BQBCC: Design of an Augmented Bioinspired Model for Improving QoS of Blockchain IoT Deployments via Context-based Consensus

Manisha Gokuldas Gedam[1]*, Swapnili Karmore[2], Waibhav Deogade[3]
[1] *Ph.D. Scholar: G. H. Raisoni University, Saikheda, manishagedam2007@gmail.com*
[2] *Associate Professor, Department of Data Science: GHRIET, Nagpur, swapnili.karmore@raisoni.net*
[3] *Lead Engineer II: Lululemon, Bengaluru, wdeogade@lululemon.com*

Article History

Article Submission
28 December 2022
Revised Submission
24 January 2023
Article Accepted
26 February 2023
Article Published
30 March 2023

Abstract

Blockchain-deployments are highly secure, but lack in terms of scalability due to exponential increase in mining delay w.r.t. chain lengths. To overcome these issues, researchers have proposes used for low-complexity mining, sharing techniques, and other machine learning optimizations. But these models either depend on underlying blockchain, or showcase larger computational delays, which limits their scalability levels. Moreover, most of these models do not consider consensus optimizations, which further limits their deployment capabilities for large-scale networks. To overcome these issues, this text proposes design of an efficient bioinspired model for improving QoS of blockchain IoT (Internet of Things) deployments via context-based consensus. The proposed model initially collects temporal mining performance from existing miner nodes, and deploys a novel Proof-of-Temporal Trust (PoTT) based consensus for validating responses of these miners. The PoTT Model uses temporal mining delay, energy consumed while mining, and throughput levels for selection of high-performance miners for processing block-addition requests. Requests approved by these miners are stored on a set of Bacterial Foraging Optimized (BFO) sidechains. These sidechains are automatically tuned based on spatial QoS performance of the network under real-time conditions. The BFO Model assists in segregating existing single-length blockchains into QoS-optimized sidechains. To perform this segregation, the BFO Model uses an exhaustive consistency metric that combines QoS & security levels that can be applied to specialized applications like Industrial IoTs. Thus, segregation into sidechains is done while maintaining high security under heterogenous attacks. Due to these optimizations, the model was able to reduce mining delay by 3.9%, reduce energy needed for mining by 2.5%, improve throughput by 4.5%, while maintaining high attack-detection efficiency under Sybil, Distributed Denial of Service (DDoS), and Masquerading attacks.

Keywords*- Blockchain, Quality, Service, Security, Temporal, Trust, Bacterial, Foraging, Optimization, Delay, Energy, Throughput, Attacks.*

I. Introduction

Blockchain technology makes it possible for data management systems to have both openness and security, making them applicable in a variety of settings [1, 2, 3]. When used for applications that generate massive volumes of real-time data, blockchain systems that store databases will need compliance with high quality of service (QoS) criteria (such as social networks, XR services, financial systems, and autonomous control). To fix the throughput problems that are brought on by the consensus mechanism, specifically blockchain-based Internet of Things (IoT) networks that have real-time Internet of Things (IoT) connection are needed [4, 5, 6]. Bitcoin and Ethereum, the two most popular blockchain systems, are only capable of handling three to four and fourteen transactions per second (TPS), respectively [7, 8, 9] via use of many-objective optimization algorithm based on the dynamic reward and penalty mechanism (MaOEA-DRP). This is insufficient to keep up with the rates of data creation that are associated with Internet of Things networks and credit card transactions. Proof-of-work, often known as PoW, is the mechanism of reaching consensus that is used by conventional blockchains [10, 11, 12] that deploy Sharding Hash Graphs (SHGs). The Proof-of-Work algorithm consumes a significant amount of power since miners are required to continuously conduct hash operations in order to solve mathematical puzzles. In addition, the average throughput of a blockchain network decreases as the number of nodes in the network rises. This is because an increase in the number of nodes causes an increase in both the cost of computation and the amount of time necessary to verify blocks. A blockchain solution that is more advanced than what is currently available is required in order to address the scalability problem. EOS [13, 14, 15] use a consensus mechanism known as delegated proof of stake (DPoS). This algorithm assigns the responsibility of mining to a select group of nodes. Sharding [16, 17, 18] was developed in order to boost the throughput of blockchains. The scalability of the blockchain technology and the security it provides are two more crucial qualities. It is possible for a group of malicious nodes to carry out a 51% attack if they have sufficient hashing power or voting rights to take control of the consensus process and change the data contained in the blockchain [19, 20]. A single-shard takeover assault is a kind of attack that may be used by a very small but well-organized group of malicious nodes to seize control of a blockchain network and alter its consensus rules [21, 22]. When consensus in blockchain networks is achieved by delegation or sharding, this is the scenario that arises (in which only chosen nodes participate in the consensus process). Even if malicious nodes do not control the majority of the network, an inaccurate block produced by a malicious block producer will be rejected by other honest nodes during the consensus process, and the block will not be added to the blockchain. This will occur even if the malicious nodes do not control the majority of the network. As a consequence of the fabrication of fraudulent blocks, trustworthy transaction ledgers are unable to be connected to the blockchain. This may lead to a large drop in the TPS or a database denial of service (DoS). The vast majority of existing blockchain solutions do not simultaneously care about scalability, security, and decentralization, despite the trilemma relationship between these three challenges. It is vital to evaluate all performance measures at the same time since improving the performance of one component of the blockchain may have a significant negative influence on the performance of the other components. In addition, there has not been a lot of research done on how to make blockchains more secure and efficient in the face of malicious nodes that disrupt consensus.

It has been shown that the scalability of these models is inferior owing to their reliance on the blockchain that serves as the underlying data structure or the occurrence of large processing delays. The vast majority of these models also ignore consensus optimizations, which severely restricts their usefulness in very extensive networks. In the next section of this paper, the author delves into the intricacies of a wide variety of blockchain-consensus models, from which parallel inferences may be made. In Section 3, we investigate how these issues may be handled by constructing a bio-inspired model for boosting the quality of service (QoS) of blockchain installations using context-based consensus. Specifically, we look at how this model might help improve the QoS of blockchain installations. In the fourth section, a number of simulations are run in order to test the performance of the design and compare it to other alternative consensus-optimization procedures. The conclusion of the article includes some closing thoughts regarding the proposed paradigm as well as some ideas for further refining the paradigm so that it may be used in real-time scenarios.

II. Literature Review for existing blockchain techniques

One of the main objectives of a number of research projects that have looked at the possible uses of blockchain technology is managing the enormous amounts of data and transactions that are produced by Internet of Things (IoT) applications in a range of businesses. Work in [1] demonstrate use of a consortium blockchain for energy trading in an industrial IoT scenario made use of a credit-based payment system as opposed to a cash-based one. In [3] introduced a novel resource exchange method based on cloud computing and using the blockchain. In their work [11], Singh et al. described a blockchain-based decentralized healthcare administration system. A secure device authentication solution based on blockchain technology was developed in [12] to guarantee privacy and security in cross-domain industrial Internet of Things networks. A decoupled blockchain solution was also proposed in [13] that can manage data from IoT health monitoring devices while maintaining data security. Work in [14] developed a fault-tolerant routing approach to autonomous Internet of Things security that makes use of machine learning. The use of cipher block chaining by the authors ensured the secrecy and validity of the data that was sent. To evaluate data blocks and offer dependable communication via a trust mechanism in 6G IoT networks, Haseeb and colleagues created a fault-tolerant supervised routing model in the study via Deep Reinforcement Learning (DRL) [15]. This was done to guard against malicious attacks on these networks.

Blockchain systems often use a wide range of distinct consensus mechanisms. Bitcoin employs a Proof-of-Work (PoW) consensus procedure [16]. A hashing algorithm is the foundation of this technique. On the other hand, since PoW requires so many hash operations, it has significant issues with the number of resources it consumes and the throughput per second (TPS) it can reach. Other consensus algorithms have been proposed as potential remedies for this problem, including practical byzantine fault tolerance (PBFT) and proof of stake (PoS). A vote consensus procedure is used to verify blocks using PBFT [17], one of the byzantine fault-tolerant algorithms. Even if PBFT might reduce pointless hash operations, a blockchain network's message complexity rises dramatically when there are a lot of nodes. Zilliqa handles transactions concurrently in addition to leveraging sharding technologies to increase TPS [8]. The two-phased consensus procedure and the added delay brought on by sharding both raise the prospect that a single shard takeover attack might compromise the network's security. Another solution to the scalability issues that afflict blockchains is the use of a delegated consensus mechanism, in which only a small number of nodes that have been designated to participate in the blockchain consensus process. For the purpose of carrying out the blockchain consensus procedure, EOS [23, 24, 25] chooses a certain number of validators in beforehand. Work in [26, 27, 28] introduced a PBFT-based proof of reputation consensus method for a blockchain-based energy trading system in electric cars (EVs). The aggregate reputation of the cars, which is established by the ratings each vehicle assigns to the others, determines the number of validators that are selected through the consensus process. Li et al. [19] offered a method to defend federated learning environments from harmful attacks that was established by committee consensus. The delegated PBFT method, which selects a representative for consensus via the vote of NEO currency owners, is used in the NEO scheme that is detailed in [29, 30]. Reduced power consumption for the blockchain system is the aim of this approach. As more nodes join the consensus process in these delegation-based blockchain consensus solutions, it is anticipated that processing costs and communication traffic would go down. However, there are several problems that may jeopardize the security and decentralization of the blockchain. The methods for decentralized consensus currently in use do not account for the possibility that malicious attacks would significantly affect the blockchain's performance. Additionally, no research has been done to determine the best method for calculating the delegation ratio in order to ensure the fairness and security of the consensus process.

A machine learning system known as DRL employs both RL and DL (RL). By providing additional context, DRL helps the agent to make decisions that are more informed. The DeepQN developed by DeepMind uses a DNN to approximate the state-action values seen in Atari games [21]. The research also focused on strategies for enhancing DQN's performance. For instance, [22] addressed the overestimation problem of DQN using a double estimator structure. [22] DNN, which consists of two different streams and utilizes an advantage function, aids in improving the performance of the DQN system. The pertinent citation is [23]. Research has also been done on how DRL technology may enhance the operating efficiency of blockchains. For instance, Liu et al. developed a DRL-based blockchain (DRLB) architecture in [24] to boost TPS while still adhering to security, latency, and decentralization requirements. With this layout, the blockchain's settings are optimized based on the network's current condition. In [25], researchers provide a sharded blockchain architecture that uses DQN to increase TPS. Work in [26] created a DRL-based data sharing system that is trustworthy and secure in order to maximize the data collection process. A DRL-based method was suggested by Yang et al. [27] with the aim of lowering total energy consumption while improving resource allocation. In their study, Dai et al. proposed a blockchain-based content caching architecture, using DRL as a method to carry out optimal content caching [28]. This framework was created to aid in the process of safeguarding the security and privacy of users. In the blockchain system proposed by [29] use of DRL to improve resource allocation while safeguarding the privacy and security of edge-enabled internet of things networks. The blockchain-enabled mobile edge computing system created in [30] also improves the performance of the blockchain and the cooperative offloading resource allocation problem. However, they do not take into account the possibility of attacks occurring even while the blockchain consensus process is still in motion, nor do they offer a defence mechanism that can effectively thwart malevolent nodes in a dynamic blockchain network. These two gaps are both significant design problems which are considered in this text.

III. Design of an augmented Bioinspired model for improving QoS of Blockchain IoT deployments via Context-based Consensus

From the review of existing blockchain models, it can be observed that although blockchain deployments are very secure, they are not scalable due to the exponential growth in mining delay relative to chain lengths. Researchers have suggested low-complexity mining methods, sharding strategies, and other machine learning optimizations to address these problems. These models' lower levels of scalability are a result of their reliance on the underlying blockchain or the presence of longer computational delays. Additionally, the majority of these models do not take into account consensus optimizations, which further restricts their applicability in large-scale networks. This section discusses creating an effective bioinspired model to address these problems by enhancing the Quality of Service (QoS) of blockchain IoT (Internet of Things) deployments through context-based consensus. In order to validate the responses of these miners, the proposed model, which is depicted in figure 1, first gathers temporal mining performance from active miner nodes and then uses a novel Proof-of-Temporal Trust (PoTT) based consensus. The PoTT Model uses throughput levels, energy consumption, and the temporal mining delay to choose high-performance miners for handling block-addition requests. These miners approve requests and store them on a collection of sidechains called Bacterial Foraging Optimized (BFO). Based on the network's spatial QoS performance in real-time, these sidechains are automatically tuned. The BFO Model helps separate existing single-length blockchains into sidechains with improved QoS. The BFO Model performs this segregation using a thorough consistency metric that incorporates security and QoS levels and can be used for specialized applications like Industrial IoTs. As a result, sidechain segregation is accomplished while still maintaining high security against diverse attacks.

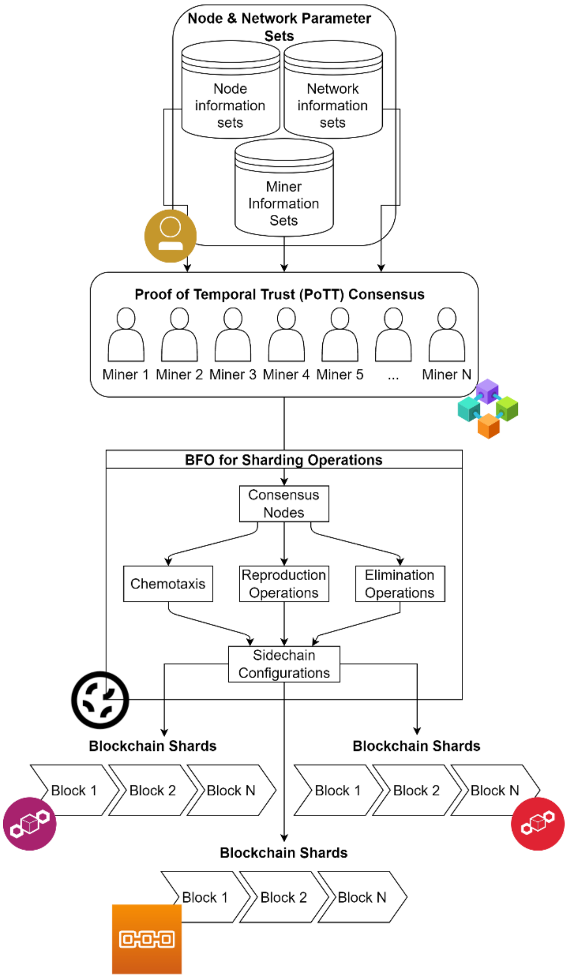

Figure 1. Flow of the optimized sharding process

ISSN: 2250-0839

As per the flow of proposed model, it can be observed that initially a Proof-of-Temporal Trust (PoTT) based consensus is used, which assists in identification of optimal miners that can add new blocks. Design of this consensus is discussed in subsection 3.1, while design of the BFO based sidechaining method is discussed in section 3.2, where the selected miner parameters and chain parameters are fused in order to create segregated chains. Researchers can refer these sections in order to design their own customized optimum sharding deployments for real-time use cases.

3.1. Design of the proposed model for PoTT based consensus

To perform a Proof-of-Temporal Trust based consensus, exiting miner performance is used for evaluation of trust levels. These trust levels are calculated between 2 nodes via equation 1, where different mining performance metrics are fused in order to identify optimal miner nodes.

$$TL(N,M) = \frac{\frac{D(N)}{D(M)} + \frac{E(N)}{E(M)} + \frac{T(M)}{T(N)} + \frac{PDR(M)}{PDR(N)}}{4} \ldots (1)$$

Where, $TL(N,M)$ represents the trust level between nodes N & M, while D, E, T & PDR represents their mining delay, energy consumed during mining, temporal throughput, and packet delivery ratios, which are calculated via equations 2, 3, 4 & 5 as follows,

$$D(M) = \frac{\sum_{i=1}^{M_r} t_{complete_i} - t_{start_i}}{M_r} \ldots (2)$$

Where, $t_{complete}$ & t_{start} represents the completion timestamp and starting timestamp for mining operations, while M_r represents total number of mining requests that have been processed by this set of miner nodes.

$$E(M) = \frac{\sum_{i=1}^{M_r} E_{start_i} - E_{end_i}}{M_r} \ldots (3)$$

Where, E_{start} & E_{end} represents the initial and final energy level of miner nodes during the mining process.

$$T(M) = \sum_{i=1}^{M_r} \frac{Rx(P)_i}{M_r * D(M)} \ldots (4)$$

Where, $Rx(P)$ represents the total number of blocks successfully mined by the miner nodes.

$$PDR(M) = \sum_{i=1}^{M_r} \frac{Rx(P)_i}{Tx(P)_i * M_r} \ldots (5)$$

Where, $Tx(P)$ represents total number of blocks given to the miner node to perform mining operations. Based on this trust level, an average trust value is estimated via equation 6,

$$T_{th} = \sum_{i=1}^{N(Miners)} \sum_{j=1}^{N(Miners)} \frac{TL(i,j)}{N^2(Miners)} \ldots (6)$$

Miner nodes with $TL > T_{th}$ are used for mining operations. The performance obtained during mining is used to update the trust levels, thus assisting in deployment of dynamic PoTT based consensus. The miner nodes along with existing blockchain configurations are used by a Bacterial Foraging Optimizer (BFO), which assists in formation of blockchain shards. This process is discussed in the next sub-section of this text.

3.2. Design of the BFO Model for sharding operations

The miner configurations along with current blockchain parameters are used to train a BFO Model, which assists in formation of blockchain shards. This is done via the following operations,

ISSN: 2250-0839

- To initialize the optimization process, a set of parameters are configured as follows,
  - A set of Bacterium used for shard formation (NB)
  - A set of iterations that will be used to form these shards (NI)
  - Rate at which the model will learn from different Bacterium particles (L_r)
  - Total number of sidechains & their lengths, that currently present in the network (N_{sc} & L_{sc})
- A set of Bacterium are continuously reconfigured for NI iterations, as per the following process,
- From the current set of chains, select a chain via equation 7, and generate a set of requests via equation 8,

$$N_s = STOCH(1, N_{sc}) \dots (7)$$

$$N_r = STOCH(Min(L_{sc}) * L_r, Max(L_{sc}) * L_r) \dots (8)$$

Where, $STOCH$ is a Markovian process for stochastically generating different number sets,

- Simulate 20% of these communications as attacks (Sybil, Masquerading, DDoS, etc.), and remaining 80% as normal requests.
- Simulate these communications via addition of blocks to the selected N_s shard, and estimate Bacterium fitness via equation 9,

$$fb = \frac{\left[\sum_{i=1}^{N_r} TL_i - \sum_{j=1}^{N_r} \frac{TL_j}{N_r}\right]}{N_r * N^2(PoTT)} * \sum_{N=1}^{N(PoTT)} \sum_{M=1}^{N(PoTT)} \left[\frac{D(N) - D(M)}{D(M)} + \frac{E(N) - E(M)}{E(M)} + \frac{T(M) - T(N)}{T(N)} + \frac{PDR(M) - PDR(N)}{PDR(N)}\right] \dots (9)$$

Where, $N(PoTT)$ represents total number of miner nodes selected by the $PoTT$ process.

- This fitness is evaluated for NB Bacterium, and then a fitness threshold is calculated via equation 10,

$$f_{th} = \frac{\sum_{i=1}^{NB} fb_i * L_r}{NB} \dots (10)$$

- Based on this fitness threshold, Bacterium with $fb > f_{th}$ are reproduced in the next iteration, while others are eliminated in current iteration, and regenerated in the next set of iterations.

- This process is repeated for NI iterations, and the given set of Bacterium are continuously reconfigured during each of these iterations.

Once all iterations are completed, then Bacterium with maximum fitness levels is selected, and its fitness is compared with a fitness threshold that is estimated via equation 11,

$$f_{th} = \frac{\left[\sum_{i=1}^{N_p} TL_i - \sum_{j=1}^{N_p} \frac{TL_j}{N_p}\right]}{N_p * N^2(PoTT)} * \sum_{N=1}^{N(PoTT)} \sum_{M=1}^{N(PoTT)} \left[\frac{D(N) - D(M)}{D(M)} + \frac{E(N) - E(M)}{E(M)} + \frac{T(M) - T(N)}{T(N)} + \frac{PDR(M) - PDR(N)}{PDR(N)}\right] \dots (11)$$

Where, N_p are the previous mining requests that were processed by the mining nodes. The selected sidechain by BFO is split into 2-shards of equal length if equation 12 is satisfied,

$$fb(BFO) < f_{th} \dots (12)$$

Else the selected shard is used to add new blocks. This process is repeated for individual block addition requests if the delay needed for previous mining is higher than average delay of mining process. Due to which the model is able to improve the efficiency of mining even for large-scale IIoT deployments. This efficiency is estimated in terms of mining delay, energy needed for mining, mining throughput and mining efficiency in the next section of this text.

IV. Comparative analysis of different blockchain techniques

The proposed model collects temporal mining performance from existing miner nodes before deploying a novel Proof-of-Temporal Trust (PoTT)-based consensus for validating responses from these miners. The PoTT Model selects high-performance miners for processing block-addition requests using temporal mining delay, energy consumed while mining, and throughput levels. The Bacterial Foraging Optimized (BFO) sidechains store requests approved by these miners. These sidechains are automatically tuned based on the real-time spatial QoS performance of the network. The BFO Model facilitates the separation of single-length existing blockchains into QoS-optimized sidechains. The BFO Model uses an exhaustive consistency metric that combines QoS and security levels that can be applied to specialized applications such as Industrial IoTs to perform these segregations. To estimate performance of this model, it was simulated under the following network conditions.

Total Miner Nodes: 1k

Block Size: 2k bytes per block

Block Addition Interval: 0.0001 seconds per block

Miner Energy Model: $ME = 1\ mJ, VE = 0.5mJ, IdleE = 0.001\ mJ$

Where, ME, VE & $IdleE$ represents the energy needed for single mining cycle, energy needed for verification and idle energy of the miner nodes. Using these configurations, a set of 2.5 million block addition requests were generated, out of which 20% were stochastically modified into attack requests. These attacks include Masquerading, Distributed Denial of Service (DDoS), Flooding, and Sybil attacks. Using this configuration, nearly 1500 blockchain shards were generated during this process. While generating these shards, the average delay of mining (D), average energy needed for mining (E), throughput obtained during mining (T), and mining efficiency (ME) was evaluated for different Number of Mining Requests (NM). This performance was compared with MaO EA DRP [9], SHG [12], and DRL [15], which are recently proposed mining optimization models used for IIoT based blockchain deployments. Based on this strategy, the average delay of mining can be observed from table 1 as follows,

NM	**D (s)** **MaO EA DRP [9]**	**D (s)** **SHG [12]**	**D (s)** **DRL [15]**	**D (s)** **BQ BCC**
250k	1.46	2.02	1.93	0.83
375k	1.80	2.48	2.38	1.03
500k	2.19	3.02	2.90	1.24
750k	2.59	3.56	3.42	1.47
1M	2.94	4.04	3.88	1.67
1.25M	3.28	4.51	4.33	1.86
1.5M	3.63	5.00	4.79	2.06
2M	3.96	5.46	5.23	2.25
2.5M	4.32	5.95	5.70	2.46

Table 1. Mining delay needed for addition of large number of blocks

As per this evaluation and figure 2, it was observed that the proposed model is able to improve the mining speed by 14.5% when compared with MaO EA DRP [9], 19.4% when compared with SHG [12], and 18.5% when compared with DRL [15] under large number of block addition requests. This mining speed is improved due to use of temporal mining delay via PoTT consensus, and use of delay metrics while forming shards. Due to which the model can be deployed for high-speed IIoT scenarios.

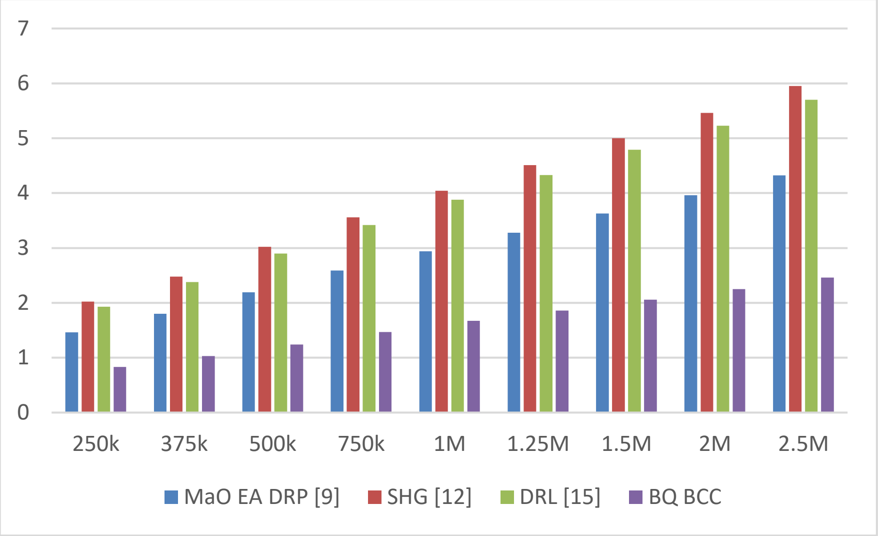

Figure 2. Mining delay needed for addition of large number of blocks

Similarly, the energy needed for these mining operations can be observed from table 2 as follows,

NM	**E (mJ)** **MaO EA DRP [9]**	**E (mJ)** **SHG [12]**	**E (mJ)** **DRL [15]**	**E (mJ)** **BQ BCC**
250k	23.43	32.35	31.08	13.29
375k	24.58	33.92	32.61	13.94
500k	25.68	35.44	34.06	14.56
750k	26.96	37.21	35.77	15.30
1M	28.34	39.12	37.59	16.08
1.25M	29.82	41.16	39.55	16.92
1.5M	31.21	43.08	41.39	17.70
2M	32.46	44.78	43.03	18.41
2.5M	33.68	46.47	44.67	19.10

Table 2. Mining energy needed for addition of large number of blocks

As per this evaluation and figure 3, it was observed that the proposed model is able to reduce the energy needed for mining by 16.4% when compared with MaO EA DRP [9], 23.5% when compared with SHG [12], and 19.2% when compared with DRL [15] under large number of block addition requests. This energy consumption is reduced due to use of temporal mining energy via PoTT consensus, and use of energy consumption metrics while forming shards. Due to which the model can be deployed for high-lifetime IIoT scenarios.

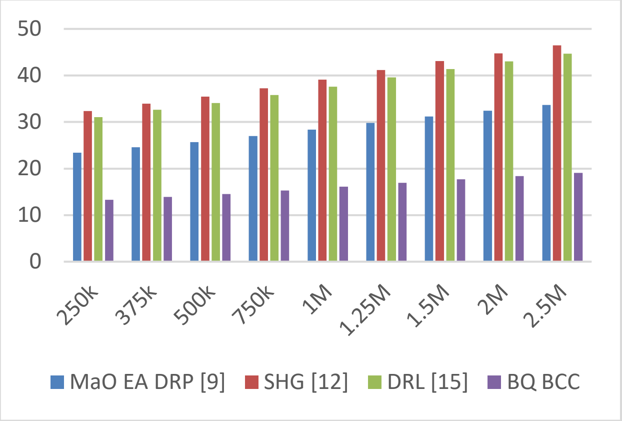

Figure 3. Mining energy needed for addition of large number of blocks

Similarly, the throughput needed for mining is tabulated in table 3 as follows,

NM	Thr. (kbps) MaO EA DRP [9]	Thr. (kbps) SHG [12]	Thr. (kbps) DRL [15]	Thr. (kbps) BQ BCC
250k	1278.6	1334.1	2115.6	2988.0
375k	1293.3	1349.6	2140.0	3022.5
500k	1302.9	1359.5	2155.8	3044.7
750k	1313.8	1370.9	2173.9	3070.3
1M	1326.2	1383.9	2194.4	3099.3
1.25M	1339.1	1397.4	2215.9	3129.5
1.5M	1352.5	1411.3	2237.9	3160.7
2M	1365.6	1425.0	2259.7	3191.5
2.5M	1378.1	1438.1	2280.3	3220.6

Table 3. Throughput obtained during addition of large number of blocks

As per this evaluation and figure 4, it was observed that the proposed model is able to improve the throughput obtained during mining by 28.5% when compared with MaO EA DRP [9], 25.4% when compared with SHG [12], and 16.2% when compared with DRL [15] under large number of block addition requests. This increase in throughput is due to use of temporal throughput during miner selection via PoTT consensus, and use of throughput metrics while forming shards. Due to which the model can be deployed for high-data-rate IIoT scenarios.

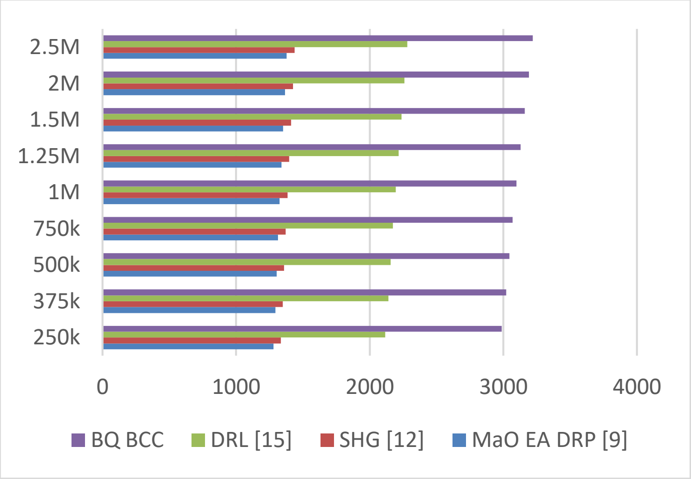

Figure 4. Throughput obtained during addition of large number of blocks

ISSN: 2250-0839

Similarly, the mining efficiency can be observed from table 4 as follows,

NM	ME (%) MaO EA DRP [9]	ME (%) SHG [12]	ME (%) DRL [15]	ME (%) BQ BCC
250k	94.2	93.1	89.0	98.9
375k	94.3	93.2	89.1	99.1
500k	94.4	93.3	89.2	99.2
750k	94.5	93.4	89.3	99.3
1M	94.6	93.5	89.3	99.4
1.25M	94.7	93.6	89.4	99.5
1.5M	94.8	93.7	89.5	99.6
2M	94.9	93.8	89.6	99.7
2.5M	95.0	93.9	89.7	99.8

Table 4. Mining Efficiency obtained during addition of large number of blocks

As per this evaluation and figure 5, it was observed that the proposed model is able to improve the mining efficiency obtained during mining by 4.5% when compared with MaO EA DRP [9], 5.3% when compared with SHG [12], and 10.5% when compared with DRL [15] under large number of block addition requests. This increase in mining efficiency is due to use of temporal PDR during miner selection via PoTT consensus, and use of efficiency metrics while forming shards. Due to which the model can be deployed for high-efficiency IIoT mining scenarios.

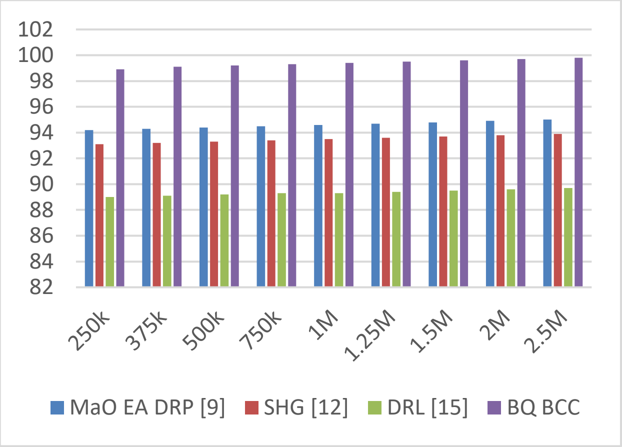

Figure 5. Mining Efficiency obtained during addition of large number of blocks

Based on these evaluations, it can be observed that the proposed model was able to improve the mining speed, reduce mining energy, while improving throughput and mining efficiency when compared with existing models. Due to which the proposed PoTT based consensus & sharding model can be used for a wide variety of IIoT based deployment scenarios.

V. Conclusion and future scope

Before deploying a novel Proof-of-Temporal Trust (PoTT)-based consensus for validating responses from these miners, the proposed model collects temporal mining performance from existing miner nodes. The PoTT Model selects high-performance miners for processing block-addition requests based on temporal mining delay, mining energy consumption, and throughput levels. The Bacterial Foraging Optimized (BFO) sidechains store these miners' approved requests. These sidechains are automatically optimized based on the network's real-time spatial QoS performance. The BFO Model enables the separation of existing blockchains with a single length into QoS-optimized sidechains. To perform these segregations, the BFO Model employs an exhaustive consistency metric that combines QoS and security levels and can be applied to specialized applications such as Industrial IoTs. In terms of mining speed, it was observed that the proposed model can increase mining speed by 14.5% when compared to MaO EA DRP [9], 19.4% when compared to SHG [12], and 18.5% when compared to DRL [15] when a large number of block addition requests are being processed. Utilization of temporal mining delay via PoTT consensus and utilization of delay metrics while forming shards increase the mining speed. Due to this, the model is deployable for IIoT scenarios requiring high speeds. Comparing the proposed model to MaO EA DRP [9], SHG [12], and DRL [15] in terms of energy consumption during mining, it was found that the proposed model reduces energy consumption by 16.4%, 23.5%, and 19.2%, respectively, for large numbers of block addition requests. Utilization of temporal mining energy via PoTT consensus and utilization of energy consumption metrics during shard formation reduce this energy consumption. Due to this, the model is deployable for IIoT scenarios with a lengthy lifetime.

Estimated in terms of data rate, it was found that the proposed model can increase the throughput obtained during mining by 28.5% when compared to MaO EA DRP [9], 25.4% when compared to SHG [12], and 16.2% when compared to DRL [15] when a large number of block addition requests are made. This increase in throughput is a result of the use of temporal throughput during miner selection via PoTT consensus and the use of throughput metrics during shard formation. Due to this, the model is deployable for IIoT scenarios with a high data rate. In terms of mining efficiency, it was observed that the proposed model can improve mining efficiency by 4.5% when compared to MaO EA DRP [9], 5.3% when compared to SHG [12], and 10.5% when compared to DRL [15] when a large number of block addition requests are made. This increase in mining efficiency is the result of the use of temporal PDR during miner selection via PoTT consensus and the utilization of efficiency metrics when forming shards. Due to this, the model is deployable for IIoT mining scenarios with high efficiency. On the basis of these evaluations, it can be concluded that the proposed model improved mining speed, reduced mining energy, and increased throughput and mining efficiency in comparison to existing models. Due to this, the proposed PoTT-based consensus and sharding model is applicable to a wide range of IIoT deployment scenarios.

In future, performance of this model must be validated on ultra-large-scale networks and can be improved via integration of hybrid consensus & miner pools. This performance can also be improved via use of deep learning-based methods that integrate Transfer Learning via Auto Encoders to learn hash generation patterns from existing blockchain deployments that are suited for IIoTs under real-time attack scenarios.

References

[1] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang and Y. Liang, "Blockchain-Enabled Federated Learning Data Protection Aggregation Scheme With Differential Privacy and Homomorphic Encryption in IIoT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 6, pp. 4049-4058, June 2022, doi: 10.1109/TII.2021.3085960.

[2] Y. Feng, W. Zhang, X. Luo and B. Zhang, "A Consortium Blockchain-Based Access Control Framework With Dynamic Orderer Node Selection for 5G-Enabled Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2840-2848, April 2022, doi: 10.1109/TII.2021.3078183.

[3] J. Li, Z. Qiao and J. Peng, "Asymmetric Group Key Agreement Protocol Based on Blockchain and Attribute for Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8326-8335, Nov. 2022, doi: 10.1109/TII.2022.3176048.

[4] J. Wan, J. Li, M. Imran, D. Li and Fazal-e-Amin, "A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3652-3660, June 2019, doi: 10.1109/TII.2019.2894573.

[5] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen and J. Chang, "Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22501-22515, 15 Nov.15, 2022, doi: 10.1109/JIOT.2022.3176192.

[6] H. Qi, J. Wang, W. Li, Y. Wang and T. Qiu, "A Blockchain-Driven IIoT Traffic Classification Service for Edge Computing," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2124-2134, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3035431.

[7] S. Khezr, A. Yassine, R. Benlamri and M. S. Hossain, "An Edge Intelligent Blockchain-Based Reputation System for IIoT Data Ecosystem," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8346-8355, Nov. 2022, doi: 10.1109/TII.2022.3174065.

[8] Y. Jiang, Y. Zhong and X. Ge, "IIoT Data Sharing Based on Blockchain: A Multileader Multifollower Stackelberg Game Approach," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4396-4410, 15 March15, 2022, doi: 10.1109/JIOT.2021.3103855.

[9] X. Cai et al., "A Sharding Scheme-Based Many-Objective Optimization Algorithm for Enhancing Security in Blockchain-Enabled Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7650-7658, Nov. 2021, doi: 10.1109/TII.2021.3051607.

[10] D. Wu and N. Ansari, "A Trust-Evaluation-Enhanced Blockchain-Secured Industrial IoT System," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5510-5517, 1 April1, 2021, doi: 10.1109/JIOT.2020.3030689.

[11] U. Javaid and B. Sikdar, "A Checkpoint Enabled Scalable Blockchain Architecture for Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7679-7687, Nov. 2021, doi: 10.1109/TII.2020.3032607.

[12] N. Gao, R. Huo, S. Wang, T. Huang and Y. Liu, "Sharding-Hashgraph: A High-Performance Blockchain-Based Framework for Industrial Internet of Things With Hashgraph Mechanism," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17070-17079, 15 Sept.15, 2022, doi: 10.1109/JIOT.2021.3126895.

[13] Y. Yang, J. Wu, C. Long, W. Liang and Y. -B. Lin, "Blockchain-Enabled Multiparty Computation for Privacy Preserving and Public Audit in Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9259-9267, Dec. 2022, doi: 10.1109/TII.2022.3177630.

[14] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour and G. Srivastava, "Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8356-8366, Nov. 2022, doi: 10.1109/TII.2022.3168011.

[15] D. Liu, A. Alahmadi, J. Ni, X. Lin and X. Shen, "Anonymous Reputation System for IIoT-Enabled Retail Marketing Atop PoS Blockchain," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3527-3537, June 2019, doi: 10.1109/TII.2019.2898900.

[16] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung and M. Song, "Performance Optimization for Blockchain-Enabled Industrial Internet of Things (IIoT) Systems: A Deep Reinforcement Learning Approach," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3559-3570, June 2019, doi: 10.1109/TII.2019.2897805.

[17] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma and C. Peng, "A Blockchain-Based Machine Learning Framework for Edge Services in IIoT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 1918-1929, March 2022, doi: 10.1109/TII.2021.3097131.

[18] M. Kaur, M. Z. Khan, S. Gupta and A. Alsaeedi, "Adoption of Blockchain With 5G Networks for Industrial IoT: Recent Advances, Challenges, and Potential Solutions," in IEEE Access, vol. 10, pp. 981-997, 2022, doi: 10.1109/ACCESS.2021.3138754.

[19] K. Yu, L. Tan, M. Aloqaily, H. Yang and Y. Jararweh, "Blockchain-Enhanced Data Sharing With Traceable and Direct Revocation in IIoT," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7669-7678, Nov. 2021, doi: 10.1109/TII.2021.3049141.

[20] P. Zhang, Y. Hong, N. Kumar, M. Alazab, M. D. Alshehri and C. Jiang, "BC-EdgeFL: A Defensive Transmission Model Based on Blockchain-Assisted Reinforced Federated Learning in IIoT Environment," in IEEE Transactions on Industrial Informatics, vol. 18, no. 5, pp. 3551-3561, May 2022, doi: 10.1109/TII.2021.3116037.

[21] K. Lin, J. Gao, G. Han, H. Wang and C. Li, "Intelligent Blockchain-Enabled Adaptive Collaborative Resource Scheduling in Large-Scale Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9196-9205, Dec. 2022, doi: 10.1109/TII.2022.3169457.

[22] L. Yang, M. Li, P. Si, R. Yang, E. Sun and Y. Zhang, "Energy-Efficient Resource Allocation for Blockchain-Enabled Industrial Internet of Things With Deep Reinforcement Learning," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2318-2329, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3030646.

[23] J. Wei et al., "A Redactable Blockchain Framework for Secure Federated Learning in Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17901-17911, 15 Sept.15, 2022, doi: 10.1109/JIOT.2022.3162499.

[24] Y. I. L. Lucio, K. Márceles Villalba and S. A. Donado, "Adaptive Blockchain Technology for a Cybersecurity Framework in IIoT," in IEEE Revista Iberoamericana de Tecnologias del Aprendizaje, vol. 17, no. 2, pp. 178-184, May 2022, doi: 10.1109/RITA.2022.3166857.

[25] J. Huang, L. Kong, G. Chen, M. -Y. Wu, X. Liu and P. Zeng, "Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3680-3689, June 2019, doi: 10.1109/TII.2019.2903342.

[26] Z. Guo et al., "RNS-Based Adaptive Compression Scheme for the Block Data in the Blockchain for IIoT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9239-9249, Dec. 2022, doi: 10.1109/TII.2022.3182766.

[27] W. Chen et al., "Cooperative and Distributed Computation Offloading for Blockchain-Empowered Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8433-8446, Oct. 2019, doi: 10.1109/JIOT.2019.2918296.

[28] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han and C. Su, "Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices," in IEEE Transactions on Industrial Informatics, vol. 18, no. 10, pp. 7059-7067, Oct. 2022, doi: 10.1109/TII.2021.3084753.

[29] P. Zhang, H. Sun, J. Situ, C. Jiang and D. Xie, "Federated Transfer Learning for IIoT Devices With Low Computing Power Based on Blockchain and Edge Computing," in IEEE Access, vol. 9, pp. 98630-98638, 2021, doi: 10.1109/ACCESS.2021.3095078.

[30] Yuting Wu, Xiu Jin, Honggang Yang, Lijing Tu, Yong Ye, Shaowen Li, "Blockchain-Based Internet of Things: Machine Learning Tea Sensing Trusted Traceability System", *Journal of Sensors*, vol. 2022, Article ID 8618230, 16 pages, 2022. https://doi.org/10.1155/2022/8618230