ASEAN Engineering Journal

Full Paper

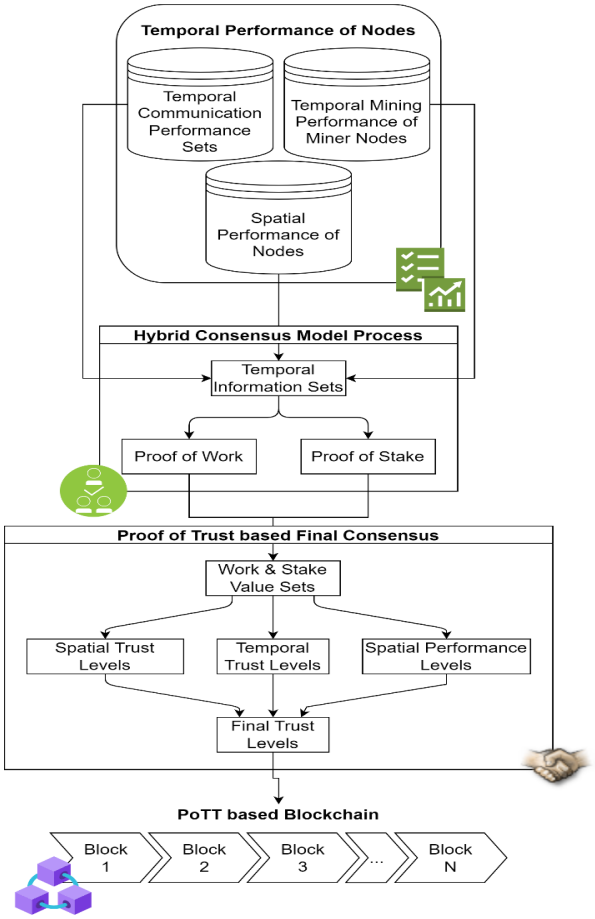
NTHCMB: DESIGN OF AN EFFICIENT NOVEL TRUST-BASED HYBRID CONSENSUS MODEL FOR SECURING BLOCKCHAIN DEPLOYMENTS

Smita Kapse[a,b]*, Latesh Malik[c], Sanjay Kumar[a]

[a]Computer Science Engineering Department, Kalinga University, Raipur, Chhattisgarh, India
[b]Computer Technology Department, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India
[c]Computer Science Engineering Department, Government College of Engineering, Nagpur, Maharashtra, India

Article history
Received
19 July 2023
Received in revised form
22 October 2023
Accepted
25 October 2023
Published online
31 May 2024

*Corresponding author
smitarkapse@ycce.edu



Abstract

Blockchain deployments require efficient consensus models in order to be scaled for larger networks. Existing consensus models either use stake-levels, trust-levels, authority-levels, etc. or their combinations in order to reduce mining delay while maintaining higher security levels. But these models either have higher energy requirements, lower security, or have linear/exponential relationship between mining delay and length of the chains. Due to these restrictions, the applicability of these models is affected when deployed under real-time network scenarios. To overcome these issues, this text proposes design of an efficient novel trust-based hybrid consensus model for securing blockchain deployments. The proposed model initially uses a hybrid consensus model that fuses Proof-of-Work (PoW), Proof-of-Stake (PoS) with Proof-of-Temporal-Trust (PoTT) for improving security while maintaining higher Quality of Service (QoS) levels. The PoTT Model fuses together temporal mining delay, temporal mining energy, throughput and block mining efficiency in order to generate miner-level trusts. These trust values are fused with Work efficiency and Stake levels and used for selection of miners. The selected miners are used for serving block addition requests, which assists in improving mining speed by 3.2%, reducing energy consumption 4.5%, and improving throughput by 8.5%, while improving block mining efficiency by 2.9% when compared with existing mining optimization models. This performance was validated under Sybil, Finney, Man-in-the-Middle, and Spoofing attacks. Performance of the model was observed to be consistent even under attacks, thereby making it useful for real-time network scenarios.

Keywords: Blockchain, Proof-of-Work, Proof-of-Stake, Proof-of-Temporal- Trust, Machine learning

1.0 INTRODUCTION

The rapid growth of blockchain technology has revolutionized the way we approach trust and security in decentralized systems. However, the traditional proof-of-work and proof-of-stake consensus models suffer from their own limitations, such as high energy consumption and susceptibility to centralization. Therefore, researchers have been exploring novel consensus models that can overcome these limitations and improve the scalability, security, and efficiency of blockchain networks [1, 2, 3]. Blockchain technology has gained significant attention in recent years due to its potential to provide a transparent, secure, and decentralized way of storing and exchanging data. However, the current consensus models used in most blockchain networks have several limitations that need to be addressed to achieve broader adoption and scalability levels via Dueling Double Deep-Q-network with Prioritized experience replay based secure trust-based delegated consensus blockchain (TDCB D3P) [4, 5, 6].

Proof-of-work (PoW) is the most widely used consensus model in blockchain networks, but it has significant drawbacks, such as high energy consumption and susceptibility to centralization. Proof-of-stake (PoS) consensus model is an alternative to PoW, but it also has its own limitations, such as stake centralization and low transaction throughput levels [7, 8, 9].

Hybrid consensus models have been proposed as a solution to overcome these limitations and improve the performance of blockchain networks. These models combine multiple consensus mechanisms to leverage their strengths and overcome their weaknesses. One such hybrid model is the trust-based consensus model, which relies on a reputation system to assign trust scores to nodes based on their past behavior and interactions. In a trust-based consensus model, nodes with higher trust scores are given more influence in the consensus process, and those with lower trust scores are penalized for different scenarios [10, 11, 12]. This approach encourages honest behavior and discourages malicious behavior in the network, thereby improving the security of the system under real-time scenarios.

However, designing an efficient and robust trust-based hybrid consensus model is a challenging task. It requires addressing several technical and economic issues, such as measuring and updating trust scores accurately, incentivizing nodes to participate and cooperate, and handling potential attacks or failures in the system when tested under different attacks. In this context, a promising approach is to develop hybrid consensus models that combine the best features of different consensus mechanisms. One such hybrid model is the trust-based consensus model, which relies on a reputation system to assign trust scores to nodes based on their past behavior and interactions [13, 14, 15]. This model can improve the security of the network by preventing malicious nodes from gaining significant influence and by incentivizing honest behavior during mining operations.

To overcome these challenges, this research proposes a novel trust-based hybrid consensus model that leverages recent advancements in temporal trust analysis. The model will use machine learning techniques to improve the accuracy and fairness of trust scores and game theory to optimize the rewards and penalties for nodes based on their behavior levels. The proposed model aims to achieve high scalability, security, and efficiency in blockchain deployments while minimizing energy consumption and ensuring decentralization under real-time scenarios.

However, the design of a trust-based hybrid consensus model poses several challenges, such as how to accurately measure and update trust scores, how to incentivize participation and cooperation among nodes, and how to handle potential attacks or failures in the system. Therefore, this research aims to address these challenges and propose an efficient and robust trust-based hybrid consensus model for securing blockchain deployments. The proposed model will leverage recent advancements in machine learning and game theory to improve the accuracy and fairness of trust scores and to optimize the rewards and penalties for nodes based on their behavior. Overall, this research will contribute to the development of more secure and scalable blockchain networks that can support various applications and use cases.

1.1 The Novelty of The Work

The novel trust-based hybrid consensus model presented in this paper brings several significant innovations to the field of blockchain technology and consensus mechanisms:

1. **Efficiency and Scalability**: The paper acknowledges the critical need for efficient consensus models to scale blockchain networks. It recognizes that existing models have limitations in terms of energy consumption, security, and scalability. The proposed NTHCMB model effectively addresses these challenges.
2. **Hybrid Consensus Fusion**: The NTHCMB model introduces a hybrid consensus approach that combines three well-known consensus mechanisms: Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-Temporal-Trust (PoTT). This fusion of different consensus mechanisms is a novel approach that leverages the strengths of each to improve overall network performance.
3. **Temporal Trust Metrics**: The paper introduces the concept of "temporal mining delay," "temporal mining energy," and other temporal metrics. These metrics are used to calculate miner-level trusts, allowing for a more nuanced and dynamic selection of miners. This approach enhances security and mitigates the risk of malicious mining activities.
4. **Quality of Service (QoS) Enhancement**: The NTHCMB model places a strong emphasis on maintaining a higher Quality of Service (QoS) level. By integrating trust-based metrics into the consensus process, the model ensures that network performance is not compromised while enhancing security.
5. **Attack Resilience**: The paper validates the performance of the NTHCMB model under various attacks, including Sybil, Finney, Man-in-the-Middle, and Spoofing attacks. The model's ability to maintain consistent performance even under adversarial conditions is a notable achievement, making it suitable for real-time network scenarios.
6. **Performance Improvements**: The results presented in the paper demonstrate substantial performance

enhancements compared to existing consensus models. The NTHCMB model improves mining speed by 3.2%, reduces energy consumption by 4.5%, increases throughput by 8.5%, and enhances block mining efficiency by 2.9%. These improvements are vital for the practical viability of blockchain networks.

7. **Applicability**: The NTHCMB model is designed with real-time network scenarios in mind, making it highly applicable to real-world use cases. Its efficiency, security, and scalability improvements address the practical challenges that blockchain deployments face as they grow and evolve.

In conclusion, the "NTHCMB" paper introduces a pioneering trust-based hybrid consensus model that leverages the strengths of multiple consensus mechanisms to enhance the efficiency, security, and scalability of blockchain deployments. Its innovative approach to temporal trust metrics, QoS enhancement, and attack resilience sets it apart as a significant contribution to the blockchain research community. This work has the potential to shape the future of blockchain technology by providing a robust solution for large-scale, secure, and efficient blockchain networks.

2.0 LITERATURE REVIEW

Since it was first introduced, blockchain technology has been getting momentum, and it has the potential to revolutionize a variety of different businesses. The consensus algorithm is an essential element of any blockchain system because it guarantees the integrity of the distributed database and ensures that transactions are recorded accurately. Confirming transactions, adding them to the blockchain, and preventing double spending are the responsibilities of the consensus algorithm sets via use of Federated Learning Consensus Mechanism (FLCM) and other methods [16, 17, 18, 19, 20].

Over the course of time, a number of different algorithms for reaching a consensus have been established. These algorithms include Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake. (DPoS), and Votes-as-a-Proof (VaaP) [21, 22, 23, 24]. However, each of these algorithms has its own set of advantages and disadvantages, which renders them inappropriate for specific application scenarios [25, 26, 27, 28]. As a result of this, there has been an increasing interest in developing blended consensus models that incorporate the advantages that various algorithms provide under real-time scenarios.

Trust-based Hybrid Consensus Models (THCMs) are one strategy that can be taken; these models make use of reputation and trust ratings to facilitate the process of reaching a consensus. In order to improve their efficacy, flexibility, and safety, THCMs incorporate numerous consensus techniques. The Byzantine Reliable Broadcast (BRB) Consensus is a trust-based consensus mechanism (THCM) that incorporates proof-of-work (PoW), proof-of-stake (PoS), and consensus based on confidence. BRB consensus implements a dynamic Byzantine fault tolerance (BFT) criterion, the value of which is based on how trustworthy the nodes are for different scenarios [29, 30]. The more reliable a node is, the more weight is assigned to the vote that it casts. BRB consensus also makes use of a feedback mechanism, which compensates nodes for the contributions they make to the process of reaching consensus. This encourages the nodes to behave in an honest manner under real-time scenarios.

Combining delegated proof of stake (DPoS) with a trust-based consensus algorithm is what a THCM known as Delegated Proof-of-Authority (DPoA) Consensus does. The reputation and confidence scores of the block producers in DPoA are determined by the block producers' historical output, and those scores are used to select new block producers. A reputation-based punishment system is also utilized by DPoA. Under this system, a block producer's reputation score is lowered if they engage in inappropriate behavior for different use cases [31, 32].

The Federated Byzantine Agreement (FBA) Consensus is a trust-based consensus mechanism (THCM) that integrates PBFT with another type of consensus mechanism. When using FBA, the network is broken up into a consortium of nodes, and each node has its own individual collection of confidence ratings. A majority of nodes that are in agreement regarding the legitimacy of a transaction is required to kick off the consensus process [33, 34]. The process of reaching a consensus gives more weight to nodes with high trust ratings, increasing the likelihood that only trustworthy nodes will participate in the process.

Proof-of-Activity Consensus (PoA Consensus) is a type of THCM that incorporates Proof-of-Work (PoW) and Proof-of-Stake (PoS). The determination of the block providers in PoA is accomplished through a combination of computational and stake-based techniques. In PoA, the selection of block providers is determined by both the computational capacity of the participants and the amount of interest they have in the networks [35]. In addition to this, PoA makes use of a reputation-based system that rewards trustworthy behavior and punishes dishonest behaviour sets.

As a result of their capacity to capitalize on the benefits offered by a variety of different consensus algorithms, THCMs are enjoying a surge in their level of adoption. These models have the potential to enhance the flexibility, effectiveness, and security of blockchain systems, which makes them appropriate for a diverse array of use cases. As the underlying blockchain technology continues to advance, we should anticipate the emergence of an increasing number of THCMs that are purpose-built for particular use cases and sectors.

3.0 METHODOLOGY

As per the review of existing trust-based consensus modelling techniques, it can be observed that these models either use stake-levels, trust-levels, authority-levels, etc. or their combinations in order to reduce mining delay while maintaining higher security levels. But these models either have higher energy requirements, lower security, or have linear/exponential relationship between mining delay and length of the chains. Due to these restrictions, the applicability of these models is affected when deployed under real-time network scenarios. To overcome these issues, this section discusses design of an efficient novel trust-based hybrid consensus model for securing blockchain deployments. As per Figure 1, it can be observed that the proposed model initially uses a hybrid consensus model that fuses Proof-of-Work (PoW),

Proof-of-Stake (PoS) with Proof-of-Temporal-Trust (PoTT) for improving security while maintaining higher Quality of Service (QoS) levels. The PoTT Model fuses together temporal mining delay, temporal mining energy, throughput and block mining efficiency in order to generate miner-level trusts. These trust values are fused with Work efficiency and Stake levels and used for selection of miners. The selected miners are used for serving block addition requests.

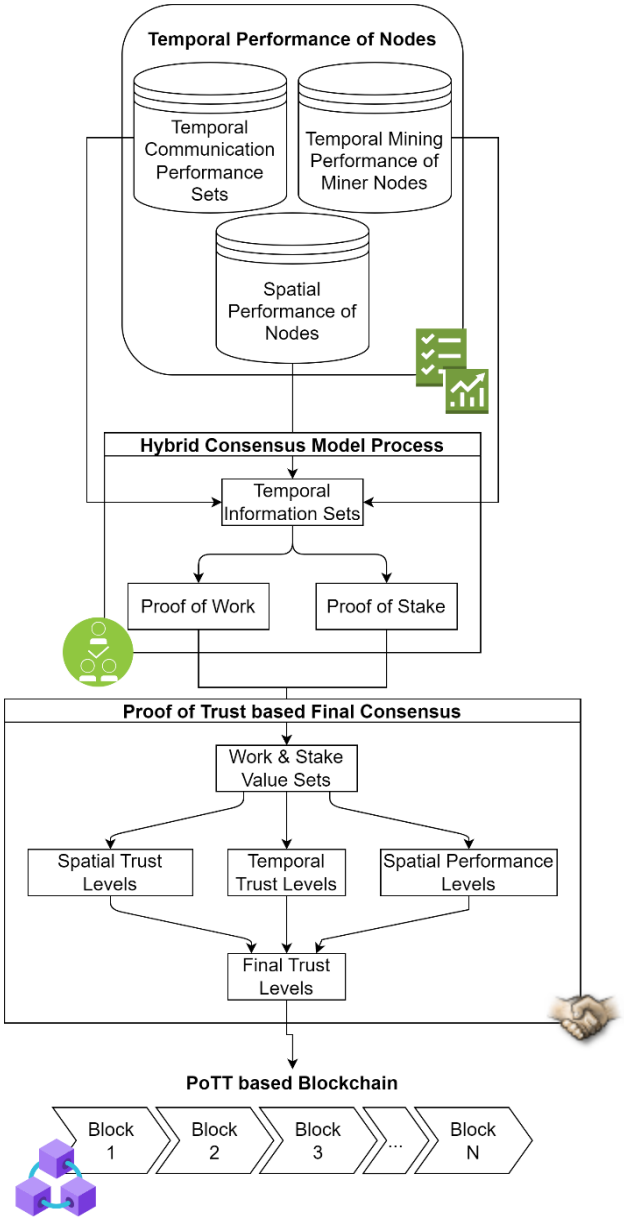


Figure 1 Design of the proposed hybrid consensus model for blockchain deployments

The model initially collects a set of temporal and spatial performance sets from different network nodes. These sets include,

- Approximate x, y location of the nodes
- Spatial residual energy (e) of the nodes
- Temporal Throughput (THR) & Packet Delivery Ratio (PDR) performance levels
- Temporal delay (d) for mining blocks
- Temporal energy (E) needed to mine the blocks

Based on these metrics, a trust-score is estimated for each node via equation 1,

$$TS_i = \frac{e_i}{Max(e)} + \frac{1}{N_c}\sum_{j=1}^{N_c}\frac{THR_i(j)}{Max(THR)} + \frac{Max(E)}{E_i(j)} + \frac{Max(d)}{d_i(j)} + \frac{PDR(j)}{Max(PDR)} \dots (1)$$

Where, N_c represents total number of temporal communications for which the nodes are being evaluated under real-time scenarios. Using these trust levels, a Relative Trust Score is estimated for each pair of nodes via equation 2,

$$RTS(i,j) = \frac{TS_i * TS_j}{\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}} \dots (2)$$

These relative trust levels is used to estimate a trust threshold via equation 3,

$$RTS_{th} = \sum_{i=1}^{N}\sum_{j=1}^{N}\frac{RTS(i,j)}{N^2} \dots (3)$$

Node pairs with $RTS(i,j) > RTS_{th}$ are selected for mining operations. For each of these nodes, their internal blockchains are verified via equation 4,

$$Prev\ Hash(i) = Hash(i-1) \dots (4)$$

Where, $i \in (1, NB)$, and NB are total number of blocks present in the blockchain for current node, and $Hash, Prev\ Hash$ represents hash and previous hash values for the current set of blockchains. Chains that satisfy condition 4 are marked as 'Validated', and their block information is used to correct invalidated blockchains.

For the current context, a blockchain with the block structure depicted via table 1 is used, where, PH represents previous hash, SN represents source node, DN represents destination node, TS represents timestamp at which the block is added to the chain, MD represents metadata of the block, while CH represents current hash value for the blocks.

Table 1. Structure of the block used for mining operations

Value of PH	SN	DN	Data
TS	MD	*Nonce*	Value of CH

To add new blocks to this chain, Nonce values are generated by individual nodes via equation 5,

$$Nonce_i = STOCH(TS_i + Stake_S + Timestamp + CL) \dots (5)$$

Where, $Stake$ of node is initially 1, and increments with addition of each set of new blocks, while CL represent length of the current chain present with individual miner nodes. For each generated hash, condition represented via equation 6 is checked,

$$Gen_{hash} \in Previous\ Hashes$$
$$T_{hash} = Min(T_i)\ where\ i \in M_{selected} \dots (6)$$

Where, $Gen_{hash}, T_{hash}, and\ M_{selected}$ represents the generated hash by the miner, delay needed to perform hashes, and list miner nodes that are selected for consensus operations. To perform final consensus, difficulty level (DL) of the mining process is calculated for each miner via equation 7,

$$DL_i = \frac{Max(Hash)_i}{Target(Hash)} \dots (7)$$

Where, $Max\ \&\ Target$ are maximum & target value of hashes. Similarly, a Validator Weight (VW) is calculated for each node via equation 8 as follows,

$$VW_i = \frac{Stake_i}{\sum Stake} \dots (8)$$

Based on this weight, a Foraging Probability (FP) is calculated for each node via equation 9,

$$FP_i = \frac{VW_i}{\sum VW} \dots (9)$$

Using these probabilities, final consensus score (CS) is evaluated via equation 10,

$$CS_i = \left(DL_i * w(DL)\right) + \left(FP_i * w(FP)\right) + \left(TS_i * w(TS)\right) \dots (10)$$

Where, $w(DL), w(FP), \&\ w(TS)$ represents weights of difficulty level, foraging probability and trust score for individual miner nodes. Hashes of miners that have highest value of CS are selected for the consensus operations. Once the node is selected, then final hash value is evaluated via equation 11,

$$Hash = SHA256\begin{pmatrix} Prev.\ Hash, Src, Dest, \\ Data, Timestamp, \\ Metadata, Nonce \end{pmatrix} \dots (11)$$

This value is used to update future blocks. Once blocks are added, then chain validity is checked via equation 12,

$$Prev\ Hash(i) = Hash(i-1) \dots (12)$$

If the chain is valid, then it is distributed to all other nodes in the network, and the process is continued for new blocks. Due to which the blockchain's authenticity is maintained even for large number of blockchain mining requests. Performance of this blockchain was validated in terms of delay, energy, throughput and packet delivery performance in the next section of this text, where these parameters are evaluated & compared with existing consensus optimization models under different attack scenarios.

4.0 RESULT ANALYSIS & COMPARISON

The proposed model initially uses a hybrid consensus model that fuses Proof-of-Work (PoW), Proof-of-Stake (PoS) with Proof-of-Temporal-Trust (PoTT) for improving security while maintaining higher Quality of Service (QoS) levels. The PoTT Model fuses together temporal mining delay, temporal mining energy, throughput and block mining efficiency in order to generate miner-level trusts. These trust values are fused with Work efficiency and Stake levels and used for selection of miners. The selected miners are used for serving block addition requests, which assists in improving mining speed, reducing energy consumption, improving throughput, while improving block mining efficiency when compared with existing mining optimization models. This performance was validated under Sybil, Finney, Man-in-the-Middle, and Spoofing attacks. To perform this validation the network was tested under 10k nodes, each sending 100 block addition requests. Out of these requests, 1% to 20% of requests were malicious (that were sent to modify internal blocks), and model's performance was tested in terms of communication delay (D), energy consumption (E), throughput (T) and PDR levels. Based on this strategy, the performance was compared with TDCB D3P [4], FLCM [16], and VaaP [22] under different number of attacks (NA) in Figure 2 as follows:

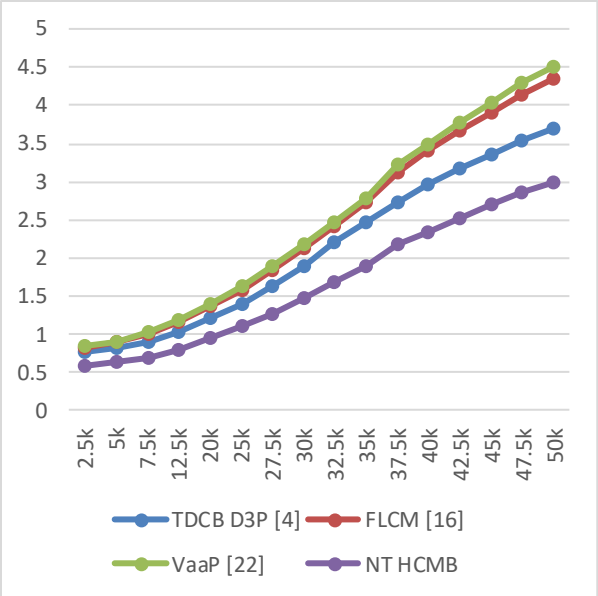


Figure 2 Communication delay under different number of attacks

As per this evaluation, it can be observed that the proposed model is able to achieve 10.5% lower delay when compared with TDCB D3P [4], 12.4% lower delay when compared with FLCM [16], and 12.8% lower delay when compared with VaaP [22] under different number of attacks. This delay is reduced due to use of low complexity consensus models with PoW, PoS & PoTT Models for different attack scenarios. Similar performance was evaluated in terms of energy consumption, and can be observed from Figure 3 as follows:

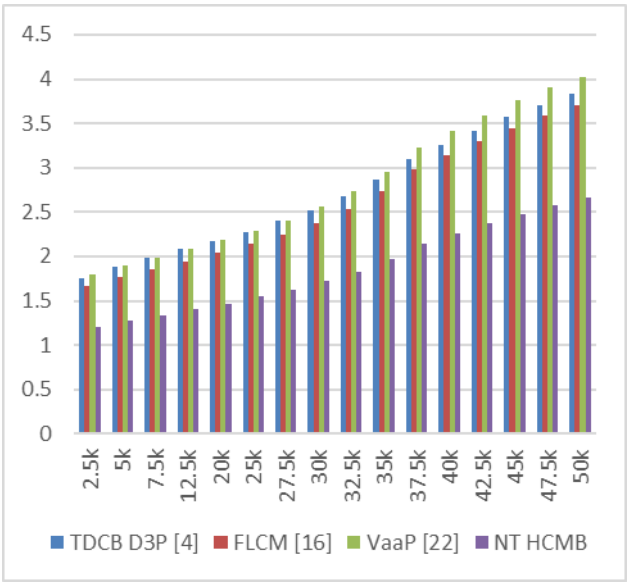


Figure 3. Communication energy under different number of attacks

This analysis shows that the proposed model can achieve 8.5% lower energy compared to TDCB D3P [4], 8.3% lower energy compared to FLCM [16], and 10.5% lower energy compared to VaaP [22] under various numbers of attacks. The use of low complexity consensus models with PoW, PoS, and PoTT models for various attack scenarios reduces this energy. Similar performance was assessed in terms of throughput levels, and the following results are shown in Figure 4 as follows,

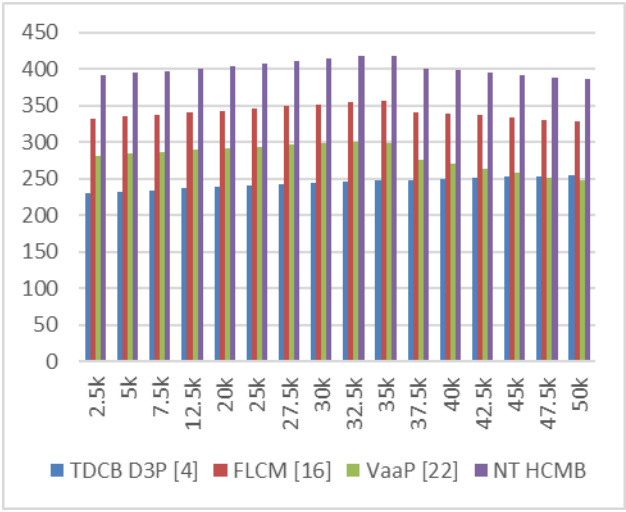


Figure 4 Communication throughput under different number of attacks

Based on the results of this analysis, it is clear that the proposed model outperforms TDCB D3P [4], FLCM [16], and VaaP [22] by an average of 16.4%, 10.5%, and 16.5%, respectively, under a variety of attack scenarios. By employing PoW, PoS, and PoTT Models for various attack scenarios, throughput is increased while still maintaining a low complexity consensus model. PDR (or block mining efficiency) evaluations showed similar results, as shown in Figure 5 as follows,

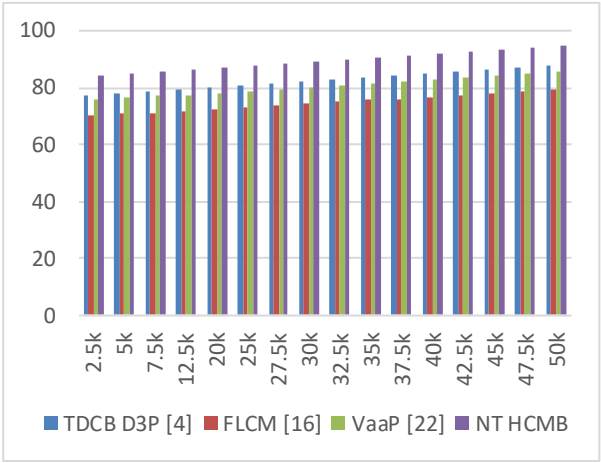


Figure 5 Communication PDR under different number of attacks

The results of this evaluation show that the proposed model is capable of achieving a PDR that is 6.5% higher when compared with TDCB D3P [4], 15.5% higher when compared with FLCM [16], and 9.4% higher when compared with VaaP [22] under a variety of different numbers of attacks. This PDR is increased as a result of the utilization of low-complexity consensus models consisting of PoW, PoS, and PoTT Models for a variety of attack scenarios. The proposed model's performance has been improved to the point where it is now capable of being deployed for a variety of different real-time scenarios.

5.0 CONCLUSION AND FUTURE SCOPE

Initial implementations of the proposed model use a hybrid consensus method that combines Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-Temporary-Trust (PoTT) to enhance security while maintaining higher Quality of Service (QoS) levels. To generate miner-level trust, the PoTT Model combines temporal mining delay, temporal mining energy, throughput, and block mining efficiency. These trust values are combined with Work productivity and Stake levels to select miners. The selected miners are used to fulfil block addition requests, which aids in enhancing mining speed, decreasing energy consumption, increasing throughput, and enhancing block mining efficiency relative to existing mining optimization models. Based on delay estimation, it can be seen that the proposed model can achieve a 10.5% reduction in delay compared to TDCB D3P [4], a 12.4% reduction in delay compared to FLCM [16], and a 12.8% reduction in delay compared to VaaP [22] under varying numbers of attacks. Utilizing low-complexity consensus models with PoW, PoS, and PoTT Models for various attack scenarios reduces this delay. In accordance with estimation of energy levels, it can be seen that the proposed model is able to achieve 8.5% less energy than TDCB D3P [4], 8.3% less energy than FLCM [16], and 10.5% less energy than VaaP [22] under varying numbers of attacks. Utilizing low-complexity consensus models with PoW, PoS, and PoTT Models for various attack scenarios reduces this energy consumption.

Based on this data rate evaluation, it can be seen that the proposed model is capable of achieving 16.4% higher throughput than TDCB D3P [4], 10.5% higher throughput than FLCM [16], and 16.4% higher throughput than VaaP [22] under varying numbers of attacks. Utilizing low-complexity consensus models with PoW, PoS, and PoTT Models for various attack scenarios increases this throughput. Based on evaluation of PDR, it can be seen that the proposed model is capable of attaining a 6.5% higher PDR than TDCB D3P [4], a 15.5% higher PDR than FLCM [16], and a 9.4% higher PDR than VaaP [22] under varying numbers of attacks. This PDR is increased due to the use of PoW, PoS, and PoTT models with low complexity consensus models. As a result of these performance enhancements, the proposed model is deployable in various real-time scenarios.

In future, performance of the proposed model must be validated for multiple attacks and can be extended via use of predictive learning operations. This performance can also be improved via the use of Auto Encoders, Generative Adversarial Networks (GANs), and other deep learning-based models under real-time scenarios.

Acknowledgement

We express our gratitude to Kalinga University, Raipur for providing valuable insights and support for conduction of this study.

References

[1] G. Praveen, S. P. Singh, V. Chamola and M. Guizani, 2022. "Novel Consensus Algorithm for Blockchain Using Proof-of-Majority (PoM)," in *IEEE Networking Letters.* 4(4): 208-211. DOI: 10.1109/LNET.2022.3213971

[2] S. Ma, S. Wang and W. -T. Tsai, 2022. "Delay Analysis of Consensus Communication for Blockchain-Based Applications Using Network Calculus," in *IEEE Wireless Communications Letters.* 11(9): 1825-1829. DOI: 10.1109/LWC.2022.3183197

[3] R. Bezuidenhout, W. Nel and J. M. Maritz, 2023. "Permissionless Blockchain Systems as Pseudo-Random Number Generators for Decentralized Consensus," in *IEEE Access.* 11: 14587-14611. DOI: 10.1109/ACCESS.2023.3244403

[4] Y. Goh, J. Yun, D. Jung and J. -M. Chung, 2022. "Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning," in *IEEE Access.* 10: 118498-118511. DOI: 10.1109/ACCESS.2022.3220852

[5] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang and L. Gao, 2022. "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things," in *IEEE Internet of Things Journal.* 9(6): 4371-4384. DOI: 10.1109/JIOT.2021.3103275

[6] G. Yang, K. Lee, K. Lee, Y. Yoo, H. Lee and C. Yoo, 2022. "Resource Analysis of Blockchain Consensus Algorithms in Hyperledger Fabric," in *IEEE Access*, 10: 74902-74920. DOI: 10.1109/ACCESS.2022.3190979

[7] M. Hu, T. Shen, J. Men, Z. Yu and Y. Liu, 2020. "CRSM: An Effective Blockchain Consensus Resource Slicing Model for Real-Time Distributed Energy Trading," in *IEEE Access*, 8: 206876-206887. DOI: 10.1109/ACCESS.2020.3037694

[8] J. Wan, K. Hu, J. Li and H. Su, 2022. "AnonymousFox: An Efficient and Scalable Blockchain Consensus Algorithm," in *IEEE Internet of Things Journal*, 9(23): 24236-24252. DOI: 10.1109/JIOT.2022.3189200

[9] M. Kaur, M. Z. Khan, S. Gupta, A. Noorwali, C. Chakraborty and S. K. Pani, 2021. "MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols," in *IEEE Access*, 9: 80931-80944. DOI: 10.1109/ACCESS.2021.3085187

[10] Z. Ai and W. Cui, 2022. "A Proof-of-Transactions Blockchain Consensus Protocol for Large-Scale IoT," in *IEEE Internet of Things Journal*, 9(11): 7931-7943. DOI: 10.1109/JIOT.2021.3108627

[11] S. Verma, D. Yadav and G. Chandra, 2022. "Introduction of Formal Methods in Blockchain Consensus Mechanism and Its Associated Protocols," in *IEEE Access.* 10: 66611-66624. DOI: 10.1109/ACCESS.2022.3184799

[12] Qingqing Xie, Fan Dong, Xia Feng, 2023. "HLOChain: A Hierarchical Blockchain Framework with Lightweight Consensus and Optimized Storage for IoT", *Security and Communication Networks.* 2023: 1-14. DOI: 10.1155/2023/3412200

[13] M. Touloupou, M. Themistocleous, E. Iosif and K. Christodoulou, 2022. "A Systematic Literature Review Toward a Blockchain Benchmarking Framework," in *IEEE Access.* 10: 70630-70644. DOI: 10.1109/ACCESS.2022.3188123

[14] R. Tapwal, P. K. Deb, S. Misra and S. K. Pal, 2022. "Amaurotic-Entity-Based Consensus Selection in Blockchain-Enabled Industrial IoT," in *IEEE Internet of Things Journal.* 9(14): 11648-11655. DOI: 10.1109/JIOT.2021.3131501

[15] M. Xu, S. Liu, D. Yu, X. Cheng, S. Guo and J. Yu, 2022. "CloudChain: A Cloud Blockchain Using Shared Memory Consensus and RDMA," in *IEEE Transactions on Computers.* 71(12): 3242-3253. DOI: 10.1109/TC.2022.3147960

[16] Y. Wang, H. Peng, Z. Su, T. H. Luan, A. Benslimane and Y. Wu, 2022. "A Platform-Free Proof of Federated Learning Consensus Mechanism for Sustainable Blockchains," in *IEEE Journal on Selected Areas in Communications.* 40(12): 3305-3324. DOI: 10.1109/JSAC.2022.3213347

[17] P. Zheng et al., 2022. "Aeolus: Distributed Execution of Permissioned Blockchain Transactions via State Sharding," in *IEEE Transactions on Industrial Informatics.* 18(12): 9227-9238. DOI: 10.1109/TII.2022.3164433

[18] H. Afzaal, M. Imran, M. U. Janjua and S. P. Gochhayat, 2022. "Formal Modeling and Verification of a Blockchain-Based Crowdsourcing Consensus Protocol," in *IEEE Access.* 10: 8163-8183. DOI: 10.1109/ACCESS.2022.3141982

[19] D. Huang, X. Ma and S. Zhang, 2020. "Performance Analysis of the Raft Consensus Algorithm for Private Blockchains," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems.* 50(01): 172-181. DOI: 10.1109/TSMC.2019.2895471

[20] C. Santiago, S. Ren, C. Lee and M. Ryu, 2021. "Concordia: A Streamlined Consensus Protocol for Blockchain Networks," in *IEEE Access.* 9: 13173-13185. DOI: 10.1109/ACCESS.2021.3051796

[21] G. Sun, M. Dai, J. Sun and H. Yu, 2021. "Voting-Based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain," in *IEEE Internet of Things Journal.* 8(08): 6257-6272. DOI: 10.1109/JIOT.2020.3029781

[22] X. Fu, H. Wang and P. Shi, 2022. "Votes-as-a-Proof (VaaP): Permissioned Blockchain Consensus Protocol Made Simple," in *IEEE Transactions on Parallel and Distributed Systems.* 33(12): 4964-4973. DOI: 10.1109/TPDS.2022.3211829

[23] Z. Liu, L. Hou, K. Zheng, Q. Zhou and S. Mao, 2022. "A DQN-Based Consensus Mechanism for Blockchain in IoT Networks," in *IEEE Internet of Things Journal.* 9(14): 11962-11973. DOI: 10.1109/JIOT.2021.3132420

[24] Y. Xiao, N. Zhang, W. Lou and Y. T. Hou, 2020. "A Survey of Distributed Consensus Protocols for Blockchain Networks," in *IEEE Communications Surveys & Tutorials.* 22(2): 1432-1465. DOI: 10.1109/COMST.2020.2969706

[25] W. Zhang et al., 2022. "A Trustworthy Safety Inspection Framework Using Performance-Security Balanced Blockchain," in *IEEE Internet of Things Journal,* 9(11): 8178-8190. DOI: 10.1109/JIOT.2021.3121512

[26] Y. Na, Z. Wen, J. Fang, Y. Tang and Y. Li, 2022. "A Derivative PBFT Blockchain Consensus Algorithm With Dual Primary Nodes Based on Separation of Powers-DPNPBFT," in *IEEE Access.*10: 76114-76124. DOI: 10.1109/ACCESS.2022.3192426

[27] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov and Y. Koucheryavy, 2021. "On Performance of PBFT Blockchain Consensus Algorithm for IoT-Applications With Constrained Devices," in *IEEE Access*, 9: 80559-80570. DOI: 10.1109/ACCESS.2021.3085405

[28] L. Yang, Y. Zou, M. Xu, Y. Xu, D. Yu and X. Cheng, 2022. "Distributed Consensus for Blockchains in Internet-of-Things Networks," in *Tsinghua Science and Technology.* 27(5): 817-831. DOI: 10.26599/TST.2021.9010065

[29] K. Otsuki, R. Nakamura and K. Shudo, 2021. "Impact of Saving Attacks on Blockchain Consensus," in *IEEE Access.* 9: 133011-133022. DOI: 10.1109/ACCESS.2021.3115131

[30] Chavan, P. V., and Balani, N., 2023. "Design of heuristic model to improve block-chain-based sidechain configuration," in *International Journal of Computational Science and Engineering.* 26(4):372-384. DOI: 10.1504/IJCSE.2023.132154

[31] F. Aponte, L. Gutierrez, M. Pineda, I. Meriño, A. Salazar and P. Wightman, 2021. "Cluster-Based Classification of Blockchain Consensus Algorithms," in *IEEE Latin America Transactions.* 19(4): 688-696. DOI: 10.1109/TLA.2021.9448552

[32] J. -S. Kim, J. -M. Shin, S. -H. Choi and Y. -H. Choi, 2022. "A Study on Prevention and Automatic Recovery of Blockchain Networks Against Persistent Censorship Attacks," in *IEEE Access.* 10: 110770-110784. DOI: 10.1109/ACCESS.2022.3214213

[33] X. Jiang, A. Sun, Y. Sun, H. Luo and M. Guizani, 2023. "A Trust-Based Hierarchical Consensus Mechanism for Consortium Blockchain in Smart Grid," in *Tsinghua Science and Technology.* 28(1): 69-81. DOI: 10.26599/TST.2021.9010074

[34] S. H. Alsamhi et al., 2023. "Blockchain-Empowered Security and Energy Efficiency of Drone Swarm Consensus for Environment Exploration," in *IEEE Transactions* on Green Communications and Networking. 7(1): 328-338. DOI: 10.1109/TGCN.2022.3195479

[35] Balani, N., Chavan, P., and Ghonghe, M., 2022. Design of high-speed blockchain-based sidechaining peer to peer communication protocol over 5G networks. *In Multimedia Tools and Applications.* 81(25): 36699–36713. DOI: 10.1007/s11042-021-11604-6