Anusandhanvallari
Vol 2025, No.1
January 2025
ISSN 2229-3388

A Privacy-Aware Blockchain Architecture for Secure Digital Voting

[*1]Bhaludra R Nadh Singh, [*2]Kaparthi Srinivas

[*1]Professor and Head, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, Telangana, India.

[*2]Associate Professor, Department of Computer Science and Engineering, Vasavi College of Engineering, Hyderabad, Telangana, India.

Abstract—Cryptographically motivated decentralized voting has already been on the rise around the world. However, over the last decade or so there are a wide range of concerns, from centralized controls and opaque aggregation methods to the delicate balance between vote anonymity and validated outcomes. Therefore, this paper proposes a fully decentralized e-voting architecture that leverages blockchain consensus for trustworthy, privacy-preserving voting, as well as automated verification, as a potential solution to these challenges. At a high level, the proposed architecture utilizes homomorphic encryption for security-critical aggregation, smart contract and Merkle-tree audit architecture. The validation mechanism also extends to multi-factor biometric authentication (facial recognition to one-time password) using both hardware and software. The architecture is designed to be modular to allow easy deployment across multiple blockchain implementations such as Ethereum, Hyperledger, and Polygon. Some preliminary comparisons show slight performance differences between these frameworks. To test the feasibility of the new system in a real-world scenario, a proof-of-concept candidate was developed that employs a web-based voting interface, an LBPH-based facial verification pipeline, a lightweight relational store containing all needed metadata, and a custom proof-of-work blockchain for enforced one-person-one-vote constraints. The results demonstrate that basic benchmarking and advanced mechanisms such as full homomorphic voting and Multichain Performance Testing demonstrate that a decentralized and cryptographically based approach supports trustworthy e-voting.

Index Terms—Blockchain, Electronic Voting, Homomorphic Encryption, Smart Contracts, Biometric Authentication.

I. Introduction

Electronic voting has the potential to increase voter participation and facilitate election procedures, but its real-world implementation has a number of significant shortcomings, in terms of transparency, security, and public trust. Early adopters of electronic voting systems, which were often located centrally, introduced single points of failure and limited auditability to their systems, resulting in concerns about tampering, coercion, and insider manipulation. As Jafar et al. point out, many e-voting platforms remain centralized

authorities, undermining fairness, anonymity, and transparency and making them vulnerable to attacks and manipulation. Even more advanced national systems require strong national ID infrastructure and stringent administrative legal infrastructures to maintain security and trust. Some countries have shown remarkable success with digital voting nearly half of all votes cast online; yet achieving similar levels of success elsewhere remains challenging due to strong institutional and technical safeguards.

Blockchain technology may have a promising prospect for solving these problems, as its decentralized ledger design spreads authority over a large number of nodes to eliminate single-point authority and render unauthorized changes immediately discoverable via cryptographic hash linking. Its immutability and its public transparency allow for end-to-end verifiability. Any observers with access to the entire process can verify that ballots have been counted as cast. Its consensus mechanisms prevent central

corruption and manipulation. Recent surveys indicate that blockchain's core features—decentralization, immutability, and non-repudiation—constitute precisely what electronic voting systems need, namely, secure, auditable, and trustworthy systems. For example, Kim et al. show that blockchain's transparent nature enables the immediate detection of any unauthorized data modification, and decentralized consensus guarantees that an independent organization would not be able to corrupt results.

An advanced blockchain-based e-voting architecture is proposed, encompassing novel cryptographic modules such as homomorphic encryption (for secret ballots and privacy-preserving tallying), optional zero-knowledge proofs, smart contract-based vote validation, deployment to multiple chains, and cryptographic audit trails (Merkle proofs, distributed key management). To demonstrate the feasibility of the architecture, an initial prototype was designed with minimal but essential elements, including a web interface, multi-factor authentication using biometric and OTP-based

token identification, and a custom blockchain to record secure and transparent votes. Advanced modules, including smart contracts, scalability improvement and cross-chain benchmarking, are described for further integration. As such, while the full architecture is proposed, this paper implements and evaluates only the foundational components and discusses both the conceptual model and the methods and results of the prototype.

II. Literature Review

Recent research into blockchain-based e-voting demonstrates both the promise and persistent issues of the technology. Surveys and systematic reviews have consistently mentioned the positive aspects of blockchain technology (decentralization, transparency, immutability, auditability) but also the limitations (particularly in terms of privacy, scalability, usability) [1]–[3]. This technology can further electoral integrity and increase fraud reduction by eliminating single points of failure and providing an environment of tamper-evident records but achieving voter anonymity while maintaining evidence of their identity remains an important challenge [1], [4], [5].

One major issue remains that, when coupled with good cryptography, blockchain's transparency can be used to glean auditability, only if the algorithm is not optimal. To address this transparency-related issue, researchers in recent years have attempted to introduce homomorphic encryption which enables voters to be counted without having their ballots decrypted, preserving their privacy [4], [6]. The anonymous voting system developed by Kim et al., for instance, utilizes homomorphic encryption to achieve its goal (i.e., a technique whereby votes are counted on encrypted ciphertexts rather than only on encoded ballots), while preserving the anonymity of individual votes. In addition, in the case where votes are tallied on ciphertexts, they are made anonymous by virtue of their resistance to vote-reconstruction attacks [4], [7].

Smart contracts are widespread and apply to all aspects of voting (registering voters, assuring eligibility for vote, and voting) & statistical computations (by establishing an audit trail) [1], [7]. Some voting systems are experimenting with adopting biometrics (such as fingerprint or facial recognition) in addition to blockchain as a means to enhance voting ID security and discourage impersonation or multiple voting using the system [2], [3], [8]. For example, software used to verify voters' identity (through face recognition) and OTP (one-time password) authentication has been used to reduce identity fraud and facilitate system robustness [9], [10].

Although some of these advances have been made, most existing proposals are written for only part of the issue. Usually, it is either cryptographic privacy or access controls that are addressed, yet few existing proposals adequately address a complete solution that combines state-of-the-art cryptography, decentralized auditability and robust multi-factor authentication [11]. One other limitation is that performance and scalability do not get sufficiently studied. There are few studies that compare blockchain e-voting systems across different platforms (e.g. Ethereum or Hyperledger) or across diverse network conditions[12]. Cross-chain assessments and large-scale deployments are rare indeed.

In summary, the literature evidences that blockchain can offer verifiability and auditability, and that homomorphic encryption and biometrics can guarantee the secrecy of vote and voter registration, but at the same time comprehensive systems that combine all these properties and are validated across multiple blockchain platforms are still not possible [11].

III.Proposed System Architecture

The proposed architecture therefore fills these gaps by applying multiple novel modules at once into a modular system these include:

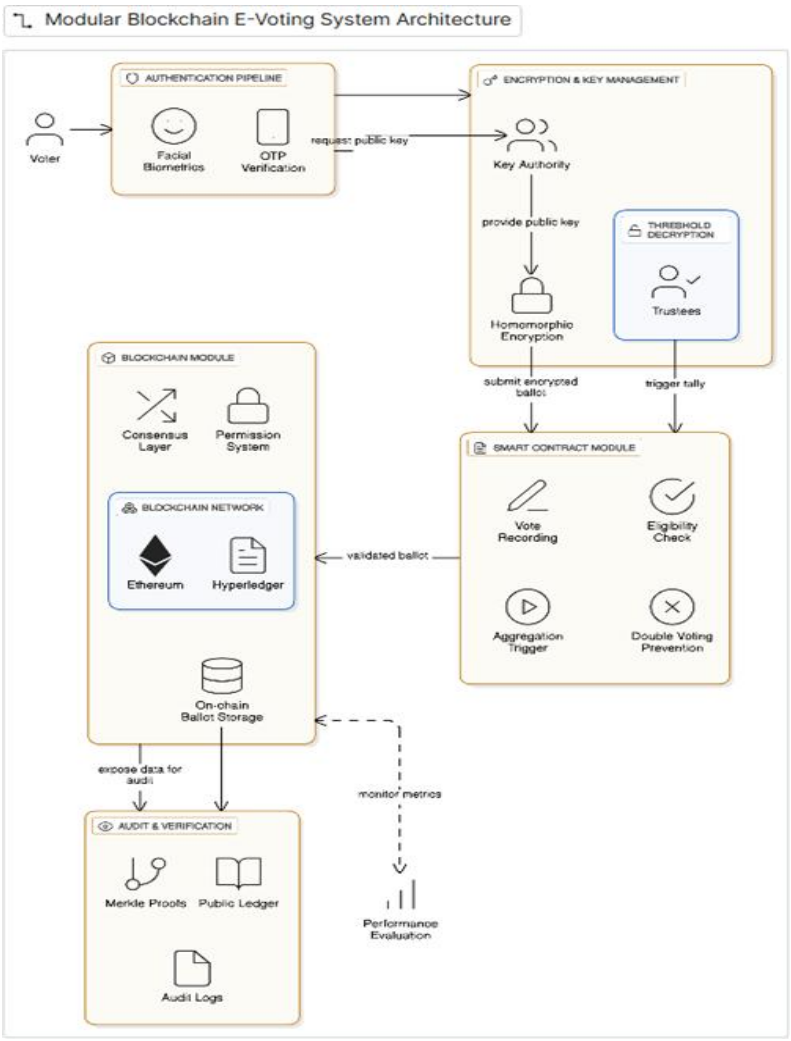

Fig. 1. Architecture diagram.

A. Blockchain Module

It implements a fully decentralized, peer-to-peer election network with ballots immutably stored on-chain (public and permissioned blockchain environments, see Ethereum, Hyperledger) based on resilience, and comparative performance analysis.

B. Smart Contract Module

This module automates vote validation, eligibility checks, and election tallying. A smart contract verifies a vote's eligibility, prevents double voting, and records the vote. At the time of the close of polls, the contract triggers homomorphic aggregation to flag a vote for totalling.

C. Encryption & Key Management

Each voter receives a public key from a distributed authority. Votes are encrypted with a homomorphic scheme (e.g., Paillier) to maintain ballot confidentiality on the public ledger. Recounting is done on encrypted votes in order to provide only the final result. A distributed threshold key management protocol divides decryption capability between trustees in order to prevent each party from decrypting any vote.

D. Authentication Pipeline

Multi-factor authentication makes voter identity verified by facial biometrics (e.g., LBPH algorithm) and OTP sent to voter's registered device. The voter can cast a vote only if both the facial biometrics and the OTP are successfully verified. This approach addresses several limitations present in many existing blockchain voting schemes.

E. Audit & Verification

The software implements cryptographic audit trails (based on Merkle proofs) to enable any observer to validate that a vote was included and counted, using logs and public ledgers, to provide transparency and support independent audits.

F. Performance Evaluation

Benchmarks are done across several blockchain networks (Ethereum, Hyperledger, etc.) to assess latency, throughput, and operational costs in order to address the lack of cross-chain performance studies in the literature.

G. Data Flow

A voter needs to sign in using a face recognition token plus an OTP. The frontend then generates an encrypted ballot and sends the encrypted ballot to the blockchain via a smart contract. The contract verifies that the voter is eligible and actually cast a ballot. Once voting is over, a homomorphic voting method is used. A distributed decryption protocol will return only the results of the votes cast. From there, privacy is maintained via the append-only ledger and cryptographic proofs. It includes a combination of advanced cryptography, decentralized auditability, and robust authentication in order to provide a scalable, secure, and privacy-preserving cryptosystem e-voting solution that addresses the key gaps identified in current research offering a more integrated and practically viable direction than what most existing systems currently achieve.

IV. Comparative Analysis

Proposed System vs. Existing Research: The proposed architecture combines the advantages of its components—blockchain transparency, homomorphic tallying, and biometric-based authentication combined with one-time password (OTP) verification—into one peer-to-peer, multi-chain platform. Existing studies have addressed individual aspects (blockchain transparency, homomorphic encryption or biometric-based authentication combined with one-time password (OTP) verification however, only a few systems could integrate all of these elements concurrently. The systems most widely published are either blockchain-centric (Ethereum or Polygon) or permission-centric (Hyperledger), a feature that allows comparative performance analysis. Additionally, the design advocates cryptographic audit trails, namely "Merkle proofs" with distributed key management being emphasized for improved verifiability.

For example, Patra et al. use smart contracts and face recognition but not homomorphic encryption (relying on centralized tallying). Umar et al. assures privacy through Paillier encryption but do not address user authentication nor multichain deployment. The proposed system addresses these gaps with homomorphic counting, automatized validation and robust multi-factor authentication under a fully decentralized framework.

Prototype vs. Similar Systems: It demonstrates a full end-to-end vote workflow and uses multi-factor authentication techniques combining biometrics (such as facial or fingerprint recognition) with OTP-based verification which is unusual for some existing prototypes. Kim et al. argue for encrypting voter information for privacy but do not present an implemented system nor address ballot-level encryption. More traditional blockchain demos of voting do not use multi-factor authentication or mention using existing blockchains; the prototype uses a custom chain to simplify the design. Performance is consistent with expectations for small custom blockchains and as such is not optimized for scalability to date, though it serves as a baseline that future studies can compare with. Compared to Saeed et al., who achieved high throughput performance on Hyperledger Fabric, Our Prototype prioritizes foundational security and auditability over raw performance.

V. Research Gaps

Despite these developments, several significant research gaps remain:

User Authentication: Many blockchain voting systems do not offer strong, end-to-end user authentication. This is due in part to the ongoing debate regarding biometric and multi-factor authentication mechanisms like facial or fingerprint recognition with OTPs. They have been widely explored but are rarely implemented fully in deployed systems [13]–[15]. To address this, the future research should focus on secure and privacy-preserving storage of biometric templates on-chain and decentralized multi-factor authentication protocols [16], [17].

Privacy vs verifiability: Blockchain's transparency can even conflict with ballot secrecy, as publicly available

ledgers easily leak details about the voters' choices if not supplemented by sophisticated cryptographic technologies [4], [18]. Homomorphic encryption and zero-knowledge proofs are known to be promising approaches for privacy-preserving tallying and transparent elections, but few systems have implemented these techniques in full implementation [4], [19]. Our architecture considers this issue in their design by planning homomorphic encryption for privacy-preserving tallies (though more work is needed in order to implement the aspects and conduct the validation on real-world prototypes).

Decentralization: A number of e-voting implementations currently depend on permissioned blockchains or centralized servers, that put in the path of decentralization at the very heart of the problem [1], [2]. Peer-to-peer election frameworks with complete decentralization with minimal reliance on central governance remain largely unproven. In practice most existing implementations still depend on some degree of system authority or trusting third party [16], [17].

Multi-Chain Evaluation: Very few studies have been published to compare the performance of e-voting between diverse blockchain platforms (e.g. Ethereum, Hyperledger, Polygon) [20]. As many previous studies rely not only on one blockchain, but assume identical load requirements for the same election [17], [21].

Total Integration: Few works have been written with an entire end-to-end e-voting, all-encompassing, architecture, with strong authentication, privacy preserving cryptography, decentralized auditability and cross-chain deployment [1], [2], [22]. Additionally, many proposals fall short at the level of simulation or partial implementations and do not include real-world validation and user acceptance tests [16], [17].

VI. Conclusion

This paper introduces a novel e-voting framework leveraging blockchain technology, emphasizing decentralization, privacy, and auditability. By employing distributed ledger tech, homomorphic encryption, and smart contracts, the suggested framework ensures vote immutability, anonymity, and verifiability. Integrating biometric verification, such as facial recognition and one-time passwords, addresses persistent gaps in robust user authentication, while cryptographic audit logs and decentralized key management uphold transparency and trust.

Although this design aligns closely with the overarching conceptual design and prototype execution, user registration, authenticated voting, and blockchain-based storage operate reliably, experimental outcomes confirm consistent performance and proper enforcement of voting rules. However, the current prototype omits homomorphic tallying and multi-chain deployment. Further improvements will prioritize incorporating advanced cryptographic components, like homomorphic encryption and zero-knowledge proofs, expanding to multiple blockchain networks, and conducting fine-grained analyses of performance and scalability. Additionally, user acceptance tests and real-world pilot studies will explore usability and trust perceptions. This study presents an initial iteration of a fully auditable, decentralized e-voting framework, suitable for nationwide elections, while acknowledging that ongoing development must address authentication, privacy, and scalability demands.

References

[1] R. Tas¸ and Ö. Ö. Tanrıöver, "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting," Symmetry, 2020.
[2] S. Tanwar, N. Gupta, P. Kumar, and Y. Hu, "Implementation of Blockchain-based E-Voting System," Multimedia Tools and Appl., 2023.
[3] B. Tang et al., "A Privacy Protection Method of Blockchain-Based E-Voting Using Homomorphic Encryption and Order-Preserving Encryption," ICAICA, 2023.
[4] H. Baniata and G. Caluna, "BP-Vot: Blockchain-Based e-Voting Using Smart Contracts, Differential Privacy, and Self-Sovereign Identities," IEEE Access.
[5] N. Indrason, W. Khongbuh, and G. Saha, "Blockchain-based Booth-less E-Voting System," in Proc. Innovative Computing and Commun., Singapore: Springer, 2021, pp. 779–788.
[6] M. J. H. Faruk et al., "Transforming Online Voting: A Novel System Utilizing Blockchain and Biometric Verification for Enhanced Security, Privacy, and Transparency," Cluster Computing, 2024.
[7] P. V. V. Satyanarayana, "Smart Contract-Based Decentralized Voting System for Transparent Elections on Ethereum Blockchain," International Scientific Journal of Engineering and Management, 2025.
[8] K. M. Khan et al., "Investigating Performance Constraints for Blockchain-Based Secure E-voting System," Future Generation Computer Systems, 2020.
[9] S. El Kafhali, Math. Probl. Eng., 2024.
[10] S. Chaudhary et al., "Blockchain-based secure voting mechanism underlying 5G network: A smart contract approach," IEEE Access, vol. 11, pp. 76537–76550, 2023.
[11] M. Chaieb et al., "DABSTERS: A Privacy-Preserving E-Voting Protocol for permissioned blockchain," in Theor. Aspects of Computing (ICTAC), Cham: Springer, 2019, pp. 292–312.
[12] K. Patidar and S. Jain, "Decentralized e-voting portal using blockchain," in Proc. 10th Int. Conf. on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2019, pp. 1–4.
[13] C. Esposito and C. Choi, "Design and implementation of a blockchain-based e-voting system by using the Algorand platform," in Proc. 38th ACM/SIGAPP Symp. on Applied Computing (SAC), ACM, 2023, pp. 715–723.
[14] U. Jafar, M. J. A. Aziz, Z. Shukur, and H. Hussain, "A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems," Sensors, vol. 22, no. 19, p. 7585, 2022.
[15] E. Bellini et al., "Designing process-centric blockchain-based architectures: A case study in e-voting as

a service," in Data-Driven Process Discovery and Analysis, Cham: Springer, 2020, pp. 1–23.
[16] N. Madhani, V. Gajria, and P. Kanani, "Distributed and anonymous e-voting using blockchain and ring signatures," in Comm. and Intelligent Systems, Singapore: Springer, 2021, pp. 839–854

AUTHOR PROFILE

Dr. Bhaludra R. Nadh Singh is working as Professor & Head, Department of Computer Science and Engineering (CSE) at Bhoj Reddy Engineering College for Women. He holds Double M.Tech degrees in Information Technology and Computer Science & Engineering and Double Ph.D. degrees in Computer Science & Engineering from State Universities, specializing in Software Engineering and Data Science with Cloud Computing and Data Mining. He has 29 years of teaching experience and has served in various academic and administrative positions with distinction. Dr. Singh is a Life Member of the Computer Society of India (CSI) and Indian Society for Technical Education (ISTE), and a member of the Institute of Electrical and Electronics Engineers (IEEE, USA). He is recognized for his contributions to engineering education, research, academic leadership, and institutional development. He has received several awards and recognitions from engineering colleges and academic organizations across Andhra Pradesh and Telangana for his contributions to technical education and academic excellence.