influenced by several factors. They can be separated into three primary categories: (1) the energy used by idle nodes, (2) redundant processing and storage required by blockchain processes, (3) consumption resulting from consensus methods. Due to the nature of permissionless blockchains, some factors such as the number of miners and their hardware requirements are necessary for precisely calculating the energy consumption. Private blockchains are the most energy-efficient initiative. Here is an Energy consumption chart of different blockchains:

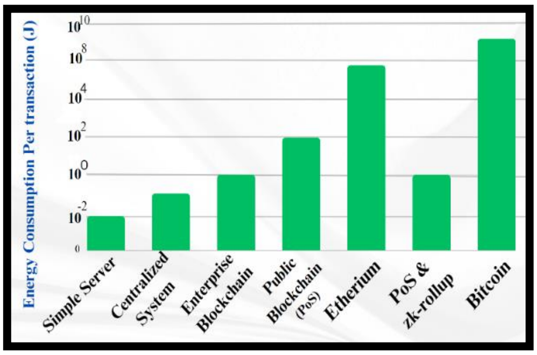

Fig. 3. Energy consumption chart [34]

The underlying technology that is utilized to reach consensus between the network's nodes has an important effect on the energy efficiency sector of blockchain systems. Current Proof-of-Work blockchains, including Bitcoin and Ethereum, are characterized by excessive energy consumption. Several use case applications have already been created employing blockchain technology in the transition to a new energy world that is decentralized, digital, and decarbonized, including automated bill payments, electric vehicle charging and sharing, and renewable cryptocurrencies [12]. Blockchain technology may one day enable millions of energy-related devices, including solar PV systems, electric vehicles, batteries, and water heaters, to interact with one another at the electric power distribution edge. By enabling quicker and more economical product delivery, strengthening product traceability, enhancing partner coordination, and facilitating access to funding, blockchain can significantly enhance supply chains.

3.3 Scalability

Scalability in simple terms is defined as the ability to process transactions. Blockchain systems position themselves as decentralized, secure, and scalable.[23] The fundamental challenge when it comes to scaling blockchain projects is rooted in a concept called scalability trilemma. This concept is connected to the project management triangle. The ideology is that every product or service can be characterized by only two of the below three characteristics. One is “fast,” the other one is “cheap” and the final one is “good.” A product can be delivered quickly and can be cheap, however, it will not be dignified as good. On the other hand, the product can be good and fast but not cheap. The scalability trilemma uses identical logic. Blockchain needs to be decentralized, secure, and fast. Unfortunately, it can contain only two peculiarities at a time. This term was originally coined by Vitalik Buterin and the Ethereum team is conscious of the problem and is working to illustrate it.

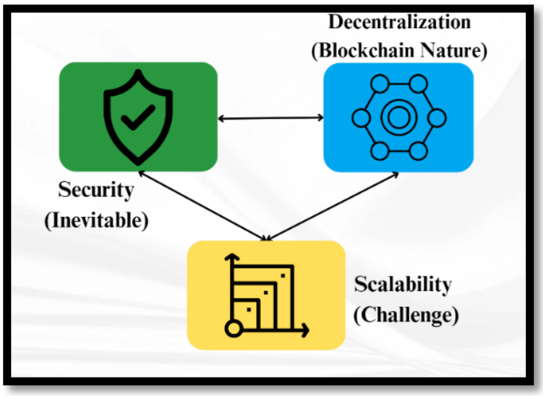

Fig. 4. Scalability Trilemma [33]

The first cryptocurrencies relied on decentralization while security and scalability became the least concern. But as the network grew, limitations began to emerge. Numerous new blockchains already immolate decentralization or even security to improve scalability. However, it is unlikely that such projects lack decentralization or security rather it is defined as a priority for the development of the blockchain system. Crypto traders' investors and ordinary users are increasingly switching to new generation blockchains. This is due to the propagated demand for transactions. In conclusion, it can be said that if a significant increase is noticed in the demand for transactions, a tremendous number of developers and users will promptly switch to the new generation networks initially supporting high bandwidth.

3.4 IoT Compatibility

Blockchain's decentralized security and accountability provide abundant advantages and integrating it with an IoT system can be immensely beneficial. However, An IoT network requires multiple devices that are consistent with restricted computational capacities. Such restrictions can be challenging when integrating with blockchain technology. Blockchain uses consensus protocols that have the potential to be modified accordingly based on the constraints of different IoT networks. Choosing the right consensus for a suitable IoT network can be difficult. The most common consensus algorithms can be inefficient for an IoT network [1,18]. It is known that Proof of Work (PoW) requires high computational power, so it is irrelevant to integrate this consensus with an IoT network. Proof of Stake (PoS) can solve the high computational problem of Proof of Work (PoW) since it solves a block chosen by lottery and uses a digital signature for verifying the ownership. However, it creates unfamiliar problems that make the system centralized. Proof of vote is a new consensus and has not been used yet in an IoT environment so its dependability in an IoT network is unknown. Honesty-based Distributed Proof of Authority also known as HDPoA (Honesty based Distributed Proof of Authority) is a new consensus model established from Proof of work (PoW) and Proof of Authority (PoA) [1,19]. HDPoA consumes low power and is utilized in low-cost devices since it requires only one block to assure transaction finality. Using HDPoA can increase the battery efficiency of IoT devices [2,19]. HDPoA can prevent attacks such as DDoS and Spam signer attacks on the blockchain [3,19]. So far, the implementation of HDPoA has been able only in small IoT networks but in the future deployment on a large IoT system will be possible. For public blockchain frameworks, Ethereum on the other hand is quite effective. It requires less power than the original PoW. Using Ethereum's smart contracts, this intrinsic blockchain can be modified according to the requirements of an IoT network. Furthermore, it has been proven successful [1,35]. However, there were limitations regarding performance and storage that could assert quite an expenditure to solve [2.35].

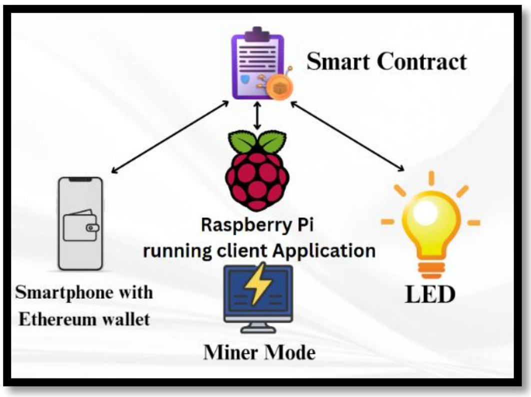

Fig. 5. An IoT Network connected using Ethereum

Alternatively, Private blockchain can be a better substitute for public blockchain [2,18]. A private blockchain is dependent on permission from a third party, making it centralized to an extent. Moreover, its faster response time and lower power consumption make it more appropriate for IoT applications.

4. Research Design and Analysis

The chosen research design for this study involves performing a comprehensive literature review and comparative analysis of existing consensus algorithms in Blockchain technology. The literature review contains an extensive search and review of 37 academic papers from reputable resources that provide insights into the consensus methods. Specific metrics and measures related to the identified characteristics are extracted for each consensus algorithm. These metrics include factors such as the security mechanisms employed, energy consumption patterns, scalability performance under varying transaction loads, and compatibility with IoT devices. The data collected are qualitative techniques and involve the comparison of statistical models, analysis of performance metrics, and textual data from the literature to identify themes and patterns related to the strengths and weaknesses of each algorithm. No numerical or mathematical computations were needed. This helped ensure the focus on our descriptive communication style and focus on conceptual understanding. The Analysis Table (Table. 1) illustrates an organized collection of data and a proper comparison between the consensus in relation to the included characteristics details. The table also explores various properties related to blockchain technology and decentralized systems. These include HashCash, Green PoW, a centralized reputation-based approach, Byzantine fault tolerance, dedicated testbeds, DPoS authorization, Sharding, and the Internet of Vehicles (IoV). Brief details about these properties have also been carried out in the analysis section to provide a concise insight. The consensus algorithms chosen for research in this paper can play a substantial role in public, private and consortium Blockchains which is the primary reason they were specifically selected for the study. Secondarily, they were chosen to maintain a uniqueness for the comparison. The accuracy of the data is assured strictly by selecting the most reliable scholarly books and publications only. This research involves no unethical conduct or misuse of any of the sources. The paper demonstrated a tenacious devotion to avoiding plagiarism. The limitations of this research are addressed in the conclusion part of this paper.

Table 1. Consensus comparison table in terms of characteristics details

Name	Security	Energy Efficiency	Scalability	IoT compatibility
PoW	Very High in HashCash and micro mint method but fairly high in data handling [2].	Very low. But by implementing Green-PoW, Energy Consumption can be reduced by 50% [1,2].	Low. The proposed parallel PoW model can increase scalability [9].	Very low. Proposed Miner Twins can enable fair PoW consensus in the IoT environment [4,8].
PoA	High. PoA is safer than PoS [1,17]. The byzantine fault tolerance model of PoA is better than the non-distributed protocols of a typical centralized system [2,17].	Higher than PoW. More efficiency and throughput than PoS due to its centralized reputation-based approach [16].	Higher than PoW but the base model is centralized since transactions are validated by an approved system [3,17].	HDPoA is a better alternative than classic PoA because it was validated through real-world implementation using a dedicated testbed utilizing diverse types of low-cost and low-power IoT devices with varying capabilities [3].
PoS	Higher than PoW in terms of double spending attack. Lower than PoW in terms of preventing pool mining [2,14].	Much higher than PoW since it does not employ any puzzles [14]. DPoS authorization can further cut resource consumption and increase consensus effectiveness [15].	High. Transaction processing rate increases using the sharding strategy [6].	Better than PoW. Offers a higher transaction speed and needs fewer processing resources in the IoV (Internet of Vehicles) network [7].
PoV	Lower than PoW but within the satisfactory level.	Higher than PoW as the butler is randomly selected and does not waste computing power like miners in PoW.	Medium. Creates blocks much faster than PoW while maintaining sustainable security.	Not yet been used in any IoT environment but holds potential for future research.

i. Properties Analysis

a) **HashCash Method:** HashCash is a proof-of-work method that has lately gained popularity for the use of Bitcoin (as well as another cryptocurrency) as part of something like the mining process. It was originally developed to prevent email spamming and denial-of-service threats Byzantine

b) **Double Spending attack:** This kind of attack is a big drawback of PoW proposed by many researchers. In a Double spending attack, The attacker makes a reverse transaction of verified nodes. By making another transaction that makes the first one look invalid thus making the attacker's transaction last longer. To perform this the attacker needs at least 51% computing power of the entire verifying network.

c) **Pool Mining:** It is a common approach widely used in many Blockchain networks. This approach is derived from the practices of miners to create blocks in a group and pool their resources. Miners do not try to guess the nonce value instead they collectively vote for a pool operator to find the nonce together.

d) **Green PoW:** Green PoW is just a power consensus mechanism that, compared to the PoW algorithm used for the original Bitcoin, minimizes compute load by almost 50% while maintaining all the other system characteristics [1,3]. The algorithm splits time into epochs, with each epoch made up of two mining rounds that follow one another.

e) **Centralized Reputation-based Approach:** Internet corporations have largely used centralized online reputation systems to aid consumers in developing trust, lowering information asymmetry, and filtering information. Reputation systems are broken down into five fundamental parts by the model: input, processing, output, feedback loop, and storage.

f) **Byzantine Fault Tolerance Feature:** A distributed network's ability to reach consensus (agreement on the same value) even though some nodes fail to react or provide inaccurate information is known as Byzantine fault tolerance (BFT).

g) **Dedicated Testbed:** A testbed is a setting for rigorous, open-ended, and repeatable testing of scientific concepts, computer programs, and emerging technologies. The phrase is used in a variety of academic fields to refer to venues and platforms for experimental research and new product creation.

h) **DPoS Authorization:** A voting system based on PoS is introduced, and the time required to generate a block is reduced to 3 s [2,15]. Consequently, it uses a lot less energy than PoW. The blockchain system's nodes are divided into three groups by DPoS: witnesses, delegates, and workers. The system's core component, witnesses, was chosen by all nodes through resource voting. The nodes receiving the top N votes take on the role of witnesses and generate blocks alternately. The delegates can request to update the blockchain even though they won't be rewarded. Workers have the right to suggest new initiatives and receive compensation for projects that have been chosen by the public.)

i) **Sharding:** Sharding along with several other techniques is being tested by start-ups, developers, and current blockchain operating systems like Ethereum to see whether it can lend a hand to Blockchain developers and subsequently rise the scalability boulder. It entails slicing a blockchain into numerous parts, or shards, and storing each one separately. It is possible to mitigate the computational load on each node by storing the data on various computers. Because of this, the network can handle more transactions at a faster rate. This operates easily. A blockchain is an example of a standard peer-to-peer (or P2P) network that includes numerous complete nodes or computers. Where copies of the history of the entire chain are recorded in each note. Sharding enables nodes to function without having to maintain all of the data at once.

j) **IoV network:** Data generated by networked cars and vehicular ad hoc networks can be used thanks to a dispersed network termed the Internet of Vehicles (IoV) [32]. One of the main goals of the Internet of Vehicles is to enable real-time communication between vehicles and their human drivers, pedestrians, other vehicles, roadside infrastructure, and fleet management systems (IoV).

ii. Results and Discussion

In Table 1, the comparison table in terms of characteristics details has been organized with our findings from the literature review. The table shows a comparison of the consensus models (PoW), (PoA), (PoS), and (PoV) with some concise relevant information in relation to their characteristics: security, energy efficiency, scalability, and compatibility with IoT networks.

With respect to security, PoW demonstrates high security in its hash cash and micro mint methods, although its data handling security is considered only fair [2]. PoA also maintains high security and is considered safer and more reliable than PoS. Its Byzantine fault tolerance model is a better alternative than the non-distributed protocols of a centralized system. PoS has lower security compared to PoW when it cannot prevent pool mining but in PoS it is exceedingly difficult to perform a double spending attack. PoV has a security integrity that is lower than PoW but it is within a sustainable level.

In terms of energy consumption, the traditional PoW has poor efficiency in the case of energy. However, developing the proposed Green-PoW technology can reduce 50% in energy consumption [1,2]. PoA offers better results compared to both PoW and PoS and finds its own way through higher energy efficiency. PoS also requires lower energy consumption than PoW as it does not use complex puzzle solutions like PoW [3,14]. Delegated Proof of Stake (DPoS) is another proposed PoS design that shows higher efficiency and security than traditional PoS Consensus algorithms. PoV is also very powerful in energy efficiency because instead of mining the solution is calculated by randomly chosen miners who do not need to waste huge computational power unlike in PoW.

While considering Scalability, the base version of PoW has low scalability but can improve significantly by developing the Green-PoW methods [2,9]. Since the proposed Green-PoW can reduce 50% of energy consumption, it can be highly scalable in a Blockchain network keeping the security extremely high simultaneously. However, less power results in requiring increased time in finding the nonce. PoA's scalability is higher than PoW but the transactions require validation from an approved system thus making the consensus centralized. The byzantine fault tolerance model of PoA is better than the non-decentralized protocols of a typical centralized system [4,17]. PoS achieves high scalability by increasing the transaction speed by using a distributed strategy called “sharding” [6]. However, shard takeover attacks can be a potential. PoV, with its ability to create blocks faster than PoW, exhibits high scalability potential. Although its security is lower than PoW, it is still at a sustainable level.

Regarding compatibility with IoT environments, PoW is far from an optimal choice. However, Proposed Miner Twins may be able to enable fair PoW consensus in IoT environments [4,8]. PoA, while being a centralized system, can use a better alternative called Hierarchical Distributed Proof of Authority (HDPoA), which has been validated through real-world implementation using a diverse range of low-cost and low-power IoT devices [3]. PoS is a much better alternative than PoW for improving IoV networks, offering higher transaction speed and requiring fewer processing resources [7]. As of now, PoV has not yet been implemented in any real-life IoT networks, it holds promise for future research and application since it has potentially high block creation speed and exceptionally low energy consumption.

It is difficult to decide directly if a single consensus is straightforward and better than the other because there are many factors to consider like specific goals, requirements and size of the network, and the overall context of the Blockchain network. Based on these goals and attributes the flexibility of implementing the consensus algorithms varies. Each consensus has its own strengths and weaknesses concurrently depending on distinctive characteristics. PoW offers high-end security but can be monstrous when it comes to energy consumption. PoA prioritizes safety and reliability but unfortunately, it is centralized. PoS delivers promising energy efficiency and scalability but has lower security integrity. PoV is a rarely used consensus. It shows potential for future research but has not been applied in an IoT environment yet. Due to the limitations of each consensus algorithm, new consensus algorithms or alternative models of each consensus algorithm (HDPoA, DPoS, Green-PoW, etc.) are constantly being proposed. It is important to perform a significant amount of study and find what meets the requirements before using the consensus and taking them into real-life scenarios.

5. Conclusion

Many applications and enterprises are shifting to blockchain-based solutions because of the recent trend toward blockchain. Before shifting to blockchain-based solutions it is crucial to know about its current protocols and consensus algorithms. In this paper, we have covered the consensus techniques, their categories, and their significance in distributed environments. It is possible to do a thorough qualitative comparison that fills in the gap in the existing literature. The comparison made between PoW, PoA, PoS, and PoV regarding their energy efficiency, security, scalability, and IoT compatibility will help readers, researchers, and developers gain valuable insights before making decisions and advancements in blockchain technology. Additionally, we analyzed a few alternative proposed consensus algorithms like DPoS, HDPoA, and Green-PoW which offer improvements on the limitations of a base consensus process. The study contributes to the current field of knowledge by conducting a comprehensive comparison of the consensus algorithms through an extensive literature review. With the expanding number of blockchain networks and technologies, there is a need to evaluate and determine the suitability of a consensus algorithm for specific requirements. This study demonstrates how the strengths and weaknesses of a consensus can have an impact on a blockchain-based network surrounding the concerns of power consumption, double spending attacks, integrity, compatibility with an IoT setup, centralization, and much more. Due to some current government restrictions on Bitcoin mining in the country, we were unable to make a real-life survey on PoW and other consensus algorithms. Therefore, our work remained within the bounds of literature analysis only. While there are many consensus models out there, resulting from a lack of time and resources we were limited to descriptive analysis on only four consensus algorithms. However, the study we conducted provides authentic and valuable information and we wish to broaden our field of research involving more consensus methods with some real-life deployment in the future.

References

[1] Lasla, N., Alsahan, L., Abdallah, M. and Younis, M., 2020. Green-PoW: An Energy-Efficient Blockchain Proof-of-Work Consensus Algorithm. arXiv preprint arXiv:2007.04086.

[2] Meneghetti, A., Sala, M. and Taufer, D., 2020. A survey on pow-based consensus. *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, pp.2516-0281.

[3] Alrubei, S., Ball, E. and Rigelsford, J., HDPoA: Honesty-based distributed proof of authority via scalable work consensus protocol for IoT-blockchain applications. *Available at SSRN 3999127*.

[4] Parinya Ekparinya, P., Gramoli, V. and Jourjon, G., 1902. The Attack of the Clones against Proof-of-Authority.

[5] Kejiao, L, Hui, L. Hanxu, H. Kedan, L. and Yongle Chen,” Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain,” 2017.

[6] Yuefei Gao, Shin Kawai, Hajime Nobuhara, "Scalable Blockchain Protocol Based on Proof of Stake and Sharding, " in 2019, Volume 23, Issue 5, Pages856-863.

[7] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications, and Opportunities," in IEEE Access, vol. 7, pp. 85727-85745, 2019, doi: 10.1109/ACCESS.2019.2925010.

[8] Qu, Q., Xu, R., Chen, Y., Blasch, E. and Aved, A., 2021. Enable Fair Proof-of-Work (PoW) Consensus for Blockchains in IoT by Miner Twins (MinT). *Future Internet*, *13*(11), p.291.

[9] Shahriar Hazari, S. and Mahmoud, Q.H., 2020. Improving transaction speed and scalability of blockchain systems via parallel proof of work. *Future Internet*, *12*(8), p.125.

[10] Wan, S., Li, M., Liu, G. and Wang, C., 2020. Recent advances in consensus protocols for blockchain: a survey. *Wireless networks*, *26*(8), pp.5579-5593.

[11] Supreet, Y., Vasudev, P., Pavitra, H., Naravani, M. and Narayan, D.G., 2020, August. Performance Evaluation of Consensus Algorithms in Private Blockchain Networks. In *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)* (pp. 449-453). IEEE.

[12] Khatoon, A., Verma, P., Southernwood, J., Massey, B. and Corcoran, P., 2019. Blockchain in energy efficiency: Potential applications and benefits. *Energies*, *12*(17), p.3317.

[13] Kaur, M., Khan, M.Z., Gupta, S., Noorwali, A., Chakraborty, C. and Pani, S.K., 2021. MBCP: Performance analysis of large-scale mainstream blockchain consensus protocols. *IEEE Access*, *9*, pp.80931-80944.

[14] Giang-TruongNguyen, Kyungbaek Kim, Journal of Information Processing Systems Vol. 14, No. 1, pp. 101-128, Feb. 2018.

[15] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism," in IEEE Access, vol. 7, pp. 118541-118555, 2019, doi: 10.1109/ACCESS.2019.2935149.

[16] Joshi, S., 2021. Feasibility of proof of authority as a consensus protocol model. *arXiv preprint arXiv:2109.02480*.

[17] A Avasthi, A. and Saxena, A., 2018. Two-hop blockchain model: resonating between proof of work (PoW) and proof of authority (PoA). *International Journal of Information Systems & Management Science*, *1*(1).

[18] Mehrdad, S., Mainak C. 2018 An Overview of Blockchain and Consensus Protocols for IoT Networks. arXiv preprint arXiv:1809.05613

[19] Subhi A., Edward B. and Jonathan R., 2022. HDPoA: Honesty-based Distributed Proof of Authority via Scalable Work Consensus Protocol for IoT-Blockchain Applications. *IEEE Access*, DOI: 10.1109/CyberSA52016.2021.9478257

[20] A. Juels, J. Brainard, "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks", Network and Distributed System Security Symposium, 1999, Available: https://www.ndss-symposium.org/ndss1999/cryptographic-defense-against-connection-depletion-attacks

[21] F. Bravo-Marquez, S. Reeves, and M. Ugarte, "Proof-of-learning:a blockchain consensus mechanism based on machine learning competitions," in 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). IEEE, 2019, pp.119–124.

[22] Oliva, G.A., Hassan, A.E. and Jiang, Z.M., 2020. An exploratory study of smart contracts in the Ethereum blockchain platform. *Empirical Software Engineering*, *25*, pp.1864-1904.

[23] The Scalability Trilemma in Blockchain. Accessed: Sep. 1, 2019. [Online]. Available: https://medium.com/@aakash_13214/the-scalability-trilemmain-blockchain-75fb57f646df

[24] Vujičić, D., Jagodić, D. and Ranđić, S., 2018, March. Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)* (pp. 1-6). IEEE.

[25] Curran, K. and Honan, J., 2007. Fighting the Problem of Unsolicited E-Mail Using a Hashcash Proof-of-Work Approach. In *Business Data Communications and Networking: A Research Perspective* (pp. 346-374). IGI Global.

[26] Navjeet k. 2015. A Survey on Online Banking System Attacks and its Countermeasures. IJCSNS VOL.15 No.3

[27] Galibus, Tatiana; Krasnoproshin, Viktor V.; de Oliveira Albuquerque, Robson; Pignaton de Freitas, Edison (2016). [SpringerBriefs in Computer Science] Elements of Cloud Storage *Security, 10.1007/978-3-319-44962-3(), –.* doi:10.1007/978-3-319-44962-3

[28] Bhattacharya, S; Kumar, C R S (2017). *[IEEE 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) - CHENNAI, India (2017.2.16-2017.2.18)] 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) - Ransomware: The CryptoVirus subverting cloud security., (), 1–6.* doi:10.1109/ICAMMAET.2017.8186691

[29] Bell D., Jane G., 1992. Distributed Database Systems. Workinham, England: Addison Wesley.

[30] Janno S., 2017. Proof-of-Stake. Research seminar in cryptography, 2017 - courses.cs.ut.ee

[31] Ahmed M., Olov S., Karl A., 2019. A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities. IEEE doi: 10.1109/ACCESS.2019.2936094

[32] Mahmood Z., 2020. *Connected Vehicles in the Internet of Things (Concepts, Technologies and Frameworks for the IoV) ||., 10.1007/978-3-030-36167-9(), –.* doi:10.1007/978-3-030-36167-9

[33] Hafid, A., Hafid, S., Samih M., 2020. Scaling Blockchains: A Comprehensive Survey. IEEE Access, 8(), 125244–125262. doi:10.1109/ACCESS.2020.3007251

[34] Johannes S., Hans B., Gilbert F., Robert K., 2021. Recent Developments in Blockchain Technology and their Impact onEnergy Consumption. Informatik Spektrum, (), doi:10.1007/s00287-020-01321-z

[35] S Huh, S Cho, S Kim. 2017. Managing IoT devices using blockchain platform. IEEE 19th International Conference on Advanced Communication Technology (ICACT) - Pyeongchang, Kwangwoon Do, South Korea (2017.2.19-2017.2.22)] -. (), 464–467. doi:10.23919/ICACT.2017.7890132

[36] SS Dash, S Das, BK Panigrahi. 2021. Advances in Intelligent Systems and Computing. Volume 1172 (Proceedings of ICICA 2019) ǁ., 10.1007/978-981-15-5566-4(), –. doi:10.1007/978-981-15-5566-4

[37] Jonathan K., Hovav S., 2017. || Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. *[Lecture Notes in Computer Science] Advances in Cryptology – CRYPTO 2017 Volume 10401 10.1007/978-3-319-63688-7(Chapter 12), 357–388.* doi:10.1007/978-3-319-63688-7_12

Authors' Profiles

Shahriar Fahim has accomplished a B.Sc. degree in Computer Science and Engineering from American International University- Bangladesh. Currently, he is an entrepreneur of a small business. He operated his business at an early age with prolonged dedication. His area of research is Blockchain, Governance, and management information systems.

S M Katibur Rahman with a B.Sc. degree in Computer Science and Engineering from American International University- Bangladesh, is currently devoted to web technology projects using JavaScript, Tailwind CSS, mambaUI, and MongoDB. He has researched numerous prospects of Blockchain's Consensus algorithms. SM Katibur has academically excelled in the field of computer science as a student.

Sharfuddin Mahmood has completed his B.Sc and M.Sc. degree in Computer Science from American International University- Bangladesh. His major was Information and Database Technologies. Currently, he is focusing on Data Mining technologies and algorithms. His area of research is Data mining and knowledge discovery and intelligent systems.

How to cite this paper: Shahriar Fahim, SM Katibur Rahman, Sharfuddin Mahmood, "Blockchain: A Comparative Study of Consensus Algorithms PoW, PoS, PoA, PoV", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.9, No.3, pp. 46-57, 2023. DOI: 10.5815/ijmsc.2023.03.04