HAC-Bchain: A Secure and Scalable Blockchain-Shard Based E-Voting System

Sohel Ahmed Joni†, Rabiul Rahat†, Nishat Tasnin†, Partho Ghose†, and Loveleen Gaur*
†Dept of Computer Science and Engineering, Bangladesh University of Business and Technology, Bangladesh
*School of computer science, Taylor's university, Malaysia
Email: (sohelahmedjony, rabiulrahatt, nishattasnin02, parth.cse.jnu)@gmail.com, gaurloveleen@yahoo.com

***Abstract*—Voting is a fundamental right of citizens in a democratic country and crucial for any thriving democracy. Reliable voting systems are essential for free and fair elections in the modern era. Biometric Electronic Voting Machines (EVMs) address many issues with paper-ballot systems, but their closed-source nature undermines voter trust. Traditional election systems are also vulnerable to cyberattacks. This paper propose a hybrid blockchain-based electronic voting system (HAC-Bchain) to address the limitations of conventional e-voting systems and ensure a secure, auditable, tamper-proof, transparent, and privacy-preserving voting process. A scripting system for proposed blockchain facilitates a limited set of predefined operations for each layer, which helps authoritative figures to manage the election securely. This research also combine a category-based sharding mechanism with the HAC-Bchain hybrid approach to create more data-concentrated shards, which improves scalability, performance, and data availability. Furthermore, this research compare and discuss the performance and efficiency of different sharding configurations. The research experiments shed new light on the overall security, performance, and scalability of blockchain-based e-voting systems.**

***Index Terms*—EVM, Secuirity, Sharding, Attacks, Blockchain**

I. Introduction

The Election system is a crucial part of the democracy and a catalyst for the progression of a country. Conducting a fair and equitable election in a country where democracy is not yet firmly established poses significant challenges, particularly in the absence of a reliable voting system[1].

Till now paper-based voting system is the most practiced election system. However, these voting system has multiple Security vulnerabilities that can easily lead to election rigging and fraud from the government or third parties. Recently, Biometric EVM systems have been used to tackle many of these issues. But, still, such a system cannot provide satisfactory levels of transparency to voters because of the close source manner of the electronic system, and voters are uncertain whether their votes were counted as they were cast, a concern commonly referred to as voter confidence [2], [3].

Blockchain, as detailed in R.S. Ganeshet al.[3], is known for its distributed, tamper-resistant, and immutable nature, making it a significant public ledger. Immutability is a key feature achieved by linking each new block with the previous one, ensuring integrity and reliability [4]. Additionally, blockchain's redundancy through duplication across multiple nodes ensures high availability and enables third-party verification [5]. In many countries, the current electoral systems are legally mandated to enforce specific regulations to prevent unauthorized activities and misconduct during elections. In [5], the authors have introduced an election mechanism to offer a controlled level of authority, resembling an authorized block. This allows for the inclusion or exclusion of specific entities based on the electoral system. This approach ensures transparency, ballot integrity, and immutability while upholding the necessary level of regulation [6], [7]. Blockchain technology is considered a significant potential tool for implementing a modern and innovative voting process because of its transparency property[8].

However, due to the transparency of blockchain, it is difficult to maintain data privacy. To resolve this problem, many studies have been done [6], [7] used various encryption approaches to protect users' privacy. In block modularity, instead of storing all of the individual sections in a block, sections are grouped as multiple records within a block. A copy of these sections is stored in the local database, and the hash of these sections is stored in the block [9]. This reduces block size significantly. Each section within the block can be independently verified, and only updated sections are stored as new records and shared with other nodes. Moreover, scalability and performance are major concerns in existing blockchain technology. To tackle this, researchers have explored sharding techniques [10], [11], which involve partitioning the blockchain into smaller shards.

With an aim to enhance the security, scalability, and efficiency of the e-voting system, this research propose a new hybrid consensus model called Hierarchical Authoritative Consensus (HAC) with the combination of blockchain and sharding. The proposed system utilizes a category-based sharding approach, where the blockchain is divided into shards based on the category or type of data stored.

The research contributions can be summarised as follows:

- The research propose a hybrid consensus model that merges the strengths of public and private consensus models to improve security, efficiency, transparency, and trustworthiness in voting systems.
- The research propose a polling-station-based sharding mechanism for e-voting, which divides the blockchain into smaller shards, each responsible for a single polling station. This allows parallel processing of votes, significantly improving scalability and reducing data concentration.

The rest of the paper is organized as follows: Section II discusses the recent research on e-voting systems based on blockchain. An overview of the proposed e-voting system is provided in Section III. Section IV gives detailed implementation information. Section V presents the performance evaluation of the proposed system, followed by the discussion given in Section VI. And finally, section VII concludes the paper.

II. RELATED WORK

This section discusses some recent researches on blockchain-based e-voting systems.

Many works attempted to develop protocols for blockchain-based e-voting systems and create incentive schemes for cryptocurrencies. This research work is motivated by recent advances [12], [13], [14], [15]. Pathak et al. [12] proposed a method based on a predetermined turn on the system for each node in the blockchain. Das et al. [13] proposed a blockchain-based voting system, integrated with the face recognition module. However, all these proposed methods have some major limitations including scalability, and extensive computational requirement.

Khoury et al. [14] proposed a decentralized trustless voting platform using Ethereum and also utilizing mobile numbers to prevent double voting. Hasan et al. [16] also proposed a blockchain-based voting system that operates on an Ethereum network and smart contract. Singh et al. [17] suggested a blockchain-based decentralized voting system that uses unique identification such as an Aadhar Card number or OTP for user authentication and Ethereum smart contract and integrated with traditional electronic voting machines. The Researchers from [13]-[17] 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.

Although Neloy et al. [18] efficiently utilized solidity smart contract space to reduce the transaction cost, still, depending on an Ethereum-based network could lead to centralization and infeasible gas cost for large-scale national-level elections. However, using two consensus mechanisms adds computational complexity and increases gas fees. Wang et al. [15] introduced CW-DPoS, improving node activity and fairness in DPoS. Following this research, Sun et al. [19] proposed DT-DPoS, enhancing security and scalability with Eigen Trust-based model and ring signatures.

Sharding is a mechanism to improve blockchain scalability by dividing the blockchain into smaller pieces, called shards. Each shard can process transactions independently, increasing throughput [20]. Tao et al. [21] proposed a new distributed and dynamic sharding system to improve throughput, requiring substantial cross-shard communication. Yousif et al. [22] Proposed a PSC-BChain e-voting system, a hybrid consensus model combining Proof of Credibility and Proof of Stake to address energy consumption, and sharding to address scalability issues in blockchain-based e-voting systems. Besides this, Kohad et al. [11] proposed a multiobjective genetic algorithm-based sharding to enhance the scalability and performance of the blockchain-based e-voting system. Based on the above discussion, it is clear that there is plenty of room to improve the blockchain-based e-voting system.

III. PROPOSED METHOD

The proposed voting system addresses the key aspects of a secure and fair voting system. This system is decentralized, secure, cost-effective, and easy to use.

As shown in Figure 1, the proposed architecture consists of three layers: application, network, and consensus layer. The application layer includes the EVM unit, Ballot unit, and Script panel. The network layer includes the P2P network, and Database. The consensus layer includes the Lookup table, Shard management system, Blockchain, Script execution, and Proof of Hierarchical Authoritative Consensus (HAC) for each block. In the following subsections, were discussed about proposed system and components in detail.

A. System Design

The main voting system is connected to a backend server that controls most functions. The server stores a copy of the blockchain or its shards in a Level-DB database. The system is written in Go and based on Gin web framework. The server handles communication with the blockchain network, the decentralized KMS server, the NID server, and the script execution mechanism. It also generates blocks and tokens. A detailed overview of the system is shown in Figure 2.

Roles of Participants: The election commission, returning officer, polling officer, and voters are the primary participants in the proposed blockchain voting system. All participants except for the candidates have a dedicated panel that corresponds to their level of access and permissions, allowing them to efficiently carry out their assigned tasks and communicate seamlessly between the various blockchain systems.

Entities: The proposed e-voting system uses NID cards, NID servers, blockchain networks, blockchain scripts, and tokens to ensure a secure, transparent, and reliable voting process. NID cards and servers authenticate voters and ensure eligibility.

Initialization: The system retrieves public keys, establishes connections, and retrieves election configuration, voter lists, candidate lists, and required commands with proof. It then executes and updates itself with the retrieved data.

Registration: Authorized personnel sign poll data and script with private keys and publish it on the blockchain network as shown in figure 2. Nodes verify the signature and script for legitimacy. The poll starts, and polling officers perform their duties. The hash of poll data is stored on the blockchain for tamper-proofing and accurate vote counting.

Election Creation: Authorized personnel sign the poll data with their private keys shown in figure 2. The signed poll script containing essential information is published on the

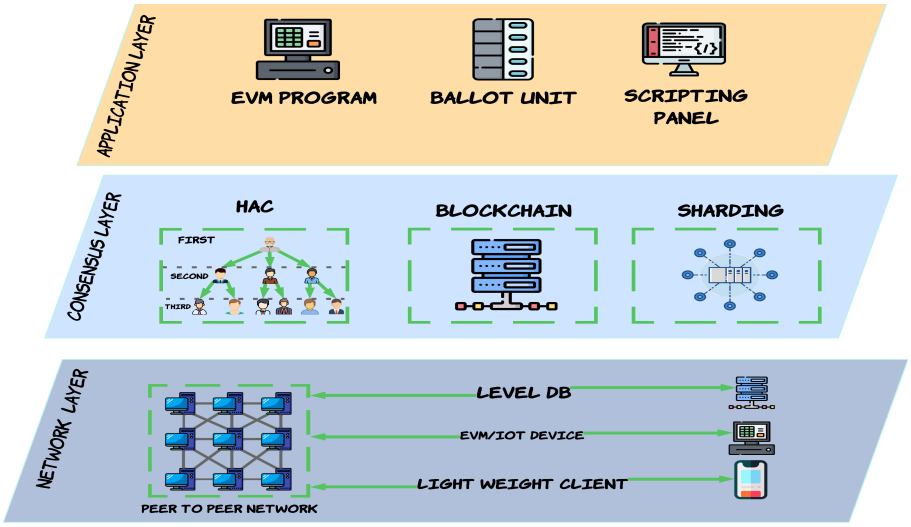

Fig. 1: shows the three-layer node architecture of the proposed system: application, consensus, and network.

blockchain. Nodes verify the signature and script, ensuring the poll's legitimacy. After creating the poll, it can be started, and polling officers can perform their duties. The hash poll data is stored on the blockchain, making it tamper-proof and ensuring accurate vote counting and legitimate election results.

B. Hierarchical authoritative consensus (HAC) model

The proposed consensus model incorporates a reliable signing mechanism that guarantees the authenticity of each entity participating in the voting process. This model utilizes a Hierarchical authorization and access control to combine advantageous features from both public and private blockchains while discarding their respective limitations.Furthermore, this hybrid model acts as a deterrent against attacks. This proposed HAC-Bchain model address the credibility,verification as well as enhances security, transparency, reliability, and integrity. HAC-Bchain uses multi-level access and authorization in the consensus mechanism, with predefined access and intended purposes for each entity involved in the voting process. This prevents unauthorized actions and ensures data security.

C. Incorporating category-based sharding in blockchain

Actually, sharding divides a blockchain into subnetworks called shards, each responsible for a subset of data and it improves scalability and performance by processing transactions in parallel across shards. However, dharding can be a setback for blockchains despite its benefits, due to increased latency and reduced throughput from data cross-shard communication and query overhead. To address these challenges, this research propose a new sharding solution called category-based sharding, shown in figure 3. The proposed consensus mechanism groups voting data by election area and polling station and generate shards accordingly. This creates more data-concentrated shards, which improves scalability, performance, and availability. Category-based sharding also aids in improving data availability by ensuring data accessibility even if a node fails.

IV. IMPLEMENTATION TOOLS

This proposed system has been developed using Protocol Buffers for platform neutrality and extensibility. Cryptographically secure hash functions such as SHA256 and Blake2b, and binary encoders like Base58 are employed for generating timestamped blocks. For asymmetric cryptography, Cloudflare's CIRCL library including Ed25519 for digital signatures is utilized. A secure token-based verification system with UUIDs and zero-knowledge proofs is also implemented to prevent double-spending. The system, along with associated data, is stored in LevelDB, a fast key-value storage solution.

The GIN web framework is utilized for developing the backend. This framework provides a REST API for handling all requests and executing appropriate actions. The backend communicates seamlessly with the application layer, network layer, script processing engine, and blockchain system. Finally, a NID server has been implemented using GIN and SQLite3, providing verifiable and tamper-proof data for voters. This allows for testing the system in a real-world scenario.

V. RESULT AND PERFORMANCE EVALUATION

In the exploration of blockchain systems, this research conducted a series of experiments to gain valuable insights into their performance and implications. This experimentation was conducted in two phases: with sharding and without sharding.

Figure 4 demonstrates that sharding with five shards outperforms sharding with two or three shards. The green line in the fig 4 shows that sharding with five shards can generate 3000 blocks in 28 seconds while sharding with two shards takes 430 seconds. However, sharding with three shards takes 153 seconds.

Figure 5 is a visual representation of the highest throughput on sharding system with five different shards configuration,

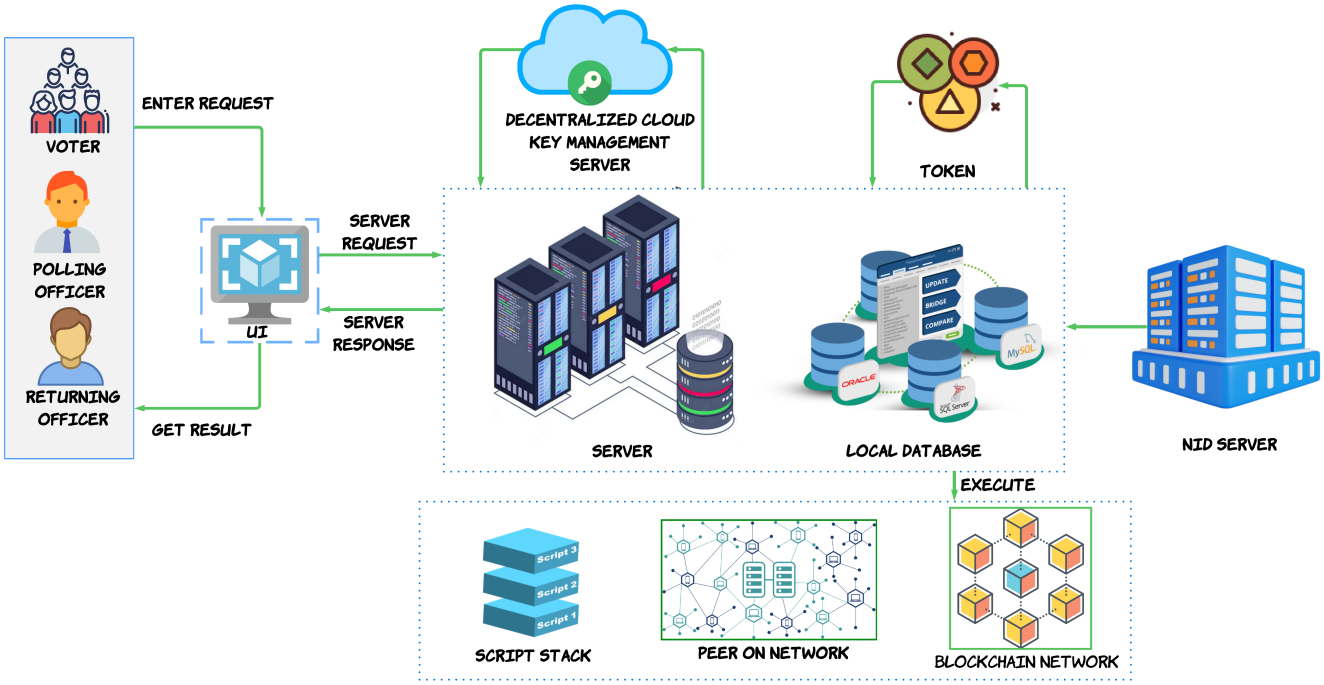

Fig. 2: The diagram shows how voters, polling officers, returning officers, and other components such as the key management server, token generation system, scripting system, NID server, and P2P network interact with the proposed election system.

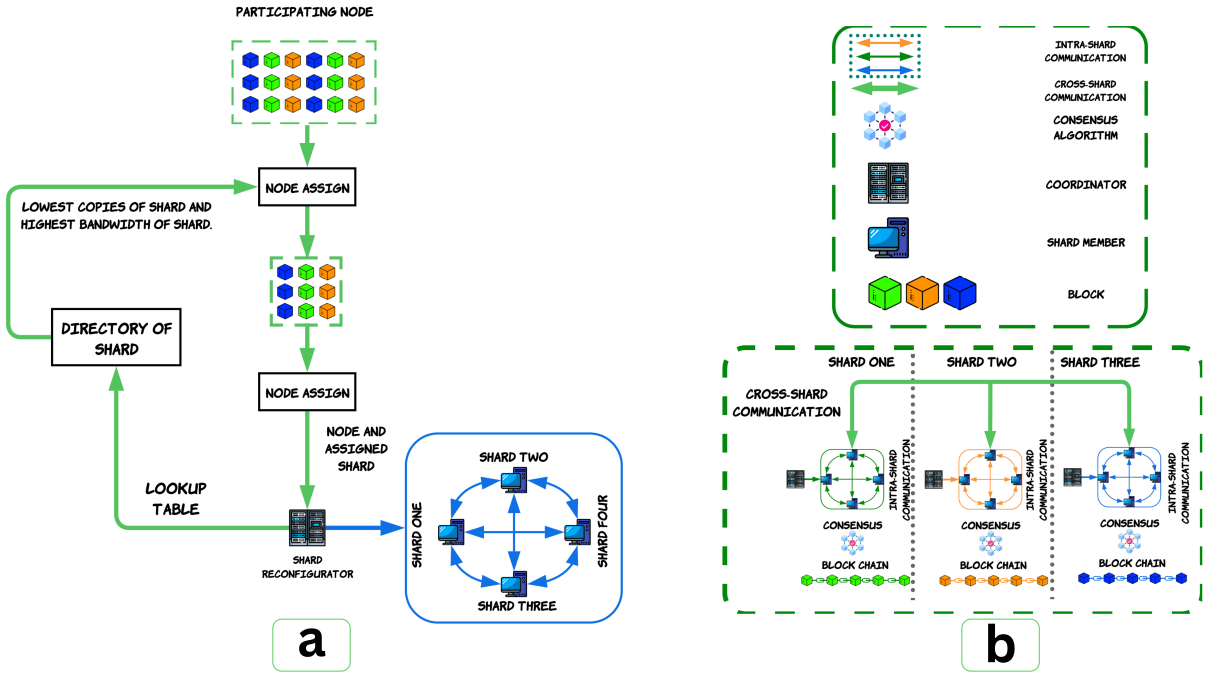

Fig. 3: This diagram represents category-based sharding in blockchain network: (a) illustrates how the coordinator manages the shards, and how the lookup table maps categories to shards. (b) illustrates how Category-based sharding divides a blockchain into categories and shards, each storing data for a specific category.

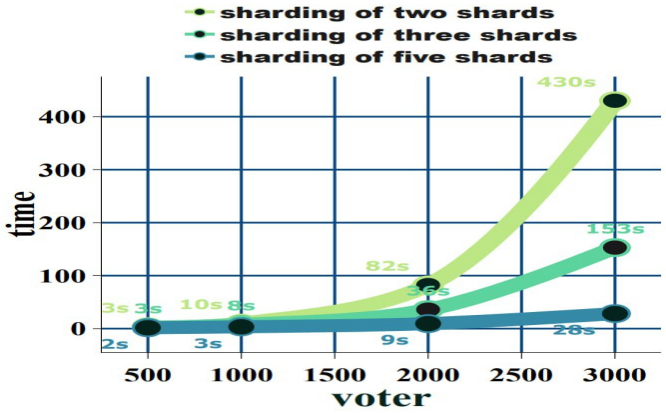

Fig. 4: This diagram represents the Block Generation Time for sharding with two, three, and five shards.

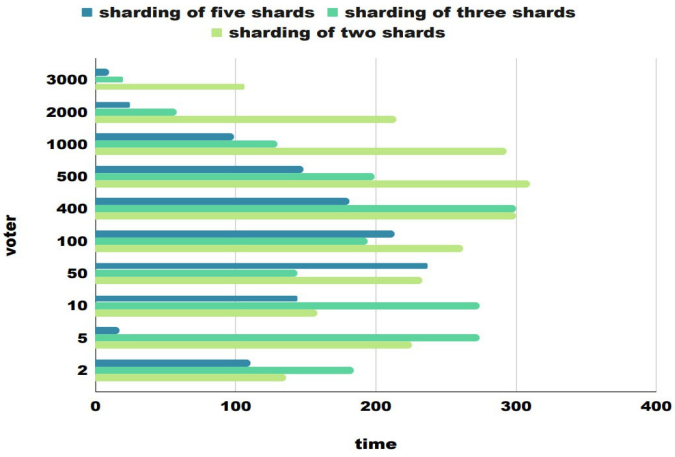

Fig. 5: This diagram shows the Throughput of the proposed system for different sharing numbers.

reaching 106 bps at 3000 voters, which is higher than some famous networks like Bitcoin and Ethereum. This is because sharding breaks data into more shards, which distributes the workload more evenly and reduces the amount of work each shard has to do.

Besides throughput, sharding significantly reduces the storage consumption in blockchain networks, especially for large numbers of blocks. This is because sharding distributes the data across multiple shards, reducing the storage requirement per block. Figure 6 illustrates that in a network with 7500 blocks, sharding can reduce storage consumption by 60%.

VI. DISCUSSION AND ANALYSIS

This section discusses about the attack analysis and security analysis. Hybrid blockchains are more secure than public blockchains because authorized personnel validate them. However, they are as accessible and transparent as public blockchains. Blockchains are not immune to attack, including insider attacks, data tampering, DNS hijacking, shard blackouts, malicious participants, and side-channel attacks.

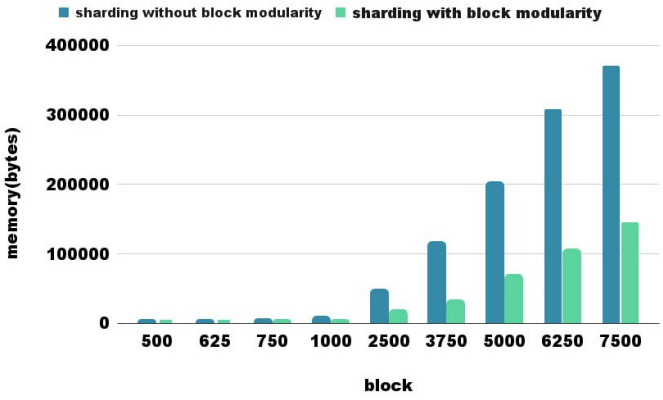

Fig. 6: The figure shows the storage required for the system with and without sharding with different numbers of blocks.

The proposed HAC-B chain, are more secure than public blockchains due to authorized validation, threshold cryptography, and decentralized KMS. The consensus model ensures security via randomness, node isolation, and secure communication. This proposed system meets key requirements such as voter eligibility, verifiability, robustness, uniqueness, ballot receipt, transparency, trustworthiness, and scalability.

This research also perform a comparative study as shown in Table I. From Table I, it is clear that the proposed system shows good performances and is comparable with the state-of-arts.

VII. CONCLUSION

With ongoing research to optimize decentralization and scalability, blockchain presents a promising approach to restoring voter confidence and overcoming vulnerabilities of current e-voting models. This could have broad implications for the future of election systems worldwide. The research demonstrates the potential of blockchain technology to enable secure, transparent, and efficient e-voting systems. This paper propose a hybrid blockchain framework that leverages the benefits of both public and private blockchains through a hierarchical authoritative consensus model. This paper also propose e-voting optimized category-based sharding. The proposed approach is 4 times faster than POS and 14 times faster than POW alternative. The experimental result confirmed, that when node size increases to only 5 nodes, the proposed HAC-Bchain model with sharding has a higher throughput (105 Tps) than PoW (5 Tps) and PoS (25 Tps).

Category-based sharding is a static data distribution approach that helps balance traffic but lacks adaptability and can lead to inefficient resource utilization. Decentralizing participation, incorporating adaptive sharding, and developing a multi-party computational token generation system could address these limitations.

TABLE I: Comparison of the proposed e-voting system with some existing works

Properties	[22]	[18]	[17]	[14]	[8]	[12]	[4]	[17]	**Proposed system**
Security	✓	✓	✓	✓	✓	✓	✓	✓	✓
Robustness	✓	✗	✗	✓	✗	✗	✗	✓	✓
Consensus	PSC	POS	QBA	POS	POW	POS	POS	POW	HAC
Throughput	60	25	25	25	7	25	7	105	
Sharding	✓	✗	✗	✗	✗	✗	✗	✗	✓
Eligibility	✓	✗	✓	✓	✗	✗	✗	✗	✓
Verifiability	✓	✓	✓	✓	✗	✓	✓	✓	✓
Uniqueness	✓	✓	✓	✓	✗	✓	✓	✓	✓
Transparency	✓	✓	✓	✓	✓	✓	✓	✓	✓
Scalability	✓	✗	✗	✗	✗	✓	✓	✗	✓
Time-based inference	✗	✗	✗	✗	✗	✗	✗	✗	✓
Confidentiality	✓	✗	✗	✓	✗	✗	✓	✓	✓

REFERENCES

[1] USAID, "Supporting free and fair elections," 2023. [Online]. Available: https://www.usaid.gov/democracy/supporting-free-and-fair-elections(Accessed:10July2023)

[2] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities," *IEEE Access*, vol. 9, pp. 34 165–34 176, 2021.

[3] R. S. Ganesh, B. Anuradha, S. Karthikeyan, P. Vijayalakshmi, M. Ashok, and V. Nagaraj, "Biometrics based smart and secured electronic voting machine," in *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*. IEEE, 2021, pp. 84–88.

[4] R. Ch, J. Kumari D, T. R. Gadekallu, and C. Iwendi, "Distributed-ledger-based blockchain technology for reliable electronic voting system with statistical analysis," *Electronics*, vol. 11, no. 20, p. 3308, 2022.

[5] M. Sallal, R. de Fréin, and A. Malik, "Pvpbc: Privacy and verifiability preserving e-voting based on permissioned blockchain," *Future Internet*, vol. 15, no. 4, p. 121, 2023.

[6] K. Varaprasada Rao and S. K. Panda, "Secure electronic voting (e-voting) system based on blockchain on various platforms," in *Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2*. Springer, 2022, pp. 143–151.

[7] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-voting meets blockchain: A survey," *IEEE Access*, vol. 11, pp. 23 293–23 308, 2023.

[8] M. Bajpai, A. Haider, A. Mishra, Y. Perwej, and N. Rastogi, "A novel vote counting system based on secure blockchain," *Int. J. Sci. Res. Sci. Eng. Technol*, pp. 69–79, 2022.

[9] S. Gopal, M. Jayaprasath, C. Poongodi, S. Johnson, D. Nanthiya, and R. Mithunkumar, "Blockchain based e-voting application–a survey," in *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. IEEE, 2023, pp. 1340–1347.

[10] I. Stančíková and I. Homoliak, "Sbvote: Scalable self-tallying blockchain-based voting," in *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, 2023, pp. 203–211.

[11] H. Kohad, S. Kumar, and A. Ambhaikar, "Scalability of blockchain based e-voting system using multiobjective genetic algorithm with sharding," in *2022 IEEE Delhi Section Conference (DELCON)*. IEEE, 2022, pp. 1–4.

[12] M. Pathak, A. Suradkar, A. Kadam, A. Ghodeswar, and P. Parde, "Blockchain based e-voting system," *International Journal of Scientific Research in Science and Technology*, vol. 8, pp. 134–40, 2021.

[13] S. K. Das, S. Saha, and S. DasGupta, "Decentralized voting: A blockchain-based voting system," in *Applications of Networks, Sensors and Autonomous Systems Analytics: Proceedings of ICANSAA 2020*. Springer, 2022, pp. 33–45.

[14] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, "Decentralized voting platform based on ethereum blockchain," in *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*. IEEE, 2018, pp. 1–6.

[15] W. Bing, L. Hui-ling, and P. Li, "Optimized dpos consensus strategy: Credit-weighted comprehensive election," *Ain Shams Engineering Journal*, vol. 14, no. 2, p. 101874, 2023.

[16] H. S. Hassan, R. Hassan, and E. K. Gbashi, "E-voting system based on ethereum blockchain technology using ganache and remix environments," *Engineering and Technology Journal*, vol. 41, no. 4, pp. 1–16, 2023.

[17] R. S. Bhadoria, A. P. Das, A. Bashar, and M. Zikria, "Implementing blockchain-based traceable certificates as sustainable technology in democratic elections," *Electronics*, vol. 11, no. 20, p. 3359, 2022.

[18] M. N. Neloy, M. A. Wahab, S. Wasif, A. All Noman, M. Rahaman, T. H. Pranto, A. B. Haque, and R. M. Rahman, "A remote and cost-optimized voting system using blockchain and smart contract," *IET Blockchain*, vol. 3, no. 1, pp. 1–17, 2023.

[19] Y. Sun, B. Yan, Y. Yao, and J. Yu, "Dt-dpos: A delegated proof of stake consensus algorithm with dynamic trust," *Procedia Computer Science*, vol. 187, pp. 371–376, 2021.

[20] Y. Liu, J. Liu, M. A. V. Salles, Z. Zhang, T. Li, B. Hu, F. Henglein, and R. Lu, "Building blocks of sharding blockchain systems: Concepts, approaches, and open problems," *Computer Science Review*, vol. 46, p. 100513, 2022.

[21] Y. Tao, B. Li, J. Jiang, H. C. Ng, C. Wang, and B. Li, "On sharding open blockchains with smart contracts," in *2020 IEEE 36th international conference on data engineering (ICDE)*. IEEE, 2020, pp. 1357–1368.

[22] 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.