Received: 13 August 2019 | Revised: 8 March 2020 | Accepted: 6 May 2020

DOI: 10.4218/etrij.2019-0362

ORIGINAL ARTICLE

ETRI Journal WILEY

Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding

Yousif Abuidris[1,3] | **Rajesh Kumar**[1] | **Ting Yang**[1] | **Joseph Onginjo**[2]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China

[2]School of Management Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China

[3]Faculty of Computer Science and Information Technology, University of Gadarif, Sudan

Correspondence
Yousif Abuidris, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China.
Email: yousif_cs@std.uestc.edu.cn

Funding information
SiChuan Department of Science and Technology, Grant/Award Number: 2018GZ0218

Abstract

The evolution of blockchain-based systems has enabled researchers to develop next-generation e-voting systems. However, the classical consensus method of blockchain, that is, Proof-of-Work, as implemented in Bitcoin, has a significant impact on energy consumption and compromises the scalability, efficiency, and latency of the system. In this paper, we propose a hybrid consensus model (PSC-Bchain) composed of Proof of Credibility and Proof of Stake that work mutually to address the aforementioned problems to secure e-voting systems. Smart contracts are used to provide a trustworthy public bulletin board and a secure computing environment to ensure the accuracy of the ballot outcome. We combine a sharding mechanism with the PSC-Bchain hybrid approach to emphasize security, thus enhancing the scalability and performance of the blockchain-based e-voting system. Furthermore, we compare and discuss the execution of attacks on the classical blockchain and our proposed hybrid blockchain, and analyze the security. Our experiments yielded new observations on the overall security, performance, and scalability of blockchain-based e-voting systems.

KEYWORDS

blockchain, E-voting system, hybrid consensus, sharding, smart contract

1 | INTRODUCTION

Voting is a process inherent to all democratic societies. Many experts consider paper balloting to be the only acceptable way to secure and guarantee each person’s right to cast a vote [1]. However, this approach is vulnerable to mistakes and exploitation. Interestingly, owing to the advancement of technology, modern day voters can exercise their democratic right and duty on-line[2], track the status of the votes they cast, verify the precise time they were cast, and check when they will be counted. At the same time, e-voting fraud, such as remote absentee ballot manipulation, is common these days. Several recent examples include the vote fraud controversy in the 2019 elections in North Carolina [3] and the server wipe in the 2017 elections in Georgia [4]. Previous studies showed that the vulnerabilities of centralized ballot storage in e-voting systems are exploited to influence elections. As a result, voters' lack of confidence in the authorities may reach crisis proportions [5,6].

Blockchain has attracted considerable attention and has found application in enterprise software employed across various business sectors [7], for example, in cryptocurrencies [8], supply chain management [9], healthcare [10], smart contracts [11], and financial services [12] as shown in Figure 1. Analogously, the adoption of blockchain technology in e-voting systems enables every single vote to be audited/tracked

This is an Open Access article distributed under the term of Korea Open Government License (KOGL) Type 4: Source Indication + Commercial Use Prohibition + Change Prohibition (http://www.kogl.or.kr/info/licenseTypeEn.do).
1225-6463/$ © 2020 ETRI

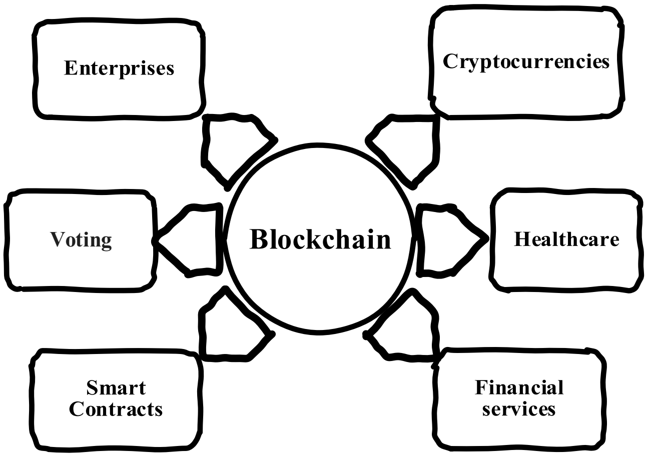

FIGURE 1 Potential use cases for blockchain-based systems

in real time, which would be difficult if not impossible to achieve with prior e-voting systems [5,13,14].

E-voting systems based on blockchain are gaining momentum and a line of research has recently been developed [15–17]. Researchers consider these systems to be scalable, transparent, verifiable, and open to the public. Nevertheless, the lack of actual system structures makes it difficult to determine whether these systems actually have the described characteristics. Many influential studies also proposed the use of a smart contract [18–20] to create decentralized autonomous voting systems, which can eliminate as many human factors as possible. In our previous survey [21], we highlighted a few recent contributions that addressed the security and privacy issues associated with a blockchain-based e-voting system.

A blockchain provides all the characteristics that are needed for an e-voting system, which is arguably the most crucial part of a democratic society. A blockchain neither allows past events to be changed, nor does it enable current events to be hacked. In addition, the system does not tolerate changes. Every machine/node that has been granted access shows the same results, and every vote can be traced to its source without exposing the voter's identity. In essence, the blockchain revolution started with the emergence of Bitcoin [22], which was the first and continues to remain the most popular digital currency in the world.

Furthermore, to guarantee consistency, when another block is created and appended to the previous block, a specific process is required to solve a computationally expensive puzzle known as Proof-of-Work (PoW) [23]. However, PoW is energy-inefficient and influences the throughput and transaction latency, which in turn impacts the scalability and performance [24]. Accordingly, Proof of Stake (PoS) has proved to be a strong competitor to overcome the problems associated with PoW [24]. Expressly, a set of validators take turns to propose and vote on the next block in the PoS consensus mechanism, and the weight of the vote relies on the value of the staked tokens. Similar to PoW, PoS offers the network a convincing financial boost to operate effectively and reduce the risk of conspiracy or attack. However, unlike PoW, it is not computationally complex; therefore, it overcomes the problem of energy-inefficiency. More recently, the hybrid consensus model has attracted considerable interest in an attempt to overcome the challenges faced by the PoW consensus method [25].

At the same time, researchers have also focused on enhancing blockchain scalability and performance using the sharding mechanism [26,27]. Sharding divides the network into multiple smaller groups known as shards, which is the primary approach to overcome the scalability limitation. These shards can operate in parallel with disjoint transactions and maintain disjoint ledgers.

Our study is devoted to updating state-of-the-art e-voting systems based on blockchain. Interestingly, we discovered that a common set of system requirements has yet to be reported. This motivated us to reinvestigate the e-voting system and propose a hybrid consensus model to secure the system. Our model depends on the combination of Proof of Stake (PoS) and Proof of Credibility (PoC) [28] for blockchain; hence, we named our model PSC-BChain. Our research explores the challenges and potential solutions to address the problems in this regard.

Our contributions: This paper presents a hybrid consensus model (PSC-Bchain) combined with the mechanism of sharding. The framework of this study is outlined as follows:

- A secure large-scale e-voting system based on a blockchain contract is introduced.
- A hybrid consensus model (PSC-Bchain) combined with the mechanism of sharding is proposed to emphasize security and enhance the scalability and performance of the e-voting system based on blockchain.
- A blockchain contract (smart contract) is introduced to provide a trustworthy public bulletin board and a secure computing environment to ensure the accuracy of the ballot outcome.
- PoC is used to increase the power of the trusted nodes and generate blocks more effectively.
- An attack and security analysis is presented to prove that the proposed PSC-Bchain model provides high security and scalability for an e-voting system based on blockchain.

The remainder of the paper is organized as follows: Section 2 presents previous work related to this research in the context of e-voting systems based on blockchain and addresses three major issues associated with this research: consensus, verification, and sharding. Section 3 provides an overview of the introduced e-voting system based on blockchain, which involves associated interacting entities and justifies the aims of blockchain to achieve the research objective. Section 4 presents the structure of the proposed hybrid consensus model combined with the mechanism of sharding as well as the designed view followed by experimental details and the performance evaluation in Section 5. Section 6 discusses our analyses of both the attack and security. Section 7 concludes the paper.

2 | RELATED WORK

In this section, we introduce previous work related to this research in the context of e-voting systems based on blockchain and consider three significant issues associated with this research: Security, Consensus and Verification, and Sharding.

2.1 | Previous work

Previous attempts to develop protocols for blockchain-based e-voting systems created incentive schemes for cryptocurrencies. Motivated by recent advances [29–31], Cruz and Kaji [29] proposed a protocol for e-voting based on the Bitcoin blockchain, and discussed certain aspects of the security requirements of e-voting. Bistarelli and others [30] proposed the End-to-End (E2E) voting system using Bitcoin, in which votes are counted by summing each candidate's tokens in the Bitcoin blockchain. Zhao and Chan [31] developed a framework similar to those mentioned above [29,30] using Bitcoin. However, all three the protocols cited above have limitations with respect to the scalability of the blockchain-based e-voting system in that the Bitcoin consensus method is time-consuming and computationally intensive [23]. Other researchers [19,32–35] introduced an e-voting protocol based on the Ethereum blockchain, which has a cryptocurrency named ether. All of these studies focused on enhancing the security of the e-voting system by using the security features offered by the Ethereum blockchain contract. However, these studies neglected to address the performance and scalability of the blockchain. The performance and scalability drawbacks for e-voting systems based on blockchain were addressed in detail [36,37]. In particular, Khan and others [36] conducted experiments with permissioned and permissionless blockchain environments based on various scenarios, including the number of voters, block size, block generation rate, and speed of the transaction. Zhang and others [37] claimed to reveal the impractical properties of blockchain-based e-voting systems. However, their paper does not provide explicit information about significant security properties, such as the uniqueness and ballot receipt. Table 1 compares our work with previous studies.

2.2 | Consensus and Verification

Consensus speed would also impact the throughput of a blockchain system. Regarding on-chain approaches for improving blockchain scalability, Fan and Zhou [38] established PoS-based scalable open network blockchain protocols. They introduced a new security property named Chain-Soundness for PoS-based protocols that catch the awareness of new stakeholders to enter the execution of the contract securely. Practically, the hybrid consensus protocols in the blockchain environment achieve high transaction throughput and low latency. In particular, Liu and others [39] produced a fork-free hybrid consensus protocol and integrated it with PoS for a flexible version of Proof of Activity (PoA) with adjustable parameters between PoW and PoS. This approach enhances the efficiency and leads to a more viable consensus protocol.

TABLE 1 Comparison of the proposed e-voting system based on a blockchain and previous related work

	References									
Properties	**[29,30]**	**[31]**	**[32]**	**[33]**	**[34]**	**[19]**	**[35]**	**[36]**	**[37]**	**Our proposed**
Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Robustness	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓
Consensus	PoW	PoW	PoS	PoS	PoS	PoS	PoS	PoW	PoS	**Hybrid**
Eligibility	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Verifiability	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓
Uniqueness	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓
Ballot receipt	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓
Transparency	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Embed trust	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Scalability	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓

2.3 | Sharding

The sharding mechanism includes splitting large databases into smaller parts (data shards), which enable efficient data management. Sharding was introduced in academia as a strategy that could solve the blockchain scalability issue. Recently, researchers introduced a sharding-based protocol [27,40] to reduce the latency and scale the throughput of the network by managing incoming transactions in parallel to multiple groups of nodes known as shards. Chen and Wang [27] proposed (SSChain), a full sharding protocol that offers security, decentralization, horizontal scalability, and inexpensive storage. This protocol enables the nodes that are involved to join one or more shards freely without periodically reshuffling the network. Al-Bassam and others [40] introduced Chainspace, which is a sharding-based smart contracts platform for high integrity. However, the integrity properties depend on the fairness of all shard-handling objects.

2.4 | Problem formulation

The outcome of any election process appears to raise doubts, particularly amid heated presidential races. The use of blockchain as a bulletin board would leave no doubt with regard to the validity and legitimacy of the outcome because of the immutable feature of the blockchain. Even though blockchain has many benefits, it still faces the following significant challenges for e-voting systems:

- Election Integrity: a core problem of e-voting systems.
- Consensus: PoW is particularly time-consuming and computationally intensive.
- Scalability and Performance: The network of the e-voting system is required to contain a substantial number of nodes, which means the growth rate is fast when factors such as the network size, throughput, and latency are considered.

Designed to address these shortcomings, the hybrid consensus model (PSC-Bchain) presented in this paper is based on a blockchain contract combined with the mechanism of sharding. The model can be applied to large-scale e-voting systems to maintain election integrity, enhance the security, performance, and scalability, and minimize the risk of manipulation and fraud in elections.

3 | BLOCKCHAIN-BASED E-VOTING SYSTEM

In this section, we provide an overview of our large-scale e-voting system based on blockchain, including the interactions between different entities, as shown in Figure 2. The basic equipment each voter requires is a smartphone or computer. Each voter has a wallet containing their own user credentials. Apart from this, each voter receives a digital coin, which represents one opportunity to vote. As an example scenario, we selected the e-voting system to identify and evaluate the security, scalability, and performance issues within blockchain-based systems.

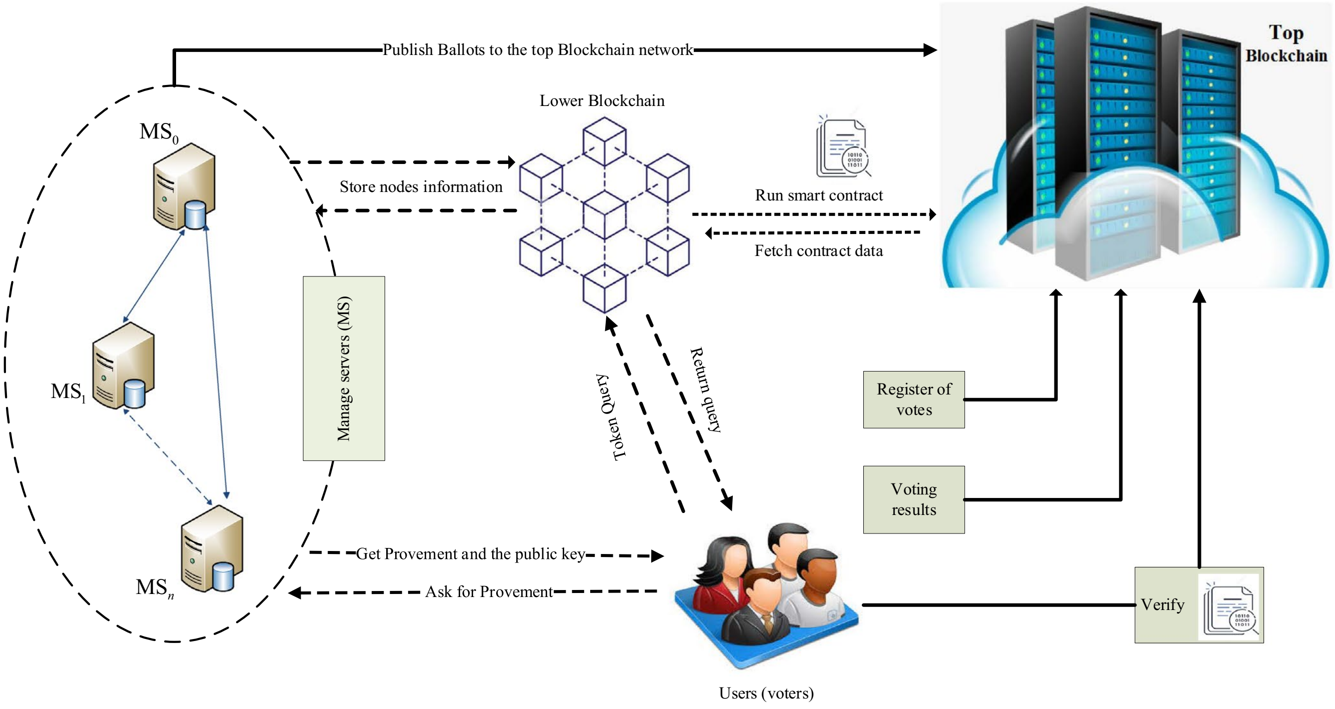

FIGURE 2 Architecture of the e-voting system based on a blockchain

The aim of implementing blockchain technology as a solution for e-voting systems is to provide decentralized architecture, promote transparency, integrity, and an independently verifiable voting scheme. Additionally, we aimed to optimize the voting process and enhance the security, speed, and cost effectiveness.

3.1 | Interacting entities

The first part of this section describes the roles of the components of the e-voting system and discusses the architecture of the proposed system design:

Manage servers (MS): The function of (MS) is to store the node information in the lower blockchain network and publish it to the higher blockchain network and provide nodes certificates. This allows node authentication and includes user credentials to log into the system.

Blockchain network: The proposed e-voting blockchain network is composed of multiple blockchains working side by side. This structure allows parallel execution, which improves the overall performance and scalability of the system. The lower-chains (private-chains) serve to store the information of the nodes and the voter identity register considering that every node in the private-chains has a local blockchain that contains the privacy-sensitive data. The upper-chain (public blockchain such as Ethereum) serves to store separate blockchain states across all voters after certain voters successfully agree on the transactions, a process known as proof-of-stake consensus, and concurrently process transactions. The transactions recorded in the upper-chain (public blockchain) are trusted transactions and are immutable. The routing management among the lower-chains and upper-chain is the same as that in a previous report [41].

Users (voters): Users are voters and also form the election committee; they can use the identity ID to authenticate and access their wallets. Voters receive a digital token that allows them to vote. Therefore, the smart contracts are deployed in the top layer of the blockchain (Ethereum blockchain).

Blockchain contract (smart contract): Smart contracts are self-executed snippets of code in the proposed decentralized system. The functions embedded in the smart contracts define the contract agreements that permit the transactions in the top layer of the blockchain network to be tracked. In our scenario, each node in the blockchain network can run the smart contract independently to reach a consensus, which leads toward the creation of a flexible cryptosystem for e-voting systems.

3.2 | Process of the e-voting system

The voting scheme comprises specific phases arranged in the following order:

- Setup: Input the security values or parameters; then, after generating the private (or public) pair of keys, encrypt (or decrypt) the processes.
- Register: Input the identifiers as IDs to generate the private (or public) key as output.
- Vote: The electors create the vote value or parameter and then compute the cipher text and the corresponding signature.
- Valid: This serves to check the legitimacy of the vote in the ballot server to select the vote as input and verify its validity.
- Append: The vote is randomized. It updates the cipher text in the polling box thereby making it a random version.
- Publish: This adds voting values to the polling box and publish them as public.
- Verify Vote: After the voting phase, the voters could request their votes in the blockchain contract during the time of polling publicity and verify the returned results by entering the public parameters, voter status, and privacy information. The returned results are either valid or invalid.
- Tallying: When all the tallies are cast and checked, the results are counted by using the related private key as input and the parameter of the polling box to generate the overall result. If the result is wrong then the system returns False.
- Verify: A vote is confirmed when the public parameters are input in the publicity phase, and verified to be a valid and correct vote cast toward the ballot result.

4 | PSC-BCHAIN MODEL

In this section, we present the structure of the proposed hybrid consensus model as well as the designed view. This model is formulated by the combination of PoS and PoC; hence, the name of the model (PSC-Bchain). The PoS consensus method is proposed as a means of saving energy relative to the PoW method. PoC is primarily used to address the problem of coin collapse in the PoS consensus method, and for credibility verification, with the function of attack deterrence, as detailed in Section (4.2, 4.3 and 4.4).

4.1 | Structure of the blockchain network in the framework

The organization of the current frameworks within the e-voting system has several credibility verification problems that need to be settled. As a result, the PSC-Bchain consensus model for e-voting systems was built with the prime goal of demonstrating that a node is able to join the network without having been tampered with by an attacker and that its credibility has also been verified. First, we define the structure of the network framework which is formed from a multi-chain

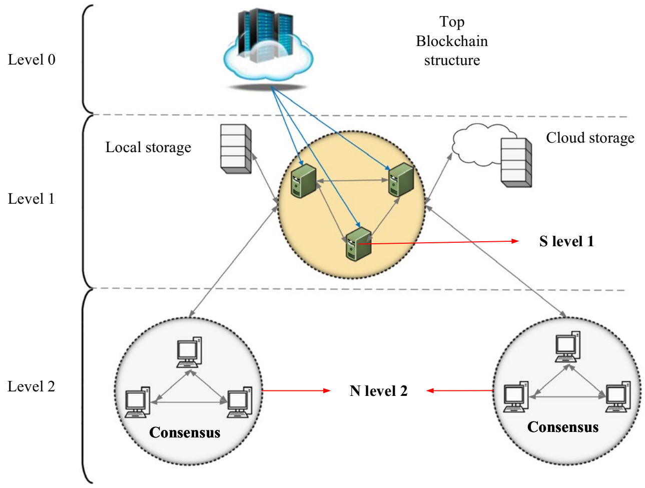

FIGURE 3 Structure of the network framework

with diverse levels, as shown in Figure 3. The blockchain at the upper level, which is a public blockchain, interacts with the blockchain at the lower level, which is a private blockchain. Following that, we define the layout of the data stream under the system. Consequently, the registered data at the bottom level are transmitted through to the top blockchain and, accordingly, are recorded in each blockchain. Lastly, we present the approach whereby the PSC-Bchain consensus model verifies the credibility of the joined node from the source to the destination.

The scenario on which the e-voting system is based includes servers that manage the underlying nodes. The computational capacity of these servers is superior to that of the base nodes, which have limited assets and transfer speed. In addition, these nodes regularly interact with the cloud computing and cloud storage stages; thus, they have great storage abilities and system correspondence capacities. We have divided the elements of the framework of the system structure into layers of nodes and managing servers to construct the network framework for verifying the credibility. We briefly present the layers of the system structure:

Nodes (N): Voters' devices.

Servers (S): Devices for overseeing or managing and designating computations as well as their capacity. The servers are summoned in various blockchain structures based on their level of position. First, the servers at level 1 are legitimately associated with the nodes. The duties of these servers include providing the certificates for the nodes at level 2, storing the information gathered by nodes and sending it to the blockchain network responsible for verifying the credibility of the nodes. Second, the servers at level 1 additionally manage the data published to the upper blockchain. The structure of the blockchain network in our framework is composed of a group of servers with each blockchain network being managed by one server and the diverse nature of the blockchain network could form a hierarchical relationship. Moreover, information in the blockchain network in our framework could be stored either in local storage or cloud storage.

4.2 | Real-life hybrid consensus model

As shown in Figure 3, for our hybrid two-tiered consensus model, we viewed the organizing committee of elections as a public blockchain, perhaps with a single node. This means the government does not need to place all of its confidence and the fate of the entire democratic process in a public blockchain network. This is unlikely to happen anytime soon, and for a good reason, because the technology is still comparatively new and therefore unexploited. Alternatively, we are introducing to the process a layer of external verification, conducted by a global and impartial community of validators who have no involvement in the election process itself. This ensures that the process control stays in its expected state, but the supervision is external and immutable. Furthermore, our system offers a holistic approach in that it can be built from the ground upward, and we validated the entire process using a hybrid consensus model. As such, a hybrid consensus exists in the hybrid blockchain that can achieve multi-party confidence. These settings are provided according to the hybrid blockchain to support the multi-party confidence consensus system as follows:

- The miners (voters) can verify transactions from a pseudonymously authenticated node in the upper-chain (Ethereum blockchain).
- The upper-chain network can agree on the transactions by using only the PoS consensus method.

Moreover, when thinking of future elections, a possible solution could be a digital, blockchain-based e-voting process. In this scenario, voters would be biometrically recognized and receive a digital token that would allow them to vote but would still anonymize their vote. The mechanism that processes these transactions would be private blockchains on the PSC-Bchain Network using a hybrid consensus method (PoS and PoC), and interested stakeholders could be the block producers, political parties, observers, and government entities. The voters could temporarily store their transactions in the virtual blocks and send the transactions stored for replication to the private blockchain network. This setting, referred to as gathering transactions, confers the following additional capabilities upon the hybrid blockchain:

- The voter machine sends sensitive transactions to the public blockchain in real time and saves the transactions in the virtual blocks.
- The voter machine can also collect and store non-real-time sensitive transactions in virtual blocks.

- The voter machine sends its virtual blocks to the private blockchain for data replication.

The blocks would be validated by the PSC-Bchain Network validators who enforce, execute, and govern, thus ensuring that the block producers do not act fraudulently.

4.3 | Method for verifying the credibility of a node

As shown in Figure 4, for nodes, the added data include an ID and a Private Key, where the ID is used as a specific node identifier for identifying one another; the private Key is used as asymmetric encryption and as a flag for node credibility verification. The Private Key is obtained and issued by the Manager Server (MS), which is responsible for node management. The ID, Private Key, and block contents are considered as additional data in the MS. Among them, the ID is the unique MS identifier. It should be noted that the MS is also a kind of system node (except for its computational ability and storage capacity, it is the same as the other nodes). Therefore, the MS should have the same attribute ID as those nodes; that is, the MS and node IDs should have the same definition.

According to blockchain technology, each block includes a blockhead and block data. The purpose of the blockhead is to store previous block information, including the block numbers and hash values. The structure of the block record includes the ID of the node or MS, flag for adding or deleting information of the objects managed by the MS, timestamp, transaction count, Merkle root, and contract. The Public Key should be created from the Private Key of the correct object in one block record.

4.4 | Deterrence by the credibility collapse

Solving the problems associated with attacks requires an alternative way to deter attacks in the event of the collapse of coin prices. The alternative we propose is the collapse of credibility. Credibility is a metric that defines honest contract owners (voters). Our approach entails measuring the credibility by calculating the number of miners and describing that number as a score of the credibility. Instead of using proof-of-stake alone, we suggest reaching consensus in the private blockchain network by requiring a block miner to generate a block to provide proof that their credibility score is sufficiently high.

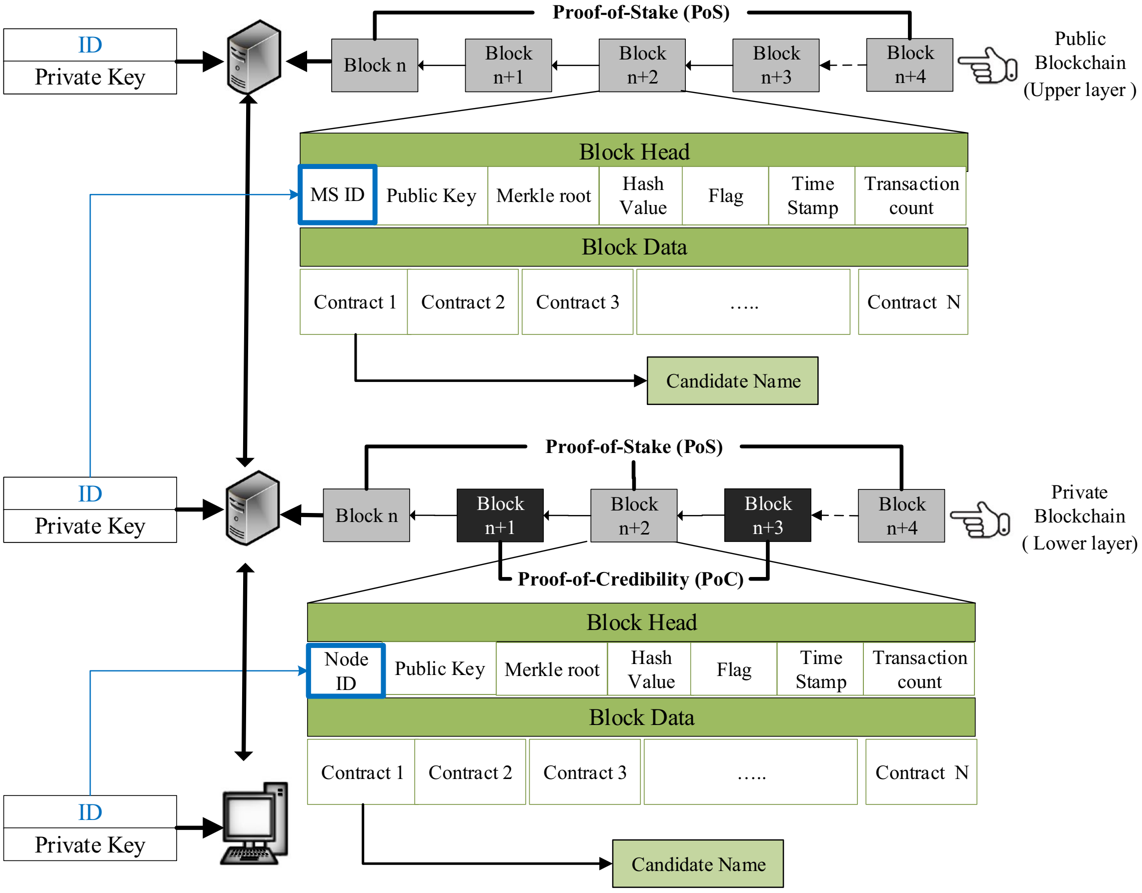

FIGURE 4 Hybrid consensus model (PSC-Bchain) for data verification

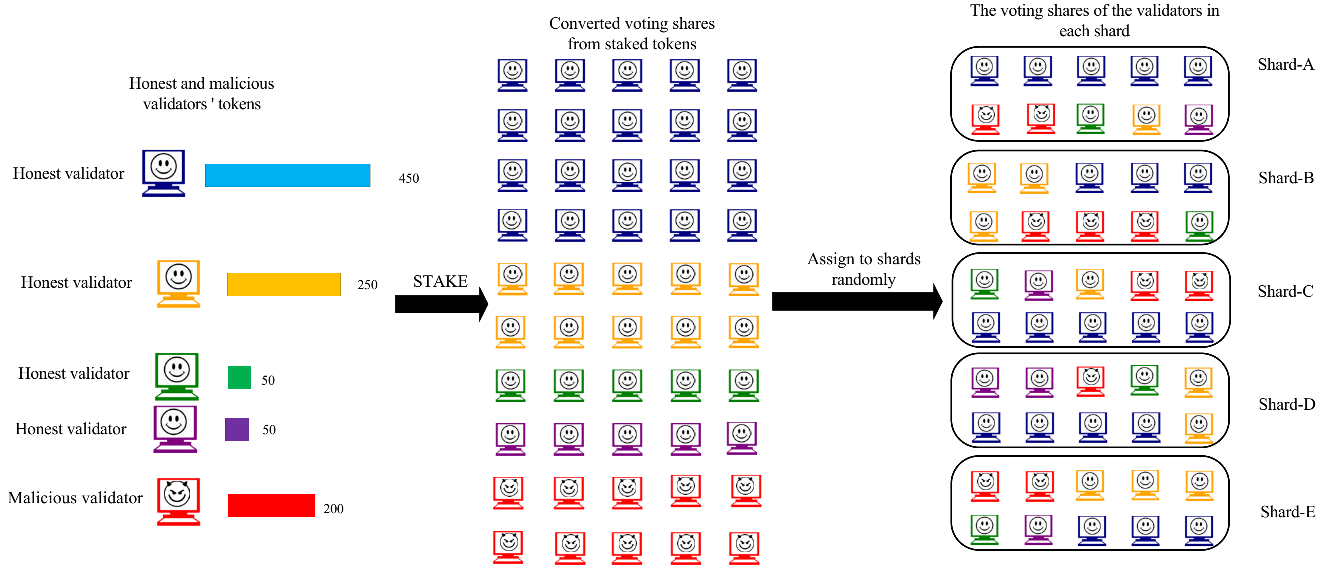
Honest and malicious validators ' tokens
Honest validator
450
Honest validator
250
Honest validator
50
Honest validator
50
Malicious validator
200
STAKE
Converted voting shares from staked tokens
Assign to shards randomly
The voting shares of the validators in each shard
Shard-A
Shard-B
Shard-C
Shard-D
Shard-E

FIGURE 5 Sharding mechanism by voting shares

Moreover, an attacker who has phony credibility could succeed with a 51 % attack. A possible approach to address this problem would to increase the cost of a 51 % to more than it was before. Therefore, we combined PoS and PoC to gain a robust consensus mechanism. In addition, the PoS method needs to store sufficient coins and the PoC needs to utilize sufficient coins to generate the block (smart contract). Consequently, the combination of the consensus methods (PoS and PoC) could be expected to lead toward creating a secure hybrid blockchain. As shown in Figure 4, if a voter records their vote in a block using the PoS, the subsequent voter has to record his/her vote in the next block utilizing the PoC, and the next block after that, has to be generated using PoS.

4.5 | Incorporation of PSC-Bchain and sharding

Assume there are three nodes n_1, n_2, and n_3, which need to verify data D. Instead of n_1, n_2, and n_3 verifying all the data D at once, the data are divided into three shards: d_1, d_2, and d_3. Then n_1, n_2, and n_3 verify each shard independently. This saves an exponential amount of time.

Sharding helps to ease the workload when the network is only as fast as the individual nodes, instead of the sum of its parts, by providing an alternative. The idea involves grouping subsets of nodes into shards, which process transactions specific to that shard in turn. This allows the system to process many of the transactions in parallel, thus significantly increasing the throughput. As presented in Figure 5, a group of consensus validators is assigned to the shard by the proposed model; nodes are assigned randomly to the shards by a secure algorithm named Verifiable Random Function (VRF) [42] and Verifiable Delay Function(VDF) [43].

Therefore, to become a validator, participants need to be eligible for a certain number of tokens. The number of tokens staked determines the number of voting shares the validator is assigned. For a fixed period of time, the validators remain assigned to the specific shard, and then the voting shares are recomputed to assign validators to the shards randomly. The reshuffle process helps to add additional security to prevent malicious attackers from overtaking a single shard over a specified period. Specifically, this technique guarantees that:

- Attackers are unable to choose on which shard they want to work.
- Attackers are unable to learn which shard they will be working on in advance.

As we mentioned earlier, our model is composed of two chains working side by side. The private-chain is a side-chain that stores the hashes to the public-chain (Ethereum) blocks in its own blocks. This side-chain provides a distributed randomness source that allows us to create a sharding system on top of it. This is accomplished by deploying the contract on the public blockchain (Ethereum) known as the Validator Registration Contract, where voters can spend ETH in return for becoming a validator in this private-chain (side-chain). The side-chain periodically checks for registered validators and, subsequently, forms a queue of those who have burned ETH into the contract. This private-chain acts as a coordination mechanism for the sharding system, allowing for distributed pseudorandomness that is crucial for the selection of sharding validator committees. The source of randomness must be general to ensure that this sampling is entirely mandatory and cannot be gamed by the validators concerned. In Section 5, we demonstrate the simulated results that address the scalability and performance of the introduced e-voting system based-blockchain via the proposed hybrid consensus model combined with the mechanism of sharding.

4.6 | Proposed model description

Pascal and Fermat examined a simulated puzzle named Gambler's Ruin in 1656 [44]. The simulation is that of a gambler venturing into a casino for a simple game of chance. Using this game as illustration and to reach the Nakamoto goal [22], we need to alter the game. First, we allow the attacker to lose a certain amount of money v before it is relinquished and then we determine the outcome when the value of v reaches infinity. Therefore, this same alteration is transformed into the original Gambler's Ruin and demonstrated in this way:

The gambler commences with $i = v$ dollars, and the game concludes with a win at $N = v + z$ dollars or at zero dollars, which translates as a loss. In these scenarios, our assumptions are as follows: $q_0 = 0$ and $q_N = 1$ where q represents a fraction of all the mining power and $p = 1 - q$ represents the set of honest miners in charge of the residual fraction. By modifying (17) in reference [45], we find that:

$$q_i = \begin{cases} \dfrac{1-\left(\frac{p}{q}\right)^{v}}{1-\left(\frac{p}{q}\right)^{v+z}} & \text{if } p \neq q, \\ \dfrac{v}{v+z} & \text{if } p = q = 0.5. \end{cases} \quad (1)$$

Considering that a gambler is ready to lose an inestimable amount of money, this means that they have infinite resources where v approaches infinity and in a scenario where $p < q$, $(p/q)^v \rightarrow 0$ as $v \rightarrow \infty$:

$$\lim_{v\rightarrow\infty} \frac{1-\left(\frac{p}{q}\right)^{v}}{1-\left(\frac{p}{q}\right)^{v+z}} = 1 \text{ when } p < q. \quad (2)$$

In the scenario where $p > q$ we take $(q/p)^v$ as a factor from the numerator and denominator, then:

$$\frac{1-\left(\frac{p}{q}\right)^{v}}{1-\left(\frac{p}{q}\right)^{v+z}} = \frac{\left(\frac{p}{q}\right)^{v}\left(\left(\frac{p}{q}\right)^{-v}-1\right)}{\left(\frac{p}{q}\right)^{v}\left(\left(\frac{p}{q}\right)^{-v}-\left(\frac{p}{q}\right)^{z}\right)} = \frac{\left(\frac{p}{q}\right)^{-v}-1}{\left(\frac{p}{q}\right)^{-v}-\left(\frac{p}{q}\right)^{z}}. \quad (3)$$

$$\lim_{v\rightarrow\infty} \frac{\left(\frac{p}{q}\right)^{-v}-1}{\left(\frac{p}{q}\right)^{-v}-\left(\frac{p}{q}\right)^{z}} = \frac{-1}{-\left(\frac{p}{q}\right)^{z}} = \left(\frac{q}{p}\right)^{z} \text{ when } p > q. \quad (4)$$

when $p > q$, $(p/q)^{-v} = (q/p)^v \rightarrow 0$ as $v \rightarrow \infty$. Because (4) assumes that the attacker has infinite resources at their disposal, our existing notation, q_∞, cannot be applied as it is no longer useful. Therefore, we switch notation and let Q_z denote the likelihood of an attacker regaining their losses from a given shortfall of z given unlimited resources:

$$Q_z = \begin{cases} 1 & \text{if } p < 1, \\ \left(\dfrac{q}{p}\right)^{z} & \text{if } p > q. \end{cases} \quad (5)$$

Nakamoto [22] provided that ∃ S is a random variable for the number of blocks an attacker discovers in the period of time in which honest miners discover z blocks.

Considering $P(S; \lambda)$ as the likelihood of the attacker producing S blocks, it is observed that $q_{(z-v)}$ is the difference associated with the likelihood of recovering to the remaining $z - v$ blocks. Therefore, to determine the total likelihood of recovering, we sum all the potentials of S:

$$= P(S=0;\lambda)Q_z + P(S=1;\lambda)Q_{z-1} + \cdots, \quad (6)$$

$$= \sum_{v=0}^{\infty} P(S=v;\lambda)Q_{z-v}, \quad (7)$$

$$= \sum_{v=0}^{\infty} \frac{\lambda^v e^{-\lambda}}{v!} Q_{z-v} \quad (8)$$

Thus, to determine the possibility (probability) of the attacker still making up the arrears, we multiply (8) of each amount of advancement they could have made, by the likelihood, in which case the attacker could regain their position from that point:

$$\sum_{v=0}^{\infty} \frac{\lambda^v e^{-\lambda}}{v!} \begin{cases} (q/p)^{z-v} & \text{if } v \leq z \\ 1 & \text{if } v > z. \end{cases} \quad (9)$$

Finally, because the possibility of an event occurring is equal to 1 minus the likelihood that it does not, where Nakamoto [22] transposes for (almost) our final result; therefore, reducing from 1 the likelihood that the attacker does not regain the arrears after mining v blocks.

$$= 1 - \sum_{v=0}^{\infty} \frac{\lambda^v e^{-\lambda}}{v!} \begin{cases} (q/p)^{z-v} & \text{if } v \leq z, \\ 1-1 & \text{if } v > z. \end{cases} \quad (10)$$

$$= 1 - \sum_{v=0}^{\infty} \frac{\lambda^v e^{-\lambda}}{v!} \left(1-\left(\frac{q}{p}\right)^{z-v}\right) + \sum_{v=z+1}^{\infty} \frac{\lambda^v e^{-\lambda}}{v!} \cdot (0) \quad (11)$$

TABLE 2 Successful attack probabilities in each chain

Attacker assets (q, q_1)	Classical blockchain	Proposed hybrid blockchain				
		$q_{2=0.1}$	$q_{2=0.2}$	$q_{2=0.3}$	$q_{2=0.4}$	$q_{2=0.5}$
0.1	2.42803 E^{-4}	2.42803 E^{-4}	0.00232	0.01256	0.05020	0.16053
0.2	0.01425	0.00322	0.01425	0.04636	0.12464	0.28690
0.3	0.13211	0.02074	0.05721	0.13211	0.26724	0.47706
0.4	0.50398	0.09039	0.17697	0.31310	0.50398	0.72980
0.5	1.00000	0.29233	0.43879	0.62224	0.82447	1.00000

Hence, the likelihood of P_z being a success is:

$$P_z = 1 - \sum_{v=0}^{z} \frac{\lambda^v e^{-\lambda}}{v!} \left\{ 1 - \left(\frac{q}{p}\right)^{z-v} \right\}, \lambda = z\frac{q}{p}. \tag{12}$$

The variable p is the likelihood of the honest node discovering the next block, whereas the variable q, as mentioned above, is determined by finding the likelihood of the assets possessed by the attacker such as the computing power, holding coins, and credibility score, where $p = 1 - q$. Equation (12) represents the classical blockchain, whereby the suggested hybrid blockchain translates to:

$$P_z = 1 - \sum_{v=0}^{z} \frac{\lambda^v e^{-\lambda}}{v!} \left\{ 1 - \prod_{n=1}^{z-v} \left(\left| \frac{q}{p} \right| \right) \right\} \lambda = \sum_{n=1}^{z} \frac{q}{p},$$

$$q/p = \begin{cases} q_1/p_1 \text{ if } n = 2m - 1(\text{odd}), \\ q_2/p_2 \text{ if } n = 2m(\text{even}). \end{cases} \tag{13}$$

According to (13), q_1/p_1 presents the rate of one resource and q_2/p_2 presents the rate of other resources, where the two rates may refer to whether it is a coin held or the score of credibility. Again, the parameter z indicates the number of blocks the elector needs to wait to prevent the attacker from achieving their goal. We set the number of blocks $z = 6$.

5 | EXPERIMENT AND PERFORMANCE EVALUATION

The experimentation is composed of three aspects. The first aspect of our experiment evaluates the implementation of the proposed model by comparing the probability of a successful attack in each chain: (proposed hybrid blockchain and classical blockchain). The second aspect is the evaluation of the performance of the proposed model with the mechanism of sharding in terms of the throughput and latency under various conditions and the comparison thereof with two existing consensus methods (PoW, PoS). The third aspect of the experiment involves deploying the smart contract in the Ethereum platform for testing the nodes and evaluating the average cost of voting among voters and the election committee.

5.1 | The experiment

The Poisson experiment is used to demonstrate the extent of an attacker's mining power and the number of successes that could happen. For example, consider a particular elector that requires $z = 4$ and an attacker with $q = 1/5$ mining power before the vote contract is released. In this scenario, the likelihood exists that the attacker produces $S = 2$ blocks as they await the validation of vote (S), thereby surpassing the blockchain.

This also occurs on the condition that $zq/p = z/4$, where q represents the attacker's assets and $p = 1 - q$. Hence, the likelihood of the attacker producing $S = 2$ blocks during an interval in which the real nodes generate $z = 4$ blocks is:

$$P(S = 2; \lambda = z/4) = \frac{(4/4)^2 e^{-4/4}}{2!} = \frac{1}{2e} \approx 0.18.$$

Now, with a known $(q/p)^{z-v}$, the likelihood exists of the attacker ultimately progressing to the remaining $z - v$ blocks, thereby reaching $(1/4)^2 \approx 0.0625$. Now, we require the results of the first and second parts to be equally true. Hence, by multiplying both results, the solution to the scenario or problem is: (0.18) (0.0625)≈1.13%.

A much broader scenario is to determine the likelihood that fewer blocks would be produced in the future by honest voters in relation to the attacker's assets q. The additional condition in this scenario is that the elector waits for z blocks before confirming the vote cast.

Notwithstanding that, this experiment used the Poisson distribution to investigate and compare the attack probabilities in the hybrid blockchain and classical blockchain. Table 2 lists the successful attack probabilities in each chain (proposed hybrid blockchain and classical blockchain).

Figure 6 shows the attacker's mining power and the probability of success in each chain (hybrid chain and classical chain).

The result of this investigation confirms that it is more difficult to attack our proposed hybrid blockchain compared to the classical blockchain. The curves shown in Figure 6 represent the attacker's assets (such as the buffer capacity or computing power, holding coins, or credibility score) as a function of the attacker's success probability. This proves/

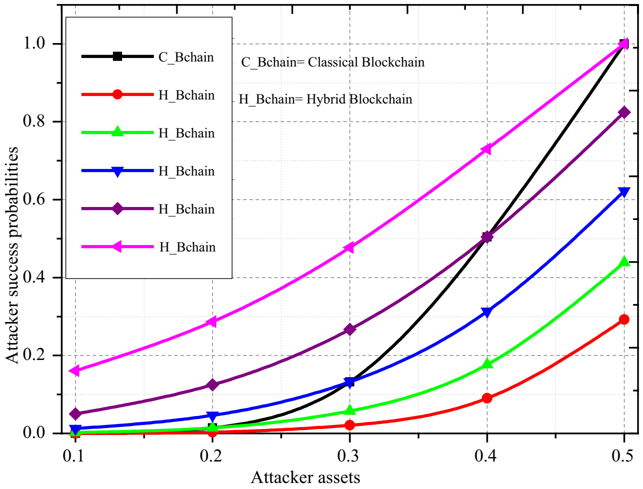

FIGURE 6 Probability of a successful attack in each chain (classical blockchain and the proposed hybrid blockchain)

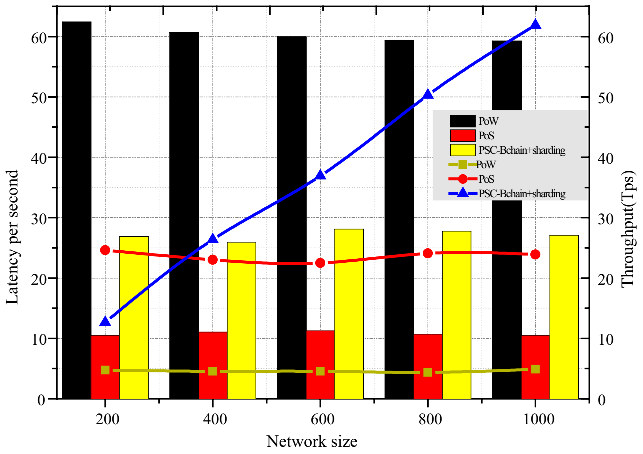

FIGURE 7 Comparison of the performance evaluation (Throughput + Latency) of the proposed model (PSC-B chain + sharding) and existing consensus methods (PoW + PoS) with a shard size of 10

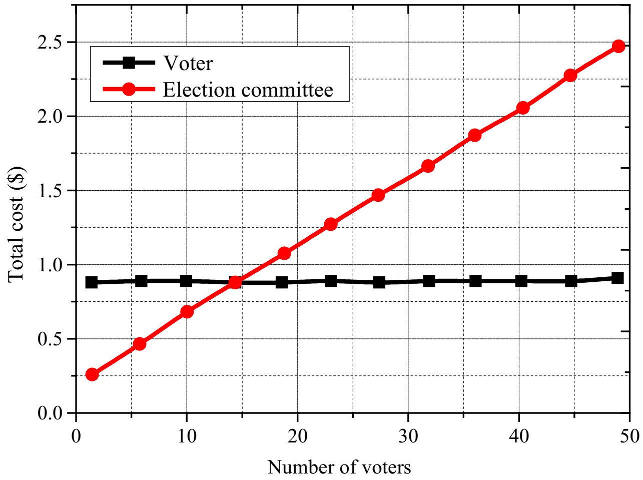

FIGURE 8 Average cost measured for the voter and election committee

confirms that the proposed hybrid blockchain is more effective than the classical blockchain.

5.2 | Performance evaluation

The experimental setup of the proposed PSC-Bchain consensus model was implemented using MATLAB with originlab and the experimental simulation was performed on the Amazon Elastic Compute Cloud (Amazon EC2) to measure the performance. The size of the simulation network ranged from 200 to 1000 for t2.medium type as a single node with vCPU = 2 and memory (GiB) = 4.

The experiment was conducted to measure the scalability of the proposed PSC-Bchain and to evaluate the performance by comparing the throughput and latency of the proposed model with those of existing consensus methods such as PoS and PoW. First, we implemented a simulation network of 200 nodes as the size of each group of nodes, and increased the network size four times to 1000 nodes. We assessed the latency and measured the throughput for ten blocks. Second, for the PoW and PoS protocols, we conducted experiments using the same simulation network with the total number of nodes (the network size) ranging from 200 to 1000. We assessed ten blocks of PoW and ten blocks of PoS to determine the latency.

Figure 7 compares the existing consensus methods (PoW, PoS) and the proposed consensus model (PSC-Bchain). The PoW consensus method had the highest latency of approximately 63 s, as shown by the data bars, whereas the PoS consensus method had the lowest latency of 10 s. The latency of the proposed PSC-Bchain consensus model was approximately 27 s. Moreover, as presented in Figure 7, an increase in the number of nodes did not increase the rate at which transactions were processed by either PoW or PoS. Nevertheless, when the number of nodes increased, the proposed PSC-Bchain model managed more transactions. When the number of nodes was increased to 1000, the throughput of the proposed PSC-Bchain exceeded 60 Tps, which is higher than that of PoW and PoS, for which the throughput was 5 Tps and approximately 25 Tps, respectively. Therefore, the result confirms that the proposed PSC-Bchain combined with the mechanism of sharding is highly scalable.

5.3 | Evaluation on Ethereum platform

To measure the average cost among voters and the election committee, we first deployed the smart contract in the Ethereum platform to test the nodes. Then, to generate the smart contract, we installed the node.js library, Meta mask extension, and Ganache server. Finally, we ran 120 transactions to check the smart contract in real time. Figure 8 shows the cost distribution between the election committee and the number of voters participating in the elections. The figure indicates that the cost of the election committee increases linearly based on the number of voters, while the cost of voting remains constant. The running cost of 50 voters was 0.73$ per vote count in the smart contract and the proposed technique was executed using the Ethereum blockchain.

6 | DISCUSSION AND ANALYSIS

In this section, we discuss the attack analysis and security analysis.

6.1 | Attack analysis

To complete an attack, the attacker needs to create another chain that is faster than a legitimate chain. We considered the probability of an attacker succeeding when attempting to use an illegal chain.

According to Nakamoto [22], an attacker is likely to recover from a given shortfall in which a block disparity exists among the legal blockchain and their illegal blockchain. The voter waits until the transaction is added to a block and z blocks are linked after it. The voter is clearly unaware of the actual advancement the attacker has made but simply knows that the legitimate blocks took the average expected time per block. This means that the attacker's progress is shown in the form of a Poisson distribution with the prospective value: $\lambda = zq/p$. To determine the expected value, a real situation is modeled on the basis of the probability by counting the number of successes in a series of intervals measured in time. This model requires several assumptions to be made:

- The likelihood of more than one success in a brief time period is insignificant.
- The likelihood of a scenario yielding a successful outcome during a short time period is relative to the duration of the time interval.
- The number of successful scenarios that occur during each time period is autonomous to each other.

We are also of the assumption that the likelihood of success does not change during the experiment, although in reality, voters can alter their resources accordingly.

6.2 | Security analysis

The security analysis comprises two aspects. The first aspect involved the security analysis of the proposed consensus model (PSC-B chain) with the sharding mechanism. Because a 51% attack is one of the security concerns of blockchain, for instance, with the PoW consensus protocol, nodes that control more than half of the total CPU power can successfully launch malicious attacks. In contrast, the PoS consensus method is considered more secure in this regard. This is because, in PoS, a certain number of coins are involved and this increases the cost of carrying out the 51% attack compared with PoW; although, in the event of a 51% attack, the attacker's gain would be small. Therefore, malicious nodes have little motivation to attack the network.

However, the proposed consensus model takes advantage of three mechanisms to reach a high security level:

- Randomness: The formation of node groups and leader node selection is random.
- Reshuffling: All the nodes are reshuffled to form new groups for each T epochs.
- Coin-age constraint: the age of the coin is restricted and reset to zero after the coins were spent.

Therefore, these three mechanisms help to prevent malicious nodes from controlling the network shards and decrease the motivation to launch an attack of 51%.

The second aspect involved the security analysis of the proposed blockchain-based e-voting system, which can afford the accuracy and security by satisfying the following requirements:

- Voter Eligibility: Only a verified voter has the right to vote.
- Verifiability: Every voter can check whether their vote has been tallied appropriately.
- Robustness: The results of tallying the votes and the recorded information are transmitted to the blockchain with which it is difficult to tamper.
- Uniqueness: The vote is verified twice: in the blockchain contract and the server.
- Ballot Receipt: After the elector submits their vote, the transaction ID (TxID) is turned back to the elector as proof that their vote is recorded successfully in the blockchain.
- Transparency: Because the nature of the blockchain offers transparency by default, it ensures that all the voting procedures are available for the people joining the blockchain network.
- Embed Trust: The blockchain contract can contribute various security features to the e-voting system such as Security, Autonomy, and Transparency with zero manipulated potential outcomes or mistakes.
- Scalability: The proposed PSC-Bchain, combined with the mechanism of sharding, provides security and a high throughput according to the performance analysis, which in turn confers scalability upon the introduced e-voting system based on blockchain.

7 | CONCLUSION

Recent studies indicated that e-voting systems based on blockchain are being developed as the next generation of modern e-voting systems to exploit the immutable feature of blockchains. However, the classical blockchain consensus protocol, that is, Proof-of-Work (PoW), as seen in Bitcoin, significantly impacts the energy consumption and compromises system scalability, efficiency, and latency. In this paper, we proposed a hybrid consensus model (PSC-Bchain) in which Proof of Credibility (PoC) works mutually with Proof of Stake (PoS). This led to the creation of a secure hybrid blockchain, which ensures integral security when applied to the e-voting system. We also combined the mechanism of sharding with the proposed PSC-Bchain model to emphasize security and enhance the scalability and performance of the blockchain-based e-voting system. Furthermore, we compared attack execution on both the classical blockchain and proposed hybrid blockchain, and also presented an attack analysis and security analysis. Finally, although the latency of the proposed approach (27 s) is higher than that of PoS (10 s) and less than that of PoW (63 s), the experimental results confirmed that, when the network size increases to 1000 nodes, the proposed PSC-Bchain model with sharding has higher throughput (60 Tps) than PoW (5 Tps) and PoS (25 Tps). These results confirm that the proposed PSC-Bchain with sharding is secure and highly scalable. In terms of future work, we would need to ensure coercion resistance and receipt freeness by employing a randomizer token, that is, a tamper-resistant source of randomness that acts as a black box, to construct the ballot for the user.

ACKNOWLEDGMENTS

The author would like to thank the editor and all the anonymous reviewers for their helpful feedback.

ORCID

Yousif Abuidris https://orcid.org/0000-0001-9809-6642

REFERENCES

1. J. Epstein, *Are all types of internet voting unsafe?*, IEEE Secur. Priv. **11** (2013), 3–4.
2. R. Araújo et al., *Remote electronic voting can be efficient, verifiable and coercion-resistant*, in Proc. Int. Conf. Financial Cryptography Data Security (Barbados), 2016, pp. 224–232.
3. A. Blinder, *Election fraud in north carolina leads to new charges for republican operative*, 2019, Accessed Aug. 2019, available at https://www.nytimes.com/2019/07/30/us/mccrae-dowless-indictment.html
4. F. Bajak, *Georgia election server wiped after suit filed*, 2017, Accessed Aug. 2019, available at https://www.pbs.org/newshour/politics/georgia-election-server-wiped-after-suit-filed
5. R. Michael Alvarez, I. Levin, and Y. Li, *Fraud, convenience, and e-voting: how voting experience shapes opinions about voting technology*, J. Inform. Technol.Politics **15** (2018), 94–105.
6. J. Paul Gibson et al., *A review of e-voting: the past, present and future*, Ann. Telecommun. **71** (2016), 279–286.
7. A. Karamchandani et al., *Perception-based model for analyzing the impact of enterprise blockchain adoption on scm in the indian service industry*, Int. J. Inform. Manage. **52** (2019), 102019.
8. A. Klarin, *The decade-long cryptocurrencies and the blockchain rollercoaster: Mapping the intellectual structure and charting future directions*, Res. Int. Business Finance **51** (2020), 101067.
9. Z. Wang et al., *Blockchain-based framework for improving supply chain traceability and information sharing in precast construction*, Automat. Constr. **111** (2020), 103063:1–11.
10. S. Tanwar, K. Parekh, and R. Evans, *Blockchainbased electronic healthcare record system for healthcare 4.0 applications*, J. Inform. Secur. Appl. **50** (2020), 102407:1–13.
11. A. Singh et al., *Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities*, Comput. Secur. **88** (2020), 101654:1–16.
12. M. Zachariadis, G. Hileman, and S. V. Scott, *Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services*, Inf. Organ. **29** (2019), 105–117.
13. K.-H. Wang et al., *A review of contemporary e-voting: Requirements, technology, systems and usability*, Data Sci. Patt. Recogn. **1** (2017), 31–47.
14. M. K. Alomari, *E-voting adoption in a developing country*, Transform. Gov. People Process Policy **10** (2016), 526–547.
15. followmyvote, *Introducing a secure and transparent online voting*, 2016, Accessed May 2019, available at https://followmyvote.com/
16. Agora, *Bringing our voting systems into the 21st century*, white paper, 2017, Accessed May. 2019, avaiable at https://www.agora.vote/
17. Voatz, *Voatz: A secure vote in every hand*, white paper, 2019. Accessed May 2019, available at https://melodygee.com/wp-content/uploads/2019/05/Voatz-Security-White-Paper_V7.pdf
18. J. Lyu et al., *A secure decentralized trustless e-voting system based on smart contract*, in Proc. IEEE Int. Conf. On Trust, Security Privacy Comput. Commun. (Rotorua, New Zealand), 2019, pp. 570–577.
19. X. Yang et al., *Decentralized voting: a self-tallying voting system using a smart contract on the ethereum blockchain*, in Proc. Int. Conf. Web Inf. Syst. Eng. (Dubai, United Arab Emirates), 2018, pp. 18–35.
20. P. McCorry, S. F. Shahandashti, and F. Hao, *A smart contract for boardroom voting with maximum voter privacy*, in Proc. Int. Conf. Financial Cryptography Data Security (Malta), 2017, pp. 357–375.
21. Y. Abuidris, R. Kumar, and W. Wenyong, *A survey of blockchain based on e-voting systems*, in Proc. Int. Conf. Blockchain Technol. Applicat (Xi'an, China), 2019, pp. 99–104.
22. S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, Tech. report, Manubot, 2019.
23. S. Zhang and J.-H. Lee, *Analysis of the main consensus protocols of blockchain*, ICT Express **6**, 2019, 93–97.
24. B. Cao et al., *Performance analysis and comparison of PoW, PoS and DAG based blockchains*, Digital Commun. Netw., (2020), https://doi.org/10.1016/j.dcan.2019.12.001

25. X. Zhu and Y. Yang, *Hybrid consensus for blockchain using proof of work and proof of stake*, 2019, US Patent App. 16/430,398.
26. Y. Abuidris et al., *Risks and opportunities of blockchain based on e-voting systems*, in Proc. Int. Comput, Conf, Wavelet Active Media Technol. Inf. Process (Chengdu, China), 2019.
27. H. Chen and Y. Wang, *Sschain: A full sharding protocol for public blockchain without data migration overhead*, Pervasive Mob. Comput. **59** (2019), 101055:1–15.
28. H. Watanabe et al., *Blockchain contract: Securing a blockchain applied to smart contracts*, in Proc. IEEE Int. Conf. Consumer Electron. (Las Vegas, NV, USA), 2016, pp. 467–468.
29. J. P. Cruz and Y. Kaji, *E-voting system based on the bitcoin protocol and blind signatures*, IPSJ Trans. Math. Model. Appl. **10** (2017), 14–22.
30. S. Bistarelli et al., *An end-to-end voting-system based on bitcoin*, in Proc. Symp. Appl. Comput. (Marrakech, Morocco), 2017, pp. 1836–1841.
31. Z. Zhao and T.-H. Hubert Chan, *How to vote privately using bitcoin*, in Proc. Int. Conf. Inf. Commun.Security (Beijing, China), 2015, pp. 82–96.
32. E. Yavuz et al., *Towards secure e-voting using ethereum blockchain*, in Proc. Int. Symp. Digital Forensic Security (Antalya, Turkey), 2018, pp. 1–7.
33. G. G. Dagher et al., *Secure voting system using ethereum's blockchain*, in Proc. Int. Conf. Inf. Syst, Security Privacy (Madeira, Portugal), 2018, pp. 96–107.
34. S. Shukla et al., *Online voting application using ethereum blockchain*, in Proc. Int. Conf. Advances Comput., Commun. Inform. (Bangalore, India), 2018, pp. 873–880.
35. S. Pareek et al., *E-voting using ethereum blockchain*, IJRTI. **3** (2018), 2456–3315.
36. K. M. Khan, J. Arshad, and M. M. Khan, *Investigating performance constraints for blockchain based secure e-voting system*, Future Gener. Comput. Syst. **105** (2020), 13–26.
37. S. Zhang, L. Wang, and H. Xiong, *Chaintegrity: blockchainenabled large-scale e-voting system with robustness and universal verifiability*, Int. J. Inf. Secur. **19** (2019), 1–19.
38. L. Fan and H.-S. Zhou, *A scalable proof-of-stake blockchain in the open setting (or, how to mimic nakamoto's design via proof-of-stake)*, Tech. report, Cryptology ePrint Archive, Report 2017/656, 2017.
39. Z. Liu et al., *Fork-free hybrid consensus with flexible proof-of-activity*, Future Gener. Comput. Syst. **96** (2019), 515–524.
40. M. Al-Bassam et al., *Chainspace: A sharded smart contracts platform*, arXiv preprint, 2017, arXiv:1708.03778.
41. L. Kan et al., *A multiple blockchains architecture on interblockchain communication*, in Proc. IEEE Int, Conf. Softw. Quality, Reliability Security Companion (Lisbon, Portugal), 2018, pp. 139–145.
42. S. Micali, M. Rabin, and S. Vadhan, *Verifiable random functions*, in Proc. Annu. Symp. Foundations Comput. Sci.in Proc. Annu. Symp. Foundations Comput. Sci. (New York), 1999, pp. 120–130.
43. D. Boneh et al., *Verifiable delay functions*, in Proc. Annu. Int. Cryptology Conf (Santa Barbara, CA), 2018, pp. 757–788.
44. A. W. F. Edwards, *Pascal's problem: The'gambler's ruin'*, Int. Stat. Rev. Revue Int. Stat. **51** 1983), 73–79.
45. A. Ozisik and B. N. Levine, *An explanation of nakamoto's analysis of double-spend attacks*, arXiv preprint, 2017, arXiv:1701.03977.

AUTHOR BIOGRAPHIES

Yousif Abuidris He received his BS degree in mathematics and computer science and MS degree in Information Technology from AL-Neelain University, Khartoum, Sudan. He received his PhD From University of Electronic Science and Technology of China (UESTC). Currently, He is working as assistant professor at University of Gadarif in Sudan. His research interests include blockchain-based systems, parallel and distributed systems, computer network security, computer security, and reliability.

Rajesh Kumar was born in the Sindh Province of Pakistan in November 1991. He received his BS and MS degrees in computer science from the University of Sindh, Jamshoro, Pakistan. He received his PhD in computer science and engineering from the University of Electronic Science and Technology of China (UESTC). Presently, he is working as postdoctoral fellow in Information Security at the UESTC in China. His research interests include machine learning, deep leaning, malware detection, Internet of Things (IoT) and blockchain technology. He has published more than 20 articles in various international journals and conferences.

Ting Yang obtained his PhD from UESTC (University of Electronic Science and Technology of China), in 2014. He is currently working as an Associate Professor at the School of Computer Science and Engineering of UESTC. His research interests include wireless sensor networks, complex networks, and Blockchain.

JosephOnginjo is a PhD candidate in Management Science and Engineering at the University of Electronic Science and Technology of China. His research interests are Innovation and Entrepreneurship, as well as innovative applications of blockchain technology especially in the financial markets.