Received: January 24, 2022. Revised: March 20, 2022. 76

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Hybrid Proof of Stake-Trust Block Chain Model in Pervasive Social Networking for E-voting System

Puppala Ramya[1*] Tumati Jashwanth[1] Dupaguntla Venkata Sathvik[1]

[1]*Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, India*
* Corresponding author's Email: mothy274@kluniversity.in

Abstract: Technological advancements in block chain (BC)-based frameworks have empowered scientists to create innovative inventions such as e-casting ballots. The traditional agreement models utilized proof-of-work (PoW) in the Bitcoin that affected energy utilization and bargained the adaptability for the ballot framework. The existing works evaluates the trust basically only on the centralized party as it was not feasible because of the dynamic changes in the pervasive social networking (PSN) topology and their characteristics. The present research work proposes a block chain based trust evaluation model for the PSN based BC. The proposed hybrid proof of stake-trust (PST) BC is based on the proof-of trust (PoT) and also the proof of stake (PoS) overcomes the issues that are occurring in the e-vote casting. The trust evaluation is performed for public verification and becomes transparent for each node of PSN. The advantage of the proposed method is that a new block will be designed for trust evaluation during the block generation. The process of sharding erases the workload when the network works fast for the individual nodes provides the sum of their alternative parts. Therefore, the model utilizes the agreements for generating the safe process that guarantee the precision to vote it from the time of the election results. The present research work utilizes the proof of stake-trust based BC resulted in security improvement. The model improves the adaptability and execution of the BC based on the ballot framework provided a secured voting system for the government. The proposed PST-BC model showed better results in terms of latency as 15/s when compared with the existing models merkle hash tree -bloom filter that obtained 107.3/s and performance constraints based electron of 18/s.

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

1. Introduction

Voting is a method to make a decision collectively to express an opinion that follows with discussions, debates, and campaigns [1]. Casting a vote in their ballot in a box is used for an election process organized by a group of members. Many researchers considered a solitary approach known as paper balloting to ensure each and every individual makes a choice [2]. It is inferred that it leads to practice the popularity based on the maximum number of votes casting for the candidate and the exact time is confirmed [3]. Simultaneously, e-casting ballot extortion and these days have made distant truant voting form control. Past examinations have proved certain limitations were incorporated into polling form were misused to take decisions impact [4]. Thus, electors' absence of trust in the specialists may be present largely [5, 6]. Block-chain technology allows the creation of a public record that has decentralized digital information across the entire network of computer systems. The 'block' is referred to as the data, which are linked together in a single list, which forms a 'chain' that consists of digital information. Block chain has drawn extensive attention and has made its way into applications of big business programming utilized across different business areas [7], for instance, in digital forms of money [8], supply chain management [9], medical care [10], brilliant agreements [11], and monetary administrations [12].

Thus, it is important to secure the e-voting as it has sensitive private information. The block chain technology was more adaptive when compared to the other existing techniques as the data is stored outside of the servers [13]. It can legitimate or be stolen that

would create problems of data security, leakage of privacy and personal data etc., However, the current data management system used by the government for voting did not guarantee the patient data in terms of reliability [14]. The present research work proposes an e-voting system that considers BC checks for various system factors like transparency, verifiable, and scalable for the public. An actual structure of the system is lacking in an environment that showed difficulty in determining the characteristics of the system. Due to this fact, a reinvestigation was initiated into the e-casting a ballot framework and a hybrid approach was proposed that made a crossover agreement to get framework. This exploration investigates the difficulties and likely provides answers that address the issues in such a manner. The proposed model relies upon the PoS and PoT for BC and subsequently, give rise to PST-BC. The present research work constructs a consensus mechanism known as PoT to generate and confirm the gain in terms of trust, efficiency and security. With this, the PoS will reduce the computation overhead which has shown attention for industry and academia. However, the node cost for forging a BC and misbehaving in the PoS is low. The motivation for the present research is that because of the model constructed by Yousif Abuidris [10] which was hybrid consensus model. An E-voting system provides security based on the block-chain contract that is constructed by combining the consensus and sharding model. The hybrid Consensus model is a combination of proof of stake and credibility (PSC-BC) which works mutually that addresses the problems for providing security for e-voting system. The smart contracts are used for providing the trust worthy public bulletin to secure computation in the environment. The sharding mechanism with PSC-BC emphasized the security and also provides enhancement for BC based e-voting system. The proposed research uses proof of trust which integrates the trust evaluation to BC consensus to achieve the trust during generation of block. Combination of PoS, PoT offer high security and adjusts consensus conditions based on the statistics of node trust which provides an essential trustworthiness on block chain management. The sharding process erases the workload if there is generation of huge number of nodes. The nodes are replaced with alternative sum of node parts that are used to generate the public notice board safe process reliably and will guarantee the precision for voting form at the time of election results. Thus, the security is enhanced by using the proposed model.

Thus, this property has made us to re-investigate the e-voting by proposing a hybrid PST-BC model for providing a secured voting system. The combination of PoS and PoT will be utilized for the proposed hybrid model. The structure of the paper is as below:

The organization of the paper is as follows: section 2 describes the existing models that were used for secure voting systems using block chain technology, section 3 describes the proposed model. Section 4 describes the results and discussion. Lastly, section 5 discusses the conclusion and future work for the research.

2. Literature review

In the following section discusses about the previous work and related research in the e-voting system based on BC as it considered to overcome the issue related to the security.

Khan [11] examined the exhibition requirements again for block chain-based secure e-casting a ballot framework. A viable arrangement was utilized for block chain by considering the scope of components, for example, block size, exchange speed, blockage rate discovered a part in deciding the exhibition as a general arrangement. The created model required to considered the factors like generation rate, speed, block size for overall performance detection. The parameters showed improvement in overall performance in terms of scalability and efficiency for e-voting. In any case, the created model neglected to meet the adaptability issues in the e-casting a ballot framework.

Shufan Zhang [16] performed Chain integrity for a huge scope e-casting a ballot framework for improving the BC improved the heartiness and obviousness of the framework. The current model utilized block chain-enabled voting (BEV) framework that developed a hybrid data structure by combining the Merkle hash tree and Bloom filter to perform fast authentication. The developed model used crypto graphic primitives like blind signature and threshold Paillier encryption were adapted in chain integrity for such properties. The created upper bound model fostered a democratic framework that made intricacy in the correspondence channel was not applicable for a real-time framework. Implementing the model through blockchain was huge because of its incorporated complexity in the model as the model consisted of number of hubs, organization size, throughput, dormancy, and other factors that implied a quick development rate.

Sadia [17] fostered a security model for E-casting a ballot with the keen agreement for providing security through blockchain. The model confronted issues of inexactness, citizens' protection and security within an hour for casting vote ballot. The created model utilized a convention that was very simpler and

a benefit of the model was that the time utilization and the memory were decreased made the process quicker. In this manner, the created convention satisfied the past characterized properties thereby overcame the problem of complexity. However, the convention can't be utilized in all spaces as the substitution of meta-information was not contemplated in the model.

Vemula [18] developed a secure E-Voting system using CryptDB guaranteed implementation. In the created model an e-casting ballot framework was considered for encrypting the data before storing them to a database as it included multiple encryption phases. The developed model was not revealing any information for the intruders at any point of level during voting and thus the online system was secured, confidential, and integrated. The created model neglected to uncover data from the interlopers at any degree of surveying framework.

Xiaoyu Zhu [19] developed an improved PoT with consensus model for credible crowdsourcing BC services. The existing model faced challenge for designing a suitable consensus model for reaching an agreement for credibility of participants automated and also to prevent the data from transaction by the process of tampering and tracing the malicious behaviours. An improved PoT scheme proposed with an underlying BC technology which is crowdsourcing the scenario services. Yet, the developed model required to combine the cryptography for enhancing the reliability and privacy of the system.

Zheng Yan [20] developed a decentralized trust evaluation based model for block-chain in PSN. The developed novel BC based decentralized system was developed for performing trust evaluation for PSN. The mobile devices lacked in computing the resources for processing the cryptographic puzzle yet the light weight consensus mechanism based PoT showed improvement effectively when compared to BC systems. The BC outperformed better in terms of computational overhead as it was expensive that required performed suitable operations.

From the literature survey, the utilization of block-chain would leave no uncertainty concerning the legitimacy and authenticity of the result given BC. Even though block-chain has numerous advantages, there are also certain difficulties of high severity faced by it in the e-vote casting in ballot frameworks:

- Consensus: PoW is especially tedious and computationally escalated.
- Scalability and performance: an organization is required for casting e-vote which is done through means of ballot framework. This framework will consist of a number of hubs, organization size, throughput, dormancy, and other factors that implied a quick development rate.

Therefore, to overcome the problem, the proposed research work intended to address these weaknesses, the half and half agreement model (PST-BC) is introduced that performs block chain contract by joining and sharding of the system. This model is applied for enormous scope e-casting a ballot frame works to keep up the trustworthiness of political decisions, to upgrade the security, execution, and versatility, and to limit the danger of control and extortion in races.

3. Preliminaries before setting up the model

The initial segment portrays the parts of the e-casting a ballot framework and talks about the engineering of the proposed framework plan:

Manage servers (MS): The MS can organize the block chain and distribute it to the higher range of block chain gave the hub declarations. This permits hub validation and incorporates client certifications to sign into the framework.

Block chain organization: this construction permits equal execution, improves the general exhibition and has an adaptable framework. The private chains or the lower chains are served for data storage in the hubs and the upper chain which is a public block chain consists of Ethereum stores and separates the states of BC all across the electors once specific citizens effectively concede to the exchanges, an interaction is known as evidence of-stake agreement and simultaneously measures the exchanges.

Clients (electors): users are citizens and structure the political decision advisory group; utilized the personal ID to verify the generation of wallet. Citizens get a computerized permitted token for casting vote on a ballot. Consequently, the brilliant agreements are conveyed to top layer of the BC (Ethereum block chain).

3.1 BC contract (shrewd agreement)

The smart agreements which are self-executed codes are decentralized with the bits are used in the proposed work. The capacities implanted in the brilliant agreements characterize the agreement arrangements that license the exchanges to the BC top layer is followed. The hub present in each scenario for BC organization runs through contract liberally to arrive at an agreement, which leads to the production of an adaptable crypto framework for e-casting ballot frameworks.

The democratic plan contains explicit stages orchestrated in the accompanying request:

- **Setup**

The setup usually provides information about the security esteems and boundaries. This setup produces a subsequent point for the private pair of keys to encode the information for every cycle.

- **Register**

The Register has the information about the identifiers in the form of ID which are used for creating the public key. The identifiers are represented as IDs which are used to create the private (or public) key as yield.

- **Vote**

The voters cast their worthy vote and later figure out the code text by mark comparison.

- **Valid**

The valid checks for the authenticity of the vote to choose and confirm the voter.

- **Append**

The votes are appended randomly and it refreshes the code text to the box makes arbitrary variant.

- **Publish**

The casting of ballot will estimate the counts by surveying the box and will announce or publish them publicly.

- **Verify vote**

After the democratic process, the electors can demand their votes present in the BC after the counting of votes, in order to confirm the results. This generates a trust among the public boundaries, as well as secures the data obtained from the citizens. The results can be either valid or invalid.

- **Tallying**

When each count is checked and projected at the point, the outputs generated are tallied based on the private key information and the surveying box from the boundary generates an outcome. If the output is not right situation is assumed, then the condition will return false.

- **Verify**

The vote is firm when the public contributes their vote to the candidate and conforms the right substantial vote towards the results.

3.2 Proposed technique

The present research work constructs a hybrid consensus algorithm that has two tiered agreements with a planned view. The combination of PoS and PoT will give rise to a hybrid model PST-BC. The PoS agreement is firstly performed to save energy with the help of PoW. Additionally, PoT is used for resolving the problem of coin break down for PoS agreement and thus performs confirmation for the assault capacity prevention.

The hybrid two-tiered consensus agreement model processed has a layer for external verification, which is used for conducting the impartial and global for the community validators who are involved in the election process. This implies that the public authority doesn't have to put the entirety of its certainty and the destiny of the whole fair interaction in a public BC network which will not happen at any point in the near future, and for a valid justification, because the innovation is still relatively new and hence unexploited. This ensures to control the process that has an expected state and has the supervision to the immutable and external model associated with a decision for measuring with itself. This will guarantee a control cycle to stay in the normal state and managing to outside state. Moreover, our framework offers an all-encompassing methodology in that it well may be worked starting from the earliest stage, and the whole interaction was approved through the utilization of a crossbreed agreement model. Accordingly, a crossover agreement exists among the hybrid BC accomplishes the multi-party certainly. The Fig. 1 shows the block diagram of the proposed model.

The PSN aims for providing the social services for an environment is trust less that means any of the parties can be trusted. The model resulted with service and trust problems as the voters were in contact with the dishonest malicious people. Thus, it is important for making decisions with respect various society scenarios and it is difficult for evaluating the trust better. Thus, it is important to design the trust worth relationship in PSN. The PSN lacks with information collection, data aggregation, and also for trust evaluation, so self-organized models are involved with the parties for practice. Thus, the evaluation of trust in PSN is performed decentralized without involving trusted parties for the

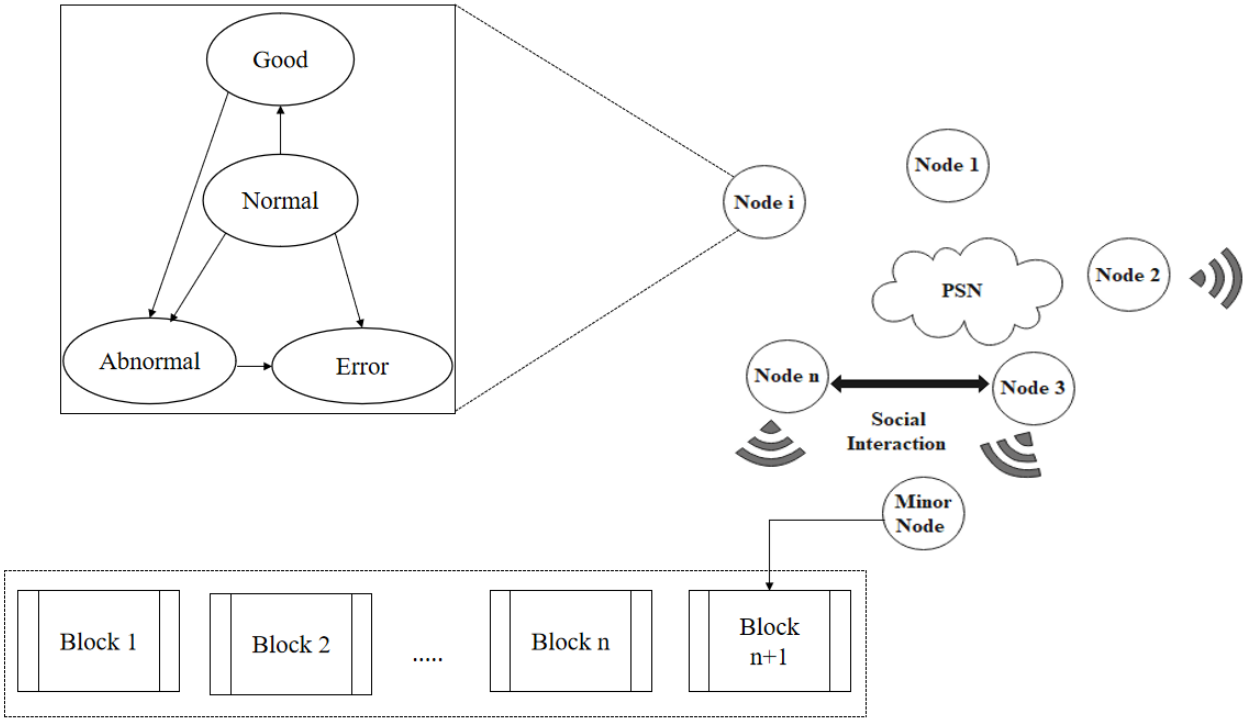

Figure. 1 Block diagram of the proposed model

process. However, it is difficult to utilize the block chain for evaluation of trust. The problem based on PoW suffered from usage of high resources, poor scalability, and also lower efficiency. The schemes were no more robust and faced the collusion attacks by a malicious system party. Therefore, the existing block chain was feasible for applying in PSN directly for gaining better trust evaluation based on the performances. A social chain for leveraging the block chain is performed for trust evaluation in PSN. The block chain is based on the trust evaluation which is designed to perform consensus process known as proof-of- trust (PoT). The mechanism has 4 main functional algorithms, firstly the block generation and the main aim is to determine the miner has ability for creating a new block. The PoT will enable to miners for generation of a new block by conquering certain trust evidence which avoids resource consumption and computation for accelerating the generation of block. The performances of all the nodes in the current cycle will be arranged for either rewarding or punishing the node. The node performs well and the value of reputation is gradually increased and also it decreases the value of reputation. The reputation value is the credibility of the node that ranges between 0 and 1. As the number is lager, the reputation is also higher thereby prevents a system node to add sets the reputation value which is higher and a new system is added is set as 0.5. The proxy and other nodes will behave distinctly during the consensus process that discusses separately two conditions:

Condition 1

Use $R_i(t)$ that represents current reputation of node S_i in the block chain with respect to the t^{th} round of voting. This will give rise to

$R_i(t+1)$

If S_i is a proxy node, then $R_i(t+1) = min(1,(1+y)R_i(t))$ generates the block successful when the block chain added.

$xR_i(t)$ is generated with lower reputation value with respect to the node votes. This can be an abnormal or error.

0 is obtained multiple times if the node is transmitting the transactions. This is considered as invalid vote casting by a voter. The condition that has to be finalized is $0.5 < 0.5$.

When the new node is added for the system, the initial state of the node will be normal and the reputation value will be stated as 0.5. The system adjusts their trust state as per the node behaviour. When the proxy node generates success, then other nodes are active during voting as per the reputation value improves the threshold. This will generate status as good and has shown its advantage subsequently. If in case the proxy node is failed for block generation with respect to time compared to other nodes for vote gives a lower reputation value

and the state will be either good, normal, abnormal, or error or by removing the nodes. The blocks are generated successfully participates in voting checks the condition with respect to the reputation value.

If $R > a$, then the block generation was failed on time with low number of reputations

If $R < b$ means the block generation was failed on time with low number of reputations for several times.

The abnormal state is generated because it decreases the reputation value. The proxy node continuously produces the invalid blocks or other for sending the transaction continuously or other behaviour that continues for dropping below and the node state results with error. The error node is returned to normal state or removed as it takes long time.

In addition to this, when considering future decisions, a potential arrangement of BC with respect to computerized showed ballot cycle during e-casting. At this time, the electors are perceived bio-metrical and would get a computerized token that would permit them to cast a ballot which parallel also anonymize their vote. If the component measures the exchanges then it would be used for cross breed agreement and integrated partners could be the square makers, ideological groups, onlookers, and government substances. The hybrid consensus model is used in BC achieve confidence for the multi-party environment. Thus, this setting will support for consensus system for multi-party is as follows:

- The voter machine has the ability to send the sensitive trades for the public BC thereby saves the trades at the virtual squares.
- A ballot system assembles and stores the non-progressed fragile trade in virtual system.
- The voter machine is used for sending the virtual squares for the private BC for replication of data. The PST-BC endorsed the network validators carried out the process for direct execution and ensure the square.
- Thus, the PoS and PoT are combined to obtain a robust trust based mechanism for e-voting. The PoS will store sufficient information about the coins and PoT will utilize those coins for generating the smart contract block for getting the confirmation for each block. The combination of PoS and PoT will lead for secured hybrid BC technique as shown in the Fig. 1.
- The vote cast by the voter will be stored in a block using PoS and gradually the voter records the vote of next his or her vote into PoT and next block will be generated by using PoS.

The PoT has a newly generated block and if the block is approved by miners then the sufficient numbers of sufficient trust values is agreed based on consensus policy setting. The block chain will hold the principle and design with limited number of miners which determines the block chain correctness. Thus, the trust evaluation is performed for public verification and becomes open and transparent for each node of PSN. Thus, to achieve consensus a new block has to be generated for trust evaluation and also designed for trust evaluation during the block generation.

The sharding process helps for easing the workload whenever the network works fast as that of individual nodes by providing an alternative sum of its parts. The subsets of nodes are grouped in where the specific transactions shard to turn which allows the system to perform the parallel transaction to increase the throughput. The consensus validators are assigned for the shard randomly by the proposed model by the secured algorithm verifiable random function. Thus, a validator is eligible for a certain token number that will determine the total number of votes shared among the assigned validator.

For particular period of time, the validators are assigned for the specific shard and the shared voting will be recomputed for the assigned validators for random sharding. The reshuffle process will provide an additional security to overtake the malicious attackers for a specified period. The technique will guarantee that,

- Attackers are not able for choosing the shard required to work.
- Attackers are unable to learn the model as the shard is working better on advance.

The model is composed of two chains that are working one after the other and the private chain stores all these hashes to the Ethereum block. These blocks are on the public chain with their own blocks. The side chain present will distribute the randomness source for creating the sharding system at the top of it. The side chain will check for all the validations who were subsequently registered and formed a queue in contract. Thus, the private chain will subsequently check for all the validators registered as it might allow for pseudo randomness to perform the crucial task for sharding selection among the validator committee.

4. Results and discussion

The specifications of the system and the tools

Table 1. Average expense estimated for the elector and political decision panel

Number of votes	0-10	10-20	20-30	30-40	40-50
Total cost ($)	1	1.25	1.65	2.15	2.4

Table 2. The performance evaluation (Throughput + Latency) of the proposed model

Network size	2000	4000	6000	8000	10000
Latency per second	15	29	37	50	64

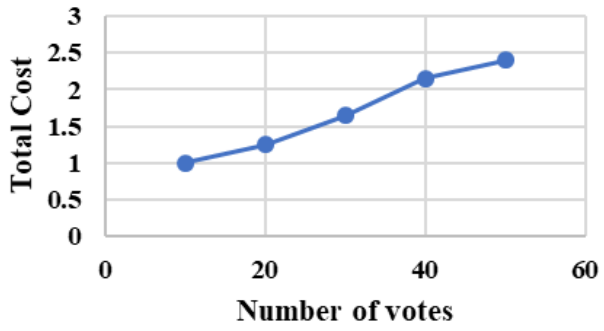

Figure. 2 Average cost measured for the voter and election committee

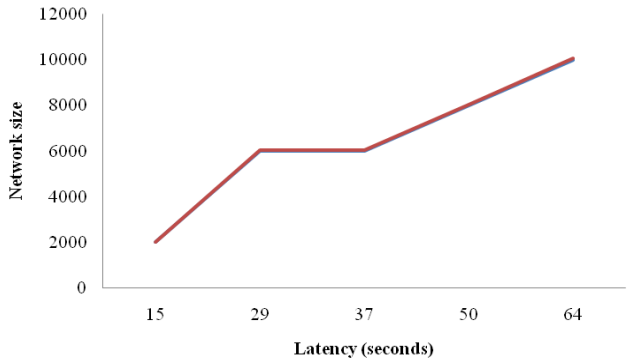

Figure. 3 Performance evaluation in terms of latency for proposed PST-BC

used for the present research code are written in python 3.7, tools used are anaconda navigator, processor of core i9, and RAM – 128 GB.

4.1 Performance measures

The parametric measures that are used to validate the performance results of the proposed block chain technology with PST technique are (i) Latency per second, and (ii) total cost.

Latency is the amount of delay (or time) that is taken by the BC for sending the information from one to another point or next which is measured in milli seconds (ms). The latency initiation time is often dependent on the input data. The total cost will define the amount of money spent for particular range of votes that gives the average expense estimated for the elector and political design panel.

4.2 Quantitative analysis

The present research work experiment is performed for two aspects such as evaluation of the proposed implemented model by comparing the successful attack for each chain. The second is by evaluating the performances with the mechanism of sharding evaluates in terms of latency and throughput for various conditions. Table 1 shows the average expense estimated for the average cost measured for election and the voter. The bends that appeared in figure shows the average cost measured for the voter and election committee. As the range of the number of votes increases from 10 to 50 the total cost also increases from 1 to 2.4. The total cost varies linearly with respect to a number of votes as shown in Fig. 2.

Fig. 3 shows the results obtained for the proposed PST-BC model. As per these results, high latency up to 63 seconds is attained as shown in the figure data. The figure denotes that when the number of nodes increases gradually, the rate of a transaction will also decrease as the nodes were processed by PoW or PoS. If there is improvement in ranging the number of nodes up- to 100 then the range of throughput will be 64 Tps which is higher than PoW and PoS. The throughput will be now ranging from 15 to 64 Tps. The results obtained are shown in Table 2 shows the performance evaluation of the throughput and latency for the proposed method where the network size is varying. As the network size increases from 200 to 1000 latency per second, also increases upto 1000 in terms of network size. The graphical representation for the result obtained is mentioned in Fig. 3. The graph shows that the network size and latency linearly vary with respect to time in seconds.

The results obtained confirmed that the proposed PST-BC improved its performances with high scalability when combined with the sharding mechanism. The present research work utilized different trusted states that are coming under distinct conditions with respect to the same number of votes having lower reputation values needed more number of proxy nodes. The proposed method was feasible for mass of resource limited PSN nodes that performed extensive security analysis provided security for BC. This overcame the problem related to problem of complexity occurred in the existing block chain systems.

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

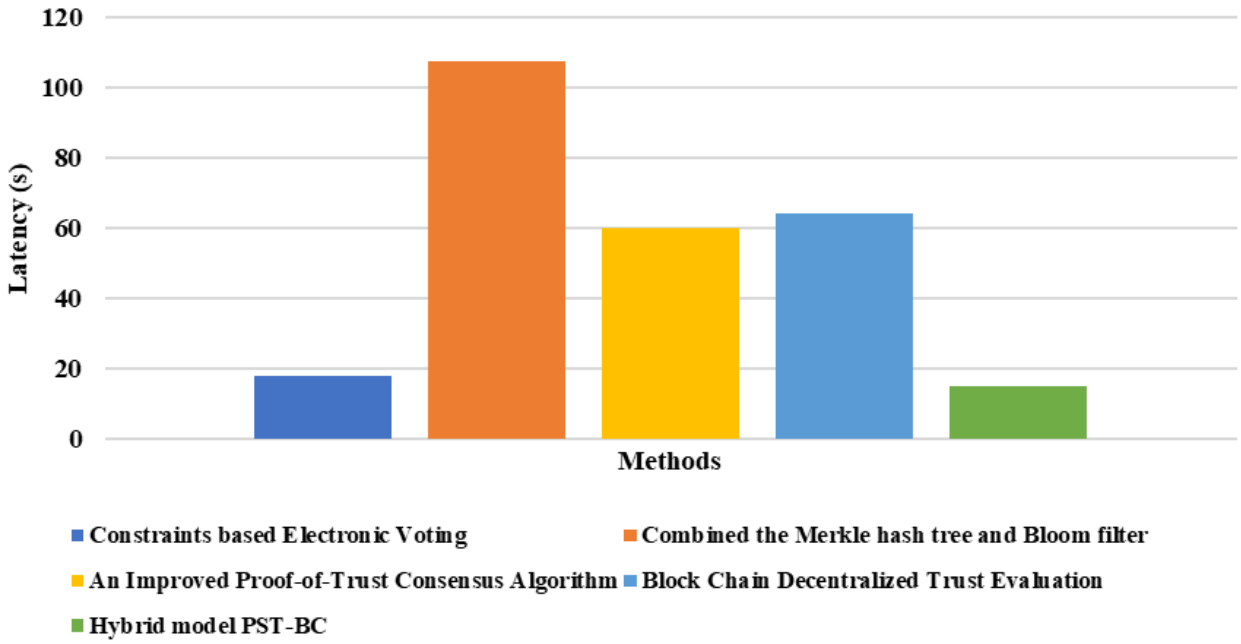

Figure. 4 Comparison of the existing model with the proposed PST-BC in terms of latency

4.3 Comparative analysis

The comparison of the proposed PST-BC with the existing model is as shown in the Table 3. In [11], the model created was considered with a range of factors relating to the speed, block generation rate and variation in the block size for determining the overall performance in terms of solutions. However, the created model neglected to meet the adaptability issues in the e-casting a ballot framework and obtained latency as 18/s. Similarly, in [16] the developed model used crypto graphic primitives like blind signature and threshold paillier encryption were adapted in chain integrity but implementing the model through block chain was huge because of its incorporated complexity in the model and obtained latency as 107.3/s. The improved PoT consensus algorithm [18] obtained latency as 45s and 50s but the model failed to provide privacy and system reliably. The block chain decentralized trust evaluation [19] obtained latency as 64 s showed complexity in the system.

The proposed PST-BC introduced performed block chain contract by joining and sharding of the system. This model is applied for enormous scope e-casting some ballot frameworks to keep up the trustworthiness of political decisions, to upgrade the security, execution, and versatility, and to limit the danger of control and extortion in races and obtained latency as 15/s. The delay time which is known as latency with respect to the existing and the proposed PST-BC is denoted in the Fig. 4.

5. Conclusion

The proposed hybrid agreement variant approach was used hybrid consensus model that combined both PoT and PoS works mutually. The main use of the block chain in the present research work is to store the evidence and to utilize those evidence for evaluation of trust on the basis of recorded block chain. This is different from block chain as it is performing the consensus mechanisms and the novelty of the PoT will lie for the following reasons. The proposed method integrates the trust evaluation to BC consensus which achieves the trust during generation of block. Secondly, the heavy computation is avoided causes cryptographic puzzle calculation. Third is to employ the PoS uniquely decides the block winner effectively. Along with PoS, PoT offers high security and the consensus condition

is adjusted on the basis of statistics of node trust as it provides an important trustworthiness for managing the BC. The mechanism of the sharding approach was combined with PST-BC which emphasized and improved the security and scalability of the block chain performance. The proposed PST-BC chain model showed better results in terms of latency 2 % improvement when compared with the existing models Merkle hash tree -Bloom filter that obtained 107.3/s and performance constraints based electron of 18/s. Similarly, the existing model improved PoT with algorithm and block chain decentralized approach obtained latency as 45 s and 64 s but the proposed proved its effectiveness and efficiency by reaching up to 15s. In future, a randomizer token needs to be employed and also receipt freeness as the randomizer token as it is resistant and can be constructed as a black box.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by 2nd and 3rd author. The supervision, review of work and project administration, have been done by 1st author.

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 multi-echelon 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.

[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 privacy-preserving 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.

[10] Y. Abuidris, R. Kumar, T. Yang, and J. Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding", *Etri Journal*, Vol. 43, No. 2, pp. 357-370, 2021.

[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 e-voting 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, "E-voting 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 e-voting 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, "E-voting system evaluation based on the Council of Europe recommendations: Helios Voting", *IEEE Transactions on Emerging Topics in Computing*, 2018.

[16] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability", *International Journal of Information Security*, Vol. 19, No. 3, pp. 323-341, 2020.
[17] K. Sadia, M. Masuduzzaman, R. K. Paul, and A. Islam, "Blockchain-based secure e-voting with the assistance of smart contract", *IC-BCT 2019*, pp. 161-176, 2020.
[18] S. Vemula, R. M. R. Kovvur, and D. Marneni, "Secure E-Voting System Implementation Using CryptDB", *SN Computer Science*, Vol. 2, No. 3, pp. 1-6, 2021.
[19] X. Zhu, Y. Li, L. Fang, and P. Chen, "An improved proof-of-trust consensus algorithm for credible crowdsourcing blockchain services", *IEEE Access*, Vol. 8, pp. 102177-102187, 2020.
[20] Z. Yan, L. Peng, W. Feng, and L. T. Yang, "Social-chain: Decentralized trust evaluation based on blockchain in pervasive social networking", *ACM Transactions on Internet Technology (TOIT)*, Vol. 21, No. 1, pp. 1-28, 2021.