

Novel approach for the design of attack-aware context-based blockchain model

Smita Kapse *

*Department of Computer Science and Engineering
Kalinga University
Raipur 492001
Chhattisgarh
India*

and

*Department of Computer Technology
Yeshwantrao Chavan College of Engineering
Nagpur 441110
Maharashtra
India*

Latesh Malik [†]

*Department of Computer Science and Engineering
Govt. College of Engineering
Nagpur 441108
Maharashtra
India*

Sanjay Kumar [§]

*Department of Computer Science and Engineering
Kalinga University
Raipur 492001
Chhattisgarh
India*

* E-mail: smitarkapse@gmail.com (Corresponding Author)

[†] E-mail: latesh.gagan@gmail.com

[§] E-mail: sanjay.kumar@kalingauniversity.ac.in

Abstract

Security and privacy are two intertwined pillars of any communication network. Blockchain plays a pivotal role to achieve this in today's market place. Blockchain network has versatile application domain in today's era as it provides transparency, robustness, and security. In this paper a hybrid model is design using Proof of Temporal Trust (PoTT) and Proof of Spatial Trust (PoST) to articulate attack-aware context-based blockchain model. This novel approach considers two perspectives temporal and spatial of consensus mechanisms. PoTT deals with miner evaluation based on delay in mining, throughput, energy requirement etc. whereas PoST deals with security issue. By synergistically combining PoTT and PoST, our model improves the mining speed by 4.5%, reduces energy consumption by 4.9%, and enhances throughput by 10.5% even under adverse conditions of targeted attacks. This hybrid model facilitates holistic, robust, high-performance technique. Through extensive simulations and real-world scenarios, we validate the efficacy and efficiency of our proposed model, marking a significant advancement in consensus algorithms for context-aware blockchains.

Subject Classification: Primary 68P27, Secondary 68M25.

Keywords: Blockchain technology, Consensus algorithms, Quality of service (QoS), Temporal trust, Spatial trust.

1. Introduction

Blockchain technology has diversified application in today's era including healthcare [1], digital forensics [2], education [3], library management [4] and many more. As it promises immutable, distributed, transparent, decentralized type of service. One of the prime concerns in blockchain network is the design of secure consensus mechanism.

The consensus mechanisms like Proof of Work and Proof of Stake have some issues in terms of energy efficiency and susceptible to various types of attacks such as Man-in-the-Middle (MITM), Sybil, Finney, and Distributed Denial of Service (DDoS).

To overcome these issues this paper proposes design of attack aware context based blockchain model. This hybrid model combines Proof of Temporal Trust (PoTT) and Proof of Spatial Trust (PoST) in order to build attack aware network and also to improvise other performance metrics block mining speed, energy requirement, throughput, etc. [5,6].

This paper introduces concept of Proof of Temporal trust (PoTT) which uses past mining performance for delay, energy consumption and throughput, which facilitates effective resource allocation.

Another contribution of this paper is introduction of Proof of Spacial Trust (PoST), which evaluates miners resilience to attacks including Man-

in-the Middle attack, Finney, Sybil, etc. which improvise security of the network.

Finally, the hybrid model is built by combining these two models namely PoTT and PoST to improve security and efficiency of the blockchain model.

To confirm the effectiveness of the proposed model comprehensive simulation and real-world tests was conducted. Specifically, we demonstrate a 4.5% increase in mining speed, a 4.9% reduction in energy consumption, and a 10.5% improvement in throughput under attack scenarios.

2. Literature Review

The fundamental component of blockchain technology that allows for secure and decentralized transaction verification is consensus models. Classical consensus techniques like Proof of Work (PoW) and Proof of Stake (PoS) having restrictions on their ability to withstand attacks. As per the demand of today's era highly scalable, fast and secure consensus model is needed. This section discusses advancements made in this area in comparison to our proposed approach process [7, 8, 9].

One of the models based on integration of space and time variable is called as Proof of Space-Time (PoST), which checks the miner nodes legitimacy with less power. Evenif this model performs well in terms of energy consumption but it lacks in providing security against temporal and spatial attack vectors, a gap that our Proof of Temporal Trust (PoTT) and Proof of Spatial Trust (PoST) aim to fill for different scenarios [10, 11, 12].

Delegated Proof of Stake (DPoS) is an advance version of PoS. It uses election mechanism to select the delegate to validate the transaction. Although DPoS is energy conservative and fast as compare to PoW but centralization and collusion among delegates are the problems associated with it. The proposed model addresses this issue using trust-based evaluations [13].

Current consensus models have shown significant reduction in energy consumption, speed and scalability but they are susceptible to attacks in terms of temporal and spatial contexts. This model combines PoTT and PoST in order to achieve high degree of efficiency and security against wide range of attacks.

3. Proposed Methodology

From the exhaustive literature survey done in the above section, it is observed that most of the consensus models are highly complex or less scalable. To resolve this issue, this paper proposes Novel approach for the design of attack-aware consensus model for context-aware blockchain. This model uses PoTT which evaluates mining performance based on historical metrics which includes mining delay, energy consumption, throughput via equation 1

$$PoTT = \frac{1}{Nt} \sum_{i=1}^{Nt} \frac{Th}{D * E} \quad \dots(1)$$

Where Nt indicates miners temporal communication, Th stand for throughput, D stands for delay levels and E stands for energy levels during Nt mining communication operations under different attacks.

While, PoST, measures the resilience of miners under security threats, and estimates the PoST score via equation 2,

$$PoST = \frac{e * PDR}{\sum_{i=1}^{NM} d(i)} \quad \dots(2)$$

In equation 2, e represents the residual energy of miner nodes, PDR is its average packet delivery ratio levels, and d is its distance from other nodes. The Th , D & E metrics are estimated via equations 3, 4 & 5, while PDR & d are estimated via equations 6 & 7 as follows,

$$Th = \frac{P(Rx)}{D} \quad \dots(3)$$

$$D = ts(complete) - ts(init) \quad \dots(4)$$

$$E = e(init) - e(complete) \quad \dots(5)$$

$$PDR = \frac{P(Rx)}{P(Tx)} \quad \dots(6)$$

$$d(i, j) = \sqrt{(xi - xj)^2 + (yi - yj)^2} \quad \dots(7)$$

Where, $P(Rx)$: number of packets received, $P(Tx)$: number of packets transmitted in the process of mining, ts : timestamps, x & y : miner node locations. PoTT and PoST levels of trust are combined via equation 8,

$$PoSTT = PoST + PoTT \quad \dots(8)$$

For each miner PoSTT ((Proof of Temporal Trust and Proof of Spatial Trust) level is calculated, and after that trust threshold was estimated via equation 9,

$$PoSTT(th) = \frac{1}{NM} \sum_{i=1}^{NM} PoSTT(i) \quad \dots(9)$$

Miners with $PoSTT > PoSTT(th)$ are selected, and used for the mining process. Because of this, the model is able to maximize throughput, energy, and delay during these mining requests while being attacked. Efficiency of this model was estimated in terms of different metrics & compared with existing models in the next section of this text.

4. Result Analysis and Comparison

The proposed model known as PoSTT represents a pioneering paradigm shift in blockchain technology. PoSTT integrates two fundamental dimensions of trustworthiness, temporal and spatial, to establish a highly adaptive, secure, and efficient consensus framework. PoTT (Proof of Temporal Trust) evaluates miners based on historical performance metrics, including mining delay, energy consumption, and throughput, thereby optimizing resource allocation and efficiency. Concurrently, PoST (Proof of Spatial Trust) assesses miners' resilience to security threats like Man-in-the-Middle (MITM), Sybil, Finney, and DDoS attacks, ensuring network security. By seamlessly combining these proofs of trust, PoSTT significantly enhances mining speed, reduces energy consumption, and improves throughput even under the most adverse attack conditions, marking a substantial advancement in consensus algorithms tailored for the intricacies of context-aware blockchain operations.

The blockchain network was deployed using open-source blockchain software, tailored to accommodate our proposed PoSTT consensus model, which was tested on the Historical Blockchain Data and Attack Scenarios Dataset.

Our experimental setup involved a variety of input parameters in order to assess PoSTT consensus mechanism. Sample values for some of these parameters include: Number of Miners (NM) which varies from 30,000 to 600,000 miners, Network Latency (NL) which varies from 1 ms to 100 ms, Transaction Load (TL) which varies from 1,000 to 100,000 transactions per minute, Attack Intensity (AI) by adjusting parameters

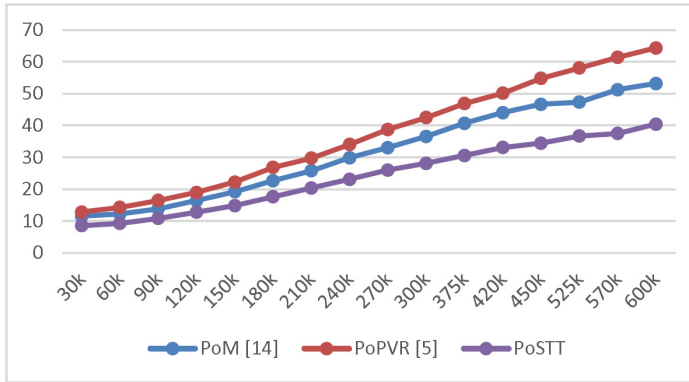


Figure 1

Delay needed for mining under attack scenarios

such as attack duration, frequency, and scale and Mining Hardware Configuration (MHC)

By systematically varying these input parameters performance of PoSTT was measured under diverse conditions, including scalability, security, efficiency, and resilience to attacks. For every miner mining delay (D) was estimated via equation 10 as follows,

$$D = \frac{1}{NM} \sum_{i=1}^{NM} ts_{reach} - ts_{start} \quad \dots(10)$$

Where, ts_{reach} & ts_{start} represents timestamp to reach to the destination and source node respectively. The delay performance was compared with PoM [14], PoPVR [5] in Figure 1.

Mining delay is a crucial parameter in blockchain systems as it directly impacts transaction throughput and overall network efficiency. Lower mining delay signifies faster transaction validation and confirmation. When examining the mining delay for a blockchain network with varying numbers of miners (NM), we observe that the proposed PoSTT consistently outperforms the other models. For instance, at 30,000 miners, PoSTT records a mining delay of 8.548 seconds, which is notably lower than PoM's 11.496 seconds, and PoPVR's 12.814 seconds. This trend continues as the number of miners increases, showcasing the superior performance of PoSTT.

The impacts of these lower mining delays are multifaceted. First, reduced mining delay directly translates to faster transaction processing, enhancing the blockchain's throughput and scalability. Second, it improves the overall user experience by minimizing the time required for transaction

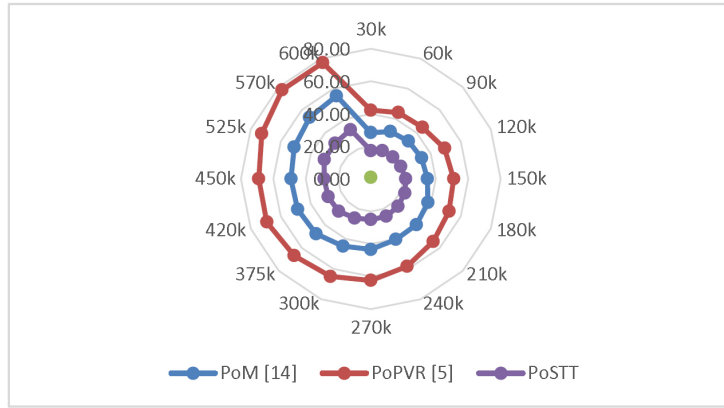


Figure 2

Energy needed for mining under attack scenarios

confirmation, making blockchain applications more efficient and user-friendly.

Equation 11 was used to estimate the performance for energy consumption, which is depicted in Figure 2.

$$E = \frac{1}{NM} \sum_{i=1}^{NM} E_{src}(start)_i - E_{src}(complete)_i \quad \dots(11)$$

Where, $E(start)$ & $E(complete)$ represents energy levels of source node during start & completion of mining operations.

In the context of energy consumption for mining under attack scenarios, the comparison among the three models - PoM [14], PoPVR [5] and the proposed PoSTT model. The energy consumption (E) is a critical metric as it directly affects the sustainability and operational costs of a blockchain network. Lower energy consumption indicates that the network is more energy-efficient, which is not only environmentally friendly but also economically advantageous.

Upon analyzing the energy consumption data across different numbers of miners (NM), results shows that the PoSTT model gives best energy efficiency. For example, when there are 30,000 miners, PoSTT requires only 17.34 mW of energy, which is significantly lower than PoM's 28.43 mW and PoPVR's 42.26 mW.

The impacts of this lower energy consumption are twofold. First, it reduces the overall environmental footprint of the blockchain network, aligning with sustainability goals. Second, it lowers the operational costs

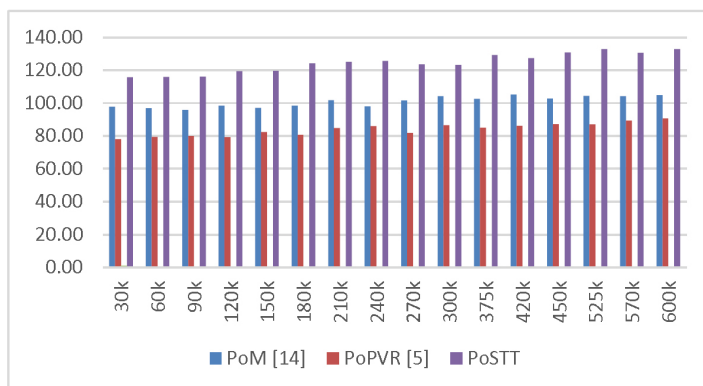


Figure 3

Total throughput for mining under attack scenarios

for miners and network participants, making it more economically viable to engage in mining activities.

Figure 3 shows performance for throughput. Analyzing the total throughput (THR) for mining under attack scenarios across different numbers of miners (NM) provides valuable insights into the efficiency and scalability of blockchain models. Total throughput is a crucial metric as it reflects the network's capacity to handle transactions effectively and is a key determinant of its overall performance.

When comparing the total throughput of three models - PoM [14], PoPVR [5] and the proposed PoSTT model - it becomes evident that PoSTT consistently outperforms the others. For instance, at 30,000 miners, PoSTT achieves a total throughput of 115.65 vpm (transactions per minute), which is significantly higher than PoM's 97.80 vpm and PoPVR's 77.95 vpm.

The impacts of this superior total throughput are substantial. It ensures that the blockchain network can handle a higher volume of transactions, making it more suitable for real-world applications with varying levels of demand. This scalability is crucial for blockchain's widespread adoption, as it ensures that the network can accommodate increased activity without sacrificing performance.

5. Conclusion and Future Scope

A hybrid consensus model which is based on Proof of temporal trust and Proof of Special Trust is proposed in this paper which overcome the

problems associated with context-aware blockchains operating under various attack scenarios.

Our extensive comparative analysis demonstrated that PoSTT outperforms existing models in key metrics such as mining delay, energy consumption, and total throughput. PoSTT consistently exhibited lower mining delays, reduced energy consumption, and higher total throughput, even in adverse conditions of targeted attacks. Experimental results show the efficiency of PoSTT in enhancing blockchain efficiency, security, and scalability.

In conclusion, our proposed PoSTT model represents a significant advancement in consensus algorithms for context-aware blockchains. It enhances the efficiency and security of blockchain operations as well as contributes to the broader goals of sustainability and scalability in the blockchain industry. The future holds exciting possibilities for further refinement and application of PoSTT in diverse blockchain ecosystems.

References

- [1] Agbo, Cornelius C, et al. "Blockchain Technology in Healthcare: A Systematic Review." *Healthcare*, 7, no. 2 : 56, pp. 1-30, (2019).
- [2] Suri, Bhawna, et al. "A blockchain based private framework for facilitating digital forensics using IoT." *Journal of Discrete Mathematical Sciences and Cryptography*, 26 : 5, pp. 1249–1263, (2023).
- [3] S. Kapse, et al. "Blockchain Based Solution for Secured Transmission of Examination Paper," *IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC), Gunupur, Odisha, India*, pp.1-6, (2023).
- [4] Sharma Shallu and Batth Ranbir Singh. "BLOCKLIB: Blockchain enabled library resource sharing." *Journal of Discrete Mathematical Sciences and Cryptography*, 25:3, pp 839-857, (2022).
- [5] R. Bezuidenhout, et al. "Permissionless Blockchain Systems as Pseudo-Random Number Generators for Decentralized Consensus." *IEEE Access*, vol. 11, pp. 14587-14611, 2023.
- [6] S. Islam, et al. "A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues." *IEEE Access*, vol. 11, pp. 39066-39082, (2023).

- [7] C. Xu, et al. "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things." *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4371-4384, (2022).
- [8] G. Yang, et al. "Resource Analysis of Blockchain Consensus Algorithms in Hyperledger Fabric." *IEEE Access*, vol. 10, pp. 74902-74920, (2022).
- [9] J. Wan, et al. "Anonymous Fox: An Efficient and Scalable Blockchain Consensus Algorithm." *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 24236-24252, (2022).
- [10] J. Abdella, et al. "HiCoOB: Hierarchical Concurrent Optimistic Blockchain Consensus Protocol for Peer-to-Peer Energy Trading Systems." *IEEE Transactions on Smart Grid*, vol. 14, no. 5, pp. 3927-3943, (2023).
- [11] Kumar, Ankit, Pankaj Dadheech, Vijander Singh, Ramesh C. Poonia, and Linesh Raja. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22, no. 4 (2019).
- [12] J. Xu, et al. "A Blockchain-Based Framework for Supervision of Livelihood Issues: Proof of Concept with Optimized Consensus." *IEEE Access*, vol. 11, pp. 73414-73434, (2023).
- [13] Z. Ai and W. Cui. "A Proof-of-Transactions Blockchain Consensus Protocol for Large-Scale IoT." *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 7931-7943, (2022).
- [14] G. Praveen, et al. "Novel Consensus Algorithm for Blockchain Using Proof-of-Majority (PoM)." *IEEE Networking Letters*, vol. 4, no. 4, pp. 208-211, (2022).