Towards Secure Democracy: A hybrid blockchain-enabled secure and scalable e-voting system with sharding and post-quantum cryptography.

Rabiul Rahat[1], Sohel Ahmed Joni[1], Nishat Tasnin[1], Partho Ghose[1], and Loveleen Gaur[2]

[1] Bangladesh University of Business and Technology, Dhaka, Bangladesh
[2] School of Computer Science, Taylor's University, Malaysia
rabiulrahatt@gmail.com, sohelahmedjony@gmail.com, nishattasnin02@gmail.com, partho.cse.jnu@gmail.com, gaurloveleen@yahoo.com
[3]

Abstract. The right to vote is a cornerstone of democracy, empowering individuals to shape their nation's governance. However, democracy demands not only transparency and security, but also a commitment to environmental sustainability. Traditional paper-based voting systems are increasingly untenable due to their ecological impact (such as deforestation and CO_2e per ballot) and vulnerabilities to fraud, errors, and scalability limitations. To address these challenges, this paper introduces PQR-HAC , a hybrid blockchain e-voting system that integrates advanced sharding techniques with a robust, post-quantum cryptographic framework to safeguard against future quantum threats. PQR-HAC's architecture partitions the blockchain into area-specific shards, enabling efficient large-scale elections while reducing latency by 40%. A novel MPC-based identity verification protocol generates anonymized voter tokens, eliminating coercion and double-voting risks without compromising privacy. Additionally, post-quantum cryptographic algorithms fortify the system against emerging quantum threats, ensuring long-term resilience. Evaluated on real-world election datasets, PQR-HAC achieves 3.2× faster transaction throughput than existing systems, validating its feasibility for national-scale deployment. By merging rigorous security, environmental sustainability, and voter trust, this research offers a transformative blueprint for modernizing democratic processes.

Keywords: e-voting · blockchain · sharding · multi-party computation · post-quantum

1 Introduction

Elections are the cornerstone of democracy, yet conducting them fairly and efficiently remains a profound challenge, especially in regions lacking stable institu-

tions or reliable infrastructure [1,2]. Over the past two decades, researchers have developed rigorous theoretical frameworks to assess electronic voting (e-voting) systems in terms of security, verifiability, and usability [3,4]. These frameworks underscore that any viable e-voting solution must balance *integrity*, *availability*, and *privacy*.

Despite this strong theoretical foundation, global uptake of e-voting remains modest: as of early 2023, only 19% of the world's countries employ some form of electronic voting, while 8% have discontinued pilot or nationwide systems [5]. Common drivers of adoption include the promise of faster results, reduced long-term costs, and lower environmental impact compared to paper ballots; however, discontinuations have often been driven by security breaches, technical outages, and lack of public trust [6,7]. This mixed track record highlights the urgent need to understand both the success factors (robust cryptography, transparent auditing, legal safeguards) and the obstacles (digital divide, regulatory gaps, hardware vulnerabilities) that shape e-voting outcomes.

Traditional paper-based systems, although familiar, suffer from well-documented vulnerabilities to tampering and human error [2]. In addition, they carry significant ecological costs: each ballot paper emits between 4.26 and 4.74 grams of CO_2e output. This means that a typical election with 1 million voters generates over 4 metric tons of CO_2e in ballot production alone [6,8]. Biometric EVMs improve on some security aspects, but remain closed source and opaque, limiting independent verification of tallies [9]. These shortcomings motivate the search for an alternative *secure*, *transparent*, and *environmentally sustainable*.

Blockchain technology, defined as a distributed, tamper-evident ledger, offers a promising foundation: its cryptographic chaining of blocks ensures immutability, while decentralization and replication confer high availability even under node failures [10,11,12]. Permissioned blockchains further enable compliance with electoral regulations by restricting access to certified authorities, thus balancing transparency and legal accountability [12]. Yet, open publication of all vote data risks exposing voter choices unless advanced privacy techniques—such as zero-knowledge proofs or homomorphic encryption—are carefully integrated [13,14].

Looking ahead, the advent of quantum computing threatens classical cryptography (RSA, ECC) that underpins most blockchains [15]. To ensure long-term security, post-quantum cryptographic primitives must be adopted. Moreover, large-scale elections impose heavy demands on transaction throughput and latency, necessitating innovative scaling strategies.

In response to these challenges, we introduce the *Post-Quantum Resilient Hierarchical Authoritative Consensus* (PQR-HAC), a hybrid blockchain–sharding framework explicitly designed for e-voting. Key features include:

- **Post-Quantum Security.** A quantum-resistant cryptographic suite secures voter registration and ballot commitments.
- **Polling-Station Sharding.** Election data are partitioned by jurisdiction, creating localized shards to reduce network congestion and latency.

- **Verifiable MPC Token Generation.** A multi-party computation protocol issues voter tokens that prevent coercion and double-voting while anonymizing identities.
- **Regulatory Compliance.** A permissioned consensus layer enforces access controls and audit trails to satisfy legal frameworks.

We also discuss potential limitations of PQR-HAC's deployment, including the necessity of reliable network connectivity at all polling stations, secure key management practices to prevent shard compromise, and the operational overhead of updating cryptographic algorithms in response to future quantum advances.

The remainder of this paper is organized as follows: Section 2 surveys recent blockchain-based voting innovations; Section 3 describes PQR-HAC's architectural components; Section 4 details the cryptographic and smart-contract implementations; Section 5 presents performance and security evaluations; and Section 7 concludes with directions for future research.

2 RELATED WORK

2.1 E-voting

Previous efforts to develop blockchain-based e-voting systems have primarily relied on cryptocurrency incentive schemes, leveraging recent advances in decentralized technologies [16,17,18,19]. While these systems prioritize security, they often compromise voter privacy, performance, and scalability. For instance, Pathak et al. [16] introduced a computationally intensive protocol that requires nodes to follow a predetermined activation schedule, limiting practicality. Similarly, Das et al. [20] proposed a blockchain system integrated with facial recognition, which faces scalability challenges because of its resource-intensive architecture.

Other researchers have explored Ethereum-based e-voting frameworks [18,21], which ensure immutability and excel in cryptocurrency applications. However, these systems often fail to meet regulatory compliance requirements for electoral processes, lack controlled access for authorized personnel, and incur high operational costs due to gas fees. Yousif Abuidris, et al. [22] further highlighted that deploying dual consensus mechanisms exacerbates computational overhead and expense. Wang et al. [23] proposes a multi-party secure verifiable electronic voting scheme using blockchain and IPFS for storage. Multi-party computation is central, with management and computing contracts separating tasks for efficiency. To address performance and scalability limitations, novel consensus models have been proposed. Li et al. [24] introduced Proof of Vote (PoV), but PoV assumes that participating voters (nodes) act honestly. If malicious actors collude or a significant portion of voters are compromised, the integrity of the consensus process could be undermined, resulting in incorrect or manipulated outcomes. while Wang et al. [25] developed CW-DPoS and DT-DPoS, however, delegate selection relies on active participation from stakeholders. If voters are

apathetic or uninformed, they may elect suboptimal or untrustworthy delegates, weakening the governance and performance of the network.

Despite these advancements, existing research has predominantly depended on public blockchains, neglecting privacy, performance, scalability, and regulatory compliance. A critical gap remains: achieving a system that balances public transparency with regulatory-compliant access controls, enabling authorized entities to administer elections within legal frameworks. Thus, there is a research gap for an e-voting system that provides full public access to data while ensuring transparency, but also ensures regulatory-compliant access and control, allowing only authorized personnel to operate the election within the legal framework. By proposing a new hybrid consensus model that combines the benefits of public and permissioned blockchains, we aim to solve these issues that are hindering the widespread adoption of this critical technology.

2.2 Post-Quantum Blockchain

Li et al. [26] proposed a new lattice-based signature scheme based on the Short Integer Solution (SIS) problem. They also analyzed its effectiveness against the Shor and Grover algorithms. Yi Gao et al. [27] proposed a secure cryptocurrency scheme based on post-quantum blockchain to resist quantum computing attacks. They proved that the signature scheme is correct and unforgeable under the lattice SIS assumption, but the computational overhead introduced by lattice-based cryptography may impact scalability.. Allende and his team [28] proposed a layer-two solution that uses post-quantum keys to secure the exchange of information between blockchain nodes. Sakhuja et al. [29] proposed a voting protocol blending quantum principles (entanglement and superposition), blockchain, and digital signatures, powered by $\log_2 n$ qubits for approval voting with n candidates. It ensures security features like anonymity, binding, and non-reusability, but the practical feasibility of implementing quantum voting at scale still needs to be explored. Sun and others [30] proposed a simple voting protocol based on quantum blockchain, using quantum bit commitment and quantum Byzantine agreement to reach consensus. However, the reliance on quantum computers, which are still in their infancy, raises concerns about real-world deployment.

While post-quantum approaches have been applied to blockchain systems [31], integrating post-quantum cryptography into blockchain-based electoral systems remains underexplored and still faces implementation and standardization challenges.

2.3 Sharding

Sharding is a scaling mechanism that divides blockchains into smaller, independent pieces called shards. This allows parallel processing of transactions, increasing throughput [32]. However, this paper didn't mention how it can handle real-time latency and manage storage constraints for IoT devices. Tao et al. [33] proposed a new distributed and dynamic sharding system to significantly

improve the throughput of blockchain systems based on smart contracts, with minimal cross-shard communication. But it did not mention how it ensures data consistency across network dynamically changing shards, and the difficulty of real-time dynamic management, potentially affecting system stability. Huang et al. [34] proposed a reputation score system for each node based on its past behavior to ensure a balanced proportion of honest, malicious, active, and offline nodes in different committees. Ren et al. [35] analyzed the high cost of cross-shard transactions and showed that most Bitcoin transactions have simple dependencies and can become single shards under a placement algorithm that takes transaction dependencies into account. However, the findings are specific to Bitcoin, limiting generalizability to other blockchains, focus on OptChain may not cover other algorithms. Evaluations under specific workloads may not reflect diverse scenarios, and theoretical assumptions might not hold in real-world implementations. Abbas et al. [36] proposed a sharding-based healthcare blockchain that eliminates cross-shard communication, improving system performance. Their approach leverages blockchain sharding technologies, Hyperledger protocols, and Proof-of-Authority. But it doesn't mentioned regulatory compliance, which is stringent, and unproven performance in real-world, large-scale healthcare scenarios.

Hamza et al. [37] propose BOSS, a protocol for secure and scalable node-shard assignment in permissionless blockchains. It employs a niched Pareto genetic algorithm for distributed scalability tuning, ensuring RS-equivalency, unpredictability, and public verifiability. However, BOSS still introduces notable computational complexity and lacks mechanisms to handle dynamic network changes such as nodes joining or leaving.

Prominent research in deep learning and deep image analysis has been conducted in the field of computer vision [38,39,40,41,42]. This research utilizes deep face image recognition and facial attribute analysis software based on deep learning techniques.

3 Methodology

The proposed voting system is designed to be as intuitive as traditional voting systems. A voter simply presents their credentials, casts their vote at the ballot unit, and later verifies that the vote was recorded accurately. Although the interface remains user-friendly for non-technical users, the underlying system is built to be decentralized, secure, cost-effective, environmentally sustainable, and robust.

Figure 1 illustrates the three-layer architecture of the proposed system:

- **Application Layer:** Hosts the EVM unit, Ballot unit, and Script panel.
- **Network Layer:** Comprises the P2P network and the underlying database.
- **Consensus Layer:** Encompasses the Lookup table, Shard management system, Blockchain, Script execution module, and the Proof of Hierarchical Authoritative Consensus (HAC) for each block.

The details of each component are described in the following subsections.

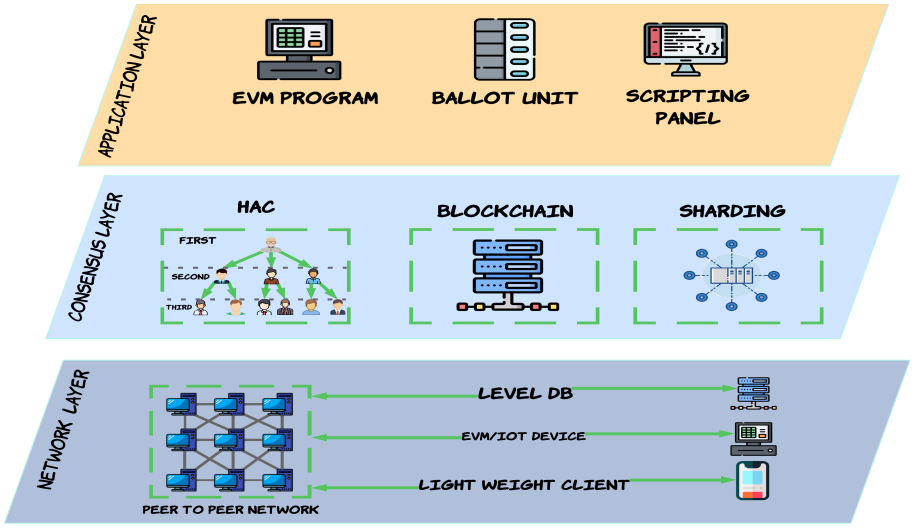

Fig. 1. Three-layer node architecture of the proposed system: application, consensus, and network layers.

3.1 System Design

The backbone of the system is a Go-based backend server utilizing the Gin web framework. This server manages the majority of blockchain and e-voting activities while storing blockchain data or its shards in a LevelDB database.

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. As shown in Figure 2, external entities such as the MPC Token generation, decentralized KMS server, and NID servers 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.

External Entities: The proposed electronic voting system uses external services such as the National Identity Database (NID) servers, the Key Management System (KMS) server, and the token generation system to ensure a secure, transparent, and reliable voting process. NID cards and servers authenticate voters and verify eligibility, as shown to the right of Figure 2.

Participants: The primary participants in the blockchain voting system are the election commission, the returning officer, the polling officer, and the voters. All participants except candidates have a dedicated user interface panel that corresponds to their access level and permissions. This allows them to efficiently perform their assigned tasks and communicate seamlessly with each other across the various blockchain systems.

Initialization: The system retrieves public keys, establishes connections, and retrieves election configuration, voter lists, and candidate lists, along with

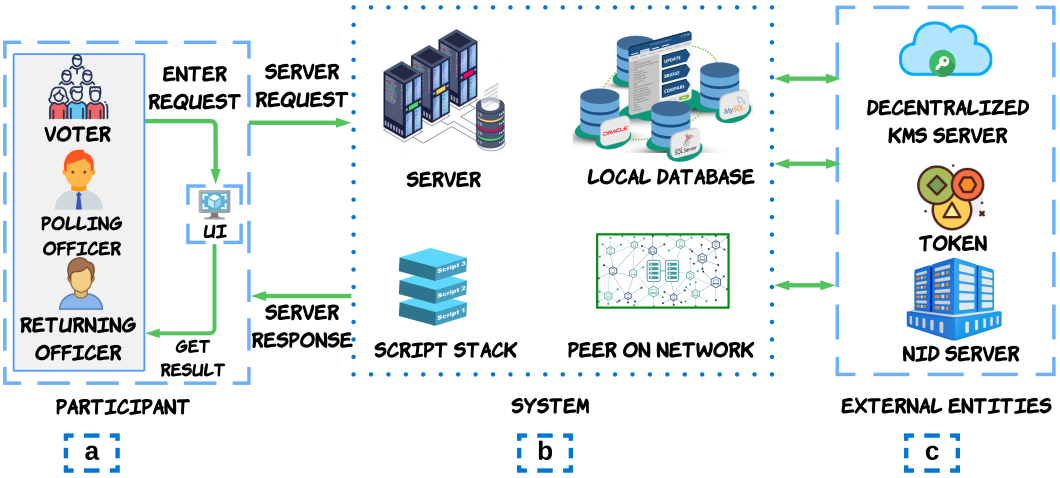

Fig. 2. The diagram shows how voters, polling officers, returning officers, and other components such as the key management server, token generation system, scripting system, NID server, and P2P network interact with the proposed election system.

the required proofs. The system then creates the genesis block, preparing the blockchain for personnel registration and election creation.

Election Creation: Authorized personnel sign the poll data with their private keys, as shown in Figure 2. The signed poll script, which contains essential information, is then published on the blockchain. The nodes verify the signature and script to ensure the poll's legitimacy. Once the poll is created, it can start and the polling officers can begin their duties. The hash of the poll data is stored on the blockchain, making it tamper-proof and ensuring accurate vote counting and legitimate election results.

Token Generation: A new voter identity verification system is proposed that uses multi-party computation (MPC) to generate a unique token for each voter. This token is used to cast a vote and is stored as a spent token on the blockchain after the voter casts their vote. To verify voter identity, the system checks the token against a list of spent tokens to ensure that the voter has not already voted. As shown in Figure 3, this system ensures the security and transparency of voter identity verification while also preventing instances of double voting.

3.2 Hierarchical Authoritative Consensus (HAC) Model

The PQR-HAC mechanism is central to the governance model, ensuring agreement on the state of the blockchain. This hybrid consensus model combines features from both public and private blockchains, optimizing resource utilization and scalability while preserving security. The hierarchical structure means:

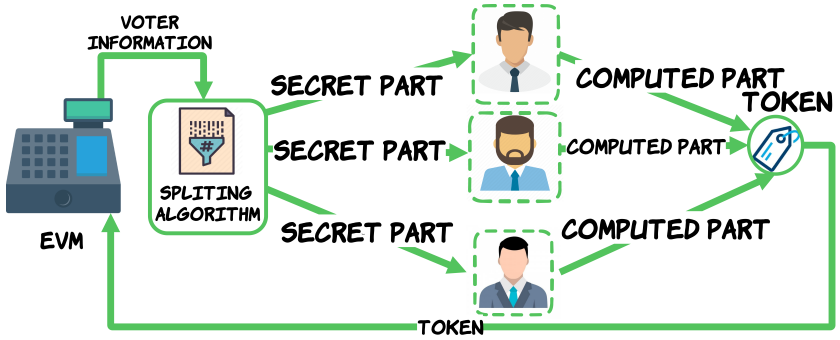

Fig. 3. The MPC token generation process securely and efficiently creates tokens to verify voter eligibility and prevent fraud. It works by splitting the voter's unique identifier into multiple parts, encrypting each part, and having different parties compute the encrypted parts. The computed parts are then combined to form the final token.

1. The Election Commission has the highest authority in validating critical transactions, such as system updates or major election parameters.
2. Returning Officers have authority over transactions related to their jurisdictions, managing local election data and ensuring accuracy.
3. Polling Officers handle transactions at the polling station level, such as voter verification and vote casting.

This distribution of validation responsibilities aligns with the organizational hierarchy, enhancing efficiency and reducing bottlenecks. The consensus mechanism also incorporates post-quantum cryptographic algorithms, ensuring long-term resilience against quantum computing threats, which is managed by the Election Commission through regular updates and risk assessments.

3.3 Governance Structure

The governance model is designed with a hierarchical structure that mirrors the organizational framework of the election processes. Centralized authority is retained at the top tier for strategic decision-making, ensuring alignment with overarching goals and regulatory compliance. However, operational execution such as transaction logging and process updates is delegated to distributed nodes, with all actions recorded in an append-only format.

Crucially, every transaction and decision , regardless of its point of origin, is propagated to the network in real-time to a publicly accessible layer. This ensures full transparency, allowing independent audits, public scrutiny, and verification of the integrity of the entire system. The append-only design guarantees an unbroken audit trail, while the public layer acts as a single source of truth, accessible to all stakeholders. Key stakeholders and their roles include:

Election Commission: Oversees the entire election process by setting parameters, ensuring integrity, and managing both voter and candidate registrations.

Returning Officer: Manages administrative tasks within a specific jurisdiction, coordinates polling officers, and ensures the smooth conduct of the election.

Polling Officer: Operates at the polling stations to verify voter identities, assist voters, and maintain the security and integrity of the voting process.

Voters: Register, verify their eligibility, and cast their votes securely and confidentially.

National Identity Database (NID) Servers: Authenticate voters by storing and managing identification data and providing reliable authentication services.

Key Management System (KMS) Server: Generates, distributes, and secures the cryptographic keys used in the e-voting system.

Token Generation System: Produces secure and verifiable tokens for voters using multi-party computation (MPC), ensuring transparency and preventing double voting.

Scripting System: Creates and publishes poll scripts on the blockchain, verifies their legitimacy, and ensures accurate vote counting.

Peer-to-Peer (P2P) Network: Facilitates communication and data exchange among blockchain nodes, maintaining the system's decentralized integrity and security.

Effective coordination among these stakeholders is crucial for the system's success.

4 Implementation

The system is constructed with a robust technological stack that emphasizes cross-platform compatibility and security:

Data Serialization: Protocol Buffers enable efficient, cross-platform data communication.

Blockchain Security: Timestamped blocks are created using robust hash functions (SHA256 and Blake2b) combined with Base58 encoding.

Digital Signatures: Asymmetric encryption is implemented with Cloudflare's CIRCL library, employing Ed25519 for generating digital signatures.

Token Validation: A secure token-based scheme, incorporating UUIDs and zero-knowledge proofs, mitigates the risk of double-spending.

Data Management: LevelDB is utilized as an efficient key-value database to handle system data.

Backend Services: The GIN web framework provides a REST API for processing requests and seamlessly integrates with the application, network, script processing, and blockchain layers.

NID Server: Developed using GIN and SQLite3, the NID server offers verifiable and tamper-proof voter data, enabling real-world testing of the system.

The implementation prioritizes security through cryptographic primitives while maintaining performance via treeset for token lookup. The modular design enables independent scaling of components while ensuring end-to-end verifiability of the voting process.

5 Result and Discussion

This section presents data collected throughout the study along with relevant graphs and charts to illustrate the findings. All performance metrics and data were generated using the Golang built-in benchmark tool with custom scripts provided by the standard test package, which were run on the blockchain network. Findings are interpreted within the framework of the research question and prior literature.

The graph in Figure 4 shows the rate of block generation with and without block modularity in a blockchain network marked "a" on the graph. The bar chart shows the throughput of that network marked as "b".

Normal experiment: Block modularity initially took the same amount of time as without block modularity. However, after passing 1,000 voters, block modularity took less time. This is because block modularity divides the system data into smaller categories, so when new data come into the network, they do not duplicate data; instead, it merges newer portions of data, which helps process and validate more quickly. Each node only needs to process and validate the blocks that are relevant to it. However, without block modularity, when new data entered the network, it did not separate the data, which resulted in duplication of all the data. As a result, it consumed more memory, had slower block generation time, and slower throughput. In addition, all blocks on the blockchain are processed and validated by all nodes on the network. This can lead to bottlenecks and performance issues, especially as the network grows and the number of voters increases.

In conclusion, block modularity provided better performance than without block modularity.

Dilithium (Post-quantum) vs EdDSA (Edwards-curve): Figure 4 compares the Dilithium 3 post-quantum algorithm with the Edwards-curve algorithm in panel "d". Both perform similarly at smaller scales, but as the number of voters increases, Dilithium 3 requires less block-generation time. This indicates stronger scalability while also improving resilience against quantum attacks. In panel "e", both algorithms achieve nearly identical throughput.

Sharding: Sharding is a technique for improving scalability and performance in distributed systems. It divides data into smaller parts, which can then be processed in parallel. The line graph in Figure 4 "c" shows how sharding with different numbers of shards affects the time it takes to generate blocks. The blue line represents sharding with two shards, the orange line represents sharding with three shards, and the green line represents sharding with five shards. The horizontal axis represents the number of voters, and the vertical axis represents the time. The graph shows that sharding with five shards provides the best performance. At its peak, the green line takes only 28 seconds to generate 3000 blocks, while the blue line takes 430 seconds and the orange line takes 153 seconds. The bar graph in Figure 4 "f" shows how sharding with different numbers of shards affects the throughput. The orange line represents sharding with two shards, the blue line represents sharding with three shards, and the light-green line represents sharding with five shards. The vertical axis represents the num-

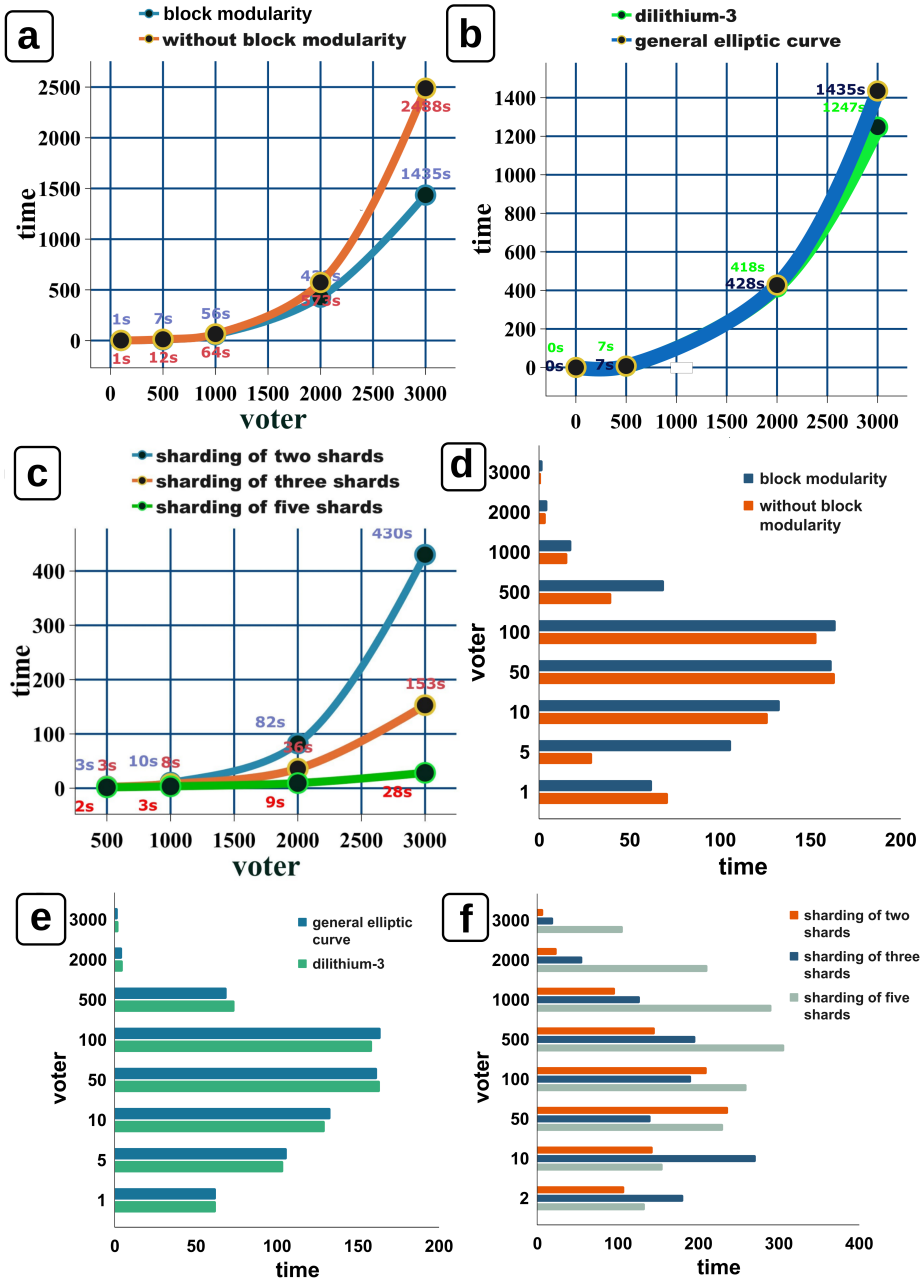

Fig. 4. Blockchain network performance: (a) Block generation time with and without block modularity, (b) block generation time for Dilithium-3 and Edwards-curve, (c) block generation time with sharding (2, 3, 5 shards), and (d, e, f) their respective throughput.

ber of blocks, and the horizontal axis represents the time. The graph shows that sharding with five shards provides the highest throughput compared to others. At its peak, sharding with five shards shows approximately 106 TPS, which is higher than some famous networks like Bitcoin and Ethereum.

In conclusion, breaking data into more shards can lead to higher performance and throughput.

5.1 Scalability and Comparative Analysis

To understand the effectiveness of our proposed system, it's useful to consider voter turnout statistics in the United States. The national average number of voters per polling station is 749, according to the Election Assistance Voter Survey [43]. However, in densely populated urban areas—such as Los Angeles or New York City—a single polling station may serve as many as 10,000 voters [44,45,46]. The system is designed to handle such high voter volumes efficiently. As shown in Figure 4, each node in this system can process voters at a rate of 105 voters per second. In a real-world context, this means a single node can manage 10,000 voters in less than 100 seconds, specifically:

$$\text{Time for one node} = \frac{10,000 \text{ voters}}{105 \text{ voters/s}} \approx 95.24 \text{ seconds}$$

Scaling this up, a network of 100 nodes can process up to one million voters in a similarly short time frame:

$$\text{Processing rate} = 100 \text{ nodes} \times 105 \text{ voters/s} = 10,500 \text{ voters/s} \tag{1}$$

$$\text{Time required} = \frac{1,000,000 \text{ voters}}{10,500 \text{ voters/s}} = \frac{2000}{21} \text{ s} \approx 95.24 \text{ s} \tag{2}$$

This demonstrates that our system can efficiently process millions of voters in under two minutes, making it well-suited for high-density precincts and significantly reducing voter wait times.

In addition, we conducted a comparative study to benchmark our system against existing solutions. As detailed in Table 1, our proposed system outperforms the best existing models in terms of processing speed and scalability, positioning it as a robust option for modernizing voting infrastructure.

6 Attack and Security Analysis

This section provides an analysis of various attacks and the corresponding security measures implemented in the proposed blockchain-based e-voting system.

1. **Spoofing:**
   - **Attack Description:** Spoofing involves an attacker masquerading as a legitimate user or device to gain unauthorized access to the system.

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

Properties	**[47]**	**[30]**	**[48]**	**[49]**	**[11]**	**[18]**	**[22]**	**[16]**	**Proposed Model**
Consensus	POW	QBA	POW	POS	POS	POS	PSC	POS	PQR-HAC
Confidentiality	✓	X	X	X	✓	✓	✓	X	✓
Throughput	7	-	7	25	25	25	60	25	105
Post Quantum	X	✓	X	X	X	X	X	X	✓
Robustness	✓	X	X	X	X	✓	✓	X	✓
Uniqueness	✓	✓	X	✓	✓	✓	✓	✓	✓
Security	✓	✓	✓	✓	✓	✓	✓	✓	✓
Eligibility	X	✓	X	X	X	✓	✓	X	✓
Transparency	✓	✓	✓	✓	✓	✓	✓	✓	✓
Verifiability	✓	✓	X	✓	✓	✓	✓	✓	✓
Time-based inference	X	X	X	X	X	X	X	X	✓

   - **Security Measures:** Use of robust authentication mechanisms, such as multi-factor authentication (MFA) and rolling passwords.
2. **Tampering:**
   - **Attack Description:** Tampering involves the unauthorized modification of data within the system, compromising its integrity.
   - **Security Measures:** Ensure data integrity by employing cryptographic hash functions such as SHA256 and Blake2b, implementing blockchain technology for an immutable transaction ledger, and conducting regular audits and integrity checks to detect and prevent tampering.
3. **Wallet Theft:**
   - **Attack Description:** Wallet theft involves the unauthorized access and theft of cryptographic keys or tokens stored in a user's wallet.
   - **Security Measures:** Ensure data security by employing token-based secure validation schemes that incorporate UUIDs and zero-knowledge proofs, implementing hardware security modules (HSM) to store cryptographic keys securely and applying regular security updates and patches to protect against known vulnerabilities.
4. **Information Theft:**
   - **Attack Description:** Information theft involves the unauthorized access and extraction of sensitive data from the system.
   - **Security Measures:** Ensure data security by using encryption for data at rest and in transit, implementing access controls and authorization mechanisms to restrict access to sensitive data, and conducting regular security audits and penetration testing to identify and mitigate vulnerabilities.
5. **Denial of Service (DoS):**
   - **Attack Description:** Denial of Service (DoS) attacks involve overwhelming the system with excessive traffic, making it unavailable to legitimate users.
   - **Security Measures:** Protect against denial of service (DoS) attacks by implementing rate limiting and traffic filtering mechanisms, using DDoS

mitigation services, and regularly monitoring and analyzing network traffic to detect and respond to threats.

6. **Privilege Tampering:**
   - **Attack Description:** Privilege tampering involves the unauthorized modification of user privileges to gain elevated access within the system.
   - **Security Measures:** Ensure secure user privilege management by using role-based access control (RBAC) to enforce strict access policies, implement audit trails and logs to track changes in user privileges, and conduct regular security reviews and audits to maintain integrity.

Hybrid blockchains can be protected from quantum computer attack by using post-quantum cryptography. This is crucial because quantum computers are growing more powerful and could eventually pose a significant threat to blockchain security. The proposed blockchain-based electronic voting system incorporates these security measures to mitigate the risks associated with identified attacks, ensuring a secure and reliable voting process.

7 Conclusion

Blockchain technology has the potential to revolutionize e-voting systems by enhancing their security, transparency, and efficiency. It can also reduce carbon emissions by eliminating the need for paper ballots, reducing the reliance on polling stations, and improving the overall efficiency of the voting process. In this study, we present a hybrid blockchain architecture that combines the strengths of both public and private blockchains to address the limitations of existing blockchain models. This blockchain-based e-voting system effectively overcomes the scalability and decentralization challenges faced by traditional blockchain models. The proposed framework significantly outperforms existing blockchain-based e-voting systems, achieving a throughput of 105 transactions per second (TPS) with just 5 nodes. This represents a four-times improvement over proof-of-stake (PoS) blockchains and a 14-times enhancement compared to proof-of-work (PoW) blockchains. The system establishes a solid foundation for secure, scalable, and sustainable e-voting. Future research should pursue technical enhancements, such as AI-driven anomaly detection for real-time identification of suspicious voting patterns, post-quantum secure communication protocols, and adaptive sharding for dynamic scalability, while embedding inclusive deployment strategies. Accessibility measures like text-free interfaces for illiterate or semiliterate users and Braille button on ballot machines for blind voters will ensure participation across all societal strata, including those with limited digital literacy or internet access. By integrating these socio-technical solutions, the platform can evolve into a universally accessible system without compromising security or decentralization.

8 Declarations

The authors declare that they have no competing interests.

9 Author Contribution

Conceptualization of the research topic and writing of the original draft was carried out by Sohel Ahmed Joni, Rabiul Rahat, and Nishat Tasnin. Resource collection, methodology design, and code development were carried out by Sohel Ahmed Joni, Rabiul Rahat, and Partho Ghose. Work administration was conducted by Partho Ghose and Loveleen Gaur. Result validation was performed by Sohel Ahmed Joni, Rabiul Rahat, and Partho Ghose. The final draft and revisions were made by Loveleen Gaur and Partho Ghose.

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. P. B. Stark and D. Wagner, "Evidence-based elections," *IEEE Security & Privacy*, vol. 10, no. 5, pp. 33–41, 2012.
4. K. R. Butler, W. Enck, H. Hursti, S. E. McLaughlin, P. Traynor, and P. D. McDaniel, "Systemic issues in the hart intercivic and premier voting systems: Reflections on project everest." *EVT*, vol. 8, pp. 1–14, 2008.
5. International Institute for Democracy and Electoral Assistance (International IDEA), "Use of E-Voting Around the World," https://www.idea.int/news-media/multimedia-reports/use-e-voting-around-world, feb 2023, accessed: 2025-05-06.
6. J. Willemson and K. Krips, "Estimating carbon footprint of paper and internet voting," in *International Joint Conference on Electronic Voting*. Springer, 2023, pp. 140–155.
7. S. Wynes, M. Motta, and S. D. Donner, "Understanding the climate responsibility associated with elections," *One Earth*, vol. 4, no. 3, pp. 363–371, 2021.
8. A. C. Dias and L. Arroja, "Comparison of methodologies for estimating the carbon footprint–case study of office paper," *Journal of Cleaner Production*, vol. 24, pp. 30–35, 2012.
9. M. Ahmad, A. U. Rehman, N. Ayub, M. D. Alshehri, M. A. Khan, A. Hameed, and H. Yetgin, "Security, usability, and biometric authentication scheme for electronic voting using multiple keys," *International Journal of Distributed Sensor Networks*, vol. 16, no. 7, p. 1550147720944025, 2020.
10. 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.
11. 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.
12. 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.

13. S. A. Joni, R. Rahat, N. Tasnin, P. Ghose, M. A. Uddin, and J. Ayoade, "Hybrid-blockchain-based electronic voting machine system embedded with deepface, sharding, and post-quantum techniques," *Blockchains*, vol. 2, no. 4, pp. 366–423, 2024.
14. 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.
15. D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, 2022.
16. 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.
17. R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for e-voting," *Symmetry*, vol. 12, no. 8, p. 1328, 2020.
18. 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.
19. 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.
20. 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.
21. 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.
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.
23. X. Wang, T. Feng, C. Liu, and J. Fang, "Multi party confidential verifiable electronic voting scheme based on blockchain," *Journal of Cloud Computing*, vol. 13, no. 1, p. 160, 2024.
24. 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.
25. 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.
26. 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.
27. Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *Ieee Access*, vol. 6, pp. 27 205–27 213, 2018.
28. 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.
29. S. Sakhuja and S. Balakrishnan, "Quantum-enhanced secure approval voting protocol," *arXiv preprint arXiv:2406.19730*, 2024.
30. 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.

31. S. A. Joni, R. Rahat, N. Tasnin, P. Ghose, and M. Mahbub-Or-Rashid, "Grainbee: A quantum-resistant blockchain-based ration distribution system with hardware security modules," in *2024 IEEE International Conference on Computing, Applications and Systems (COMPAS)*. IEEE, 2024, pp. 1–6.
32. 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.
33. 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.
34. H. Huang, X. Zhao, and J. Liu, "Best: A blockchain sharding scheme based on nodes performance for enhancing both security and effiency," 2023.
35. L. Ren and P. A. Ward, "Transaction placement in sharded blockchains," *arXiv preprint arXiv:2109.07670*, 2021.
36. A. Abbas and M. A. Hamid, "Adapting hybrid approaches for electronic medical record management and sharing using blockchain sharding," *Periodicals of Engineering and Natural Sciences*, vol. 11, no. 1, pp. 5–14, 2023.
37. H. Baniata, A. Anaqreh, and A. Kertesz, "Distributed scalability tuning for evolutionary sharding optimization with random-equivalent security in permissionless blockchain," *Internet of Things*, vol. 24, p. 100955, 2023.
38. M. Biswas, P. Ghose, M. Alavi, M. Tabassum, M. Ashraf Uddin, K. Mahbub, L. Gaur, S. Mallik, and Z. Zhao, "Detecting covid-19 infection status from chest x-ray and ct scan via single transfer learning-driven approach," *Frontiers in Genetics*, vol. 2490.
39. P. Ghose, M. A. Uddin, U. K. Acharjee, and S. Sharmin, "Deep viewing for the identification of covid-19 infection status from chest x-ray image using cnn based architecture," *Intelligent Systems with Applications*, vol. 16, p. 200130, 2022.
40. P. Ghose, M. Biswas, and L. Gaur, "Brainsegnet: a lightweight brain tumor segmentation model based on u-net and progressive neuron expansion," in *International Conference on Brain Informatics*. Springer, 2023, pp. 249–260.
41. P. Ghose, S. Sharmin, L. Gaur, and Z. Zhao, "Grid-search integrated optimized support vector machine model for breast cancer detection," in *2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*. IEEE, 2022, pp. 2846–2852.
42. P. Ghose, M. A. Uddin, M. M. Islam, M. Islam, and U. K. Acharjee, "A breast cancer detection model using a tuned svm classifier," in *2022 25th International Conference on Computer and Information Technology (ICCIT)*. IEEE, 2022, pp. 102–107.
43. U.S. Election Assistance Commission, "2022 election administration and voting survey comprehensive report," U.S. Election Assistance Commission, Tech. Rep., 2023, accessed: 2025-03-07. [Online]. Available: https://www.eac.gov/sites/default/files/2023-06/2022_EAVS_Report_508c.pdf
44. Route Fifty, "100,000 fewer election day polling places in 2024," *Route Fifty*, March 2024, accessed: 2025-03-07. [Online]. Available: https://www.routefifty.com/management/2024/03/there-are-100000-fewer-election-day-polling-places-2024/394959/
45. New York City Campaign Finance Board, "Voter analysis report: 2022 - 2023," New York City Campaign Finance Board, Tech. Rep., 2023, accessed: 2025-03-07. [Online]. Available: https://www.nyccfb.info/media/reports/voter-analysis-report-2022-2023/

46. County of Los Angeles, "Elections & voting – county of los angeles," [n.d.], accessed: 2025-03-07. [Online]. Available: https://lacounty.gov/government/elections-voting/
47. 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.
48. 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.
49. 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.