Enhancing Electoral Integrity: A Hybrid Blockchain-Based E-Voting System with Deep Learning and Post-Quantum Cryptography

Sohel Ahmed Joni[1], Rabiul Rahat[1], Nishat Tasnin[1], Partho Ghose[1], and Milon Biswas[2]

[1] Bangladesh University of Business and Technology, Dhaka, Bangladesh
[2] Department of Computer Science, University of Alabama, Birmingham, USA
{sohelahmedjony,rabiulrahatt,nishattasnin02,partho.cse.jnu,milonbiswas4702}@gmail.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 (EVM) 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 proposes a hybrid blockchain-based e-voting system (PQHAC-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 the Proposed blockchain facilitates a limited set of predefined operations for each layer, helping authoritative figures manage the election securely. This research uses Deepface face recognition and facial attribute analysis framework to confirm voter identity and prevent fraudulent voting. This research proposes a token-based approach to ensure secure and transparent voter identification while simultaneously preventing instances of double voting. This proposed blockchain system includes Post-quantum cryptography to protect against attacks from quantum computers. Through the integration of these technologies, an E-voting system that is both secure and transparent has been proposed in this paper. This system provides voters with the assurance that their votes are being accurately counted while safeguarding their privacy.

Keywords: e-voting · blockchain · deep learning · deepface · post-quantum

1 Introduction

The election process plays an important role in promoting democracy and driving progress for a nation. However, conducting a just, unbiased election in a country

This version of the chapter has been accepted for publication, after peer review and is subject to Springer Nature's AM terms of use, but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record is available online at: https://doi.org/10.1007/978-981-97-3937-0_47.

with an unstable democracy presents many difficulties, particularly when there is no dependable voting system in place [1].

Paper-based voting systems are still the most common way to vote, but they are vulnerable to fraud and rigging. Biometric EVM systems have been introduced to address these security concerns, but they are not transparent enough to ensure voter confidence [2,3]. Voters cannot be sure that their votes are being counted correctly because the electronic system is closed-source.

Blockchain technology, as described by Ganesh et al.[3], is a distributed, tamper-resistant, and immutable ledger that has the potential to revolutionize the voting system [3]. Blockchain's immutability is achieved by linking each new block of data to the previous one, creating a chain of blocks that cannot be altered without the knowledge and consent of all participants in the network [4]. Additionally, blockchain's redundancy is achieved by replicating the blockchain across multiple nodes in the network, which ensures that the blockchain is always available and that even if some nodes fail, the blockchain will remain intact [5]. In many countries, current electoral systems are legally mandated to enforce specific regulations to prevent unauthorized activities and misconduct during elections. To address this need, Sallal et al. [5] have proposed an election mechanism that offers a controlled level of authority, resembling an authorized block. This allows for the inclusion or exclusion of specific entities based on the electoral system, and it ensures transparency, ballot integrity, and immutability while upholding the necessary level of regulation [5,6,7]). 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.

Block modularity divides system data into smaller, independent, and verifiable modules. When new data arrives, only the latest portion is processed, while existing verified data is referenced, eliminating duplication and redundant verification. This speeds up data processing and validation with less computational overhead. Each node only needs to process and validate the blocks that are relevant to it [9]. This reduces block size significantly.

To make e-voting systems more secure, scalable, and efficient, This research proposes a new hybrid consensus model called Hierarchical Authoritative Consensus (HAC) that combines blockchain and sharding. This research uses a category-based sharding approach, which means that the blockchain is divided into shards based on the type of data stored.

Post-quantum cryptography is needed in blockchain because current blockchain protocols and networks use non-quantum-resistant cryptographic algorithms. When quantum computers become powerful enough to run Shor's algorithm on a large scale, they will be able to break these algorithms within a short period of time. This would put the security of blockchain networks and the assets they store at risk.[10]

DeepFace, a lightweight face recognition and facial attribute analysis framework, uses deep learning techniques to recognize and authenticate individuals based on their facial features [11]. This technology has been widely used in various applications, including security systems, biometric authentication, video surveillance, and social media.

One of the challenges of electronic voting systems is preventing fraudulent voting. Deep-face verification systems, offer a promising solution to this challenge. Deep Face is a deep learning-based facial recognition system that uses a convolutional neural network architecture to identify faces in digital images with high accuracy [12,13].

The research contributions can be summarized as follows:

1. This research proposes a hybrid consensus model that merges the strengths of public and private consensus models to improve security, efficiency, transparency, and trustworthiness in voting systems.
2. The research includes a comprehensive performance analysis of Dilithium2 and Dilithium3-based implementations with Ed25519-based blockchains to check whether post-quantum asymmetric cryptography can be a viable alternative to its traditional counterpart.
3. A novel multi-party computation (MPC) protocol has been proposed to generate a secure and verifiable token for each voter that solves coerced and double voting while protecting their identity.
4. Finally, This research conducted a performance analysis similar to real-world election data, and the results are promising. The proposed system can potentially handle large-scale elections without sacrificing security or performance.

The rest of the paper discusses the proposed blockchain-based e-voting system in detail. Section 2 reviews recent research on this topic, while Section 3 provides an overview of the proposed system. Section 4 describes the system's implementation, and Section 5 presents the results of a performance evaluation. Section 6 discusses the system and its implications, and Section 7 concludes the paper.

2 RELATED WORK

In this section, This research examines some recent research on blockchain-based e-voting systems.

Past attempts to Develop blockchain-based e-voting systems relied on cryptocurrency incentive schemes. Inspired by recent advances, [14,15,16]. These systems have focused on improving the security of e-voting systems, but they often neglect performance and scalability [14,15]. For example, Pathak et al. [14,16] proposed a method based on a predetermined turn-on time for each node in the blockchain, and Das et al. [15] proposed a blockchain-based voting system integrated with a face recognition module. While these methods are secure, they can be computationally expensive and difficult to scale to large-scale elections.

Many researchers have proposed e-voting systems based on the Ethereum blockchain. While Ethereum-based systems can be secure, they can also be centralized and expensive, due to the high gas fees associated with Ethereum transactions. Additionally, using two consensus mechanisms, as proposed by Neloy et al. [17], can add computational complexity and increase gas fees.

Other researchers have proposed new consensus mechanisms to improve the performance and scalability of blockchain-based e-voting systems [18,19,20]. For example, Li et al. [18] proposed a Proof of Vote (PoV) consensus algorithm. Several researchers have proposed post-quantum cryptography (PQC) schemes to protect blockchains from quantum attacks. For example, Li et al. [21] proposed a new lattice-based signature scheme that is resistant to Shor's and Grover's algorithms Allende et al. [10] proposed a layer-two solution that uses post-quantum keys to secure information exchange between blockchain nodes [10]

In summary, previous research on blockchain-based e-voting systems has focused on security, with less attention paid to performance and scalability. This research work aims to address this gap by proposing a new hybrid consensus model that combines the benefits of blockchain and sharding.

To address the limitations of previous e-voting systems, this research proposes a new consensus model called the Post-Quantum Hierarchical Authoritative Consensus Model (PQHAC). PQHAC combines the advantages of public and private blockchains while mitigating their limitations. This new mode is designed to be secure even against quantum computers and can be used to create a secure, transparent, and scalable e-voting system. This system could help to eliminate doubts about the outcome of elections and ensure that the voting process is fair and accurate.

3 Proposed Method

This proposed voting system addresses the key aspects of a secure and fair voting system. This system is decentralized, secure, cost-effective, environmentally sustainable, 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 later subsections, this research discusses the proposed system components in detail.

3.1 System Design

The main voting system is connected to a backend server that controls most blockchain and e-voting activity. The server stores a copy of the blockchain or its shards in a LevelDB database. The system is written in Go and based on the Gin web framework.

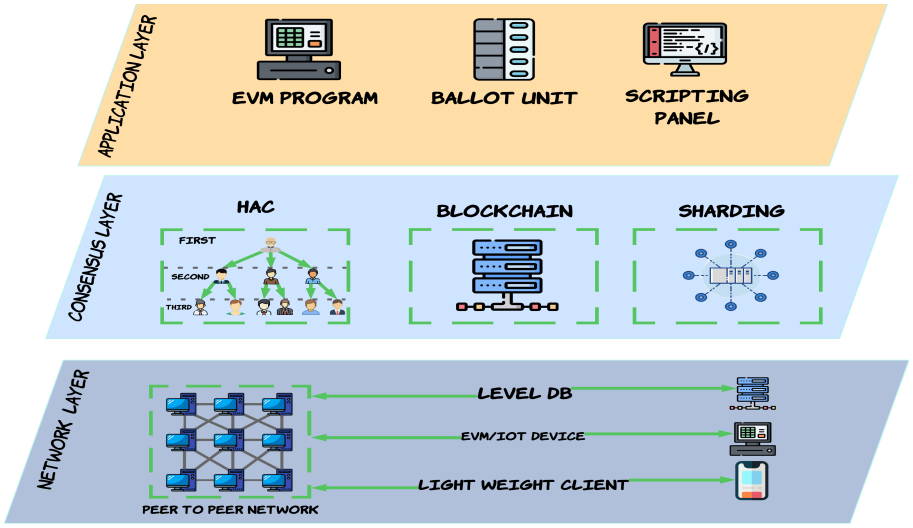

Fig. 1. shows the three-layer node architecture of the proposed system: application, consensus, and network.

System: The system manages communication with the peer-to-peer network, stores and serves the blockchain from a local database, and executes various operations on blockchain data, including script execution. Figure 2 shows The External entities such as the MPC Token generation, decentralized KMS server, and the NID servers to provide tokens, keys, signatures, and voter information to assist the election process. Users, such as voters, returning officers, and polling officers, access the system through a user interface.

The proposed e-voting system leverages external services like NID servers and a KMS for secure, transparent, and reliable voting. Key participants include the election commission, voters, and officials, each with dedicated UI panels and permissions. The system initializes by retrieving data and creating a genesis block, followed by election creation where personnel sign poll data and publish it on the blockchain. Once created, the poll can be started and officials can manage it. All poll data is stored on the blockchain for tamper-proof vote counting and legitimate results.

3.2 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, the proposed hybrid model acts as a deterrent against attacks.

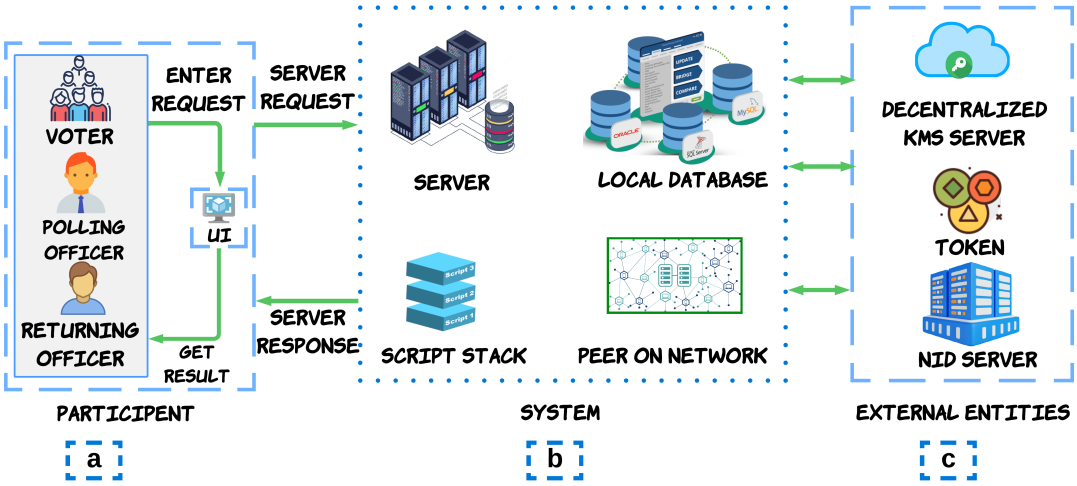

Fig. 2. The diagram shows how voters, polling officers, returning officers, and other components such as the key management server, token generation system, scripting system, NID server, and P2P network interact with the proposed election system.

The proposed PQHAC-Bchain model addresses credibility, and verification as well as enhances security, transparency, reliability, and integrity. PQHAC-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.

3.3 Incorporating post-quantum security

The proposed blockchain model relies heavily on public-key cryptography, digital certificates, and hash functions to provide transparency and secure authorization [22]. Although public-key cryptography is still secure today, quantum computing is progressing rapidly, and there is a possibility that it could be used to perform attacks based on Grover's and Shor's algorithms in the near future [23]. These algorithms could pose a threat to both public-key cryptography and hash functions, which means that blockchains would need to be redesigned to use cryptographic systems that are resistant to quantum attacks. To address this threat, in this research have implemented and tested a post-quantum asymmetric encryption algorithm called Dilithium in Proposed blockchain [24]. Dilithium is one of the algorithms that has been selected by the National Institute of Standards and Technology (NIST) for post-quantum proof standardization [23]. This research tested two versions of Dilithium in the Proposed implementation: Dilithium2 and Dilithium3. Dilithium3 is a more secure algorithm than Dilithium2, but Dilithium2 signs faster and produces smaller public keys and signatures [25]. The face recognition feature in the system adds an extra layer of

security by verifying users before they can access their respective systems. The system uses DeepFace, a face recognition and facial attribute analysis library for Python, OpenCV, and TensorFlow.

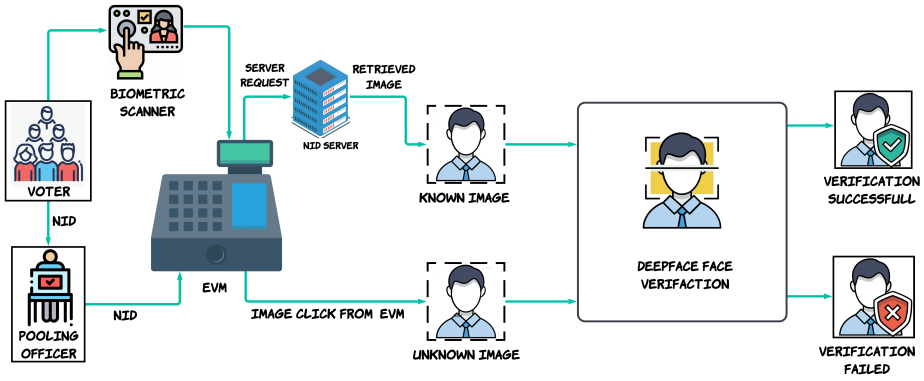

Fig. 3. The overview of the biometric face verification system is represented in figure 3. From the figure, this research can see how the system scans the voters' faces in front of the EVM unit. DeepFace, a facial recognition and facial attribute analysis deep learning model has been employed to compare the image of the voter with the database image to ensure voter integrity.

After rigorous testing, the authors determined that a threshold of approximately 0.10 provides optimal performance for face recognition and facial attribute analysis. The accompanying Figure3 shows how to use face recognition with the DeepFace package. KnownIMG is the known image obtained from the system database, and UnknownIMG is the image clicked through the system. "R" is the details of the face match records between two different images, and "d" is the distance of difference.

4 IMPLEMENTATION

The proposed system is built for platform neutrality and extensibility using Protocol Buffers. Secure cryptographic algorithms like SHA256, Blake2b, and Ed25519 are used to generate tamper-proof timestamps and signatures. Additionally, a token-based verification system with UUIDs and zero-knowledge proofs prevents double-spending. Data is stored in LevelDB, a fast key-value database. The backend utilizes the GIN web framework for API management and interacts seamlessly with the application, network, script processing, and blockchain layers. A NID server implemented with GIN and SQLite3 allows for testing in real-world scenarios.

The face recognition feature is an extra layer of security used to verify users before they can access the system, as shown in Figure 4. The system uses the

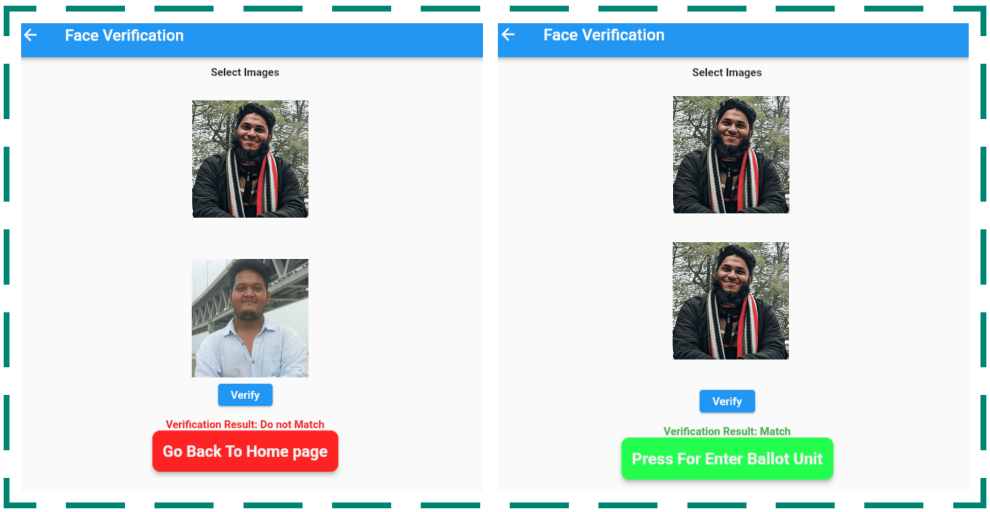

Fig. 4. This figure shows how DeepFace and Flutter have been used to create a face verification system. The system compares two images of faces to see if they match. If the faces match, the system authenticates the user. If the faces don't match, the system denies access.

Deep Face library for Python, OpenCV, and TensorFlow. After extensive testing, This research found that 0.10 is the optimal threshold for face recognition and facial attribute analysis.

In simpler terms, the face recognition feature uses Deep Face to compare a known image of a user to a new image of the user to verify their identity. The algorithm works by calculating the distance between the two images. If the distance is below a certain threshold (0.10 in this case), the user is verified.

5 RESULT AND PERFORMANCE EVALUATION

This research conducted a series of experiments to explore the performance and implications of post-quantum block modularity in blockchain systems. This research compared the performance of Dilithium-2 and Dilithium-3, with and without block modularity, in terms of block generation time and throughput. The research data and results show that Dilithium-3 with block modularity outperforms Dilithium-2 with block modularity in both block generation time and throughput, shown in graph 5 and 6. Similarly, Dilithium-3 without block modularity outperforms Dilithium-2 without block modularity in both block generation time and throughput.

In general, Dilithium-3 offers better performance and throughput than Dilithium-2. This is because Dilithium-3 uses a smaller number of larger polynomials, which can be more efficiently processed by hardware and software.

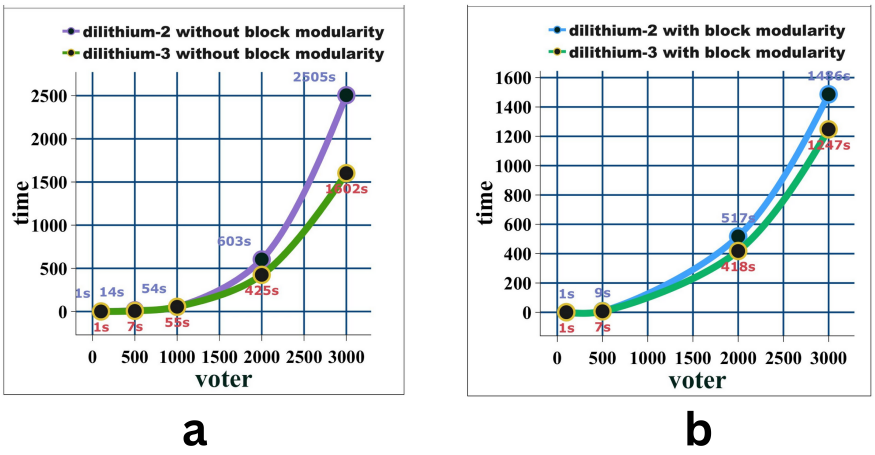

Fig. 5. The line graph compares the block generation time of Dilithium-2 and Dilithium-3 in terms of block modularity and without block modularity. The left side of the line graph, labeled "a", represents the block generation time of Dilithium-2 and Dilithium-3 without block modularity. The right side of the line graph, labeled "b", represents the block generation time of Dilithium-2 and Dilithium-3 with block modularity. The x-axis of the graph represents the number of voters, and the y-axis represents the block generation time. The line graph shows that Dilithium-3 outperforms Dilithium-2 in terms of block generation time, both without and with block modularity.

6 DISCUSSION AND ANALYSIS

In this section, this research discusses the attack analysis and security analysis.

This PQHAC-Bchain is more secure than public blockchains because this research uses authorized validation, threshold cryptography, decentralized key management systems (KMS), and post-quantum cryptography. The consensus model ensures security via randomness, node isolation, and secure communication. While mitigating previous attack vectors, post-quantum hybrid blockchains meet key requirements such as voter eligibility, verifiability, robustness, uniqueness, ballot receipt, transparency, trustworthiness, and scalability.

Post-quantum cryptography is a type of cryptography that is resistant to attacks from quantum computers. Quantum computers are very powerful computers that could potentially break many of the encryption algorithms that are used today. Post-quantum cryptography is designed to be secure even against quantum computers.

By using post-quantum cryptography, hybrid blockchains can be protected from attacks from quantum computers. This is important because quantum computers are becoming more powerful and could pose a serious threat to blockchain security in the future

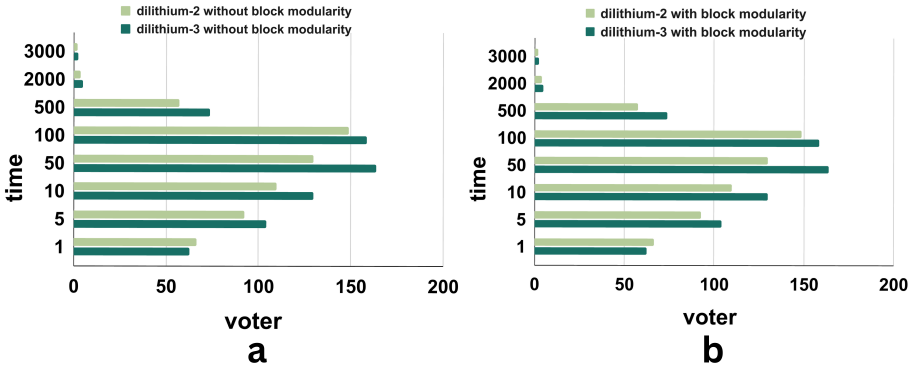

Fig. 6. The bar graph compares the throughput of Dilithium-2 and Dilithium-3 in terms of block modularity and without block modularity. The left side of the bar graph, labeled "a", represents the throughput of Dilithium-2 and Dilithium-3 without block modularity. The right side of the bar graph, labeled "b", represents the throughput of Dilithium-2 and Dilithium-3 with block modularity. As shown in the bar graph, Dilithium-3 outperforms Dilithium-2 in terms of throughput, both without and with block modularity.

This research also performs a comparative study as shown in Table 1. From Table 1, This system has clearly demonstrated an impressive performance and can be favorably compared with the best models out there.

7 CONCLUSION

Blockchain technology has the potential to revolutionize e-voting systems by making them more secure, transparent, and efficient. However, existing blockchain-based e-voting systems face challenges in terms of scalability and decentralization. This paper proposes a hybrid blockchain framework that leverages the benefits of both public and private blockchains to address these challenges. The proposed framework uses a hierarchical authoritative consensus model to ensure decentralization and security, while also using DeepFace and post-quantum cryptography to provide additional security against facial recognition attacks and quantum computing attacks. The experimental results show that the proposed framework is significantly faster than existing blockchain-based e-voting systems, with a throughput of 105 transactions per second (TPS) when the number of nodes is increased to only 5. This is 4 times faster than proof-of-stake (PoS) and 14 times faster than proof-of-work (PoW) blockchains. While the proposed framework is already significantly faster than existing blockchain-based e-voting systems, it can be further scaled by using sharding. Sharding is a technique that divides the blockchain into smaller partitions, each of which is processed by a different node. This allows the blockchain to process more transactions in parallel, which improves scalability.

Table 1. Contrasting This proposed e-voting system with some existing works

Properties	**[26]**	**[17]**	**[27]**	**[16]**	**[8]**	**[14]**	**[4]**	**[28]**	**The proposed**
Security	✓	✓	✓	✓	✓	✓	✓	✓	✓
Robustness	✓	X	X	✓	X	X	X	✓	✓
Consensus	PSC POS	QBA POS	POW POS	POS POW					HAC
Throughput	60	25	-	25	7	25	25	7	105
Eligibility	✓	X	✓	✓	X	X	X	X	✓
Verifiability	✓	✓	✓	✓	X	✓	✓	✓	✓
Uniqueness	✓	✓	✓	✓	X	✓	✓	✓	✓
Transparency	✓	✓	✓	✓	✓	✓	✓	✓	✓
Post Quantum	X	X	✓	X	X	X	X	X	✓
Deepface	✓	✓	X	X	X	X	X	X	✓
Time-based inference	X	X	X	X	X	X	X	X	✓
Confidentiality	✓	X	X	✓	X	X	✓	✓	✓

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. M. Allende, D. L. León, S. Cerón, A. Pareja, E. Pacheco, A. Leal, M. Da Silva, A. Pardo, D. Jones, D. J. Worrall *et al.*, "Quantum-resistance in blockchain networks," *Scientific Reports*, vol. 13, no. 1, p. 5664, 2023.
11. S. I. Serengil and A. Ozpinar, "Lightface: A hybrid deep face recognition framework," in *2020 Innovations in Intelligent Systems and Applications Conference (ASYU)*. IEEE, 2020, pp. 23–27. [Online]. Available: https://doi.org/10.1109/ASYU50717.2020.9259802
12. F. Z. Chentouf and S. Bouchkaren, "Security and privacy in smart city: a secure e-voting system based on blockchain," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, p. 1848, 2023.
13. Y. A. F. Ali, O. T. M. Ahmed, M. A. M. Diab, M. A. E. Sayed, M. K. Abd Elaziz, and B. W. Aboshosha, "Blockchain-based online e-voting system," in *2023 International Conference on Smart Computing and Application (ICSCA)*. IEEE, 2023, pp. 1–8.
14. 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.
15. 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.
16. 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.
17. 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.
18. K. Li, H. Li, H. Wang, H. An, P. Lu, P. Yi, and F. Zhu, "Pov: an efficient voting-based consensus algorithm for consortium blockchains," *Frontiers in Blockchain*, vol. 3, p. 11, 2020.
19. J. Wang, H. Chenchen, Y. Xiaofeng, R. Yongjun, and S. Sherratt, "Distributed secure storage scheme based on sharding blockchain," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 4485–4502, 2022.
20. 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.
21. C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2018.
22. G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta *et al.*, "Status report on the third round of the nist post-quantum cryptography standardization process," *US Department of Commerce, NIST*, 2022.
23. G. L. Series, "The national institute of standards and technology (nist)," 2010.
24. L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 238–268, 2018.
25. D. O. Greconici, M. J. Kannwischer, and A. Sprenkels, "Compact dilithium implementations on cortex-m3 and cortex-m4," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 1–24, 2021.

26. 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.
27. X. Sun, Q. Wang, P. Kulicki, and M. Sopek, "A simple voting protocol on quantum blockchain," *International Journal of Theoretical Physics*, vol. 58, pp. 275–281, 2019.
28. 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.