Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.025516
Article

Tech Science Press

Proof-of-Improved-Participation: A New Consensus Protocol for Blockchain Technology

N. Anita*, M. Vijayalakshmi and S. Mercy Shalinie

Thiagarajar College of Engineering, Madurai, 625015, India
*Corresponding Author: N. Anita. Email: anita@student.tce.edu
Received: 26 November 2021; Accepted: 21 February 2022

Abstract: The Internet of Things (IoT) is converting today's physical world into a complex and sophisticated network of connected devices on an enormous scale. The existing malicious node detection mechanism in traditional approaches lacks in transparency, availability, or traceability of the detection phase. To overcome these concerns, we provide a decentralized technique using blockchain technology. Despite the fact that blockchain technology is applicable to create that type of models, existing harmony set of instructions are susceptible to do violence to such as DoS and Sybil, making blockchain systems unfeasible. Here, a new Proof-of-Improved-Participation (PoIP) harmony instruction was suggested that benefits the participation rules to select honest peers for mining while limiting malicious peers. Under an evaluation the PoIP outperforms the Proof-of-Work (PoW) instructions are demonstrated, Proof of Stake (PoS) instructions in terms of energy consumption, accuracy, and bandwidth. To compare the three consensus protocols with respect to efficiency, we build a lightweight mining model and find that PoIP consensus has greater efficiency than PoW and PoS. PoIP has 25% lower attack risk than existing consensus. As a consequence, our suggested methodology can provide the needed security with minimal attack risk and high accuracy, according to the analysis results. As a result, suggested consensus is more efficient than existing methods in terms of block generation time. Hence we suggest that suggested consensus is very suitable for IoT-based applications especially in healthcare.

Keywords: Blockchain; confidentiality; proof-of-improved-participation consensus; security

1 Introduction

Blockchain is a distributed technology proposed by cryptocurrency for a digital cash system that does not rely on a trusted third party [1]. Blockchain technology has enormous features, such as accountability, confidentiality, quality management, global peer-to-peer transactions, and decentralization [2]. There are different kinds of blockchain networks: public, private, and consortium blockchain [3]. Due to the permissionless concept of modern blockchain, anybody in the network can read or write data on the blockchain, and anyone can take part in the consensus mechanism. Ethereum and bitcoin are types of

permissionless blockchains that use the PoW and PoS consensus mechanisms [4]. Everyone can see the information in the blockchain, but the data is not modified.

Blockchain is a distributed database inside for all dedicated connections is listed in a sequence of connection blocks, which grows chronologically when new blocks are added to it. Consequently, blockchain technology is applied in different fields of applications, including cyber security, IoT, supply chain, big data, identity management, financial management, health care, and e-government [5]. The most salient uniqueness of a block-chain network be the agreement method. In a blockchain network, blocks are verified, distributed, simulated, and created across all nodes in blockchain networks using a peer-to-peer and decentralized consensus mechanism. Consensus ensures the newly added node in the blockchain network is agreed upon by all the nodes in the blockchain.

Fortunately, a current consensus in blockchain systems is vulnerable to attacks as well. A well-known attack identified as the DAO attack happened in June 2015. The DAO attack was carried out by a group of attackers who broke into the Ethereum system and tried to steal the crypto tokens ETH [6]. An attacker could deploy a wide range of attacks (e.g., Malicious Node Injection Attack, Warm hole Attack, Denial-of-Service (DoS), Data Spoofing, 51% attack, etc.) from the Internet or the internal network of an organization by leveraging it [7]. The working proofs are the first suggested consensus for bitcoin in the permissionless blockchain. But it requires a lot of energy and time to make a decision. Several blockchain-based alternative solutions to the working proofs have already been planned; The working proofs are the most well-known, even if it is not without flaws. . It have a few cons, which are discussed further in this paper; Hence PoW is not recognized as reliable. Existing consensus has drawbacks and does not meet all of the blockchain experimental results [8]. As a result, it is essential to create a new consensus protocol that tackles the problems of traditional consensus mechanisms while also providing high efficiency, scalability, and decentralization.

The goal of this paper is to provide a lightweight consensus method for IoT systems. The PoIP consensus protocol aims to develop a consensus mechanism solution that uses less energy and is more secure than standard blockchain consensus.

Here are the main tasks of the defined modules:

- Here we suggest an improved method to further enhance the blockchain design required to verify different types of different guarantee systems in a particular ledger.
- It is very suitable to identify different types of workers working in a mine. That is, its primary mission is to find honest and skilled miners working there. And its special feature is that it is also used to detect malicious workers.
- Furthermore this improved and improved method suggested in this series works with consensus process so this method provides special components to integrate it with functions similar to Ethereum architecture.
- Micro functions based on analytics further enhance this and provide better improvements in terms of protocols.
- It is also set in block capacity which helps to further simplify the operations based on the appropriate timing.

The rest of the work is organized into 6 sections: Section 2 discusses the motivation and existing consensus mechanisms, as well as their limitations. Section 3 describes the literature survey. The working process of PoIP and the lightweight mining process are described in Section 4. Section 5 includes an analysis and evaluation of the consensus. In Section 6 we also explain in detail the future scope of this Quran and the modules of advanced systems, along with the complex mechanisms and possibilities that we have suggested. We finally conclude this with the drafts of this updated module in Section 7.

2 Preliminaries

This section describes the motivation and basic building blocks of the suggested authentication scheme for better understanding. Blockchain and Consensus are the two basic fundamental concepts needed to understand the suggested work.

2.1 Motivation

For millions of nodes validating a transaction on the blockchain network, a consensus is essential to run the system smoothly [9]. The Blockchain network is trustless because of the consensus mechanism, so nodes might not trust each other, but they can trust the consensus algorithms that run source code written on it. Existing consensus mechanisms such as PoW and PoS have drawbacks regarding resource usage and bandwidth requirements [10]. This paper presents a work of fiction harmony algorithm called work of Proof-of-Improved-Participation (PoIP) consensus, which introduces an access control authentication mechanism to substitute PoW and PoS for resource-constrained devices while maintaining high security. Many issues that arise in the current blockchain consensus are discussed below.

- How to choose an honest miner as dynamic is the main issue in the permissionless blockchain consensus mechanism.
- How to increase the speed of transaction throughput is one of the vital issues of blockchain.
- High storage overhead occurs due to continuous block creation and each block stores all data in the entire blockchain.

In this suggested method, we dedicate our efforts to addressing the aforementioned permissionless blockchain challenges.

2.2 Consensus

2.2.1 PoW

The process called PoW is a very important concept in blockchain classification. This is the only way to predict random user volumes on a particular network module. That is, a group of users compete with each other to complete a variety of transactions on a network. This process creates a tunnel-like structure there. Here a user with a higher set of powers manipulates the advanced results for his cryptographic puzzle and finishes defining the exact need for that puzzle. Its choice shows him as the winner. Thus he gets various rewards. Similarly the various blocking and decision-making methods available in the Ethereum network are defined in terms of the PoW process. Its limitations are as follows: 1. Electric waste is seen as the most complex and insurmountable major problem in these blockchain packages. Due to this more energy is expended while performing the calculation tasks. This leaves users on that network with the right amount of data and resources. 2. Excessive attacks that develop on a small network make its time change nostalgia so much less. These help manage the pool of data on which some of the pools in the mining system and its enhanced games are based [11]. Its resources are even greater as its upgrade procedures are managed by computers. Its accuracy is high.

2.2.2 Proof of Stake (PoS)

Among the most commonly used consensus algorithms in blockchain seems to be PoS. In the PoS consensus mechanism, block creators act as validators rather than miners in PoW. The validators are chosen using a variety of random selection methods and stake in the currency. Every validator is allowed

to create a block that saves energy and time. Validators are compensated based on a percentage of a transaction fee [12]. Since there is no incentive mechanism, all stakes is fashioned next to the initial stage, in addition to the amount on no report transformations.

- Limitations of PoS

Work of Stake structure is a reduced amount of protected than Proof-of-Work systems, more than ever when there are no punishments. Because a Proof-of-Stake algorithm has never had a mandatory policy for the hash produced, the system is vulnerable to attack [13].

3 Related Work

A narrative Work-of-Block and Trade (PoBT) harmony algorithm is suggested for an IoT blockchain-based framework that validates blocks and trades [13]. A ledger distribution mechanism is used to reduce the IoT memory requirements of peers. As a result, the framework significantly improved as a whole performance in terms of communication time, memory, and bandwidth requirements. The encryption process in Proof-of-Work (PoW) is developed to be a resource consumption. A green blockchain framework is proposed to optimize computational complexity and storage complexity. The authors have imposed a consensus mechanism Proof-of-collaboration (PoC) [14]. Additionally, edge devices begin competing for a new generation of blocks by transmitting Integrated Incentive (*II*) rather than solving mathematical puzzles. Proof of stake uses an internal resource that is the balance of the coin within the blockchain to secure the blockchain [15]. Security methodology in PoS requires the value of the stake.

Suggested authentication method uses external resources for the computation process [16]. The encryption process in Proof-of-Work (PoW) is developed to be a resource consumption that uses external resources, and PoW is vulnerable to severe attacks [17]. As a cryptographic authentication mechanism Proof-of-Authentication (PoAh) is designed for blockchain-based resource-constrained IoT. The performance of the suggested system is measured in three steps: theoretical validation, simulation results, and test bed deployment. This consensus secures systems while also ensuring scalability and sustainability. In repute-based consensus protocol, two approaches are intended to help the blockchain network reach a consensus quickly [18]. Devices in the reputed model with a high repute value produce blocks more efficiently. The effectiveness is proven by the fact which collaborative behavior is rewarded and no cooperative behavior is punished.

Reputation scheme is designed to identify normal nodes and malicious nodes to participate in the network [19]. A credit-based incentive mechanism is proposed to reward honest nodes. An author in [20] proposes Proof of Consensus (PoC) for public blockchain based on contribution value calculated using user behaviors and actions in the blockchain. The node with the highest contribution value is allowed to create a new block.

Existing blockchain-based solutions have some serious flaws that make them unsuitable for dealing with secure IoT. Issues: Since IoT systems are dynamic and not all computers can run the same data encryption at the required speed, high processing power, and time required completing data encryption for Blockchain-based IoT systems. The ledger must be stored on each node in blockchain will increase storage size. In the suggested PoIP scheme, every new block is validated through a variable number of nodes based on simple rules which are less computation-intensive but ensure high security of the same level. Tab. 1. Represent the summarization of related work.

Table 1: Summarization of existing work

	Consensus	Security	Privacy	Lightweight mining	Less computational overhead	Less attack risk possibility	Less block creation time
[13]	PoBT	✓		✓	✓		
[14]	PoW	✓	✓				
[15]	PoC			✓		✓	
[16]	PoS		✓				✓
[17]	PoW	✓		✓	✓		
[18]	PoAh		✓		✓	✓	
[19]	RPoS				✓		✓
[20]	PoC		✓			✓	
Proposed	PoIP	✓	✓	✓	✓	✓	✓

4 Proposed Protocol

Participation works by choosing a trustworthy miner to dig for the botch with arbitrary complexity that is additional efficient and straightforward than current blockchain consensus mechanisms.

In contrast to previous connected works, the estimation techniques intended pro the originator conviction rate and valuator conviction rate are developed in our work. Through the progress of a conviction haphazard range method, some responsible miners may subsist singled out random to function as originators or validators in a block generation.

4.1 Honest Miner Selection

The miner may send genuine (Gi) or malicious (Mi) block proposals in the blockchain. The value of is (Gi) increased by 1 when it is validated as malicious by validators. If the real determination exists amplified with 1, the conviction rate of miner through block proposer BTi is calculated as follows:

$$BTi = \begin{cases} \dfrac{Fi * \lambda + Gi - Mi}{Gi + Mi + 1} \; if \;\; Mi > Gi \end{cases} \tag{1}$$

where Fi is fault tolerance to the miner behavior to the block proposal and λ is the threshold value. Fault tolerance is calculated as follows:

$$Fi = \begin{cases} 1, \; Mi = 0 \\ 0, \; Mi > 0 \end{cases} \tag{2}$$

4.2 Proof-of-Improved-Participation (PoIP)

In the suggested work, new block creation is associate near the resolution, that is distinct as a instance because the final transform. The suggestions have the subsequent 3 basic policy, supported via and, toward ensure a sustainable blockchain:

Rule 1:

The mining in the suggested PoIP be improved and dissimilar as of the traditional mining equation in the blockchain. The mining during PoIP is prejudiced by means of non-static complicatedness that is unusual since a range of contributor. This has the subsequent appearance.

To discover n,

$$KECCAK(KECCAK256(c.n)) < destination$$

Somewhere "." is represents a sequence concatenate operative, and *c*represents the contents of a new block. The smaller destination means the mining difficulty is more.

Rule 2:

Block developers be required to recompense fees on behalf of themselves as erect a fresh slab. The construction of the new slab expenses the *II* of developer and gives the similar quantity of *II* as come back, i.e., the expenses alters the *II* of a developer, but the developer does not lose*II*. An incentive for developer calculated as follows:

$$Incentive = II \times c \times .005 \tag{3}$$

Rule 3:

Block developer must have $C\varepsilon[\eta, \rho]$, where η is calculated by

$$\eta = \frac{n}{\Phi} \text{ and } \Phi = 5\eta \tag{4}$$

The value of Φ can varies according to the participation claim. The higher in Eq. (4) makes the competitors more powerful, and the lower reduces the defense of the blockchain. The recommended value of Φ is 0.50.

The requirement of the calculated possessions $\Re cr$ is lower than existing consensuses such as PoW and PoS. According to rule 1, the computational requirement of PoIP is calculated as

$$\Re cr = \frac{destion_{\max}}{II \times R \times destination} \times 2^{32} \tag{5}$$

Limitation on rule2, only the recipient of participant can clear its R. If the edge connection fails to suggest a block when it competes, its R is retained. It tends to give its superiority for the suggested block in the next round of competition. Conversely, with PoW and PoS, unsuccessful nodes spend all of its computation. Sustained by the participation rules, the procedure for some of the improved methods suggested here are clearly shown in Fig. 1. Method 1- further illustrates the use of similarities to prototypes implemented in its PoIP mode.

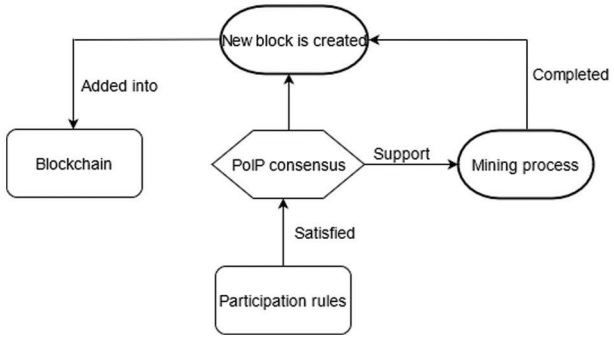

Figure 1: Procedure of PoIP consensus

The data transmission process is a procedure in which trusted nodules collect the information desirable to be development since the device and executes slab deep-mining, slab deep-validation, and keeps

modernize the register in the complete network. Primary, the trusted nodule assemble intellect information beginning grassland policy and moreover controls orders from organize at preset time intervals *(t)*. The blockchain node processes data collected for transactions and needs to perform a lightweight block mining function. The process of lightweight block mining management consists of two procedures. First, a mix up utility is chosen by contrast the numeral of transactions to the entrance values (λ_1, λ_2). Second is by constantly monitoring the hash value here it is possible to minimize the hassle of its data processing tunnel and create any conditions for its nodes to communicate ($Hash(M_i)$, $onblock(M_i)$). Generally, this is the same as the "PoW" procedure. While the accurate node is established, the blockchain nodule requests corroboration of the slab to other nodule in the block-chain system (Broadcast(M_i)) and remains for a answer enclose the justification answer.

Its synchronization functions are checked by comparing the hash value with the value at different nodes in the previously classified mine block. It's not just about calculating the hash value. If the data gives positive results when the synchronization process is performed correctly, that result is sent immediately. Also the hash ratings in the previous post will be updated regularly.

Algorithm: Lightweight block mining algorithm using PoIP Consensus

1. Procedure Mining Transactions
2. Initialize(M_i)
3. ($M_i.prevhash \leftarrow previoushash$)
4. $M_i.hashvalue \leftarrow hash$
5. $M_i.nonce \leftarrow 0$
6. *While* $hash(M_i) < difficulty$ then
7. $M_i.nonce++$
8. $\upsilon \leftarrow (M_i)$
9. *If* $\upsilon \leftarrow true$ then
10. *Return true*
11. *Else*
12. *Return false*
13. *If* $C\varepsilon[\eta, \rho]$
14. Incentive given to block developer
15. Else
16. Incentive is not given
17. End Procedure

5 Evaluation Results

Various data based on the structure and protocols of the mines with different estimates are analyzed here. Here it has been conducted more than 100 times using the Python model. It is designed taking into account the selection methods of the mine, its ability to generate different types of design blocks, and the general expended power of the calculation. The structural functions of this proposed method are described in terms of mini-net development.

5.1 Performance Evaluation

Some estimates are proposed here based on the performance of the different types of mines presented here and its different potential. Here is how the methods of implementing these structures work. The existing mini-net simulator [21] analyzes existing problems and guides the data needed to implement the IoT system. The Pyethereum Test Tool [22] is also used to further improve and validate the functionality of the blockchain system designed here. In the next 90 s, 1852 transactions took place. 10 more developments are estimated here. Thus its accuracy will be calculated.

5.1.1 Consensus Accuracy

Here are some tips based on the initial creation described. That is, when some mines select miners the behavior of the anodes there will be monitored based on certain vote ratios. The mines will be further upgraded during the alternative definition of some of the blocks on which it is based. Some of the touches that take place there will be further enhanced as the results of this analysis are generated in line with its enhanced accuracy. Some of the data on which those excavations are based will be subjected to further analysis and its accuracy will be further improved. When at least 50% of the miners are involved in the work proposed here an agreed block terminal is created at that location. The different terminals that form here are classified as 100 and 500. Thus the number of terminals there is constantly increasing. The minor module categorization with 500 terminals is depicted in Fig. 2 and it depicts the gain in velocity based on positive tunneling. This reduces changes in the base processor of the volume terminals of the existing data processors when it is less than 50%. Its malfunctions greatly reduce the accuracy associated with it. Fig. 3 shows that the suggested technique is successful and efficient in delivering safe data exchange and access control solutions for the IoT-based Supply chain.

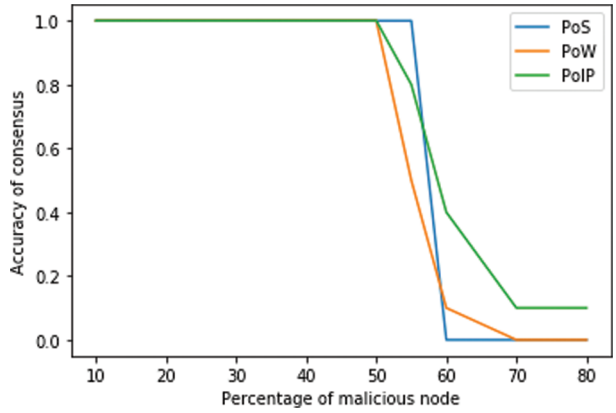

Figure 2: Accuracy comparison of PoW, PoS and PoIP

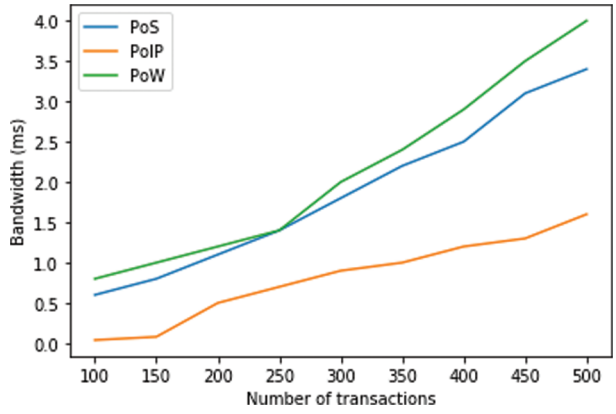

Figure 3: Bandwidth comparison of PoW,PoS and PoIP

5.1.2 Attack Risk Factor

The stake value (*Sv*) is calculated using the actual cost of various values estimated from exchanges as follows

$$Sv = \sum_{i=0}^{n} CiRi \tag{6}$$

where *Ci* is the current value of a token in the staking queue, that is modified every block interval.

Ri is the total number of tokens staked during the current block interval and *n* is the number of tokens adequate for mining the transactions. Agreement nodes in PoIP are referred to as miners since they are responsible for validating, confirming, and constructing honest blocks. Miners can invest their original tokens or receive tokens assigned by other existing shareholders. To calculate the security risk of PoIP systems, we assume that the number of different tokens in the stake pool is same and add a "generic" token $\tilde{T}$, its price is the total of a token values in the PoIP staking blacklist Eq. (6).

$$\tilde{T} = \sum_{i=0}^{n} Ti \tag{7}$$

where n is number of tokens used for computation in PoIP. $Ti \approx (\lambda, \delta^2)$ represents the value of token i in the PoIP stake blacklist where $\tilde{\lambda} = n\lambda$ and $\tilde{\delta} = n\delta^2$. To initiate an attack on the PoIP blockchain system, intruders need possess a sufficient amount of $\tilde{\lambda}$ and hold the majority of stake value. The probability density function of $\tilde{\lambda}$ is calculated as follow

$$f_{\tilde{\lambda}}(y) = \frac{1}{\tilde{\delta}\sqrt{2\pi}} \exp\left\{\frac{(y-\tilde{\lambda})}{2\tilde{\delta}^2}\right\} \tag{8}$$

The price ρ for the associated security risk element $\tilde{\lambda}$ is computed as follows:

$$\begin{aligned} P(0 \le \tilde{\lambda} \le \rho) &= \int_0^{\rho} f_{\tilde{\lambda}}(y)dy \\ &= \int_0^{\rho} \frac{1}{\sqrt{n\delta}\sqrt{2\pi}} \exp\left\{-\frac{(y-n\lambda)^2}{2n\delta^2}\right\} \end{aligned} \tag{9}$$

An attacker can initiate an attack at the lowest possible cost, that is less than or equivalent to λ, i.e., $\rho \le \lambda$. As a result, an attack on PoIP network is impossible. Fig. 4 shows the attack risk possibility of presented consensus with existing work.

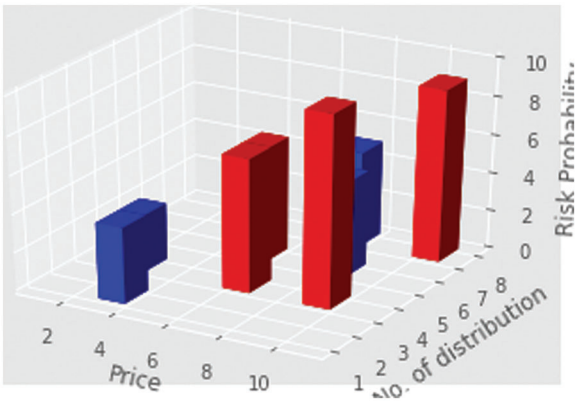

Figure 4: Risk probability

5.1.3 Efficiency

The comparative result of PoC, PoIP, and PoX in terms of block generation effectiveness is shown in Fig. 5. Because the duration to obtain the nonce value in PoX is unpredictable, the efficiency in each consensus round differs significantly. In PoC, the time cost for block production is usually 0 and remains constant across the rounds of consensus. It is due to the fact that under PoC, a node required to produce a new block is decided by evaluating the trust values of the nodes inside the distributed ledger.

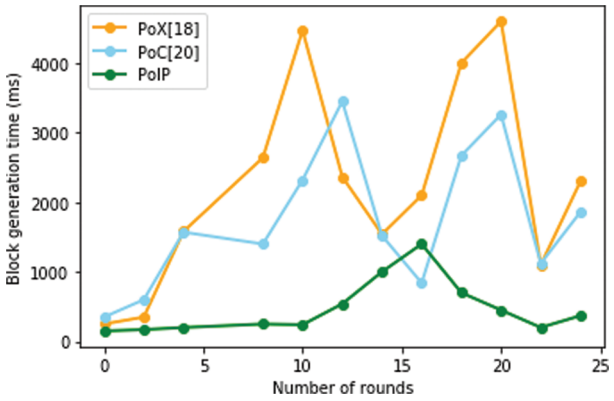

Figure 5: Comparison of efficiency on block generation time

PoIP is 25% less vulnerable to attack than the PoS consensus process. Tab. 2. shows the key differences between the consensus protocols. We introduce the results as follow

Table 2: Comparison of three protocols: PoW, PoS, PoIP

Features consensus	Scalability	Latency	Resource usage	Energy consumption	Robustness	Transactions per second (TPS)
PoW	Low	Low	High	High	Low	7
PoS	High	High	Low	High	Low	30–40
PoIP	High	Low	Low	Low	High	>50

Scalability: PoW's initial block size is 1 MB, which is insufficient to support hundreds of transactions. PoS consensus is substantially highly scalable than PoW but not as much as PoIP. Many of the scalability concerns of PoW and PoS were addressed by obtaining high latency with minimal computing, storage, and connectivity. These PoIP provide consistency because validators are picked at random per round and complete transaction even if the block does not become a part of the blockchain.

Latency: PoIP provides two possible ways of minimizing latency compared to existing scheme: raising block size to allow larger transactions as well as decreasing difficulty for lightweight mining process.

Resource usage: In PoW, the competitor who finds the hash value that is lower than predicted objective does have the ability to construct a new block and get reward. To reduce excessive resource utilisation of PoW, PoS offers token system which is product of unused coins and period of winning time and current time. Instead of these functions, PoIP Transactions are compared to a threshold value and evaluated to ensure that its nonce satisfies overall target difficulty in order to reduce high resource utilisation.

Energy Consumption: PoW consensus necessitates the use of computational power to solve a mathematical challenge. PoS miners rely on stake for packing competition; hence it consumes less energy

than PoW but more than PoIP consensus. The presented agreement reduces energy consumption than the existing system because of its easy validation method that does not need additional computational puzzle.

Robustness: In a bitcoin system, PoW is becoming centralized because there are fewer mining pools, posing a significant danger of a 51 percent assault on the network. As we indicated in Section 2.1.2, PoS consensus is vulnerable to both DoS and 51 percent attacks. This prompted us to propose PoIP, which would strengthen the blockchain system against such threats.

TPS: As indicated in Table1, the transaction rates of PoIP consensus is much more efficient than the existing blockchain consensus. PoIP alleviates the burden of both ledger storage and block mining computations in order to create a lightweight blockchain network.

6 Discussion and Future Work

Evidence generated on the basis of the improved mine is deemed inappropriate to calculate its internal values and external values. But its different ends are designed with the ability to give different mines essential contact. It works to increase security in that blockchain, because the most sophisticated mining nodes operate within the set of data managed here, its data management methods are surrounded by complex systems. Thus the systems of the nipples are then connected into various scatterings. This connection further strengthens the unpredictable security structures [23]. The PoIP method is best suited for managing the upgraded data in blockchain and enhancing security nodes. Thus the primary token does not take any value. PoIP is recommended for efficient handling of blocks of data and pointers designed based on PoW mining. Its development will effectively manage even the toughest and most complex crypto challenges.

7 Conclusion

In this paper, we designed a PoIP consensus protocol in a public blockchain. We aimed to provide a new module for the consensus mechanism and demonstrate the potential for maintaining authenticity in consensus. In this model, honest miners are encouraged while malicious miners are discouraged, thereby improving the authentication of the consensus protocol. Participation appears to have overcome the restrictions of Proof-of-Work and Proof-of-Stake strategies. The experimental results show that our method performs well in terms of efficiency and bandwidth. Participation has some limitations, such as multiple block creation and multiple miner selection for a blockchain transaction; however, it is a significant improvement over the current system.

Funding Statement: The authors received no funding for this study.

Conflicts of Interest: The authors state that they have no conflicts of interest to report in relation to this work.

References

[1] Y.Yuan and F. Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *Ieee Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, 2018.

[2] J. H. Ryu, P. K. Sharma, J. H. Jo and J. H. Park, "A Blockchain-based decentralized efficient investigation framework for IoT digital forensics," *The Journal of Supercomputing*, vol. 75, no. 8, pp. 4372–4387, 2019.

[3] P. P. Ray, D. Dash, K. Salah and N. Kumar, "Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases," *IEEE Systems Journal*, vol. 15, no. 1, pp. 85–94, 2020.

[4] D. D. F. Maesa and P. Mori, "Blockchain 3.0 applications survey," *Journal of Parallel Distributed Computing*, vol. 138, pp. 99–114, 2020.

[5] H. Chen, M. Pendleton, L. Njilla and S. Xu, "A survey on ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Computing Survey*, vol. 53, no. 3, pp. 1–43, 2020.

[6] F. Q. Liao, J. F. Wang and J. Shen, "BCDP: A blockchain-based credible data publishing system," *Journal of Internet Technology*, vol. 20, no. 2, pp. 323–331, 2019.

[7] N. Anita and M. Vijayalakshmi, "Blockchain security attack: A brief survey," in *2019 10th Int. Conf. on Computing, in Communication and Networking Technologies (ICCCNT)*, Kanpur, India, pp. 1–6, 2019.

[8] S. Naz and S. U. -J. Lee, "Why the new consensus mechanism is needed in blockchain technology?" in *2020 Second Int. Conf. on Blockchain Computing and Applications (BCCA)*, Antalya, Turkey, pp. 92–99, 2020.

[9] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," *Journal of Industrial Informatiom Integration*, vol. 13, pp. 32–39, 2019.

[10] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun *et al.,* "A Proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services," *IEEE Tranactions on Service Computing*, vol. 12, no. 3, pp. 429–445, 2018.

[11] M. Baza, M. Nabil, M. M. E. A. Mahmoud, N. Bewermeier, K. Fidan *et al.,* "Detecting sybil attacks using proofs of work and location in vanets," *IEEE Transactions on Dependable Secure Computing*, vol. 19, no. 1, pp. 39–53, 2022.

[12] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang *et al.,* "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, pp. 480–485, 2020.

[13] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere *et al.,* "Interoperability and synchronization management of blockchain-based decentralized e-health systems," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1363–1376, 2020.

[14] M. Kamran, H. U. Khan, W. Nisar, M. Farooq and S. -U. Rehman, "Blockchain and internet of things: A bibliometric study," *Computers and Electrical Engineering*, vol. 81, pp. 106525, 2020.

[15] D. Liu, A. Alahmadi, J. Ni, X. Lin and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3527–3537, 2019.

[16] M. Á. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto and A. Kind, "PUF-Derived IoT identities in a zero-knowledge protocol for blockchain," *Internet of Things*, vol. 9, pp. 100057, 2020.

[17] D. Puthal, S. P. Mohanty, V. P. Yanambaka and E. Kougianos, "PoAh: A novel consensus algorithm for fast scalable private blockchain for large-scale IoT frameworks," arXiv Preprint, arXiv2001.07297, 2020.

[18] E. K. Wang, R. Sun, C. -M. Chen, Z. Liang, S. Kumari *et al.,* "Proof of X-repute blockchain consensus protocol for IoT systems," *Computers & Security*, vol. 95, pp. 101871, 2020.

[19] E. K. Wang, Z. Liang, C. -M. Chen, S. Kumari and M. K. Khan, "PoRX: A reputation incentive scheme for blockchain consensus of IIoT," *Future Genernation.*, *Computing Systems*, vol. 102, pp. 140–151, 2020.

[20] H. Song, N. Zhu, R. Xue, J. He, K. Zhang *et al.,* "Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection," *Information Processing & Management*, vol. 58, no. 3, pp. 102507, 2021.

[21] J. Cao, X. Wang, M. Huang, B. Yi and Q. He, "A security-driven network architecture for routing in industrial internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, pp. e4216, 2021.

[22] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang and K. -K. R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Transactions on Service Computing*, vol. 13, no. 4, pp. 625–638, 2020.

[23] N. Gajendran, V. Shanthi and M. Aalelai Vendhan, "Rejuvenation of online research interactive for a during COVID-19," *Indian Journal of Science and Technology*, vol. 13, no. 47, pp. 4603–4605, 2020.