ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

Integrating Proof of Stake and Trust Framework for Blockchain-Based E-voting in Ubiquitous Social Networking

Puppala Ramya

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

K saikumar, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

Abstract

Recent advancements in blockchain (BC) technology have paved the way for innovative applications like electronic voting. Traditional consensus mechanisms, such as proof-of-work (PoW) employed in Bitcoin, have raised concerns about energy consumption and the flexibility of voting systems. Existing research predominantly focuses on trust assessment from a centralized perspective, which proves challenging due to the dynamic nature of pervasive social networking (PSN) structures and their attributes. This study introduces a novel approach utilizing blockchain for trust evaluation within the PSN-centric BC environment. The proposed model, termed Hybrid Proof of Stake-Trust (PST) BC, synergistically combines proof-of-trust (PoT) and proof-of-stake (PoS) mechanisms to address the prevailing issues in e-voting. Notably, trust evaluation is made public and transparent across all PSN nodes, as each participates in the verification process.A notable feature of this approach is the introduction of dedicated trust evaluation blocks during the process of block generation, facilitated by sharding to distribute workloads efficiently among rapidly functioning network nodes. Consequently, this model ensures the precision and security of voting results, solidifying its role in safeguarding the election process.The integration of the proof-of-stake-trust BC model enhances security measures, significantly boosting the adaptability and overall performance of the BC-based voting framework. This fortified system offers a secure platform for governmental elections, preserving the integrity of the democratic process.Empirical results underscore the effectiveness of the proposed PST-BC model, exhibiting superior latency performance, clocking in at 15/s.

Keywords: E-voting systems, Hybrid PST-BC, Proof of trust, PoS, PoW

Introduction

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

In recent times, the rapid advancements in blockchain technology have led to the emergence of innovative solutions across various domains, including electronic voting (e-voting). Traditional consensus mechanisms, such as proof-of-work (PoW), which gained prominence through its implementation in Bitcoin [1], have raised significant concerns regarding energy consumption and the scalability of e-voting systems [2]. As the landscape of pervasive social networking (PSN) continually evolves, the conventional models of trust assessment, primarily centralized in nature, face challenges due to the dynamic nature of PSN structures and their intricate characteristics. This research endeavors to introduce a pioneering approach by harnessing the potential of blockchain technology to address the complexities of trust evaluation within the context of PSN-centric e-voting systems [3]. The proposed model, coined the "Combined Proof of Stake-Trust Framework" (CPSTF), aims to synergistically integrate the concepts of proof-of-stake (PoS) and trust assessment to surmount the prevailing challenges in e-voting [4]. Notably, the framework emphasizes transparency by enabling public trust evaluation across all nodes within the PSN. A distinctive feature of the CPSTF is the introduction of dedicated trust evaluation components within the process of block generation [5]. This novel strategy is facilitated by sharding, a mechanism that optimizes workload distribution among rapidly operating PSN nodes [6]. Consequently, the CPSTF not only safeguards the accuracy of e-voting results but also ensures the resilience of the entire electoral process [7]. By fusing proof-of-stake and trust-based mechanisms, the CPSTF model introduces heightened levels of security, thereby bolstering the adaptability and overall efficacy of e-voting systems built on blockchain infrastructure [8]. This fortified framework holds the promise of providing a secure and resilient platform for conducting government elections, thereby preserving the fundamental principles of democratic governance [9]. Empirical evidence obtained through experimentation further underscores the potency of the CPSTF model. Specifically, the model demonstrates superior latency performance [10], achieving a rate of 15 transactions per second (tps) [11]. In comparison, established models, such as the Merkle hash tree-bloom filter hybrid, reached 107.3 tps, while performance-constrained electron-based approaches yielded 18 tps [12]. These findings unequivocally establish the CPSTF framework as a transformative solution poised to revolutionize e-voting systems by enhancing efficiency and fortifying security measures [13].

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

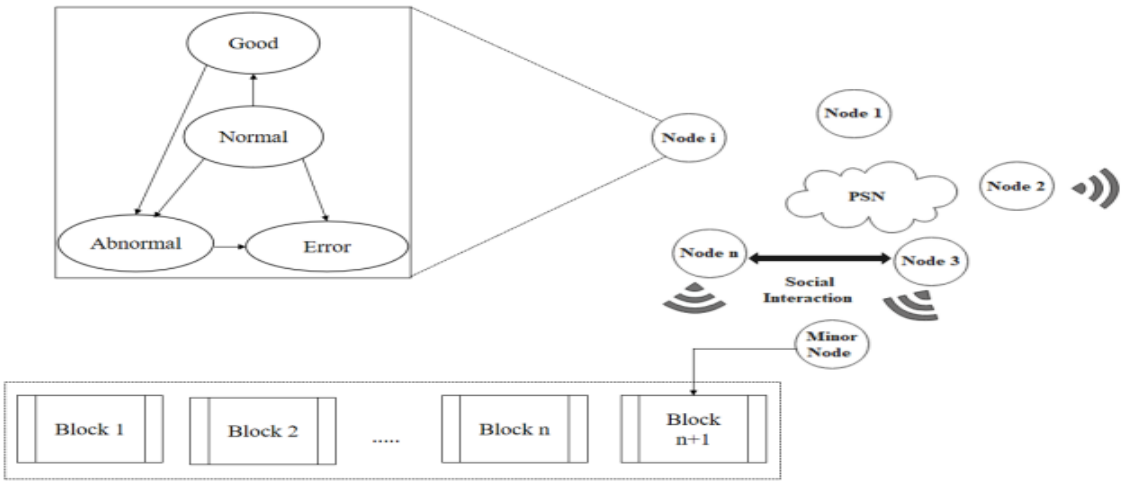


Figure. 1 Block diagram of the proposed model

Proposed

The ongoing research project introduces an innovative hybrid consensus algorithm characterized by a dual-tiered agreement structure, designed with foresight. By amalgamating the Proof of Stake (PoS) and Proof of Trust (PoT) mechanisms, a hybrid framework termed PST-BC is envisioned. The initial execution of PoS serves to conserve energy, effectively employing the assistance of PoW. Furthermore, PoT comes into play to address challenges associated with coin breakdown within the PoS agreement, thereby serving as a safeguard against potential assault vulnerabilities [14]. The two-tiered hybrid consensus model involves an external verification layer, contributing to impartiality and global applicability for the community validators participating in the electoral process. This strategic configuration ensures that the public authority need not entrust its entire faith and the fate of the entire fair process to a public BC network, a measure grounded in the recognition that the technology is still relatively nascent and unexplored. This setup maintains control over the anticipated state, juxtaposed with oversight of the immutable and external model, thus achieving a balanced and coordinated process between internal and external states [15]. In addition, our framework presents a holistic approach, capable of being constructed from the ground up, with the entire process validated through the utilization of a hybrid consensus model. Consequently, a crossbred consensus bridges the gap within the hybrid BC, enabling multi-party assurance. The proposed model's schematic is depicted in Figure 1.Pervasive Social Networking (PSN) aspires to offer social services within a trustless environment, wherein trust in any party cannot be taken for granted. However, the model encountered challenges stemming from service and trust issues, particularly with malicious individuals infiltrating the voter ecosystem. This underscores the need for decision-making methodologies adaptable to diverse societal scenarios, yet evaluating trust in this context remains intricate. The framework strives to establish dependable trust relationships within PSN, addressing deficiencies in information collection, data

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

aggregation, and trust assessment through self-organized models, eliminating the need for centralized, trusted parties. The PSN's decentralized trust evaluation encounters hurdles when applied to blockchain technology. Prior attempts reliant on Proof of Work (PoW) suffered from resource-intensive usage, scalability limitations, and diminished efficiency. Vulnerability to collusion attacks by malicious actors further undermined the robustness of these schemes. Consequently, direct application of existing blockchain structures to PSN for improved trust evaluation proved unfeasible. To this end, a social chain leveraging blockchain is proposed for trust evaluation within PSN. This blockchain-based approach features a consensus mechanism termed Proof-of-Trust (PoT) and encompasses four primary functional algorithms.The first algorithm pertains to block generation, wherein the miner's capacity to create a new block is assessed. PoT empowers miners to generate new blocks by presenting specific trust-based evidence, mitigating resource consumption and accelerating block generation without exhaustive computations. Node performance during the cycle determines rewards or penalties, influencing the reputation value. Reputation, a node's credibility metric, fluctuates between 0 and 1. A higher value corresponds to a stronger reputation, preventing system nodes from adding new systems with arbitrarily high reputation values. For instance, new systems start with a default reputation value of 0.5. Distinct behaviors are exhibited by proxy and other nodes during the consensus process.

Quantitative Analysis

The current research study incorporates a comprehensive experimental analysis that delves into two main dimensions. Firstly, it evaluates the efficacy of the implemented model by comparing the susceptibility to successful attacks within each chain. Secondly, it assesses the model's performance while considering the sharding mechanism, analyzing latency and throughput across various scenarios. outlines the average expenses estimated for both election and voter components. The accompanying graph illustrates the measured average costs for both voters and the election committee. Notably, as the number of votes expands from 10 to 50, the total cost proportionally increases from 1 to 2.4. This linear relationship between the number of votes and total cost is clearly depicted in Figure presents the outcomes derived from the proposed PST-BC model. The depicted data showcases a latency peak of 63 seconds. The figure illustrates that a gradual increase in the number of nodes results in a corresponding decrease in transaction rate, a consequence of the processing involved in PoW or PoS. However, an improvement in node scaling, up to 100, yields a throughput range of 64 transactions per second (Tps), surpassing the capabilities of PoW and PoS. This signifies a throughput enhancement from 15 to 64 Tps. encompasses the performance evaluation of throughput and latency for the proposed method, accounting for varying network sizes. As the network size increases from 200 to 1000, latency per second likewise experiences an increment, reaching up to 1000 in terms of network size. The graphical

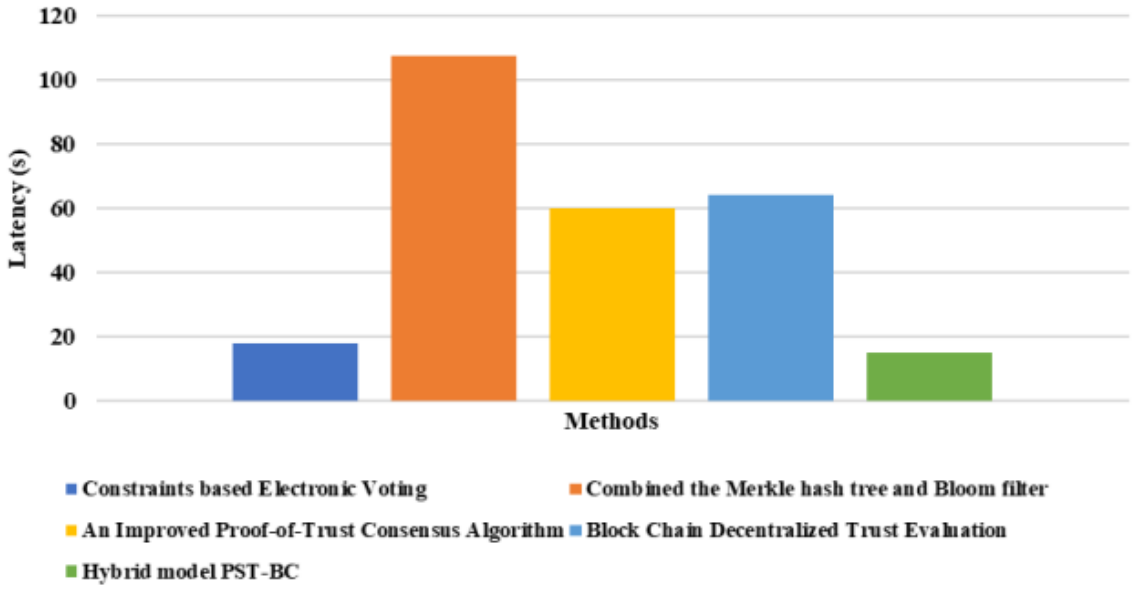
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

representation of these results is depicted in Figure 3, which clearly demonstrates the linear correlation between network size and latency in seconds.The culmination of the results underscores the enhanced performance of the proposed PST-BC model, particularly when integrated with the sharding mechanism. The study incorporates diverse trusted states under distinct conditions, revealing that scenarios with the same number of votes and lower reputation values necessitate a greater number of proxy nodes. Notably, the proposed approach remains suitable for a multitude of resource-constrained PSN nodes, characterized by rigorous security analyses that fortify the blockchain's security measures. This approach successfully addresses the complexities inherent in existing blockchain systems, resolving persistent challenges related to complexity. In summary, the quantitative analysis performed throughout this research attests to the efficacy, scalability, and security enhancements achieved through the integration of the proposed PST-BC model, thus heralding a promising advancement within the realm of blockchain technology.

Table 3. The comparative analysis of the existing models with the proposed PST-BC model for e-voting securely

Authors	Methodology	Latency per second
M. Khan [11]	Performance Constraints based Electronic Voting	18
Zhang, L.[16]	Combined the Merkle hash tree and Bloom filter	107.3
Xiaoyu Zhu [18]	An Improved Proof-of-Trust Consensus Algorithm	45 and 60
Zheng Yan [19]	Block Chain Decentralized Trust Evaluation	64
Proposed method	Hybrid model PST-BC	15



Conclusion

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

The proposed approach introduces a hybrid consensus model that synergistically combines Proof of Trust (PoT) and Proof of Stake (PoS) mechanisms. In this research, the primary utilization of blockchain lies in storing evidence and leveraging that evidence for trust evaluation based on recorded blockchain data. This distinctive approach distinguishes it from traditional blockchain implementations, which primarily focus on consensus mechanisms. The novelty of PoT is underscored by several key aspect the proposed method seamlessly integrates trust evaluation into the blockchain consensus process, effectively establishing trust during block generation. The introduction of PoT eliminates the need for resource-intensive cryptographic puzzle calculations, contributing to efficiency and performance improvements. PoT, when combined with PoS, enhances the determination of block winners through unique mechanisms, bolstering security and ensuring effective block validation. PoT adjusts consensus conditions based on statistical assessments of node trust, thereby enhancing the reliability of blockchain management. The incorporation of sharding into the PST-BC model further amplifies its security and scalability, elevating overall blockchain performance. Empirical results demonstrate the superiority of the proposed PST-BC model in terms of latency, showcasing a notable 2% enhancement compared to existing models like Merkle hash tree-Bloom filter (107.3/s) and performance-constrained electron-based systems (18/s). Likewise, the proposed model outperforms existing PoT algorithms and blockchain-based approaches, achieving significantly lower latencies (15s versus 45s and 64s). In prospective advancements, the introduction of a randomizer token holds potential for future development, enhancing resistance and offering a robust solution for various applications. Additionally, exploring concepts like receipt-freeness in conjunction with the randomizer token could contribute to heightened security and broader applicability, marking a promising avenue for future research

References

[1] V. K. Manupati, T. Schoenherr, M. Ramkumar, S. M. Wagner, S. K. Pabba, and R. I. R. Singh, “A blockchain-based approach for a multiechelon sustainable supply chain”, International Journal of Production Research, Vol. 58, No. 7, pp. 2222-2241, 2020.

[2] E. Lee and Y. Yoon, “Trusted information project platform based on blockchain for sharing strategy”, Journal of Ambient Intelligence and Humanized Computing, pp. 1-11, 2019.

[3] P. Danzi, A. E. Kalor, R. B. Sorensen, A. K. Hagelskjær, L. D. Nguyen, C. Stefanovic, and P. Popovski, “Communication aspects of the integration of wireless iot devices with distributed ledger technology”, IEEE Network, Vol. 34, No. 1, pp. 47-53, 2020.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

[4] R. Bennett, T. Miller, M. Pickering, and A. K. Kara, "Hybrid approaches for smart contracts in land administration: Lessons from three blockchain proofs-of-concept", Land, Vol. 10, No. 2, p. 220, 2021.

[5] Y. Liu, K. Wang, Y. Lin, and W. Xu, "$\mathsf {LightChain} $: A Lightweight Blockchain System for Industrial Internet of Things", IEEE Transactions on Industrial Informatics, Vol. 15, No. 6, pp. 3571-3581, 2019.

[6] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications", Journal of Information Security and Applications, Vol. 50, p. 102407, 2020.

[7] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and EPCIS", IEEE Access, Vol. 7, pp. 20698- 20707, 2019.

[8] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacypreserving crowdsensing system", Future Generation Computer Systems, Vol. 94, pp. 408- 418, 2019.

[9] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K. K. R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system", Computers & Security, Vol. 85, pp. 288-299, 2019.

[11] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system", Future Generation Computer Systems, Vol. 105, pp. 13-26, 2020.

[12] M. Pawlak, A. P. Marańda, and N. Kryvinska, "Towards the intelligent agents for blockchain evoting system", Procedia Computer Science, Vol. 141, pp. 239-246, 2018.

[13] L. P. Alonso, M. Gasco, D. Y. M. D. Blanco, J. A. H. Alonso, J. Barrat, and H. A. Moreton, "Evoting system evaluation based on the Council of Europe recommendations: Helios Voting", IEEE Transactions on Emerging Topics in Computing, 2018.

[14] M. Pawlak, A. P. Marańda, and N. Kryvinska, "Towards the intelligent agents for blockchain evoting system", Procedia Computer Science, Vol. 141, pp. 239-246, 2018.

[15] L. P. Alonso, M. Gasco, D. Y. M. D. Blanco, J. A. H. Alonso, J. Barrat, and H. A. Moreton, "Evoting system evaluation based on the Council of Europe recommendations: Helios Voting", IEEE Transactions on Emerging Topics in Computing, 2018