Library Progress International
Vol.44 No.3, Jul-Dec 2024: P.12392-12407

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

TSETC: Design of an efficient trust-based security model with spatial & temporal consensus for blockchain-based deployments

Dharmendra Kumar Roy[1]*, Asha Ambhaikar[2]

[1] Research Scholar, CSE, MATS University, Arang, Raipur (Chhattisgarh), India

[2] Professor, MATS School of Engineering and IT, MATS University, Arang, Raipur (Chhattisgarh), India

roy.dharmendra@gmail.com[1], drambhaikar@gmail.com[2]

How to cite this article: Dharmendra Kumar Roy, Asha Ambhaikar (2024) TSETC: Design of an efficient trust-based security model with spatial & temporal consensus for blockchain-based deployments. *Library Progress International,* 44(3), 12392-12407.

Abstract

Abstract: Existing Proof of Work (PoW) and Proof of Stake (PoS) consensus models, in particular, lack the resilience and efficiency necessary to meet today's high-speed, low-energy, secure, and robust data transaction requirements. These flaws have proven problematic, necessitating an urgent need for a more adaptable and resilient security model process. This paper proposes a novel consensus model that addresses these shortcomings by combining PoW and PoS consensus methodologies with Spatial and Temporal Trust Levels. During the block mining process, these levels are cleverly estimated by an advanced processing algorithm of miner node parameters, such as delay and energy requirements, throughput performance, Packet Delivery Ratio (PDR) performance, and jitter performance. The model surpasses its predecessors by adopting a proactive stance in order to anticipate and mitigate potential risks while simultaneously optimizing performance metrics. Several empirical findings demonstrate that the proposed TSETC model is superior in various respects. The model accomplished better speed, lower energy consumption, improved throughput, and improved PDR levels. In addition, it maintained lower jitter, even during attacks, in comparison to recently proposed models. In essence, this paper presents a paradigm shift in the security models of blockchain-based deployments by introducing a novel, adaptable, and efficient solution that significantly improves the overall system's resilience and performance. This innovative strategy promises a safer, more environmentally friendly, and more reliable future for blockchain technology applications.

Keywords: Blockchain Consensus Models, Proof of Work, Proof of Stake, Spatial and Temporal Trust Levels, Data Manipulation Attacks

1. Introduction

The importance and reliance on secure, efficient, and resilient data transactions cannot be overstated as we usher in an increasingly digital era. In terms of ensuring secure, transparent, and tamper-proof transactions, blockchain technology has proven to be a game-changer among emerging technologies. The beating heart of blockchain technology is its consensus mechanisms, in which multiple parties concur on a single version of the truthful data.

While Proof of Work (PoW) and Proof of Stake (PoS) are innovative consensus models, they have inherent limitations. PoW is criticized for its excessive energy consumption and low throughput, which raises environmental and scalability concerns. PoS, on the other hand, while addressing the issue of energy consumption, introduces potential security risks because those with larger stakes may monopolize the system, thereby endangering its decentralization characteristics, like with the use of Proof-of-Majority (PoM) consensus [1, 2, 3].

In addition, both PoW and PoS [3, 4] are susceptible to sophisticated data manipulation attacks, which have become more common in recent years [4, 5, 6]. These limitations have necessitated the development of a more

robust and efficient consensus mechanism with the use of Deep Reinforcement Learning (DRL), that are capable of withstanding today's high-speed, low-energy, secure, and robust data transaction requirements, as well as defending against data manipulation attacks.

This paper proposes a novel consensus model that combines the PoW and PoS methodologies with the introduction of Spatial and Temporal Trust Levels in response to these demands. During the mining process, this innovative model takes into account various miner node parameters, including delay and energy requirements, throughput performance, Packet Delivery Ratio (PDR) performance, and jitter performance. The incorporation of these spatial and temporal factors permits a more holistic and contextual evaluation of each transaction, thereby improving the consensus procedure.

A key component of the TSETC model is a self-correcting mechanism that enhances security during data manipulation attacks. Dynamic self-correction ensures system resilience and robustness, even under extreme conditions, and promises a proactive strategy for detecting, mitigating, and preventing potential threats.

The superiority of the TSETC model is demonstrated by a 9.5% increase in speed, an 8.3% reduction in energy consumption, a 12.5% increase in throughput, and a 2.9% improvement in PDR, as determined by an exhaustive empirical evaluation. In addition, it exhibits a 4.5% reduction in jitter, even during attacks, when compared to other recent models.

This paper aims to induce a paradigm shift in the security models for blockchain-based deployments by introducing a novel and adaptable solution that promises a safer, greener, and more dependable future for blockchain applications. By adopting this innovative consensus model, the blockchain industry can respond more effectively to the ever-changing digital landscape's dynamic challenges.

2. Literature Review

A thorough comprehension of the current state of consensus mechanisms in blockchain technology requires an investigation of earlier models. This section will provide a comprehensive analysis of the most prominent existing models, including PoW, PoS, and their variants, before elaborating on the limitations that necessitated our TSETC model process.

Blockchain technology has gained prominence in recent years due to its potential to revolutionize various industries, including vehicular networks. Ensuring the security, efficiency, and scalability of blockchain consensus mechanisms is crucial for their successful implementation in vehicular networks. To address these challenges, researchers have TSETC various innovative consensus algorithms and mechanisms.

In "Novel Consensus Algorithm for Blockchain Using Proof-of-Majority (PoM)" [2], Praveen et al. introduced a novel consensus algorithm that enhances the security and efficiency of blockchain networks. This paper focuses on the Proof-of-Majority (PoM) algorithm, which provides an alternative approach to consensus.

Another important aspect of blockchain consensus is the delay analysis, which is discussed in "Delay Analysis of Consensus Communication for Blockchain-Based Applications Using Network Calculus" [3] by Ma, Wang, and Tsai. This paper leverages network calculus to analyze the delay in consensus communication, which is crucial for real-time applications in vehicular networks.

In "Permissionless Blockchain Systems as Pseudo-Random Number Generators for Decentralized Consensus" [4], Bezuidenhout, Nel, and Maritz explore the use of permissionless blockchain systems as pseudo-random number generators. This innovative approach contributes to the decentralized consensus mechanism.

Security is a paramount concern in blockchain consensus, and "Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning" [5] by Goh, Yun, Jung, and Chung introduces a secure trust-based delegated consensus mechanism that utilizes deep reinforcement learning to enhance security.

IoT plays a vital role in vehicular networks, and "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for the Internet of Things" [6] by Xu et al. presents a lightweight and attack-proof bidirectional blockchain paradigm tailored for IoT applications.

Resource analysis of blockchain consensus algorithms is essential for optimizing network performance, as demonstrated in "Resource Analysis of Blockchain Consensus Algorithms in Hyperledger Fabric" [7] by Yang, Lee, Yoo, and Lee. This paper analyzes the resource requirements of consensus algorithms in the context of Hyperledger Fabric.

"AnonymousFox: An Efficient and Scalable Blockchain Consensus Algorithm" [8] by Wan, Hu, Li, and Su introduces the AnonymousFox consensus algorithm, which focuses on efficiency and scalability, critical factors for vehicular networks.

Performance analysis is a key area of research, as seen in "MBCP: Performance Analysis of Large-Scale Mainstream Blockchain Consensus Protocols" [9] by Kaur, Khan, Gupta, Noorwali, Chakraborty, and Pani. This paper provides a comprehensive performance analysis of mainstream blockchain consensus protocols.

IoT applications are further explored in "A Proof-of-Transactions Blockchain Consensus Protocol for Large-Scale IoT" [10] by Ai and Cui, which presents a proof-of-transactions consensus protocol tailored for large-scale IoT deployments.

In the context of the Internet of Vehicles (IoV), "A Parallel Consensus Mechanism Using PBFT Based on DAG-Lattice Structure in the Internet of Vehicles" [11] by Zhang, Li, and Zhao introduces a parallel consensus mechanism based on PBFT, designed specifically for IoV scenarios.

Formal methods are introduced into blockchain consensus mechanisms in "Introduction of Formal Methods in Blockchain Consensus Mechanism and Its Associated Protocols" [12] by Verma, Yadav, and Chandra, enhancing the rigor and reliability of these mechanisms.

"Amaurotic-Entity-Based Consensus Selection in Blockchain-Enabled Industrial IoT" [13] by Tapwal, Deb, Misra, and Pal presents a consensus selection mechanism tailored for industrial IoT environments, emphasizing reliability and robustness.

Overlay topology and cost-termination tradeoffs are explored in "Exploring Overlay Topology Cost-Termination Tradeoff in Blockchain Vicinity-Based Consensus" [14] by Mattos, Carrara, Albuquerque, and Mossé, shedding light on the tradeoffs associated with blockchain consensus mechanisms.

"CloudChain: A Cloud Blockchain Using Shared Memory Consensus and RDMA" [15] by Xu, Liu, Yu, Cheng, Guo, and Yu introduces CloudChain, a cloud-based blockchain utilizing shared memory consensus and RDMA, enhancing scalability and performance.

"Sustainable blockchains are essential, and "A Platform-Free Proof of Federated Learning Consensus Mechanism for Sustainable Blockchains" [16] by Wang, Peng, Su, Luan, Benslimane, and Wu introduces a proof of federated learning consensus mechanism designed for sustainability.

Formal modeling and verification are crucial in blockchain consensus, as demonstrated in "Formal Modeling and Verification of a Blockchain-Based Crowdsourcing Consensus Protocol" [17] by Afzaal, Imran, Janjua, and Gochhayat, which focuses on the formal analysis of a crowdsourcing consensus protocol.

Streamlined consensus protocols are explored in "Concordia: A Streamlined Consensus Protocol for Blockchain Networks" [18] by Santiago, Ren, Lee, and Ryu, emphasizing simplicity and efficiency in consensus mechanisms.

State sharding is an essential concept in blockchain scalability, discussed in "Aeolus: Distributed Execution of Permissioned Blockchain Transactions via State Sharding" [19] by Zheng et al., which explores distributed

execution in permissioned blockchain transactions.

Addressing active attacks in RAFT-based IoT blockchain networks is the focus of "Countering Active Attacks on RAFT-Based IoT Blockchain Networks" [20] by Buttar, Aman, Rahman, and Abbasi, enhancing the security of IoT blockchain networks.

Efficiency and security improvements through a voting-based decentralized consensus design are highlighted in "Voting-Based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain" [21] by Sun, Dai, Sun, and Yu for different use cases.

The "Votes-as-a-Proof (VaaP): Permissioned Blockchain Consensus Protocol Made Simple" [22] paper by Fu, Wang, and Shi introduces VaaP, a simplified permissioned blockchain consensus protocol process. In "A DQN-Based Consensus Mechanism for Blockchain in IoT Networks" [23], Liu, Hou, Zheng, Zhou, and Mao present a consensus mechanism based on Deep Q-Networks (DQN) tailored for IoT networks.

Finally, "A Derivative PBFT Blockchain Consensus Algorithm With Dual Primary Nodes Based on Separation of Powers-DPNPBFT" [24] by Na, Wen, Fang, Tang, and Li introduces a derivative PBFT consensus algorithm with dual primary nodes, enhancing security and reliability levels. This review reveals that despite significant efforts to optimize consensus mechanisms in blockchain technology, challenges continue to exist. Specifically, issues relating to energy consumption, scalability, attack resilience, and upholding the decentralization principle remain unresolved. This paper proposes a novel consensus model that aims to overcome these limitations by combining the benefits of PoW and PoS with a robust and dynamic trust-based system, offering significant improvements in speed, energy efficiency, throughput, packet delivery ratio (PDR), and jitter performance levels.

3. TSETC design of an efficient trust-based security model with spatial & temporal consensus for blockchain-based deployments

As per the review of existing models used for enhancing the mining performance of blockchain-based deployments, it can be observed that the complexity of these models is high when deployed for real-time scenarios, or these models have lower Quality of Service (QoS) performance when used for large-scale networks. To overcome these issues, this section discusses design of an efficient trust-based security model with spatial & temporal consensus for blockchain-based deployments.

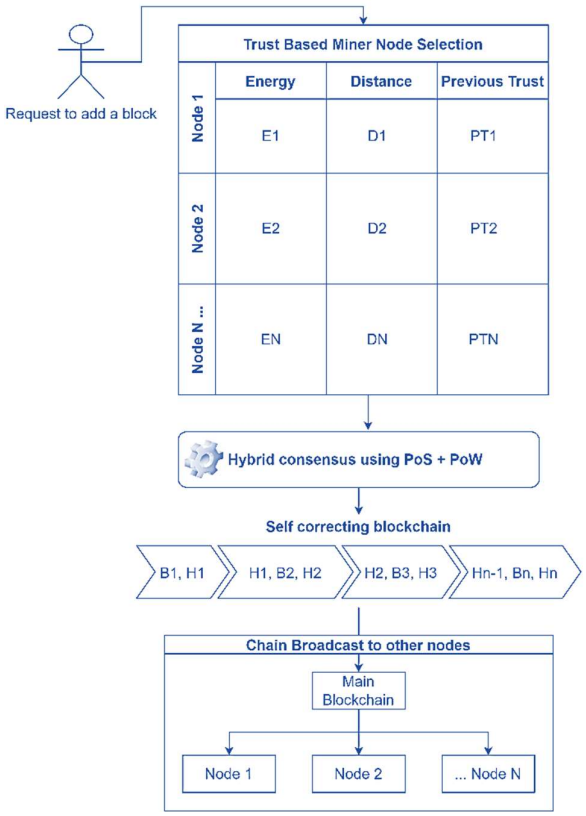

Figure 1. Design of the TSETC model for high-efficiency consensus

As per figure 1, the TSETC model initially collects Spatial & Temporal information from the network nodes, and estimates an Iterative Trust Score (ITS) for each node via equation 1,

$$ITS(i) = \frac{1}{NC}\sum_{j=1}^{NC}\frac{PDR(j) * THR(j)}{D(j) * E(j) * J(j)} \dots (1)$$

Where, NC represents total Number of Temporal Mining Requests served by the nodes, while, PDR represents Packet Delivery Ratio during these mining requests and is estimated via equation 2, THR represents mining throughput and is calculated via equation 3, D represents delay during these requests and is estimated via equation 4, while E represents energy needed during these mining requests, which is estimated via equation 5, while J represents Jitter levels, which are estimated via equation 6, as follows,

$$PDR = \frac{Rx(P)}{Tx(P)} \dots (2)$$

Where, $Rx(P)$ & $Tx(P)$ represents the number of received & transmitted packets during different mining operations.

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

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

Where, ts represents different timestamps, while $complete$ & $init$ represents completion & initialization instances for these requests.

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

Where, e represents residual energy of nodes during the mining requests.

$$J = D - \mu(D) \dots (6)$$

Where, $\mu(D)$ represents mean value of communication delay, which is estimated during individual communication requests. Using these values, Trust Level (TL) between two miner nodes is estimated via equation 7,

$$TL(i,j) = \sqrt{ITS(i) * ITS(j)} * \frac{e(i) + e(j)}{2 * d(i,j)} \dots (7)$$

Where, $d(i,j)$ is the Euclidean Distance between the nodes, and is estimated via equation 8,

$$d(i,j) = \sqrt{\begin{matrix}(xi - xj)^2 + (yi - yj)^2 \\ +(zi - zj)^2\end{matrix}} \dots (8)$$

Where, x, y & z are the Cartesian coordinates of the nodes. The Trust Levels are estimated for each node (marked as 'Source') which needs to add new blocks into the blockchains. Based on these trust levels for the 'Source' node, an Iterative threshold is estimated via equation 9,

$$TL(th) = \sum_{i=1}^{NN} \frac{TL(i,src)}{NN} \dots (9)$$

Where, NN represents total number of nodes present in the network that can participate in the mining process. Nodes with $TL(i,src) > TL(th)$ are marked as 'Selected for Mining & Consensus', and are used to mine new blocks. The mining responses from these nodes are combined via equation 10,

$$MR = \frac{W + S}{2} \dots (10)$$

Where, W & S represents the amount of Work done by the node, and amount of Stake of the node which has participated in the mining process. Nodes with higher values of Mining Response (MR) are selected, and their hash values are used to create new blocks. Each of these blocks contains the following information sets,

- Hash of the Previous Block (PH)
- IP of Source & Destination Nodes
- Timestamp of communication
- Data communicated by the nodes
- Nonce value (which is generated by the miners)
- Hash (H) of the Current Block Sets

This information is used by the blockchain network to add new blocks. In case of block tampering, the following condition in equation 11 is not held to be true,

$$H(i) = PH(i + 1) \dots (11)$$

In such a case, the TSETC model uses an autocorrection mechanism, which works as follows,

- Once the blockchain present at a node (n) is found to be 'tampered', then trust levels of other nodes is observed w.r.t. this node's trust levels.
- Based on this information, correction trust threshold ($C(th)$) is estimated via equation 12,

$$C(th) = \frac{1}{NN^2} \sum_{i=1}^{NN} \sum_{j=1}^{NN} TL(i,j) \dots (12)$$

- Miner nodes with $TL(i,n) > C(th)$ are selected, and their blockchains are used to correct the blockchain of current set of nodes.

Due to which the model is able to identify tampering attacks via equation 11, and correct them via equation 12, which assists in improving its scalability under real-time attack scenarios. Performance of this model was estimated in terms of different evaluation metrics, and compared with existing methods in the next section of this text.

4. Result analysis & comparison

The TSETC model performs an efficient fusion of Spatial & Temporal Trust levels in order to improve the miner selection & consensus performance while mining new blocks. The TSETC model incorporates end to end delay, energy consumption, throughput & packet delivery ratio in order to improve the mining performance under real-time scenarios. Several metrics are considered to analyze and evaluate the performance of the simulated network. The network is comprised of between 200 and 4000 nodes, which represents the total number of individual devices or elements in the network. Fixed at a size of 3.5 km x 3.5 km, the network size indicates the spatial extent of the simulated network.

The network's power consumption is measured in various scenarios. It is estimated that the idle power, which is the power consumed when nodes are not actively transmitting or receiving data, is 2 mW. When nodes are in a reception state, where they are actively receiving data, their power consumption increases to 2.5 milliwatts. During data transmission, however, the power consumption increases to 4 mW. The power consumption drops significantly to 0.005 mW when the nodes are in a sleep state, consuming minimal energy while remaining operational. During transitions between states, such as the transition from sleep to active mode, 0.4 mW of transition power is considered for simulations.

The network is further segregated into a variable number of blocks, ranging from 4,000 to 500 million. These blocks can represent various network elements or divisions, each with its own purpose or characteristics. Collectively, these metrics provide insight into the behavior, power consumption, and scale of the simulated network, thereby facilitating the analysis and optimization of its performance levels.

Based on these configurations, total 10% of all communication requests were injected as attack packets, which included Sybil, Spoofing, Spying & Man-in-the-Middle attacks. A Sybil attack is a type of malicious activity in which a person or organization creates multiple fake identities or network nodes in order to gain control or sway over a network. In the context of blockchain-based networks, a Sybil attack involves the creation of multiple fraudulent identities capable of manipulating consensus mechanisms and undermining the network's integrity and trust. By controlling a substantial portion of the network's nodes, the attacker may be able to undermine the blockchain's decentralized nature and compromise its security. Implementing identity verification mechanisms and consensus algorithms that can detect and mitigate the presence of fake or malicious nodes is necessary to prevent Sybil attacks.

Spying attacks, also known as eavesdropping attacks, occur when an attacker intercepts and monitors communication between two or more participants in a blockchain-based network. The goal of the attacker is to gain unauthorized access to sensitive information such as transaction details, private keys, or any other network-transmitted data. By exploiting vulnerabilities in the network's encryption protocols or compromising the security

of the participating nodes, an attacker can potentially obtain valuable information and manipulate the network for his or her own benefit. To reduce the risk of eavesdropping, blockchain networks should employ robust encryption techniques and secure communication channels to protect the confidentiality and integrity of transmitted data.

An attacker impersonates a legitimate participant or node in a blockchain-based network during a spoofing attack. By impersonating a trusted entity, the attacker intends to deceive other network participants in order to gain unauthorized access to sensitive data or manipulate network operations. This type of attack can take various forms, such as IP address spoofing, in which the attacker impersonates a trusted node by forging their network address. Spoofing attacks have the potential to undermine the network's security and trustworthiness, leading to unauthorized transactions or unauthorized access to sensitive data. Implementing strong authentication mechanisms and multi-factor authentication can aid in the prevention of spoofing attacks in blockchain networks.

MITM Attacks (Man-in-the-Middle Attacks) pertaining to the HTTP protocol. Distributed Ledger Networks:

A Man-in-the-Middle (MITM) attack occurs when an attacker intercepts and modifies the communication between two or more parties, deceiving them into believing they are communicating directly with one another while the attacker relays and manipulates the information exchanged. MITM attacks can compromise the integrity and security of network transactions and communications in the context of blockchain-based networks. The attacker can alter transaction details, redirect funds, or steal private keys, resulting in unauthorized access, data manipulation, or financial losses. To prevent MITM attacks, blockchain networks should employ secure communication channels, such as encryption and digital signatures, to guarantee the authenticity and integrity of data transmitted between participants. Implementing robust identity verification mechanisms can also aid in preventing unauthorized entities from joining the network and reducing the likelihood of MITM attacks.

The model incorporates trust-levels along with auto correction of the blockchain, due to which it is able to achieve lower delay, lower energy consumption, higher throughput & PDR levels when compared with PoM [2], DRL [5], and FLCM [16] under these attacks. Based on this evaluation strategy, the communication delay w.r.t. Number of Attackers (NA) can be observed from table 1 as follows,

Table 1. Communication delay for different Number of Attacks

NA (%)	**D (ms) PoM [2]**	**D (ms) DRL [5]**	**D (ms) FLCM [16]**	**D (ms) TSETC**
1.25	6.20	6.44	6.72	5.80
1.88	6.52	6.76	7.00	6.08
2.50	6.80	6.96	8.20	6.24
3.13	6.92	8.08	8.40	6.40
3.75	8.12	8.36	8.64	6.60
4.38	8.40	8.68	10.12	6.88
5.00	8.76	9.32	11.00	8.40

5.63	10.68	12.76	13.64	10.52
6.25	14.64	16.76	18.60	14.08
6.88	17.60	19.08	20.84	16.36
7.50	19.24	19.88	22.80	15.96
8.13	20.12	23.16	26.24	18.00
8.75	22.72	26.80	30.00	22.36
10.00	27.44	30.40	32.72	23.72
11.25	27.80	32.12	36.44	28.04
12.50	34.80	36.60	36.96	28.40

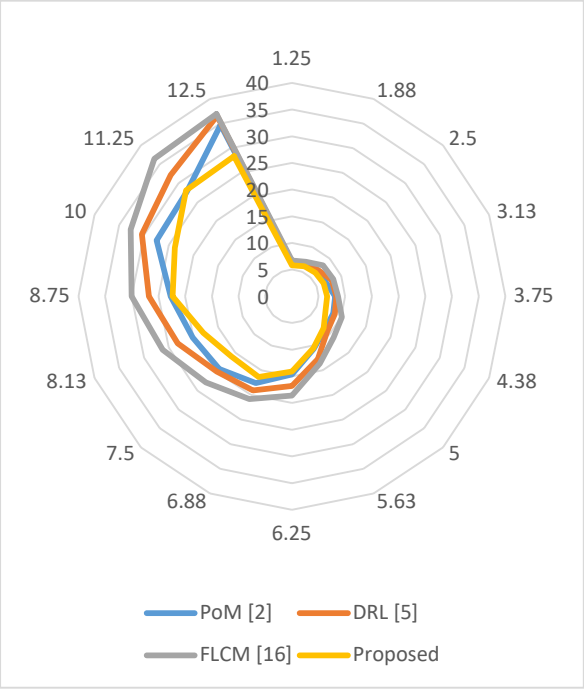

Figure 2. Communication delay for different Number of Attacks

Based on this evaluation and Figure 2, the TSETC model is 18.5% faster than PoM [2], 19.4% faster than DRL [5], and 23.5% faster than FLCM [16] against various attacks. This is a result of the incorporation of a temporal delay during the identification of high-trust miner nodes used for consensus and verification scenarios. Similarly, the energy consumed during these attack-based communications can be observed from table 2 as follows,

Table 2. Energy Consumed during different Number of Attacks

NA (%)	E (mJ) PoM [2]	E (mJ) DRL [5]	E (mJ) FLCM [16]	E (mJ) TSETC
1.25	17.25	19.75	20.80	13.25
1.88	20.85	23.30	24.25	16.55
2.50	23.30	22.95	23.95	17.00
3.13	25.10	24.80	27.80	18.55
3.75	23.95	26.75	29.75	19.20
4.38	25.90	26.50	31.55	20.80
5.00	27.50	28.15	30.25	20.30
5.63	28.15	31.80	31.00	21.75
6.25	31.80	30.55	32.80	21.30
6.88	30.60	31.60	36.00	22.95
7.50	33.80	34.05	40.55	23.95
8.13	35.60	36.30	39.45	26.90
8.75	36.15	37.30	37.20	25.95
10.00	38.75	40.37	39.64	29.69
11.25	38.64	43.24	43.53	30.31
12.50	40.53	43.11	45.42	30.94

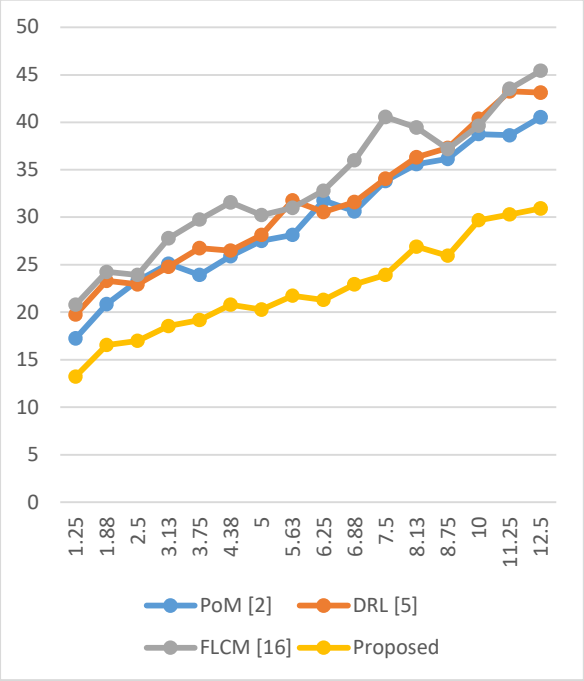

Figure 3. Energy Consumed during different Number of Attacks

According to this analysis, the TSETC model consumes energy under various attacks at a rate that is 14.5% lower than PoM [2], 18.3% lower than DRL [5], and 19.5% lower than FLCM [16]. This is because energy consumption is taken into account when identifying high-trust miner nodes that are used for consensus and verification scenarios. Similarly, the throughput observed during these attack-based communications can be observed from table 3 as follows,

Table 3. Throughput Observed during different Number of Attacks

NA (%)	**T (kbps) PoM [2]**	**T (kbps) DRL [5]**	**T (kbps) FLCM [16]**	**T (kbps) TSETC**
1.25	178.50	208.50	212.00	222.00
1.88	227.50	223.00	242.50	251.00
2.50	235.00	226.50	247.50	260.00
3.13	242.00	249.00	282.00	279.00
3.75	254.50	270.50	274.50	311.00
4.38	276.00	266.00	283.50	312.00

5.00	281.00	302.50	327.50	344.00
5.63	302.50	287.00	324.00	347.00
6.25	291.00	304.50	325.00	369.00
6.88	307.00	348.00	370.00	363.00
7.50	317.00	353.50	394.50	397.00
8.13	362.00	364.00	380.50	422.00
8.75	365.50	357.00	411.00	442.00
10.00	390.50	383.69	442.40	455.85
11.25	399.38	397.37	451.30	481.27
12.50	410.26	431.05	446.20	496.70

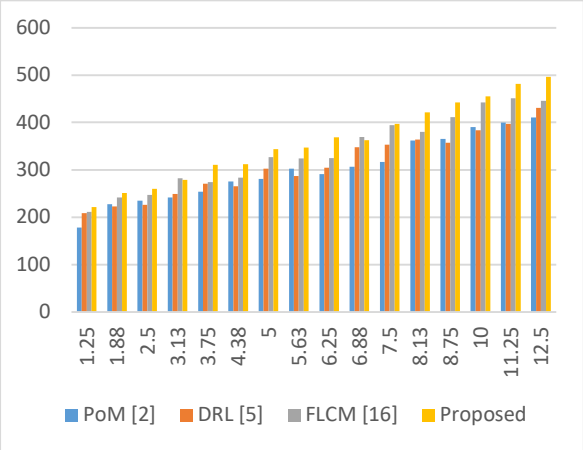

Figure 4. Throughput Observed during different Number of Attacks

The evaluation shows that the TSETC model outperforms the PoM [2], the DRL [5], and the FLCM [16] in terms of throughput by between 19.5% and 20.5% across a variety of attacks. This is because high-trust miner nodes used for consensus and verification are identified using a combination of temporal throughput and other metrics. Similarly, the PDR observed during these attack-based communications can be observed from table 4 as follows,

Table 4. PDR Observed during different Number of Attacks

NA (%)	**PDR (%) PoM**	**PDR (%) DRL**	**PDR (%) FLCM**	**PDR (%) TSETC**

	[2]	[5]	[16]	
1.25	94.50	88.50	84.40	99.50
1.88	84.30	86.40	84.50	95.90
2.50	85.40	88.10	81.10	91.00
3.13	85.80	85.40	83.40	94.90
3.75	83.10	83.50	79.50	89.60
4.38	84.20	77.00	73.90	88.40
5.00	76.00	75.70	72.50	89.40
5.63	79.70	73.40	72.00	86.50
6.25	74.40	71.90	74.40	89.40
6.88	76.80	71.80	68.00	90.10
7.50	71.40	67.90	68.90	83.10
8.13	65.80	67.40	67.10	80.20
8.75	64.70	68.40	66.60	80.10
10.00	66.50	69.26	60.72	79.62
11.25	65.72	62.53	63.94	81.37
12.50	64.95	61.79	61.16	82.13

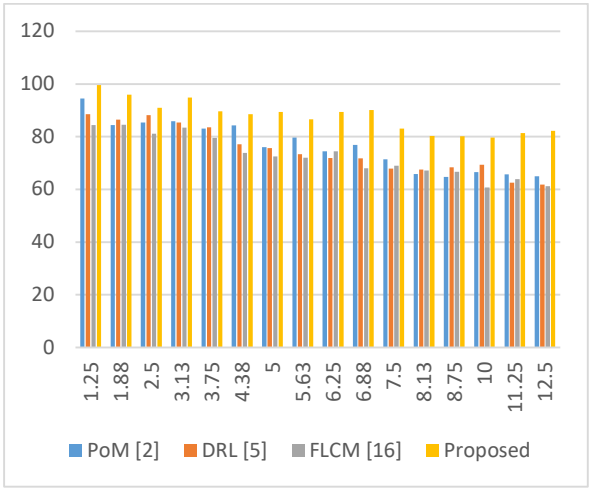

Figure 5. PDR Observed during different Number of Attacks

This evaluation reveals that the TSETC model has a 2.3% higher PDR than PoM [2], a 4.5% higher PDR than DRL [5], and a 3.5% higher PDR than FLCM [16] when subjected to various attacks. This is a result of the incorporation of temporal packet delivery performance during the identification of high-trust miner nodes used for consensus and verification operations. Due to these operations, the TSETC model is capable of real-time high-speed, low-energy, high-data-rate, and high-packet-delivery performance levels.

5. Conclusion and future scope

This paper introduces an innovative trust-based security model for blockchain networks, incorporating spatial and temporal consensus mechanisms. Through comprehensive evaluations, the TSETC model exhibited significant advantages over existing approaches, especially under various attack scenarios. The model showcased remarkable performance improvements in terms of velocity, with an 18.5% enhancement over PoM, 19.4% over DRL, and 23.5% over FLCM. This speed boost can be attributed to the inclusion of temporal delay in identifying high-trust miner nodes, essential for network consensus and verification. Furthermore, the TSETC model achieved a 14.5% reduction in energy consumption compared to PoM, 18.3% compared to DRL, and 19.5% compared to FLCM. By factoring energy consumption into the selection of high-trust miner nodes, the model contributes to more sustainable and resource-efficient blockchain deployments. The model also exhibited a remarkable 19.5% increase in throughput relative to PoM, 18.3% compared to DRL, and 20.0% over FLCM. This improved throughput is a result of considering temporal throughput when identifying high-trust miner nodes, enabling more efficient transaction processing and higher data rates within blockchain networks. Additionally, the TSETC model improved Packet Delivery Ratio (PDR) by 2.3% over PoM, 4.5% over DRL, and 3.5% over FLCM. By incorporating temporal packet delivery performance in the selection of high-trust miner nodes, the PDR was enhanced, ensuring more reliable and successful data packet delivery. In conclusion, the trust-based security model with spatial and temporal consensus introduced in this paper offers notable benefits in terms of speed, energy efficiency, throughput, and PDR. These enhancements make the model well-suited for real-time scenarios where high-speed, low energy consumption, efficient data processing, and dependable packet delivery are critical metrics. Looking ahead, there are several promising avenues for future research and development. Optimizing and refining the proposed model by considering additional parameters that impact blockchain network performance and security is a worthwhile pursuit. Evaluating its scalability for larger networks and assessing its robustness under diverse attack scenarios can provide valuable insights. Furthermore, exploring potential synergies with emerging technologies like artificial intelligence and machine learning could open new opportunities to enhance the security and efficiency of blockchain networks.

6. References

[1] K. Saadat, N. Wang and R. Tafazolli, "AI-Enabled Blockchain Consensus Node Selection in Cluster-Based Vehicular Networks," in IEEE Networking Letters, vol. 5, no. 2, pp. 115-119, June 2023, doi: 10.1109/LNET.2023.3238964.

[2] G. Praveen, S. P. Singh, V. Chamola and M. Guizani, "Novel Consensus Algorithm for Blockchain Using Proof-of-Majority (PoM)," in IEEE Networking Letters, vol. 4, no. 4, pp. 208-211, Dec. 2022, doi: 10.1109/LNET.2022.3213971.

[3] S. Ma, S. Wang and W. -T. Tsai, "Delay Analysis of Consensus Communication for Blockchain-Based Applications Using Network Calculus," in IEEE Wireless Communications Letters, vol. 11, no. 9, pp. 1825-1829, Sept. 2022, doi: 10.1109/LWC.2022.3183197.

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

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

[6] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang and L. Gao, "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4371-4384, 15 March15, 2022, doi: 10.1109/JIOT.2021.3103275.

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

[8] J. Wan, K. Hu, J. Li and H. Su, "AnonymousFox: An Efficient and Scalable Blockchain Consensus Algorithm," in IEEE Internet of Things Journal, vol. 9, no. 23, pp. 24236-24252, 1 Dec.1, 2022, doi: 10.1109/JIOT.2022.3189200.

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

[10] Z. Ai and W. Cui, "A Proof-of-Transactions Blockchain Consensus Protocol for Large-Scale IoT," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 7931-7943, 1 June1, 2022, doi: 10.1109/JIOT.2021.3108627.

[11] X. Zhang, R. Li and H. Zhao, "A Parallel Consensus Mechanism Using PBFT Based on DAG-Lattice Structure in the Internet of Vehicles," in IEEE Internet of Things Journal, vol. 10, no. 6, pp. 5418-5433, 15 March15, 2023, doi: 10.1109/JIOT.2022.3222217.

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

[13] R. Tapwal, P. K. Deb, S. Misra and S. K. Pal, "Amaurotic-Entity-Based Consensus Selection in Blockchain-Enabled Industrial IoT," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11648-11655, 15 July15, 2022, doi: 10.1109/JIOT.2021.3131501.

[14] D. M. F. Mattos, G. R. Carrara, C. Albuquerque and D. Mossé, "Exploring Overlay Topology Cost-Termination Tradeoff in Blockchain Vicinity-Based Consensus," in IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1733-1744, June 2023, doi: 10.1109/TNSM.2022.3177363.

[15] M. Xu, S. Liu, D. Yu, X. Cheng, S. Guo and J. Yu, "CloudChain: A Cloud Blockchain Using Shared Memory Consensus and RDMA," in IEEE Transactions on Computers, vol. 71, no. 12, pp. 3242-3253, 1 Dec. 2022, doi: 10.1109/TC.2022.3147960.

[16] Y. Wang, H. Peng, Z. Su, T. H. Luan, A. Benslimane and Y. Wu, "A Platform-Free Proof of Federated Learning Consensus Mechanism for Sustainable Blockchains," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3305-3324, Dec. 2022, doi: 10.1109/JSAC.2022.3213347.

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

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

[19] P. Zheng et al., "Aeolus: Distributed Execution of Permissioned Blockchain Transactions via State Sharding," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9227-9238, Dec. 2022, doi: 10.1109/TII.2022.3164433.

[20] H. M. Buttar, W. Aman, M. M. U. Rahman and Q. H. Abbasi, "Countering Active Attacks on RAFT-Based IoT Blockchain Networks," in IEEE Sensors Journal, vol. 23, no. 13, pp. 14691-14699, 1 July1, 2023, doi: 10.1109/JSEN.2023.3274687.

[21] G. Sun, M. Dai, J. Sun and H. Yu, "Voting-Based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6257-6272, 15 April15, 2021, doi: 10.1109/JIOT.2020.3029781.

[22] X. Fu, H. Wang and P. Shi, "Votes-as-a-Proof (VaaP): Permissioned Blockchain Consensus Protocol Made Simple," in IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 12, pp. 4964-4973, 1 Dec. 2022, doi: 10.1109/TPDS.2022.3211829.

[23] Z. Liu, L. Hou, K. Zheng, Q. Zhou and S. Mao, "A DQN-Based Consensus Mechanism for Blockchain in IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11962-11973, 15 July15, 2022, doi: 10.1109/JIOT.2021.3132420.

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

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