

Blockchain-based E-Voting: A Comprehensive Review

Tahia Hoque¹, Iyolita Islam^{1*}

Abstract

One of the most significant challenges encountered by electoral process is ensuring the integrity, transparency and accessibility of election systems, particularly in developing democracies where problems with trust, security and scalability remain a problem for traditional and central electronic voting procedures. Blockchain technology has emerged as one potential solution to these challenges by providing decentralization, immutability, and cryptographic techniques, and consensus methods to analyze blockchain-based voting systems in-depth. This article reviews the key challenges of existing voting systems in context of voter authentication, ballot secrecy and verifiability; how blockchain can include digital signatures, hash functions, homomorphic encryption, and zero-knowledge proofs to mitigate the challenges. Beyond technical research, this study outlines that the blockchain-based voting system might be used in Bangladesh's socio-technical and regulatory framework, paying special emphasis to new technology-assisted efforts for foreign voters. In addition, the inquiry evaluates the potential of blockchain-based voting being implemented in Bangladesh's socio-technical regulatory framework, with particular focus on novel technology-aided solutions for overseas voters. The aim of this study is to provide insight on the benefits and drawbacks of blockchain-based voting system for advancing electoral security in Bangladesh. Although prototype implementation using Hyperledger fabric is developed to evaluate system feasibility, and performance metrics such as latency and throughput are analyzed under simulated voting conditions. Furthermore, a phased adoption roadmap is also suggested, and the technological, legal, and societal obstacles Bangladesh might encounter are covered.

Keywords: Blockchain-based electronic voting, cryptography, on-chain and off-chain storage, voter verification, ballot secrecy, Hyperledger fabric.

1. Introduction

Democracy depends on elections, which require fairness and trust. The foundation of democratic decision-making is the ability of voters to select their representatives and influence the government through voting systems. Elections

*Corresponding Author email: iyolitaislam@bup.edu.bd

¹ Department of Computer Science & Engineering, Bangladesh University of Professionals (BUP), Dhaka, Bangladesh.

DOI: <https://doi.org/10.64494/JFST/v4i1/ii/2026/08/143-164>

have traditionally been conducted using paper-based ballots, which are straightforward and transparent but require a lengthy counting process and are prone to human error. To get rid of these limitations, electronic voting systems were created with the intention of improving accessibility and efficiency. In modern voting systems, digital technologies are becoming more and more important for voter registration, ballot casting, and result tabulation. However, many of these systems remain centralized, requiring trust in electoral officials and technical operators.

Electronic voting machines increase efficiency but raise concerns about trust, whereas traditional paper voting faces logistical and manipulation risks. By using cryptography and decentralization, blockchain voting systems seek to increase security and verifiability while preserving voter privacy.

Several significant obstacles exist in centralized Electronic Voting Methods (EVM) and traditional paper-based voting systems. Voter impersonation, ballot tampering, vote rigging, and a lack of real-time transparency are some of these. While centralized databases produce single points of failure susceptible to insider manipulation and cyberattacks, manual counting procedures tend to be laborious and error-prone (Khan, 2022; Shiraj, 2022). Moreover, public confidence in election results can be decreased by restricted auditability and delayed result publishing, especially in the major national elections.

Blockchain technology generates a decentralized nature where votes and other transactions are permanently recorded across the nodes and protected by the technique named cryptography (Islam, 2020). Decentralization, immutability, transparency, and cryptographic security are important characteristics that are relevant to voting systems (Farooq, 2022). Therefore, blockchain can be a tamper-resistant solution to the shortcomings of conventional voting systems. Also, blockchain guarantees transparency, integrity, and traceability without depending on any central authority by considering votes as unchangeable transactions on a distributed ledger. Voter privacy is protected while verifiable vote counting is made possible by using cryptographic techniques. By automating tallying procedures and election rules, smart contracts can minimize human interaction and lower the possibility of any type of fraud. In a blockchain, any node can start a transaction that can be spread to all other nodes inside the network (Islam, 2023). Blockchain is a compelling choice for a safe and reliable electronic voting system because of these characteristics.

Even though distributed consensus and cryptographic hashing guard against tampering and illegal alterations to the ledger, public-key cryptography guarantees that only authorized voters can cast ballots. Election regulations can

be automatically enforced, voter registration can be managed, also safe vote counting can be carried out by using smart contracts, which are self-executing code implemented on a blockchain Hung (2022). By facilitating end-to-end verifiability and lowering dependency on reliable third parties, these approaches are taken together to improve trustworthiness.

Therefore, the primary objective of this research is to propose a safe blockchain-based voting system using Hyperledger Fabric that guarantees voter privacy, transparency, and integrity. To attain this objective, existing cryptographic techniques as well as system architectures for safe voting and verification are explored. Additionally, the feasibility of a blockchain-based voting system in terms of societal considerations, legal restrictions, and technical infrastructure in Bangladesh, was studied.

2. Related Works

This section discusses about the existing studies on traditional voting, EVMs, and blockchain based voting system. Major scholarly databases like Scopus, IEEE explorer, ACM, springer were searched to collect the articles related to this study.

Centralized EVMs and manual paper ballot elections are examples of traditional voting methods. The norm for democratic elections is: voters mark tangible ballots that are gathered, analyzed, and validated by election officials in the paper-based voting system. Though this manual process seemed to be straightforward and transparent, they are vulnerable to human mistakes, logistical inefficiencies, lengthy counting delays, and chances of ballot loss or tampering. EVMs were introduced to enhance effectiveness and efficiency. However, many EVMs are dependent on proprietary software and centralized servers, which can lead to a single point of control and failure. Concerns in data integrity and public trust may arise from the centralized architectures' sensitivity to cyber-attacks, insider threats, and illegal manipulation. Besides, particularly in large-scale elections, a lack of transparency in vote recording and result verification may reduce confidence in democratic results.

Blockchain-oriented voting systems that use distributed ledgers to ensure immutability, transparency, and decentralization have been proposed in several studies. For example, researchers have created systems that allow for independent verifiability without sacrificing the anonymity of a voter by recording every vote as a blockchain transaction (Daraghmi, 2024). Election regulation has been automated, voting deadlines have been enforced, and safe tallying procedures have been made possible via smart contracts in another research (Alvia, 2022). Eusha proposed and evaluated a blockchain-based

alternative voting system, *BE-Voting*, for Bangladesh to ensure vote integrity, transparency, and security through a developed prototype. Berenjestanaki conducted an extensive review of 252 selected papers using a hybrid review approach to investigate the benefits, challenges, impacts, technologies, implementations, and future research directions of blockchain-based electronic voting systems (Berenjestanaki, 2023). These studies represent how blockchain technology might improve transparency and lower fraud in online elections. Pilot implementations in controlled settings, like university elections or corporate decision-making platforms, are frequently reported in research, offering practical insights into technical feasibility. A few researchers have fully evaluated real-world problems in developing nations, despite the fact that many offer architectural blueprints and simulation findings.

There are a number of gaps in the current blockchain-based voting research, despite encouraging advancements. Firstly, without adequately addressing the scalability issues related to national-level elections, the majority of ideas concentrate on architectural and cryptographic validity. When scaled to a million votes, blockchain networks frequently have latency and transaction throughput issues. Secondly, there is still a lack of research on usability and accessibility issues; voter-facing interfaces need to be inclusive and accommodate a range of reading levels, particularly in developing nations. Thirdly, a few research investigated the contextual applicability in particular political and regulatory contexts, like Bangladesh. Again, few studies analyzed how blockchain based systems interact with current legislative frameworks, election processes, infrastructure security, and socio-cultural elements. Finally, security vulnerabilities in real-time election situations are yet to discover due to lack of empirical data from field studies.

3. Comparative Analysis and Technical Insights

This section outlines the analysis findings of techniques adopted in existing voting systems and research.

3.1 Architectural Models in Blockchain-Based Voting System

Existing research suggests architectures that differ according to system control, network accessibility, and data storage techniques rather than coming to a single standardized design (Islam, 2020). The security, scalability, and usability of the blockchain voting systems are greatly impacted by these architectural decisions.

A comparative view between centralized and decentralized approaches has been presented in Figure 1. Voter registration, vote storage, and tabulation are all handled by a single authority or server in the centralized voting infrastructure.

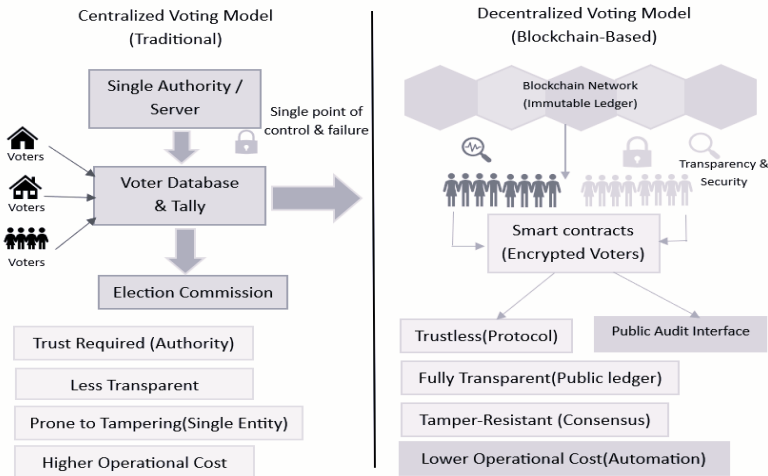


Figure 1: Comparing between centralized & decentralized voting system

These systems have a single point of failure and enforce a high level of faith in the controlling authority, despite being easier to implement and maintain (Kohnno, 2004). On the other hand, decentralized blockchain-based architecture can spread control among several nodes, lowering the possibility of manipulation and enhancing fault tolerance. However, decentralization presents issues with latency, system complexity, as well as network coordination (Henry, 2024).

Another important comparison is public vs private blockchains. Any node can validate transactions and view the ledger on public blockchains, which provide open participation. Although this architecture improves transparency, scalability, and privacy, transaction costs may be an issue (Sharp, 2024). Only approved parties, like election authorities, are allowed to participate in private or permissioned blockchains.

A range of architectural models that are targeted at enhancing electoral security, transparency, and dependability are presented in the literature on blockchain-based voting systems.

3.2 Cryptographic Methods Adopted in Current Voting Systems

Cryptography is the fundamental security component of blockchain-based voting systems. The use of cryptographic techniques to guarantee voter authentication, data integrity, ballot secrecy, and verifiability is constantly emphasized throughout the examined literature.

Public-key cryptography is commonly used for secure vote transmission and voter authentication. Votes can be encrypted using a public key and decrypted only by authorized organizations, as each vote is usually given a unique cryptographic key pair. This system safeguards vote confidentiality and stops unauthorized access. However, safe distribution and key management continue to be major obstacles, especially for broad and diverse electorates (Huang, 2021).

To confirm the validity and integrity of votes, digital signatures are used, which guarantee that votes come from real voters and have not been tampered with during transit by signing each ballot transaction. Digital signatures are useful in preventing tampering and impersonation, but they can't provide voter anonymity on their own unless they are paired with other privacy-preserving methods.

Cryptographic hash functions are essential for guaranteeing the immutability and integrity of data. Blocks are connected by hashing, which also makes it possible to efficiently verify votes that have been saved without disclosing their content. Although hash-based systems do not automatically guard against vote tampering or privacy breaches, they enable voters and auditors to confirm that votes stay the same.

Additionally, on-chain and off-chain vote-storing strategies are distinguished in the literature, as shown in Figure 2. Votes are immediately recorded on the blockchain by on-chain storage, which ensures maximal immutability and auditability but may have scalability issues as well as higher storage costs. While keeping cryptographic references or hashes on-chain, off-chain storage options store encrypted votes off-chain. Despite this, the hybrid method increases efficiency and scalability; it also boosts dependency on external storage systems, which could have an impact on general trust assumptions (Patil, 2018). Each architectural model emphasizes that no single architecture is always best by reflecting trade-offs between security, performance, and practicality.

Advanced approaches like homomorphic encryption allow votes to be recorded while being encrypted, ensuring ballot confidentiality throughout the counting process. Homomorphic encryption is quite safe, but it has a considerable processing overhead that makes it unsuitable for large-scale elections. In a similar mode, voters can demonstrate the legitimacy of their votes without disclosing their vote choices through zero-knowledge proofs. Although these methods indicate value for privacy and verifiability, they are frequently difficult to implement and may have an impact on system performance and usability. The literature features the trade-off between strong cryptographic guarantees and the effectiveness of the system.

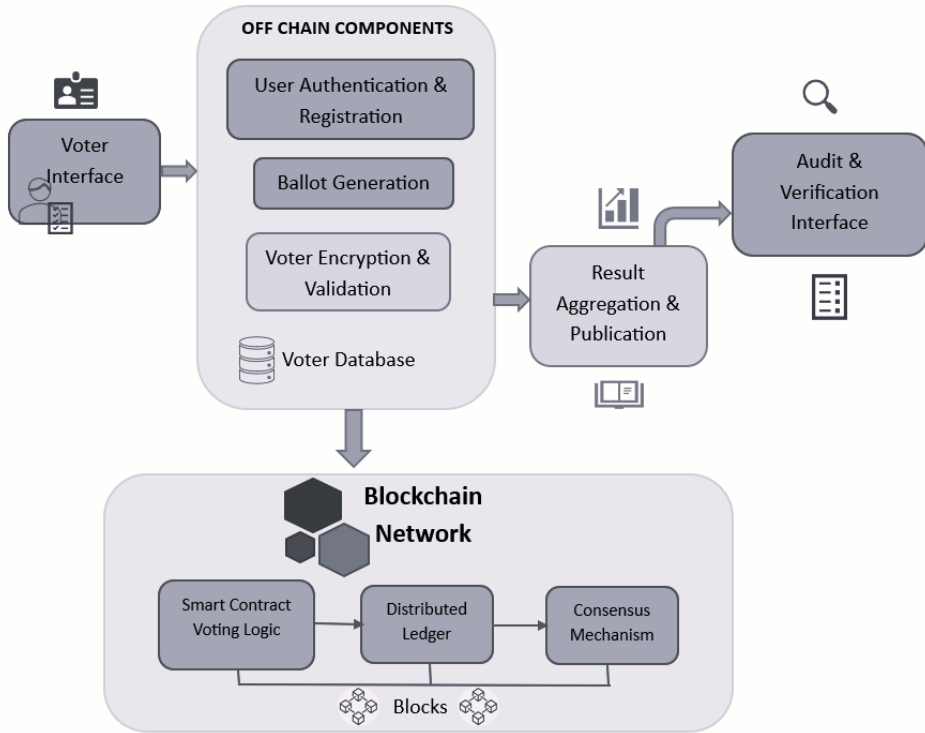


Figure 2: Generic architecture of a blockchain voting system

3.3 Feasibility of Consensus Techniques in Voting

Consensus methods are essential to the dependability of voting systems as they specify how blockchain networks validate transactions and preserve ledger integrity. Several consensus models with differing applicability for electoral applications are explored in the current research.

One of the oldest and most secure consensus systems is Proof of Work (PoW), which relies on computational challenges to verify transactions. PoW is heavily criticized for its high energy consumption, limited throughput, and transaction delay, despite its robust defense against attacks. PoW is not feasible for nationwide voting systems because of these types of restrictions.

Proof of Stake (PoS) overcomes many of the inefficiencies of PoW by selecting validators based on stake rather than compute capability. PoS drastically reduces energy consumption and increases scalability. However, issues with validator

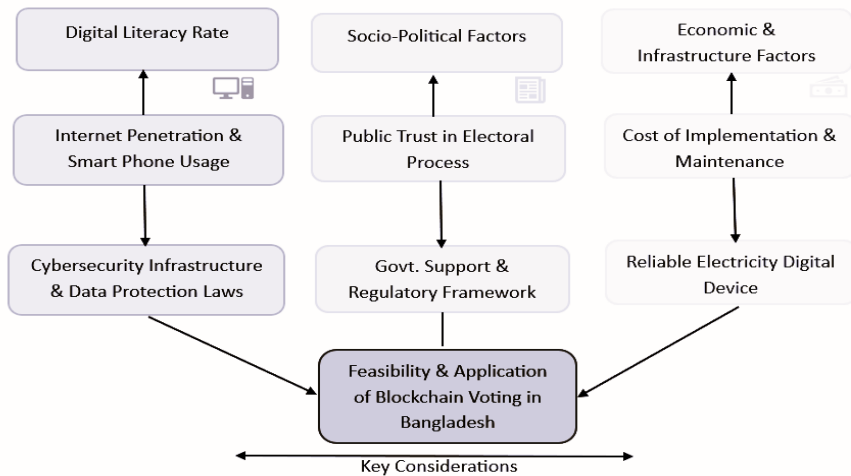


Figure 3: Blockchain voting applicability factors of Bangladesh

control and centralization still exist, especially in situations when proper neutrality and fairness are required (Kumar 2020).

Permissioned consensus techniques, such as Practical Byzantine Fault Tolerance (PBFT) and Raft, are frequently mentioned in voting-related research. These systems function in regulated settings with recognized and approved validators. They are appropriate for election systems that are run by reliable organizations because they provide high throughput, low latency, and robust fault tolerance (Al-Madani 2021). Reduced transparency and decentralization are the trade-offs, which must be carefully weighed against the demands of governance and performance.

3.4 Feasibility in the Context of Bangladesh

The socio-technical and institutional framework of Bangladesh must be taken into consideration while assessing the suitability of blockchain-based voting systems (presented in Figure 3). With rising internet adoption and mobile usage which are broad, the digital infrastructure helps to investigate technology-driven voting reforms, especially for voters who live far away or are in foreign countries.

However, a few limitations may exist in case of digital literacy, particularly in rural areas where access to technology and technical expertise may be restricted. Therefore, usability, accessibility, and voter education must be given the top priority in any blockchain-based voting system. Moreover, election laws and

regulations of Bangladesh would need to be modified to allow for blockchain-based verification systems and digital voting method.

Additionally, the disparity in infrastructure connectivity between urban and rural areas emphasizes the need for hybrid deployment tactics as opposed to instant nationwide implementation (Raikar, 2021). Overall, research indicates that if blockchain-based voting is carefully adopted to local circumstances, backed by legislative changes and implemented gradually as well as under proper regulation, it may be a useful supplementary solution in Bangladesh.

4. Proof of Concept

This section contains the conceptual architecture and experimental setup for performance evaluation as a case study for Bangladesh.

4.1 System Architecture

To validate the feasibility of blockchain-based voting system in the context of Bangladesh, the proposed system architecture using Hyperledger fabric is presented in Figure 4. The system is able to simulate a decentralized voting environment consisting of multiple peer nodes representing election authorities.

- a. **User layer:** This layer is the user interface for the voters on web or mobile applications and the election authority to interact with the system.
- b. **Application layer:** Application layer contains the authentication module for NID verification, the voting interface for casting ballots, and the encryption module utilizing homomorphic encryption.
- c. **Blockchain network layer:** This layer is developed on Hyperledger Fabric, it includes peer nodes acting as election commission observers, an ordering service, and smart contract chain code executing functions like *registervoter()* for storing hashed voter identity, *castvote()* to record encrypted vote transactions, and *tallyvotes()* to compute result transparently.
- d. **Security and cryptography layer:** The final layer incorporates digital signatures, hash functions, optional zero knowledge proofs, and optional homomorphic encryption to ensure data protection and anonymity.

Voter identities are anonymized using cryptographic hashing and each vote is recorded as an immutable transaction in the distributed ledger. This ensures integrity, transparency, and resistance to tampering.

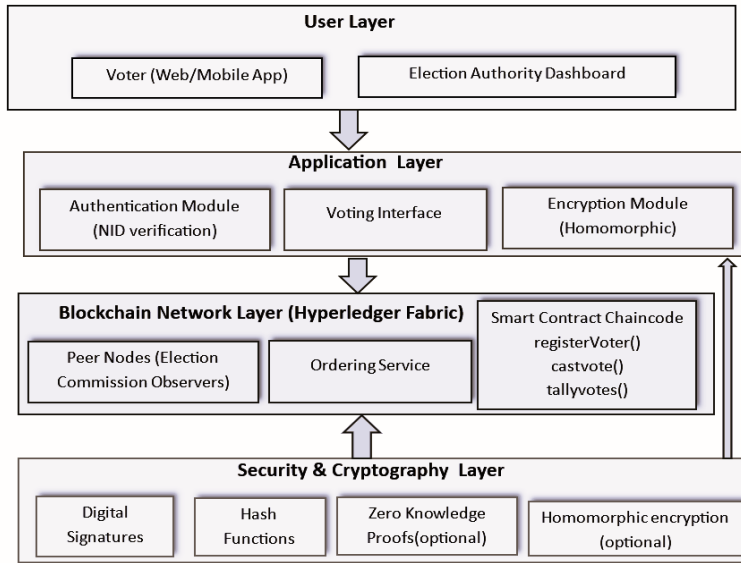


Figure 4: Structural overview of blockchain-based E-Voting system

Table 1: Experimental setup for this study

Category	Tools
Platform	Hyperledger fabric
Peer nodes	4
Consensus	RAFT
Simulated Voters	100-1000
Environment	Local Test Network
Hardware	Intel i5, 8Gb RAM

4.2 Experimental Setup

A limited version prototype was developed based on the system architecture and evaluated in a controlled local environment with simulated voters. The environment configuration is presented in Table 1.

The performance of the system can be evaluated in terms of latency and throughput. Latency increases with the number of voters due to consensus overhead but remains acceptable for small to medium scale elections. Throughput improves initially with more nodes but slightly decreases due to coordination complexity in distributed consensus.

The security observations for these systems are:

- a. Immutability: Once recorded, votes cannot be altered.
- b. Integrity: Smart Contracts prevent duplicate voting.
- c. Transparency: Ledger is auditable.
- d. Privacy: Voter identity is protected via hashing.

4.3 Case study analysis for Bangladesh

The proposed system was analyzed in the context of the Bangladesh Election Commission, which conducted electronic voting, and the socio-technical infrastructure of the country. Current challenges for Bangladesh can be listed as:

- a. Limited public trust in centralized systems.
- b. Risk of vote tampering and lack of transparency.
- c. Accessibility issues for overseas voters.
- d. Infrastructure gaps in rural areas.

A comparative view is represented in Table 2 considering the factors transparency, security and trust. The feasibility insights for adopting blockchain-based voting system in Bangladesh are:

- a. Bangladesh already has a strong NID infrastructure, which can support voter authentication.
- b. Urban regions are suitable for pilot deployment.
- c. Overseas voting (expatriates) is a strong use case for early adoption

Table 2: A comparative view of existing and blockchain based system

Factor	Current System	Blockchain-Based System
Transparency	Limited	High (public ledger)
Security	Moderate	High (cryptographic protection)
Trust	Medium-Low	Improved via decentralization
Accessibility	Limited	Remote voting possible
Scalability	Moderate	Needs optimization

The combined experimental and contextual analysis illustrates that blockchain-based voting is technically feasible for pilot-scale deployment in Bangladesh, particularly in controlled environment such as: universal elections, organizational voting and overseas voter participation

However, nationwide adoption faces several challenges:

- a. Infrastructure limitations in rural areas.
- b. Legal and regulatory barriers.
- c. Need for public awareness and trust.

Thus, this article recommends a phased adoption strategy is starting with small-scale pilots before expanding to national elections.

5. Blockchain and Current Global Voting Initiatives in Bangladesh

The election commission and the government of Bangladesh have made it a top priority to guarantee widespread election participation, even from individuals residing overseas. Due to logistical issues, and a lack of accessible procedures, millions of Bangladeshi expatriates estimated in the millions – have historically been unable to practice their right to vote. By incorporating technology into voter registration and postal voting procedures as well as investigating the possibility of more sophisticated digital solutions, recent changes have attempted to alter this.

5.1 Current Initiatives for Technology-Assisted Voting

In 2010, Bangladesh implemented EVMs on a small scale, first for local government elections (The Daily Observer, 2025). In the 11th National Parliamentary Election in 2018, their use progressively spread to a few cities and, for the first time, six seats. Additionally, EVMs were utilized in a number of local government elections from 2020 to 2023 and in a few constituencies during the January 2024 12th National Parliamentary Election. Faster vote counting, more accurate vote recording, less reliance on paper ballots, and fewer opportunities for traditional ballot tampering are the key benefits of EVMs. However, because of worries about cybersecurity, transparency, the lack of political agreement among key parties, and inadequate chances for independent verification, the use of EVMs has remained contentious. The Election Commission decided in 2025–2026 to switch back to paper-based voting and stop using EVMs in all future elections due to ongoing concerns about transparency, political consensus, and public trust.

The EC has implemented an IT assisted expatriate voting system for the 13th National Parliamentary Election. which mainly uses postal ballots and online registration. Through a mobile application connected to their National identity (NID) details, Bangladeshi Residents residing abroad can register under this program known as “Postal Vote BD.” After registration, eligible voters get paper

ballots at their foreign locations, cast their ballots and mail the completed forms back to Bangladesh (Yadav, 2020).

The EC's online registration platform simplifies the enrollment process for foreign nationals by replacing the previous manual method with digital submission and authentication, including NID verification. The platform allowed users over 140 countries to register by the end of 2025, and hundreds of thousands of foreigners did so, demonstrating a high level of participation.

Even though postal vote will remain the primary method of voting overseas in the 2018 election, authorities are looking into hybrid approaches, including online components, to improve reliability and reduce logistical challenges. The EC has considered proxy voting, IT-assisted postal voting and internet voting as part of broader reforms, even though fully remote electronic voting has not yet been implemented.

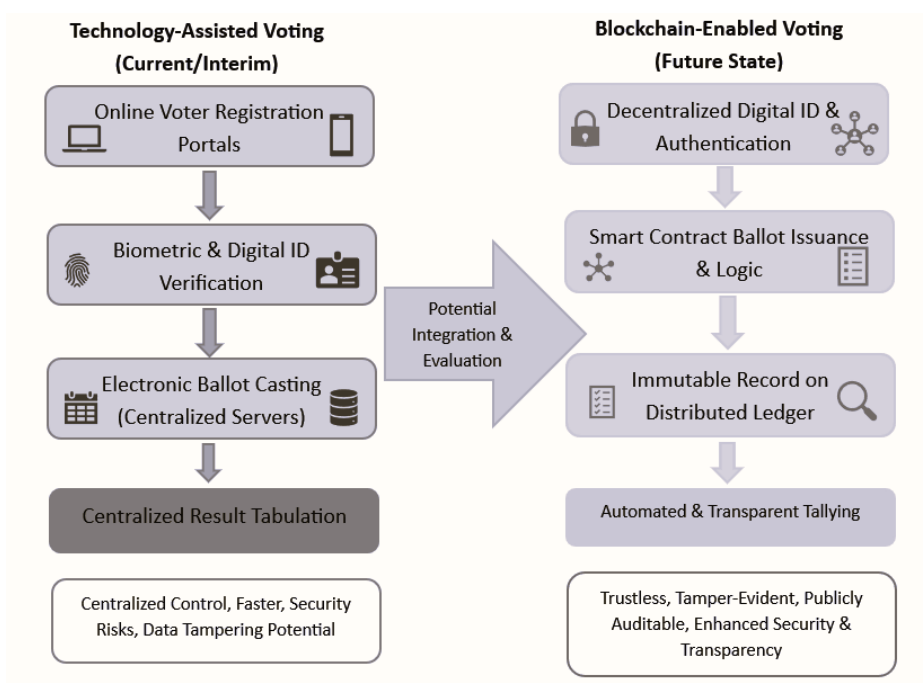


Figure 5: Overview of technology-assisted and blockchain-enabled voting approach in Bangladesh

5.2 The potential role of blockchain in voting system of Bangladesh

Blockchain-based voting has not yet been formally introduced in the national election of Bangladesh, but its basic principles align with the country's primary electoral challenges:

- a. Security and resistance to tampering: The decentralized ledger of blockchain technology can create vote records that cannot be altered, reducing the likelihood of fraud or manipulation.
- b. Transparency and verifiability: The end-to-end verifiability of blockchain technology allows independent stakeholders to audit election results without revealing particular ballot choices.
- c. Decentralized Authority: By distributing validation among nodes, blockchain solution reduces the need for a single authority, potentially increasing public confidence in the integrity of elections.

Blockchain could facilitate safe remote voting for foreign voters, enabling them to encrypt and send their ballots straight to a distributed ledger while guaranteeing authenticity through the cryptographic identity verification linked to current government databases such as NID system. The current IT-assisted system would give way to a more direct online participation mechanism with such integration (Kumari, 2022).

However, the shift to blockchain-based voting in Bangladesh must take into account the country's current digital infrastructure and readiness. Although the nation has made significant progress in digital identification issuance and mobile connectivity, including the widespread use of smart NID cards, complete online voting would necessitate strong cybersecurity protections, legislative frameworks, and public digital literacy campaigns. These have certain significance when contemplating blockchain integration as a long-term electoral upgrade rather than an immediate replacement for existing system. A diagram is shown in Figure 5 comparing the technology-assisted voting system and the blockchain-based voting system. In order to implement blockchain voting in Bangladesh, the following major issues would need to be resolved:

- a. Technical infrastructure: Ensuring digital connectivity across the country is essential for equal participation, especially in rural areas.
- b. Legal adaption: To formally acknowledge digital and blockchain-based voting methods, electoral rules and regulations must be revised.

- c. Public knowledge and trust: In order for voters, particularly foreigners, to comprehend as well as have faith in technology-based voting procedures, they need to be given clear instructions and education.

Observing the ongoing international voting projects allows policymakers to use these realistic implementations as stepping stones for more advanced blockchain elections in future cycles.

6. Roadmap for Blockchain Voting Adoption in Bangladesh

Adoption of a blockchain-based voting systems should be done gradually and in phases, especially in developing democracies, according to the literature. There is serious technical, legal, and societal concerns associated with the immediate nationwide implementation of fully online blockchain voting. A stepwise roadmap enables controlled experimentation, risk mitigation, and public confidence building in Bangladesh, where election procedures are strongly linked to institutional trust, legal obligations, and diverse voter demographics. Policymakers can assess viability, resolve shortcomings and match technology innovation with democratic values using this method. Figure 6 shows a proposed blockchain voting system adoption eligibility.

Phase-1: Preparation and Regulatory Acceptance

Instead of live voting, the first phase relies on institutional, legal, and technical preparation. This includes reviewing current cybersecurity rules, data protection guidelines, and electoral laws to determine their suitability for digital and blockchain-based voting systems. At this point, training on distributed ledger technology, cryptography as well as system auditing is essential for the Election Commission and Associated entities. This stage build confidence and guarantees that adoption in the future is supported by institutional preparedness and legal validity.

Phase-2: Pilot Deployment for a limited set if use cases

Blockchain-based voting may be used in the second stage through carefully monitored pilot projects. Expatriate voting, student elections, professional groups, and municipal government elections are examples of appropriate use cases. These scenarios allow for technical evaluation under real-world conditions because they have smaller electorates and lower political risk. Permissioned blockchains with limited validators may be used by pilot systems to guarantee performance, governance and regulatory supervision. During this stage, input from voters, administrators, and observers is important for improving operational procedures, security measures, and system usability (Sing, 2018).

Phase-3: Integration of Hybrid Systems with Current Election Systems

Blockchain can be included as a supplementary layer rather than taking the place of conventional voting methods. For instance, blockchain might be utilized for audit trails, vote verification, or result dissemination without affecting electronic or physical voting methods. This hybrid strategy improves openness and post-election accountability while maintaining well-known voting procedures. Blockchain could enable safe remote voting for foreign voters while preserving current authentication methods connect to national identity systems. (Chouhan, 2022). This stage lessens opposition from institutions and voters by maintaining a balance between innovation and consistency.

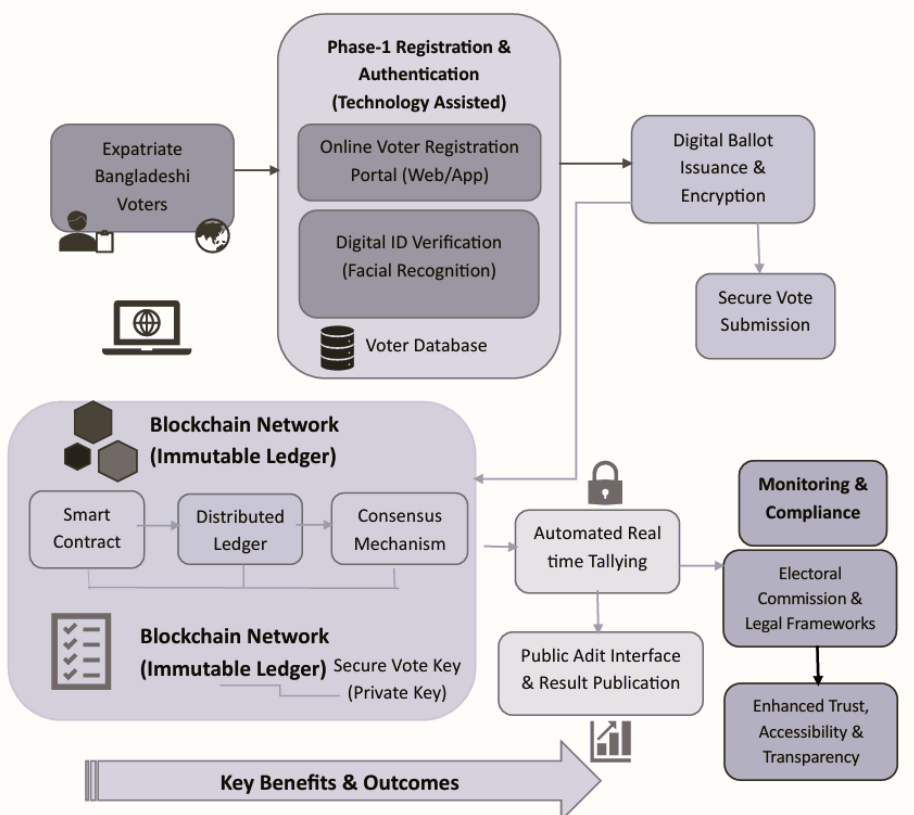


Figure 6: Conceptual Framework for expatriate voting in Bangladesh using technology-assisted and blockchain-based method

Phase-4: Policy-Driven Scaling and Gradual Expansion

If earlier phases show reliability and general approval, blockchain-based voting could be gradually expanded to more diverse political scenarios. Policy-driven expansion should continue to be backed by empirical data from audits and pilot projects. To guarantee long-term sustainability, independent security evaluations, ongoing monitoring, and legal supervision are important.

6.3 Technical Issues

Several technical problems must be addressed before adoption can be considered effective. Scalability is still a major issue because blockchain networks have to manage millions of voters in a short amount of time. Voting consensus methods must guarantee low latency, high throughput, attack resistance. Online voting settings are also seriously threatened by cybersecurity issues like malware, denial-of-service attacks, and identity theft.

Secure Integration and strong access controls are necessary for interoperability with current national databases, such as National Identity (NID) system. Another important issue is system usability, since excessively complicated cryptographic procedures may have an impact on voter confidence and participation.

6.4 Regulatory & Legal Limitations

From a legal standpoint, physical ballots and traditional verification methods are currently prioritized in the voting legislation of Bangladesh. Adopting blockchain-based voting would necessitate the legal acceptance of distributed ledgers, digital ballots and cryptographic signatures as legitimate election tools. To specify who is responsible in situations of system failure or disagreement, clear accountability frameworks must be put in place.

Concerns about data privacy and sovereignty also surface, particularly while could infrastructure or blockchain nodes are housed across borders. Maintaining voter anonymity and legal validity requires commitment to national data protection laws.

6.5 Institutional and Social Conflicts

One of the most important elements affecting adoption is social acceptance. Different age groupings have quite different levels of public faith in voting institutions and technology. Digital literacy disparities, particularly between urban and rural communities, may lead to unequal participation if not addressed by inclusive design and voter education.

Concerns about transparency, loss of control, or lack of experience with technology may also give rise to resistance from election authorities and political stakeholders. Transparent governance systems, independent audits, and clear communication methods are required to overcome such opposition.

7. Conclusion

With a focus on the political environment of Bangladesh, this study explored previous research on the architectural models, cryptographic techniques, consensus mechanisms, as well as contextual applicability to explore blockchain-based secure voting systems. The literature continuously emphasized how blockchain might improve voting systems' transparency, integrity, and auditability by utilizing decentralization and cryptographic security.

The study concludes that no single blockchain design or consensus method is generally suitable for voting applications. Permissioned blockchains provide superior performance and governance control at the expense of less decentralization, whereas public blockchains prioritize openness but have scalability and privacy concerns. For blockchain-based voting systems to be effective, security, scalability, transparency, and practicality must be carefully balanced. Overall, this research emphasizes the necessity for context-aware, interdisciplinary research while highlighting the potential and challenges of implementing blockchain technology in democratic elections.

This study proposed a conceptual model with pilot implementations rather than large-scale real-world deployments. The article emphasized technical and architectural aspects with a limited discussion of political, legal, ethical, and sociocultural dimensions. In addition, the rapid evolution of blockchain technologies and regulatory frameworks may affect the long-term relevance of some findings. Although this study considered the context of Bangladesh, it does not incorporate stakeholder perspectives or empirical field data, which could provide deeper practical insights.

Future research may address the identified technical, usability, and contextual gaps. Key priorities include developing scalable, low-latency blockchain architectures, lightweight privacy-preserving cryptographic schemes, adaptive consensus mechanisms, stronger security validation, and better interoperability with existing electoral infrastructure. Further studies should also focus on human-centered interface design, accessibility, digital literacy, voter trust, and post-election usability assessment to improve public acceptance. In the context of Bangladesh, future work should investigate legal and regulatory reforms, rural infrastructure readiness, phased deployment strategies, and empirical evaluations through pilot projects and field studies. Since blockchain-based voting integrates

distributed ledgers, cryptographic protocols, and physical voting infrastructure, it should also be explored from a cyber-physical systems perspective to enhance security, reliability, and practical implementation.

Acknowledgment

The authors acknowledge the support and guidance received from Department of Computer Science and Engineering, Bangladesh University of Professionals (BUP), during the preparation of this manuscript.

Declaration of Competing Interest

The author declares that there are no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Data Availability

The data is available on request.

Funding

This research received no external funding.

AI Declaration

AI tools were used only for language refinement, grammar correction, and minor coding assistance for error fixing during manuscript preparation. They were not used for research design, experimentation, or result interpretation. All analysis, implementation, and conclusions were carried out and verified by the authors.

References

- Al-Madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. (2020, October). Decentralized E-voting system based on Smart Contract by using Blockchain Technology in *international conference on smart innovations in design, environment, management, planning and computing (ICSIDEMPC)* (pp. 176-180). IEEE.
- Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2022). DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *Journal of King Saud University-Computer and Information Sciences*, 34(9), 6855-6871.
- Ch, R., Kumari D, J., Gadekallu, T. R., & Iwendi, C. (2022). Distributed-ledger-based blockchain technology for reliable electronic voting system with statistical analysis. *Electronics*, 11(20), Article 3308.
- Chouhan, V., & Arora, A. (2023). Blockchain-based secure and transparent election and vote counting mechanism using secret sharing scheme. *Journal of Ambient Intelligence and Humanized Computing*, 14(10), 14009-14027.
- Daraghmi, E., Hamoudi, A., & Helou, M. A. (2024). Decentralizing democracy: Secure and transparent e-voting systems with blockchain technology in the context of Palestine. *Future Internet*, 16(11), 388.
- Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. *IEEE Access*, 10, 59959-59969.
- Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2023). Blockchain-based e-voting systems: a technology review. *Electronic s*, 13(1), Article 17.
- Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K. K. R. (2021). The application of the blockchain technology in voting systems: A review. *ACM Computing Surveys (CSUR)*, 54(3), 1-28.
- Islam, I., & Islam, M. N. (2023). A blockchain based medicine production and distribution framework to prevent medicine counterfeit. *Journal of King Saud University Computer and Information Sciences*, 36(1), 101851.
- Islam, I., Munim, K. M., Oishwee, S. J., Islam, A. N., & Islam, M. N. (2020). A critical review of concepts, benefits, and pitfalls of blockchain technology using concept map. *IEEE Access*, 8, 68333-68341.

- Jason C. Hung, H.-Y. J. (2022). Implementation and Early Adoption of an Ethereum-Based Electronic Voting System for the Prevention of Fraudulent Voting. *MDPI*, 16.
- Khan, E., Rahman, M. H., Mustary, S., Islam, I., & Mahmud, S. R. (2022, December). Be-voting: A secure blockchain enabled voting system. In *2022 4th International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE)* (pp. 1-6).
- Kohno, T., Stubblefield, A., Wallach, D., & Rubin, A. (2004). *Analysis of an electronic voting system*. IEEE Computer Society Press.
- Kumar, D. D., Chandini, D. V., Reddy, D., Bhattacharyya, D., & Kim, T. H. (2020). Secure electronic voting system using blockchain technology. *International Journal of Smart Home*, 14(2), 31-38.
- Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., Nuhu, B. K., Ibrahim, M. M. (2025). Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. *Cluster Computing*, 28(2), Article 132.
- Patil, H. V., Rathi, K. G., & Tribhuwan, M. V. (2018). A study on decentralized e-voting system using blockchain technology. *Int. Res. J. Eng. Technol*, 5(11), 48-53.
- Raikar, D., & Vatsa, A. (2021, July). BCT-voting: a blockchain technology based voting system. In *The 27 th International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA '21)*, July (pp. 26-29).
- Sharp, M., Njilla, L., Huang, C. T., & Geng, T. (2024). Blockchain-based e-voting mechanisms: A survey and a proposal. *Network*, 4(4), 426-442.
- Shiraj T. B., Mortuza A., Rahman K. M. A., Karim T. (2024). Non-communicable Disease Detection Based on Early Symptoms Using Machine Learning Approach Enabling Smart Healthcare Model (IoMT). *Journal of FST*, 1(1).
- Singh, A., & Chatterjee, K. (2018, September). SecEVS: secure electronic voting system using blockchain technology. In *2018 International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 863-867).

The Daily Observer. (2025, August 12). 'No vote' returns, EVM dumped: EC decides. <https://www.observerbd.com/news/538825>

The Daily Star. (2026, April 6). EC weighing fate of EVMs. <https://www.thedailystar.net/news/bangladesh/news/ec-weighing-fate-evms-4144621>

Transparency International Bangladesh. (2026, May 5). *The disposal of inactive and out-of-service Electronic Voting Machine (EVM): TIB's observations and recommendations*. <https://ti-bangladesh.org/en/articles/policy-brief/7479>

Yadav, A. S., Urade, Y. V., Thombare, A. U., & Patil, A. A. (2020). E-voting using blockchain technology. *International Journal of Engineering Research & Technology*, 9(7), 375-378.