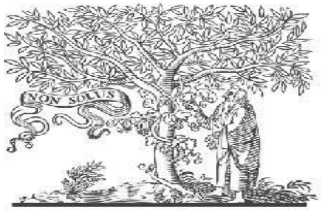
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 05th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/46

Title **A Border Perspective Of Blockchain Consensus Techniques And It's Challenges**

Volume 12, ISSUE 04, Pages: 354-377

Paper Authors

Akshya S, Kalpana G

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A Border Perspective Of Blockchain Consensus Techniques And It's Challenges.

Akshya S[1], Research Scholar, Department of Computer Science, SRM Institute of Science and Technology, Chennai, India.
Kalpana G[2], Associate Professor, Department of Computer Science, SRM Institute of Science and Technology, Chennai, India.
[1]as1872@srmist.edu.in, [2]kalpanag@srmist.edu.in.

Abstract

Blockchain is the primary technology behind Bitcoins, which has lately received a great deal of focus. Blockchain is an emerging technology changing the simulated reality by bringing a raw perspective to network protection, elasticity, and functionality. Blockchain is in charge of an indelible history that allows for localized exchanges. Blockchain based solutions were gaining traction in various areas, notably banking and government, reputational services, and the Internet of Things (IoT). Therefore, obstacles to distributed ledger systems must be overcome, such as stability and privacy measures. It delivers a protected means of exchanging all sorts of items, resources, and trade. Honest connections were critical to commercial success; nevertheless, rising oversight, cyberattacks, as well as deceit were hindering progression. Blockchain will allow highly adaptable value networks, speedier creation, improved client relations, and greater convergence of IoT and cloud technologies to tackle various issues. Furthermore, Blockchain lowers trade costs by utilizing a trustworthy contract that is supervised without the interference of outsiders who cannot provide a tangible benefit. This allows smart-contracts, commitments, and deals with robust cybercrime embedded. This article aims to establish the groundwork for exhibiting and demonstrating the use of Distributed ledger technology in a broad range of commercial situations. The ideas may be used in various sectors, including banking, administration, and production, wherever safety, portability, and effectiveness are necessary. The blocks contain transactions linked together as a cryptographic link. The original record will not be visible to the user. It presents only the encrypted value of records to the user is termed Cryptography. When deployed across an extensive network of users, blockchains perform better and more efficiently. Blockchain is more than just a technology that underpins the Bitcoin network, blockchain technology is capable of doing much more work. This article covers an insight into blockchain architecture before delving into numerous popular consensus technology found in several blockchains. Furthermore, methodological limitations and rapid advances are briefly explored. We also go through a study of Blockchain applications that use Blockchain technology, as well as the hurdles and potential blockchain emerging outcomes. This review study will be helpful for future research on blockchain safety problems.

Keywords: Blockchain, Consensus algorithm, Neural Architecture Search (NAS), Security, Smart contracts

I. Introduction

A Blockchain is, at its most basic, a spread of information of documents or an open database of all of it conceived of or upgraded events that are deceased and distributed among collaborating parties. Blockchain is unchangeable. Once inputted, data cannot be deleted. The blockchain keeps a transparent and unambiguous log of every trade that occurs. Blockchain transactions cannot be modified once they are accumulated [8]. Blockchain may target an audience for enterprises that demand outstanding reliability and fairness. Blockchain is distributed and can prevent specific breakdown problems [10], [22]. Blockchain may be considered a shared ledger, with all confirmed interactions kept in a series of blocks. This link grew when innovative components were created for it on a routine basis. Asymmetric cryptography and distributed consensus approaches were implemented to secure information and guarantee ledger stability. Blockchain technology is characterized by decentralization, persistence, secrecy, and traceability [7]. Trades on the Bitcoin system may take place without the involvement of an outside entity, and blockchain is the basic technology used to develop Bitcoin. A chain is an electronic, ever-growing catalog that contains datasets. A collection like this consists of many datanodes that were organized topically, interconnected, and then safeguarded using cryptography evidence. Although it supersedes Bitcoin, blockchain technology is essential to the overwhelming bulk of cryptocurrency exchanges. This functions as a decentralized, fairly-distributed, and universal shared ledger which keeps a persistent history (sequence with nodes) from all formerly validated activities. [11].

In particular, Personal Defence Blockchain Mining, Coin.AI , Weka Coin, DLBC, and PoDL were superior to innovative consensuses that carried out deep learning training algorithms as proof-of-useful-work (PoUW). Miners' computational strength in blockchain applications might be utilized to speed NAS with innovative consensuses. The permission-less blockchain system's integrity relies on the enormous count of private mine workers—the motive to mine to gain tokens. Singular miners are only profitable if the amount of the obtained token exceeds the cost of the electric bill [1]. In a robust explicit permission blockchain-based system, the compute horsepower of the entire community is often extraordinarily high so that it can act as a fallback option for the blockchain system's security feature. As a result, the likelihood of a single miner earning the prize is exceedingly low. Without the improvement of the skilling work schedule, the miners who are the poorest would serve as the burden of entire quality. Also, the majority of miners would

stay inactive. As a result, miners with lower computational capability will not degrade overall effectiveness, and their materials will not be squandered [1].

Blockchain extensibility aims to handle a large number of operations every nanosecond while preserving privacy and decentralization. The essential thought underlying experience a significant is to divide the network into smaller functional units called as shards. The network is broken up into groups by Elastico, each of which manages a distinct series of records. The number of fragments increases approximately exponentially with network growth. To manage and accomplish speedier transactions, the OmniLedger consensus mechanism employs a type of ByzCoin. OmniLedger offers similar global and committee resilience as Elastico. RapidChain is a public blockchain protocol based on sharding that outperforms previous sharding algorithms [2].

The massive amount of power required for the PoW algorithm to deal with perilous pointless problems to generate newfangled blocks is gradually destroying the earth [8]. Blockchain technology differs in some ways, such as its sustainability, scalability, automation, and transparency, making it beneficial in some fields but worthless in others [10], [22]. The Hash Methodology involves reproducible, instantaneous computing and the Avalanche phenomenon. Deterministic means if data changes with minor changes, then the hash value also will vary according to the data [17].

A block contains multiple transactions as a record. A block includes Data, Previous Data (Hex code in terms of 0x), and Hash Value (Final Hex code in terms of 0x). A personal network currently running in the blockchain will create a first block and contain the network's configuration. Every Block that has been created will have a Block Number. “Fig 1.2” categorize the architecture of the blockchain layer and how the Hash value is generated by combining the current block number with all previous block number, data, and Nonce is used to calculate the Hash value.

The process of deploying the blocks into the network is called Mining. The cryptographic link will no longer work if an Intruder wants to temper a specific block. Miners changes Nonce (Number Used Only Once) Miner’s work keeps changing the Values in Nonce. When the number is exactly the same as in the acceptable range, it will become successful and get a reward. In BITCOIN- If you got more resources, miners will take less time to solve the cryptographic puzzle and get more rewards. “Fig 1.1” describes a Structure of a Blockchain which is an Ever-Expanding Chain of Ordered and Valid Transactions is the Blockchain Structure and explains how the hash data is calculated; these hashes are interconnected in a chain, which is known as a blockchain. The blockchain's most crucial feature is that transactions can be monitored into the past.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

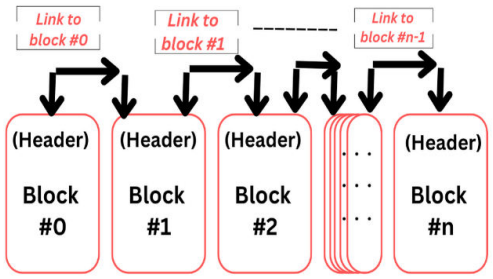


Fig 1.1: Blockchain structure, which is a had-ever network of organized as well as authorized occurrences.

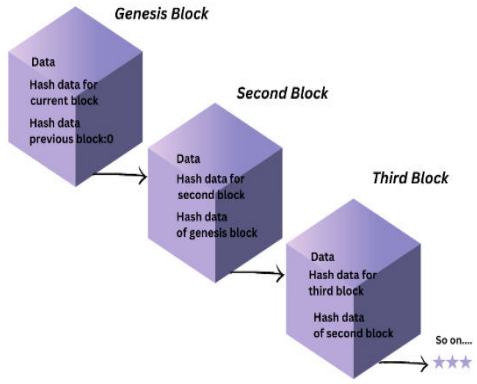


Fig 1.2: Blockchain Layer Architecture

"Fig 1.3" illustrate Blockchain Technology's peer exchange decentralized unchangeable accessible database that has transformed system administration.

Blockchain technology is peer-to-peer networking, works as a randomized record with one or even many digitized properties, referring to a fragmented peer-to-peer platform where every device maintains an entire shared database also checks the validity of all neighboring locations to ensure the correct record [6], [22], [11].

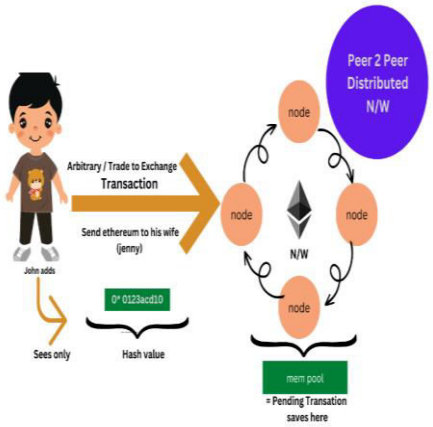


Fig 1.3: Working Process of Blockchain

II. CHALLENGES IN BLOCKCHAIN

A) Rising network installation costs	Everything ultimately comes reduced to early spending obligations. Certain firms may face high operational charges. Regardless of the preponderance of current answers are complimentary, significant investment is required in hiring expert computer programmers with expertise in blockchain networks, as well as license expenses if upgrading to a paid program edition, total management, and beyond. It is among the enormous serious blockchain implications.
B) Scalability	The pivotal obstacle to its applicability is scalability even if payment systems may manage numerous payments every moment with no failure, when it arrives in Bitcoin (approximately 4-8 operations every sec) but instead Ethereum (about 16-21 functions every sec), data analysis slows drastically, making blockchain technology impractical for significant developments. The Lightning Network and Plasma for Ethereum are scalability technologies that enable quick, low-cost transactions. Blockchain must enhance its speed in order to achieve general adoption. The incapacity to service various

	people is among the greatest significant drawbacks of blockchain technology and, by extrapolation, corporate digital currency. Organizations that can effectively grow their business blockchain systems will benefit from the increased supply of enterprise blockchain and related apps.
C) Security and privacy	Many industries nowadays operate within the bounds of the law. Whenever this concerns delicate details, visitors put their entire trust in professionals. If every bit of the data is kept in a public ledger, it won't be entirely secure. Therefore, for instance, personal or communal blockchains may well be deployed. You could just receive confined, but all personal data will be treated securely. Even while blockchain-base-application, grids, and firms remain extra safe than conventional supercomputer organizations, intruders could always gain access to things. The solution is not merely to have the government protect our privacy.
D) Regulations	The critical factor that could cause problems is the absence of guidelines. Scammers or financial fraud that may result in a global recession aren't unimaginable. As a result, Bitcoins have gotten a tremendous amount of criticism from individuals everywhere over the globe. Some nations have explicitly outlawed bitcoin, whereas others have attempted, with limited success, to manage a blockchain platform.
E) Criminal behavior	The dearth of solid legislation and the reality that blockchain remains just a fledgling concept have aided its creation for scam firms and other unethical players aiming to prey on inexperienced individuals.
F) Consumption of energy	An additional source of concern is that Proof of Work, the best often adopted consensus approach, necessitates a great deal of effort. Its limits ordinary people's access to PoW networks, cares about the establishment of massive taking-out pools, hampers regionalization through imposing people towards contribute cutting-edge bulky withdrawal pools and generates ecological issues.
G) Low workforce availability	The chain corporation's paucity of competent engineers has been compounded by fierce competition between enterprises offering extremely aggressive payouts to lure and keep such employees. As a result, several cryptocurrencies businesses offer staff inside specialized occupational groups and over $millions of dollars annually. Architects are being sought by companies to help overcome the blockchain skill gap. A significant blockchain policy implication is getting closer to resolution by the day.
H) Interoperability	Interoperability is among the most critical challenges that must be solved since it is one of the key reasons organizations are still reluctant to adopt blockchain technology. Most blockchains run independently and are unable to link to similar social circles since those could perhaps transmit as well as collect information via rival blockchain-based platforms.
J) Nonexistence of standardization	Despite the numerous networks accessible, there is no global standard. Due to the lack of uniform standards, there are issues with interconnectivity, different prices, and complicated processes. Since blockchain technology has no

	specific version, it discourages professional developers and investors from entering the industry.
K) Legacy system integration	If a business decides to use blockchain, it must either entirely rebuild its existing system or devise a plan for adequately connecting the two technologies. An additional difficulty is that firms lacking blockchain experts cannot gain exposure to the skill pool necessary to engage in this process. The use of an external factor might worsen this situation. Furthermore, most technological solutions require the organization to commit substantial time and money to accomplish the transformation.

III. CONSENSUS PROTOCOL ISSUES

a) Attackers - Attackers attempt to place a fresh block maliciously.

b) Competing Chains - In competing chains, if two blocks with identical information are formed, one should be the winner. In this situation, the winner will have the most resources. The information will be communicated with all blocks using the 51% majority protocol. The remaining minority blocks will become orphanage blocks and will be overtaken by majority blocks. They can be traced since all ledgers and peers in the Blockchain network have replicas of the blocks [11], [10]. "Fig 3.1" depicts a transaction's lifecycle and adding a new block to Blockchain.

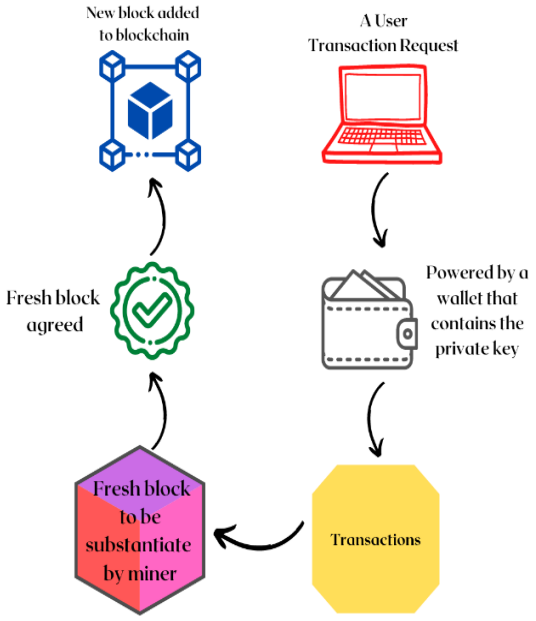


Fig 3.1: Blockchain Life-Cycle

IV. METHODOLOGY

a) Proof-of-Work (PoW)

In PoW (proof of work) consensus, an independent miner's ability to obtain a reward is determined by the proportion of its computing power to the entire network's computation power [1]. When using the Proof-of-Work consensus process, the node that resolves the very first mathematical challenge uploads the chunk is uploaded towards the network and is rewarded (by the network and transaction fees). If nodes do not have an

identical version of the blockchain, they will construct a most incredible link. Scalability is amid the primary limits of proof-of-work-based blockchains; indeed, the amount of data that can be processed every single moment is restricted [13]. Modern general agreement approaches, like proof of work or stake, have significant flaws. Proof of work, for instance, consumes excessive power capacity, while a phenomenon of the affluent becoming wealthier might occur during the Proof of stake consensus stage [2]. Miners are nodes that calculate hash values, and Bitcoin mining employs the PoW algorithm. Throughout the PoW protocol, a restraint that grows bigger is considered authentic. [12]. Bitcoin-based PoW drawing out for electronic devices. The primary distinction is that MIB's Mobile Proof-of-Work (MPoW) mines blocks using the computer chip power of mobile policies. The program is intended to consider the device's potential; users may choose the ideal mining intensity to preserve the cell phones as of warmness, permitting cheap smartphones of somewhat giving out the capability to join the web [5]. PoW is a type of this almost coordination aimed toward a blockchain system's emerging behavior [14].Proof of work began as a promising option to the alarming issue of spam email.

• Proof of work (PoW) is a randomized approach that forces internet users to work together to solve a unique cryptographic problem and eliminate computer tampering.

• In cryptocurrency extraction, proof of work is widely used to accept payments and also develop creative currencies.

• Due to proof of work, Bitcoins and various cryptocurrencies trades can be completed anonymously, without needing a trustworthy 3rd person. To Scale proof of work needs massive amounts of resources, which still increases as further producers enter the network.

• Proof of Stake (POS) was among the novel consensus mechanisms to target proof of work. Threats by selfish mining can impair and destabilize blockchain POW effectiveness. As a result, further assessment of mining computer power is required to protect the platform from an assault [13]. “Fig 4.1” depicts the iterative process of proof of work solution (pow). To create a peer-to-peer distributed timestamp system, we will be required to employ a proof-of-work method. Checking for a value that, when hashed, such as using SHA-256, starts with some zero bits is used as proof-of work. The average amount of effort necessary is proportionate toward the amount of single index required, which could be validated by performing a simple hash.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Fig 4.1: The iterative process of solving the proof of work (pow).

b) Proof-of-Stake (PoS)

Most blockchain commence with PoW and then progress to PoS. Proof of money ownership is required of PoS miners [12]. The Leading PoS (LPoS) choice outcome stands formerly saved as information hunks, which can be validated by some-node. The choice is grounded on a permutation mechanism or voting by supplementary PoS nodes — for example, a majority of PoS nodes must accept the disclosed possible LPoS for it to carry on this block's function [5].

- Proof-of-stake (POS) empowers bitcoin holders that approve log entries by staking a certain number of units [16].
- Proof-of-stake (POS) is created as a substitute for Proof-of-work, the original settlement process needed to audit a database and uploads newer transactions (POW).
- To earn charges, PoS approaches involve a consensus algorithm that must hold and place coins, while PoW methods involve workers to resolve riddles.
- Proof-of-stake (POS) is thought to be lesser harmful in the sense of networking assault risk because it organizes rewards in that kind of a way in which an attacker is low appealing [16].
- The blockchain's subsequent log creator was picked as arbitrary, having networks bearing higher interest values getting the advantage.

You must bet 32 ETH to establish your validator; although you do not need to stake as much ETH to participate in validation. You may engage validation pools through "liquid staking," which involves utilizing an ERC-20 token to symbolize your ETH. The PoS system functions to eliminate the PoW algorithm's drawbacks, such as colossal energy consumption. Aside from the benefit of reduced energy usage, PoS processes have a faster transaction validation performance than PoW strategies [15]. “Fig 4.2” Using the networking node stakes, the recursive method of selecting the following crusher to generate a block.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

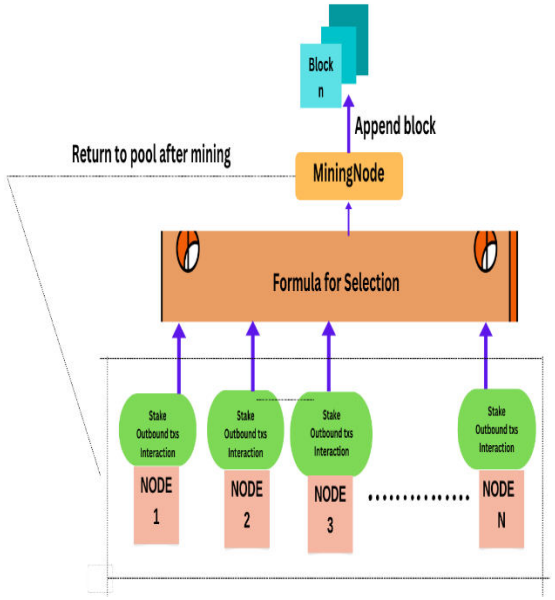


Fig 4.2: Using the networking node stakes, the recursive method of selecting the following crusher to generate a block.

c) Byzantine Fault Tolerance BFT

Byzantine-Fault-Tolerance (BFT) remains a consensual technique near avoiding the Byzantine Generals' issue. It also implies that the system should remain operational regardless of whether only-one of the nodes (or the whole network) malfunctions. Furthermore, BFT seeks to mitigate the influence of malevolent byzantine nodes (or all-purpose) on the network. To achieve effective byzantine state machine replication to tolerate malicious or byzantine nodes [11]. The BFT-based blockchain technology optimally tackles telecommunication intricacy and endurance difficulties in the event of malfunctions [20]. To ensure the generals' team's success, they require an algorithm that can comply with the following conditions:

- The troop generals must all agree on the plan's next action.
- The generals must be trustworthy and committed to the process.
- Generals must not be swayed into becoming network criminals.
- They must adhere to the system's algorithm.
- Regardless of the conspirators acts, the generals must achieve a consensus or make a decision.
- At any point of action, the network or computer system should not allow a 51% assault.

The Pros of PBFT

- A pBFT, unlike PoW, does not need to perform complicated mathematical computations.
- It is a consensus model that uses less energy.
- A block of transactions, in this case, does not require repeated approvals by each node. As a result, it takes less time.
- Because pBFT needs individual nodes to participate and service the customer requests, the reward is distributed to each node. As a result, the reward variation across nodes is modest.

The Cons of PBFT

- PBFT has a high communication cost that grows with the number of nodes in the network.
- It has scalability concerns with more extensive networks.

- Sybil attacks, in which one node controls or behaves as numerous network nodes, are possible with pBFT.

d) Proof-of-Importance (PoI)

Proof of Importance eliminates the restrictions of PoS in blockchain by giving consensus addresses and significance ratings. In 2015, the NEM (New Economy Movement) blockchain debuted the PoI consensus method. Their cryptocurrency is known as XEM. Consider relevance scores to be a network's trust or reputational score. A higher score indicates that the network has greater faith in you to validate or fabricate the fresh block of transactions. As a result, you have a better probability of being chosen as a block harvester (miner in PoI mechanism). With PoI, your odds of successfully validating the transaction are not only determined by your interests. However, this is determined by the overall volume of business trades you have completed in the history and the quality of those transactions [11]. "Fig 4.3" convinces an explanation of the PoI Consensus architecture, which determines an Instructional Strategy that is applied to select the subsequent miner location.

Improve the importance score by doing regular and high-quality transactions:

- PoI rewards nodes that conduct usual transactions rather than simply storing the money.
- It encourages the exchange of cryptocurrencies throughout transaction parties.
- Unauthorized transactions performed just to boost the significance score are identified and destroyed by the network.
- PoI assigns a value to specific sorts of transactions.
- Greater transactions, for example, receive higher marks than lesser transactions.
- In the scenario of the NEM blockchain, an account must have made at least 1000 XEM transactions in the recent 30 days to qualify statements that have at least 10,000 XEM at a vested stake.

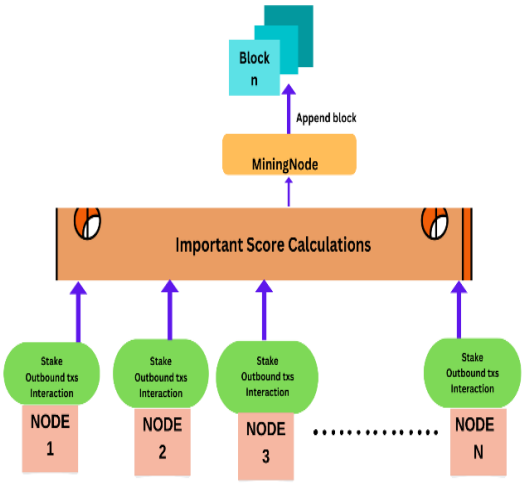


Fig 4.3: Proof-of-Importance (PoI) mining process

e) Proof-of-Elapsed Time (PoET)

Proof of elapsed time (PoET) allows examined in this section networks to determine who creates each subsequent block. It utilizes a random system to

distribute the possibilities of gaining uniformly distributed across network members, giving each node a similar chance. This system computes an arbitrary wait period for each node in the blockchain network, during which each node should rest. The node with the least wait time will be among the first to wake up and gain the block, allowing it to contribute a unique block blockchain. The PoET process is identical to bitcoin's proof of work (PoW). Still, the subject uses low energy since it permits a node to rest and move to all other activities for a defined period, enhancing network energy consumption [12], [17]. Proof of elapsed time consumes relatively less energy than proof of work because it chooses a node arbitrarily rather than contesting across all miners on a network.

For example, "CreateTimer," generates a time for a transaction block certified to have been produced by the stronghold. The following method, perhaps "CheckTimer," validates that the stronghold generated the timer and, if exhausted, generates an affidavit that can be utilized to confirm that the checker did, in reality, wait the specified time prior to claiming the position of leadership [11].

The PoET network consensus process must ensure the two critical aspects. First, it assures that the engaging nodes choose an arbitrary period rather than a smaller length selected intentionally by the participants to succeed. Second, it proves that the winner has accomplished the grace period. Unlike proof of work, proof of elapsed time does not support decentralization and transparency since it needs a license granted to everybody who wishes to contribute to the network. “Fig 4.4” defines the Architecture of PoET Consensus Mechanism as designed to pick every Using the Software Guard Extension (SGX) innovation, the future operator is selected depending on an unpredictable latency duration.

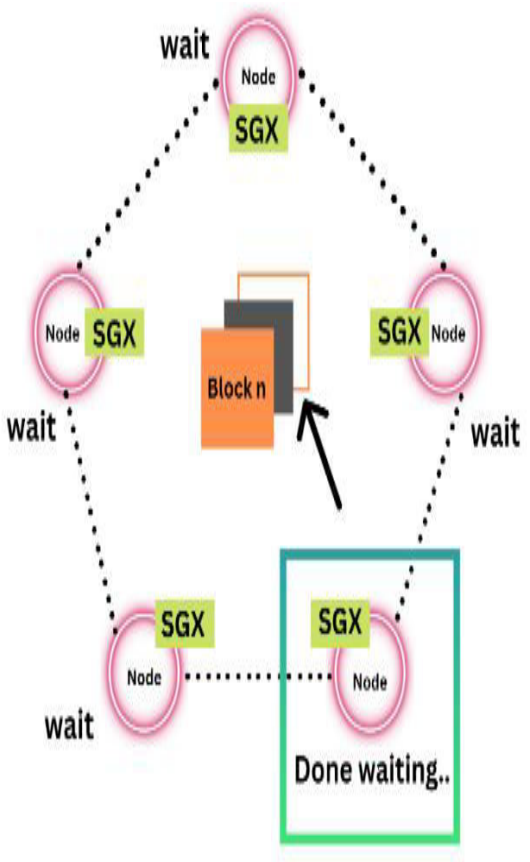


Fig 4.4: The Architecture of PoET Consensus Mechanism.

f) Proof-of-Authority (PoA)

Proof-of-Authority (PoA) is a series of Byzantine-fault-tolerant (BFT) consensus algorithms that are widely utilized in reality to provide higher performance than classic Practical Byzantine Fault

Tolerance (PBFT). After being generated, each k-block is propagated over the network to PoS and, perhaps, PoA nodes [5]. In PoA, the consensus is reached by consulting a list of authority (Validators), nodes permitted to join in the consensus, validating both blocks and transactions. PoA is more protected than PoW for permissioned DLTs because a hacker with an unnecessary correlation or security breach authority cannot overload the entire network, less computationally efficient because no mining is associated, quick and more predictable because blocks are given at predetermined periods [18], [19].

Unlike PBFT, PoA takes fewer message exchanges and gives more incredible results [11]. "Fig 4.5" states the architecture of the PoA Consensus Protocol, whereby nodes stake their credibility by validating their credentials until becoming network miners.

PoA unanimity will differ depending upon technology, but it can generally be used underneath certain conditions:

- Auditors may prove actual identities.
- An candidate ought to be willing to invest money and jeopardize their credibility. A thorough method reduces the risk of selecting suspicious verifiers and supports widespread dedication to the chain.
- The technique of selecting verifiers should be unique across all entrants.
- The authentication of verifiers must be checked to ensure the validity of the network. There must be a procedure in order to choose reliable verifiers.

The advantages of PoA :

- Confidence level is excellent as provided, as 51% of nodes are still not acting upon purpose.
- The time difference between the creation of consecutive sections is foreseeable. Every time is determined by PoW and PoS consensuses.
- A large storage volume.
- Much less expensive to approaches that need computing speed, like Proof of Work.

Constraints of PoA consensus:

- PoA is not decentralized; instead, it is an attempt to improve the efficiency of centralized control.
- Someone may see the PoA validators. Revealing the identity of validators might lead to third-party tampering.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

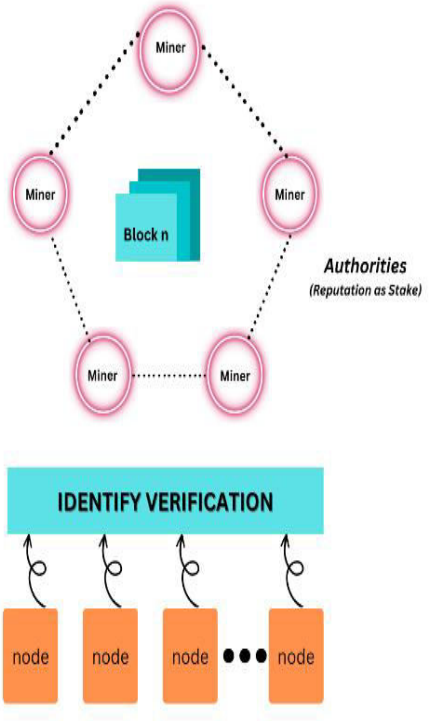


Fig 4.5: The architecture of the PoA Consensus Protocol.

g) Proof-of-Weight (PoWeight)

To avoid duplicate spending assaults and other dishonest behavior on the blockchain, the preponderance of the weighting component must belong to truthful consumers [11]. The Proof-of-Weight consensus method secures the network from double-spend attacks as long as most loaded members are trustworthy. When a transaction on a blockchain is created using the Proof-of-Weight consensus mechanism, the network generates a working group of stochastic network users. It allocates each individual their 'weight' (depending on the amount of currency they grab on the network), which gently controls the consensus algorithm within the stochastic review panel.

V. LITERATURE REVIEW

a) Mining Pool for Proof-of-neural-architecture

Boyang Li et al., (2022) discusses that this sort of mining pool's effectiveness outperforms a single worker's experience. Since, the unpredictable nature of mineworkers behavior, the withdrawal pool manager examines the departure from the mean of high-reward miners execution and provides alternative miners to ensure the execution of high reward miners' work. As a result, there is not chance that perhaps a poor miner would degrade the large mining pool's end scores, and powerful hackers will be able to use significant processing power to seek for additional space. The authors provide a thorough examination of blockchain technology, including the Deep Learning Consensus Algorithm, Proof-of-Useful-Work (PoUW) mechanisms, Proof-of-Deep-Learning (PoDL), pool manager, dividingspace partition algorithm and Neural Architecture Search (NAS) [1].

b) Sharding-Based Blockchain Protocol

Hafid, Abdelatif, et al., (2019) examine the privacy of scaling solutions that employ the idea of sharding. It is extremely difficult to strike a balance between scalability, security, and decentralization. To evaluate the concept, we used sharding protocols such as RapidChain, OmniLedger, and Zilliga. The crucial focus of this research is that over the summation of upper-bounded

hypergeometric and binomial distributions, we employ probabilistic conditions to limit the fault level for one panel and hence to every period. There are 3 probabilistic boundaries used: Chvátal, Hoeffding, and Chebyshev. Furthermore, we devised a method for determining the parameter requirements that should be gratified by a sharding-based blockchain system to reduce the likelihood of outages below a particular threshold [2].

c) Contract and Work Flow Management

Downey, et al., (2019) explains that the consensus algorithm works in conjunction with the distributed ledger in a corporate network. Consensus confirms that all corporate network stakeholders accept the type of documentation to be gathered. Lineage ensures that stakeholders can track an asset's documents to its genesis. Proof of Work, Proof of Stake, Byzantine Agreement, Tendermint, and Federated Byzantine Agreement are examples of current consensus procedures. Proof of Work is used by Bitcoin and Ethereum Blockchains, whereas The Public Byzantine Fault Tolerant algorithm is the foundation of Hyperledger Network. Although some knowledge of blockchain technology may be necessary, a manufacturing engineer might not be required to grasp the consensus process. [3].

d) DLT-Land Transaction System with Trusted Nodes Consensus

Singh et al., (2021) demonstrate a Trusted Node Consensus Algorithm (TNCA) constructed on the criterion of the workers, which reduces the networking burden of dissemination of the creative block. Performance assessment is evaluated with PoW, PoS, DPoS, TNCA, and a trust-based consensus approach. This work proposes an innovative and scalable technique for transferring assets / land-living from one organization to an alternative. Blockchain characteristics can give a visible, safe, quick processing, and decentralized system [7].

e) DLT-Transaction Mechanism and Its Block Size Assessment

Singh and Vardhan (2019) explain and present a consensus approach for land registration using blockchain-based Distributed Ledger Technology (DLT). They are primarily concerned with establishing a foundation for a dependable and decentralized P2P platform for administering the electronic stamp and asset record-keeping processes. The researchers expanded their DLT exploration and presented a decentralized distributed framework for actual transactions and confirmation desires. (2019, Singh and Vardhan) [8].

f) Proof-of-Stake Consensus Mechanism

Nguyen, Cong T., et al. (2019) portrays that PoS smart contracts in the realm of IoV were addressed, as well as the

development of stake pools in PoS networks. We demonstrated that preserving a suitable relation among block plunders and overall network interests were critical for network decentralization [15].

g) On Selfholding Attack Impact on Imperfect PoW

Yang, Runkai, et al. (2021) Displays that cyberattacks from selfish mining can diminish and interrupt POW efficiency. As a result, a further appraisal of mining computer power is required in order to defend the system from an assault [14].

h) A Survey of Consensus Algorithms

Alsunaidi, Shikah J., and Fahd A. Alhaidari. (2019) It has eradicated the possible failure point prevalent in the central environment and lowered network administration expenses by improving how the data and assets are distributed. It hinges on consensus methods to govern all network transactions, and there are various suggested algorithms [17].

i) Building a Product Origins Tracking System Based

Cong An, An, et al. (2019) This illustrates that the performance trade observed in differential amplifier circuits also applies. Compared to the 2-TFT pixel, the circuit shown here necessitates the inclusion of an extra TFT and read line. As a result, the network would not enforce pixel size constraints, albeit the constraints for driving sequence, including swapping power lines, may need a bespoke controller. [18]

j) A Lightweight and Attack-Proof Bidirectional Blockchain

Xu, Chenhao, et al. (2022) Studies are carried out to demonstrate that the suggested paradigm's privacy and adaptability outperform those built on PoW in addition PoS. Forthcoming work is being carried out to analyze the likelihood of chain reliance on BLB with PoW or PoS based blockchains to help increase capacity or safety, as well as a property that makes assessment rules to limit the effect of Sybil assaults. [19]

k) Window-Based BFT Blockchain Consensus

Jalalzai, Mohammad M., and Costas Busch. (2018) deploys that in order to eliminate superfluous communications and increase the efficiency of blockchain processes, a BFT-based consensus protocol was developed. This enhancement does not reduce downtime because our system still needs minimal cycles. [20].

l) Analysis of the Consensus Protocols

Anupama, B. S., and N. R. Sunitha. (2022) describe the Consensus foundation of blockchain technology. Consensus methods are intended to improve Cryptocurrency functionality and still satisfying the specific needs of certain domains. The consensus method boosts the effectiveness of the blockchain by

enabling for better bandwidth. This article examines the protocols PoW, PoS, DPoS, PoET, PoA and PBFT [21].

m) Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network.

Singh, Saurabh, et al. (2021) analyzes the blockchain idea and pertinent elements, comprehensively analyzing potential security threats and presenting current solutions that may be applied as counters to such assaults. It offers blockchain network protection solutions by outlining essential points that could be utilized to construct decentralized applications and protection measures that solve security vulnerabilities, covering open challenges and potential research opportunities in blockchain-IoT systems [22].

Table 1: Comparison of methodology

S. NO	TITLE, AUTHOR & YEAR	METHODS / PROPOSED WORK	ASSESSMENT / CRITIQUE	INFERENCE /WORK RESULTS	FUTURE IMPROVEMENT
1	A collaboration strategy in the mining pool for proof-of-neural-architecture consensus. Boyang Li et al., (2022).	Deep learning consensus, Subspacepartition algorithm, and exploration &exploitation strategy.	Studies showed that the efficiency of this sort of mining pool outperforms which of an isolated mineworker. Because prospectors behavior is unpredictable, the extraction group administrator examines the confidence interval. of good profit miners efficiency and provides standby miners to	Since personal workers are unstable, the extraction pool administration may help detect the top performers and give standby laborers.	Individual miners should be predictable and should be at a certain time to account for the top of the ladder labourers (No need for backup miners).

			assure fulfillment of good profit miners work.		
2	New Mathematical Model to Analyze Security of Sharding-Based Blockchain Protocols. Hafid, Abdelatif, et al., (2019).	Sharding protocols including Rapid Chain, Omni Ledger, and Zilliga. Harding-based blockchain protocols; Chebyshev, Chvátal, and Hoeffding	Our research mainly involves using Boundaries for the summation of topmost hypergeometric and binomial models to restrict the absorption coefficient once per panel and thus for every era.	Lastly, given a failing chance barrier, researchers recommend estimating the typical length of time until the system fails. As a result, to ensure a certain level of protection, our technique computes the smallest capacity of the advisory board to investigate using sharding-based blockchain protocols.	The computation of the Maximal size of the committee can be used for future enhancement.
3	Blockchain for Business Value: A Contract and Work Flow Management to Reduce Disputes Pilot Project. Downey, Liang Xi, et al., (2018)	Smart Contract, Contract2work, Proof-of-work.	In conclusion, we discussed a prototype IBM project in Europe that used blockchain technology to assist A power company in working to improve its contract2work procedure. It goes through two components of the tendering system: technical work and administrative labor, as well as how partly finished	It goes through two components of the tendering process: scientific job and managerial labor, and how nearly built task generates half compensation anywhere along way to the help expedite the billing procedure. The component is concerned with scope change monitoring, which includes the start, analysis, acceptance, work executed, and revenue earned.	Subscriptions of events are another instance where Block chain technology may be used. Authorities and safeness, licensing, and accountability

			work prompt fractional payment and a long way to expedite the financial transactions. The second component focuses on scope change management, including change request origination, assessment, acceptance, work performed, and money colleced.		
4	An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges, and Future Trends. Ometov, Aleksandr, et al., (2020)	Combination of Proof of Work (PoW), Proof-of Activity (PoA), and Proof of-Stake (PoS) algorithms.	A collection of procedures linked altogether Blockchain solutions like Proof-of-Work, Proof-of-Stake, and Proof-of-Activity have been developed in command to incorporate devices in the new structure formation process.	The results show that using PoA systems on a smartphone has no substantial impact on battery life, but traditional PoW-based approaches have a significant negative impact. Blockchain technology's primary uses for smartphones and wearable devices moving away from the traditional bitcoin viewpoint and comparing real business systems.	The study concludes with future prospects and the primary mobile blockchain challenges associated with implementing blockchain-based solutions on cell phones.
5	Blockchain Technology and Its Applications: A Systematic	Decentralized, Ledger, Applications, Consensus.	BT can shift people's methods of building trust from third-party administration to	The accessibility, permissionless ness, and borderlessness of BT allow everyone equal access to the	Blockchain technology is constrained by time commitments for complicated

	Review of the Literature. Arora, Priyanka, and Ritu Nagpal. (2022)		technology-assisted assembly. There is no need to contact a private entity or spend a service charge on a 3rd person.	system and, as a corollary, the blockchain network built with it.	inspection and significant energy needs. To decrease confirmation and mining operation computation time and energy
6	Distributed Ledger Technology-based Land Transaction System With Trusted Nodes Consensus Mechanism. Yadav, Amrendra Singh, et al., (2022)	Trusted NodeConsensus Algorithm (TNCA)	The proposed Trusted Nodes Consensus Algorithm (TNCA) reduces the duration required to fresh a node to the blockchain while requiring fewer communication than the current PoW approach.	All of this offers a Trusted Node-Consensus Algorithm (TNCA) based on the workers security model, reducing the processing cost involved in announcing the fresh block. The wished-for approach - trusted node consensus algorithm requires lesser duration to get the item to the blockchain, and message transmission of every agreement takes 58.94% less time than the old-style Proof-of-Work (PoW) approach and 26.44% less time than the prior enormous quantity way.	There will be no general or uniform chain infrastructure in the future. Maintaining these massive blockchains and executing effective search operations necessitates using appropriate search methods.

7	Digital Ledger Technology Based Real Estate Transaction Mechanism and Its Block Size Assessment. Singh, Nikita. (2019)	*time slice based fair leader determination algorithm*	The work offers a web-based interface for user inquiries and performs a query attempt to find analysis.	The suggested distributed and decentralized architecture protects against such invasive behavior, which is compensated for by the democratic majority attained in the consensus process for every transaction and inspection request.	If a small quantity of contacts occurs in a particular period and the period required by mineworkers to verify these contacts exceeds the tolerance edge, the chunk dimensions ought to be increased.
8	Augmented System for Food Crops Production in Agricultural Supply Chain Using Blockchain Technology. S, Dayana D., and Kalpana G. (2022)	Smart contracts and Trust based farming system.	They were designed to generate profits for all companies. Even though Network professes to be unbiased, Agri Assurance assures that small growers earn limited compensation.	This method makes big promises about food security by emphasizing the provenance of agricultural product suppliers and farm production clearance. A safeguard is in existence to prevent the source of the infection from becoming recognized.	When a customer scans a QR code,the agricultural activities, marketing materials, provenance information, and sensitive data may be tracked. In addition, by employing analytical approaches, the price of Bitcoin may be projected.
9	Distributed Ledger Technologies and Their Applications: A Review. Soltani, Reza, et a., (2022)	Smart Contract and Consensus algorithm.	To investigate if distributed ledger technology may be used instead of standard computing approaches in other domains	Tangle is nearing adulthood amongst examined technologies because of its unique characteristics and architectural concentration on IoT	Further, numerous DLTs, like Sidechain, Holochain, and Hashgraph, remain in their adolescence, and we anticipate

				networks.	significant research in this field in the next years.
10	Distributed Ledger Technologies Consensus Mechanisms. Marchionni, Pietro. (2018)	A consensus algorithm, Hashgraph, Tangle, Blockchains, Side Chain, and Holochain.	In industries such as insurance, these innovations can bring numerous advantages when combined with old ways; although they are still in the initial phases of totally replacing conventional methods, they must be equipped to concentrate on the distinctive features of each industry.	To determine the effectiveness of DLT in issue resolution, the most often utilized and commented applications are chosen.	Furthermore, it is projected that many programs would leverage DLT-based solutions to deal with conventional system challenges such as one single point of failure, data protection, confidentiality, and visibility.

VI CONCLUSION

Blockchain is a type of ledger employed to preserve records in a dispersed environment. We additionally defined the distinctions between both Blockchain and Bitcoin. The method allocates a similar time to each miner for block generation. Varies from one node is constructing blocks, the remaining peers should agree on the legality and creativity of the newly generated block. The paper has outlined blockchain and discusses how it is used in conjunction with related advancements to improve various sectors. As a result, the land registration process must be digitized, necessitating a safe, efficient, and decentralized solution with the help of blockchain consensus algorithms. As a consequence, investigators are becoming interested in a cryptocurrency policy based on Distributed Ledger Technology (DLT) to implement several budgetary and e-governance programs. A significant amount of study is still required to understand the potential of blockchain and its potential uses fully. Blockchain-based tenders are gaining popularity, and we want to do meticulous research in the forthcoming.

REFERENCE

[1]. Li, Boyang, et al. “A Collaboration Strategy in the Mining Pool for Proof-of-neural-architecture Consensus.”

Blockchain: Research and Applications, vol. 3, no. 4, Elsevier BV, Dec. 2022, p. 100089. Crossref, https://doi.org/10.1016/j.bcra.2022.100089.

[2]. Hafid, Abdelatif, et al. "New Mathematical Model to Analyze Security of Sharding-Based Blockchain Protocols." IEEE Access, vol. 7, Institute of Electrical and Electronics Engineers (IEEE), 2019, pp. 185447–57. Crossref, https://doi.org/10.1109/access.2019.2961065.

[3]. Downey, Liang Xi, et al. "Blockchain for Business Value: A Contract and Work Flow Management to Reduce Disputes Pilot Project." IEEE Engineering Management Review, vol. 46, no. 4, Institute of Electrical and Electronics Engineers (IEEE), Dec. 2018, pp. 86–93. Crossref, https://doi.org/10.1109/emr.2018.2883328.

[4]. Solanki, Madhav Singh. "'Overview of Blockchain Technology: Consensus, Architecture, and Its Future Trends.'" International Journal of Innovative Research in Computer Science & Technology, Innovative Research Publication, Nov. 2021, pp. 47–51. Crossref, https://doi.org/10.55524/ijircst.2021.9.6.11.

[5]. Ometov, Aleksandr, et al. "An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends." IEEE Access, vol. 8, Institute of Electrical and Electronics Engineers (IEEE), 2020, pp. 103994–4015. Crossref, https://doi.org/10.1109/access.2020.2998951.

[6]. Arora, Priyanka, and Ritu Nagpal. "Blockchain Technology and Its Applications: A Systematic Review of the Literature." SSRN Electronic Journal, Elsevier BV, 2022. Crossref, https://doi.org/10.2139/ssrn.4121824.

[7]. Yadav, Amrendra Singh, et al. "Distributed Ledger Technology-based Land Transaction System With Trusted Nodes Consensus Mechanism." Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 8, Elsevier BV, Sept. 2022, pp. 6414–24. Crossref, https://doi.org/10.1016/j.jksuci.2021.02.002.

[8]. Singh, Nikita. "Digital Ledger Technology Based Real Estate Transaction Mechanism and Its Block Size Assessment." International Journal of Blockchains and Cryptocurrencies, vol. 1, no. 1, Inderscience Publishers, 2019, p. 1. Crossref, https://doi.org/10.1504/ijbc.2019.10021397.

[9]. S, Dayana D., and Kalpana G. "Augmented System for Food Crops Production in Agricultural Supply Chain Using Blockchain Technology." International Journal of Advanced

Computer Science and Applications, vol. 13, no. 4, The Science and Information Organization, 2022. Crossref, https://doi.org/10.14569/ijacsa.2022.0130468.

[10]. Soltani, Reza, et al. "Distributed Ledger Technologies and Their Applications: A Review." Applied Sciences, vol. 12, no. 15, MDPI AG, Aug. 2022, p. 7898. Crossref, https://doi.org/10.3390/app12157898.

[11]. Marchionni, Pietro. "Distributed Ledger Technologies Consensus Mechanisms." SSRN Electronic Journal, Elsevier BV, 2018. Crossref, https://doi.org/10.2139/ssrn.3389871.

[12]. Solanki, Madhav Singh. "'Overview of Blockchain Technology: Consensus, Architecture, and Its Future Trends.'" International Journal of Innovative Research in Computer Science & Technology, Innovative Research Publication, Nov. 2021, pp. 47–51. Crossref, https://doi.org/10.55524/ijircst.2021.9.6.11.

[13]. Gemeliarana, I. Gusti Ayu Kusdiah, and Riri Fitri Sari. "Evaluation of Proof of Work (POW) Blockchains Security Network on Selfish Mining." 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), IEEE, Nov. 2018. Crossref, https://doi.org/10.1109/isriti.2018.8864381.

[14]. Yang, Runkai, et al. "On Selfholding Attack Impact on Imperfect PoW Blockchain Networks." IEEE Transactions on Network Science and Engineering, vol. 8, no. 4, Institute of Electrical and Electronics Engineers (IEEE), Oct. 2021, pp. 3073–86. Crossref, https://doi.org/10.1109/tnse.2021.3103558.

[15]. Nguyen, Cong T., et al. "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities." IEEE Access, vol. 7, Institute of Electrical and Electronics Engineers (IEEE), 2019, pp. 85727–45. Crossref, https://doi.org/10.1109/access.2019.2925010.

[16]. Keenan, Thomas P. "Alice in Blockchains: Surprising Security Pitfalls in PoW and PoS Blockchain Systems." 2017 15th Annual Conference on Privacy, Security and Trust (PST), IEEE, Aug. 2017. Crossref, https://doi.org/10.1109/pst.2017.00057.

[17]. Alsunaidi, Shikah J., and Fahd A. Alhaidari. "A Survey of Consensus Algorithms for Blockchain Technology." 2019 International Conference on Computer and Information Sciences (ICCIS), IEEE, Apr. 2019. Crossref, https://doi.org/10.1109/iccisci.2019.8716424.

[18]. Cong An, An, et al. "Building a Product Origins Tracking System Based on Blockchain and PoA Consensus

Protocol." 2019 International Conference on Advanced Computing and Applications (ACOMP), IEEE, Nov. 2019. Crossref, https://doi.org/10.1109/acomp.2019.00012.

[19]. Xu, Chenhao, et al. "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things." IEEE Internet of Things Journal, vol. 9, no. 6, Institute of Electrical and Electronics Engineers (IEEE), Mar. 2022, pp. 4371–84. Crossref, https://doi.org/10.1109/jiot.2021.3103275.

[20]. Jalalzai, Mohammad M., and Costas Busch. "Window Based BFT Blockchain Consensus." 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, July 2018. Crossref, https://doi.org/10.1109/cybermatics_2018.2018.00184.

[21]. Anupama, B. S., and N. R. Sunitha. "Analysis of the Consensus Protocols Used in Blockchain Networks – an Overview." 2022 IEEE International Conference on Data Science and Information System (ICDSIS), IEEE, July 2022. Crossref, https://doi.org/10.1109/icdsis55133.2022.9915929.

[22]. Singh, Saurabh, et al. "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network." IEEE Access, vol. 9, Institute of Electrical and Electronics Engineers (IEEE), 2021, pp. 13938–59. Crossref, https://doi.org/10.1109/access.2021.3051602.