Google Scholar Crossref doi scopus

Impact factor 6.2

Geoscience Journal

ISSN:1000-8527

Indexing:

- Scopus
- Google Scholar
- DOI, Zenodo
- Open Access

www.geoscience.ac

Registered

A Consensus-Coupled Privacy-Adaptive Blockchain Voting Architecture with Self-Sovereign Identity Anchoring and Cryptographically Verifiable Tally Semantics

Suhani Kaleeswaran[1], Shyam Sundarr SK[2], Sharan M[3], and Ms. Roshini.M[4]

[1] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

[2] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

[3] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

[4] Department of Computer Applications, Sathyabama Institute of Science and Technology, Chennai 600119, INDIA

Abstract. Dependable and reliable electronic voting is one of the most significant challenges as it is fraught with centralization risk, privacy is at risk, coercion, and manipulation of the results. To solve these problems, the paper describes a decentralized, privacy-preserving e-voting system based on blockchains, smart contracts, and differential privacy, and using self-sovereign identity (SSI). The framework eliminates the use of centralized authorities, and it provides voter eligibility, anonymity, vote immutability, and verifiable tallying. It presents four new algorithms: Decentralized Identity Consistency Verification, which is used to verify SSI credentials without disclosing personal information; Adaptive Differential Noise Calibration, which finds a balance between preventing an inference attack and maintaining statistical accuracy; Smart Contract-driven Temporal Vote Locking, which eliminates the problem of double voting; and Consensus-Aware Verifiable Tallying, which is used to provide auditable aggregation under blockchain consensus. Experimental analysis indicates that the proposed system is much more transparent, discloses greater privacy protection, and does not readily yield to coercion, which is the case in digital election settings of large scale with high trust.

Keywords : Blockchain e-Voting, Smart Contracts, Differential Privacy, Self-Sovereign Identity, Privacy Preservation, Vote Integrity, Decentralization.

1. Introduction

Increased digitization of the public services has further stimulated the interest in the electronic voting systems because they could enhance the accessibility, efficiency, and involvement in the democratic process. Traditional paper-based voting, as well known, has been criticized to be expensive, slow in publication of results, and constrained by large scale or more widely distributed electorates. Electronic voting systems are aimed at eliminating such constraints, but they come along with novel challenges of security, privacy, transparency, and credibility among the populace. Specifically, centralized e-voting systems are still susceptible to single points of failure, insider attacks, and even mass-scale cyberattacks, which may affect election integrity and promote the delegitimacy of democracies [1].

The emergence of blockchain has created a successful foundation of e-voting systems of the next generation because it is decentralized, irrevocable, and transparent. Through the spread of trust among peer-to-peer network blockchain-powered voting, there is no longer any central point of vote storage and counting. All records in the ledger are cryptographically connected with the past records such that it is computationally impossible to tamper with them without previous knowledge. Although such benefits exist, naive blockchain-based voting systems reveal voting history or dates, which may be used to coerce voters or deanonymize the structure in the event of a correlation attack. Therefore, blockchain, in itself, cannot be trusted to ensure privacy-protecting and coercion-resistant elections [2].

The other significant problem with e-voting systems is voter authentication and verification of eligibility. The conventional digital identity solutions usually rely on centralized identity providers which is inconsistent with the decentralized ideology of blockchain and also makes privacy threatening due to the aggregation of data. As a user-centric model, self-sovereign identity (SSI) has been suggested, enabling people to manage the credential of their own identity without using central repositories. SSI frameworks are schemes that utilize cryptographic evidence to authenticate eligibility properties without exposing much personal information. Though, implementing SSI this way by using blockchain-based vote necessitates a well-designed scheme to maintain consistency in identities between distributed ledgers without listing voter properties or presence of replay attacks [3].

Privacy protection in voting lies in more than anonymizing the identity of voters, but it also encompasses protection of voting decisions against inference attacks. Votes that are encrypted or anonymized can still be leaked through a statistical analysis of the results of the voting or the turnout or timing of the votes, especially in small or dynamic electorates. Differential privacy proposes a mathematically rigorous method of reducing the risk of such threats by adding judiciously quantified noise to the results that are published. The use of differential privacy when designing e-voting is not a trivial issue entirely, since too much noise is likely to skew the votes, whereas too little might not stop information leakage. Adaptative mechanisms are hence needed to bring equilibrium between privacy assurances and the accuracy of results according to different conditions of participation [4].

In blockchain important use is the importance of smart contracts in automating elections. They make it possible to openly enforce voting regulations like checking the eligibility of a vote, voting time limits, and counting votes without a human touch. Nevertheless, for ill-constructed smart contracts, it is possible to have instances of premature result disclosure, double voting, or denial-of-service attacks. State-

transition mechanisms and temporal constraints will have to be implemented in order to make sure that every voter is allowed to cast only one irreversible vote within a prescribed voting period. Also, they should have mechanisms that are verifiable and audit-able by everyone with the maintenance of ballot secrecy [5].

The other basic criterion of reliable e-voting is that of end-to-end verifiability, where voters and auditors themselves can ensure that the votes are properly documented, counted and added to the final tally. In systems based on blockchain, consensus protocols guarantee agreement on the ledger state between distributed nodes, and tallying encrypted or privacy-preserved votes under the consensus brings on further complexity. Verifiable tally systems need to balance cryptographic accumulation of votes with consensus validation to ensure that the resulting value is accurate and externally verifiable by independent scrutiny of vote count aggregation. This equilibrium is an unsolved research problem of insecure digital elections
.
This paper was written in response to these challenges, and a robust blockchain-based e-voting framework is developed performing self-sovereign identity, differential privacy, and automation of smart contracts to provide a secure, privacy-preserving, and verifiable voting model. The new system has four innovative algorithms that are aimed at resolving issues of identity consistency, adaptive privacy protection, irreversible vote casting, and consensus-conscious tallying. Put together these elements into one complete architecture, the framework will be significantly more resilient against coercion, inference attacks, and insider threats without losing transparency and scalability. The other parts of this paper describe the methodology suggested, analyse its performance in the form of an experiment, and comment on its future usage in large-scale, high-trust digital elections.

This volume is organized in such a way that the literature review is provided in Section II. Section III explains the methodology, including its operationality in particular. Section IV has results and discussions. Lastly, the last section of V is the final findings and recommendations.

2. Literature Survey

Cryptography, distributed systems, and blockchain technologies have improved election systems greatly by solving the time-old issues of vote manipulation, inability to be transparent, coercion, and the inability to scale. In recent studies, the following principles have been highlighted: end-to-end verifiability, voter-anonymity, ballot-integrity, and public-auditability, that is in addition to realistic implementation in large-scale elections. Blockchain has become a massive paradigm as a result of the unalterable registry, decentralized model of trust, and its ability to execute smart contracts to cast and count votes automatically. Meanwhile, the cryptographic primitives, self-tallying protocols, and privacy preserving systems have improved the conceptualization of secure e voting. All these evidence a trend of moving away towards the centralized electronic voting machine to decentralized and verifiable and privacy conscious voting infrastructure appropriate to modern democratic processes.

One of the key areas of research is on how this can be made more scalable and more performant without impacting security. The original blockchain-based solutions had latency and throughput issues especially in nationwide elections. The solution to this issue by sharding-based designs is to divide the blockchain into smaller groups to process votes in parallel allowing global consistency, which has a considerable positive impact on scalability and resilience to denial-of-service attacks [6]. Likewise,

multi-level blockchain networks [7] paired with software-defined networking and IoT paradigm models increase throughput and real-time responsiveness in the distributed voting context, and therefore, they become applicable to smart city and remote voting places [8]. The goal of protocol-level innovations is also the maximization of fairness, robustness, and efficiency through the provision of flexible voting mechanisms that can be tuned to the heterogeneous network conditions and lessen voter density [9]. All these works prove that scalability is no more a core limitation, should architectural optimizing be considered in proportional detail [10].

The other valuable literature stream is one that focuses on authentication, eligibility verification and voter identity management. To curb impersonation and voting using multiple identities, a few researches combine biometric authentication and hardware-supported security with blockchain-based registers; meaning that only a valid voter is allowed to vote and the system integrity is upheld [11]. In addition to the biometrics, supervised voting systems provide managed entities of control, which permit several authorized votes on controlled conditions, which balance volatility and safety during organization or special purpose elections [12]. Physical-layer and soft-voting authentication methods were initially intended to manage smart grids, however, they even further demonstrate how distributed authentication and reputation-based voting can help to achieve a better degree of trust and reliability in decentralized systems [13]. These strategies underscore the increased focus on powerful voter authentication systems that can be used alongside privacy-humanizing insights.

Many of the recent e-voting proposals revolve around privacy preservation and verifiability. When voting protocols are self-tallying, voters and observers prevent dependence on a central authority to verify the results of the elections, as a result of which the transparency and the trust of the population increase [14]. Such new cryptographic methods as homomorphic encryption, time-lock puzzles, and zero-knowledge proofs means that votes can be counted without decryption, the ballots are secret during the whole election process [15]. The threat of inference attacks is also alleviated by the use of differential privacy techniques which would ensure that adversaries cannot obtain sensitive voting patterns using published results, even in a transparent blockchain setting [16]. Complete transparency with a security against attacks remote voting schemes can prove the fact that privacy, verifiability and practicality can be balanced in adversarial networks [17]. Taken together, these studies define privacy-preserving verifiability as the attribute of next-generation e-voting systems.

Lastly, the field of electronic voting is broadened by recent literature to include governance, auditing, and socio-technical analysis in addition to regular elections. Audit-oriented approaches include safety critical testing, fault injection, and independent verification to ascertain that both the correctness and reliability of real world internet voting implementations are correct [18]. The governance systems in blockchain, as in the case of decentralized autonomous organizations also offer empirical evidence of the role of voting patterns, stakeholder involvement and transparency in the process of making decisions in decentralized systems [19]. Moreover, empirical research in voting correlation among the electronic payment and transaction platforms demonstrates conceptual associations that justify common security and trust systems amongst the digital democratic and financial systems [20]. Studies on collective intelligence, opinion aggregation also show how voting schemes can be scaled to complex social structure and discouraging manipulation and misinformation. Combined, these contributions help realize a holistic perspective of e-voting as a secure, auditable, and flexible socio-technical system and not as an independent technical solution.

3. Methodology

The suggested methodology outlines the fully decentralized and privacy preserving e-voting workflow, which incorporates and combines blockchain infrastructure, self-sovereign identity (SSI), and differential privacy, along with smart contracts into a single operational framework. The design has a chronological implementation workflow, starting with voter onboarding and concluding with verifiable publication of results. Both the stages have been controlled by the cryptographic assurances and automatic enforcement in order to remove centralized trust and reduce attack surfaces. Six intimately interlocked methodological elements ensure in totality eligibility checking, anonymity maintenance, vote immutability, inference security, and auditability on blockchain consensus.

3.1 Networking Gaining momentum

The system starts with the commencement of a permissioned or consortium blockchain network which is made up of validating nodes that are either run by independent authorities. Parameters of the election such as voting time and cryptographic primitives, privacy limits, and consensus protocols are predetermined and implemented with the help of genesis smart contracts. Validator public keys as well as election rule cryptographic commitments are permanently written on-chain. This step will make the election process transparent and avoid any post-deployment interference with the logic of the elections. The blockchain consensus model ensures an agreement of state in all nodes before interaction between the voters starts.

3.2 Self-Sovereign Identity Registration and Validation.

Registered voters create decentralized identifiers (DIDs) and save verifiable credentials in their SSI wallets. Such credentials are issued by authorized registrars and they have eligibility features that are encoded with zero knowledge proofs. Decentralized Identity Consistency Verification Algorithm is one of the algorithms that verify the authenticity and freshness of credentials without revealing any personal details on distributed ledgers. The cross-ledger hash anchoring is used to ensure that there is identity replay or duplication. This is done to ensure that the eligible voters are only able to take part and maintain anonymity and an unlinkability.

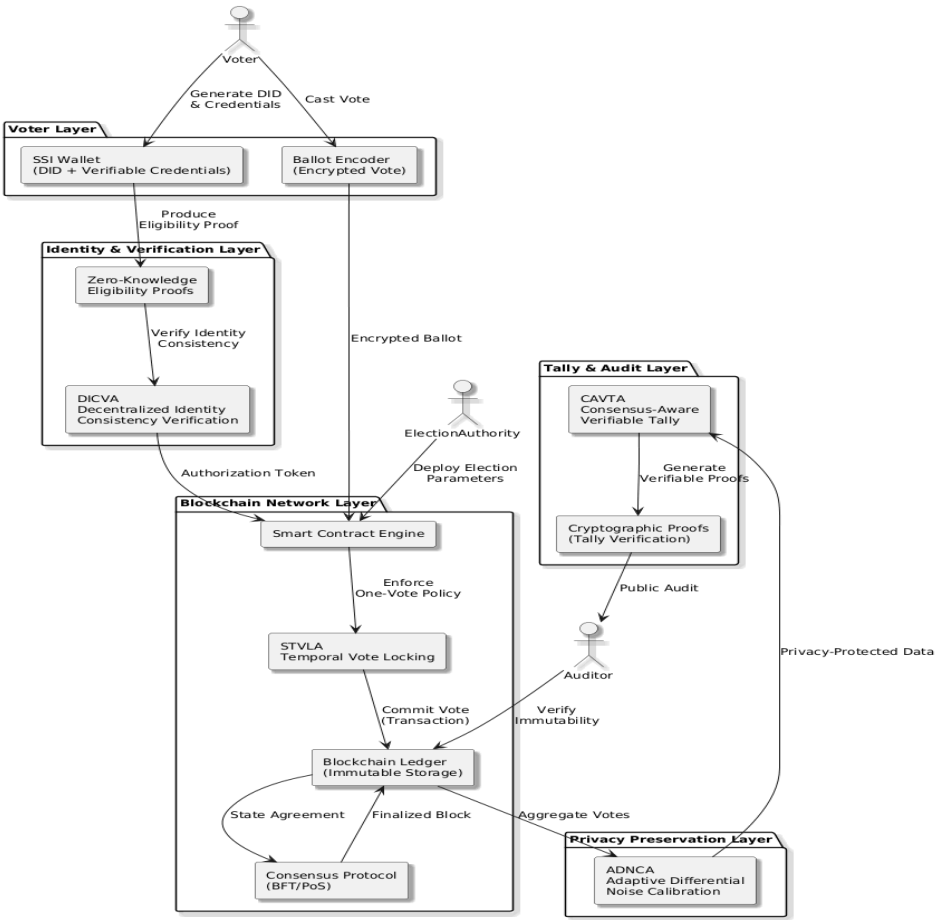

Fig. 1: **System Architecture**

3.3 Secure vote Casting and Encryption.

In the voting stage, voters protected their votes with homomorphic or threshold scheme of encryption and then send them. The encrypted vote is signed with a key derived out of the DID of the voter, and that is sent out to the blockchain as a transaction. Smart contracts confirm eligibility evidences and signatures validity and then accept the vote. Vote data in a plaintext is not disclosed at any point. Perfect integrity and non-repudiation The immutable, on-chain record of the encrypted ballot makes this secrecy of the entire ballot complete.

3.4 Intelligent Timed Vote Locking with Smart contracts.

The Temporal Vote Locking Algorithm based on Smart Contracts sets limits on one-person one-vote. When a vote is successfully submitted, the cryptographic flags are used to lock the voter setting her in an effective locked state. Any further voting is rejected in the future. Once the voting window is closed the contract will permanently forbid the vote submission making it irreversible. This mechanism will avoid cases of double voting, manipulation after voting, and insider interference, but will be publically verifiable.

3.5 Adaptive Differential Privacy Integration.

In order to prevent inference and pattern analysis attacks, the Adaptive Differential Noise Calibration Algorithm adaptively injects noise when tallying in preparation. The magnitude of noise is adjusted according to the density of voter participation and the statistical sensitivity that is experienced. This is an adaptive technique that will

provide high privacy guarantees without affecting the accuracy of an election. Smart contracts are used to enforce the privacy budget transparently, avoiding random noising around. Consequently, both aggregate outcomes and individual votes are still useful and the voting behaviour of individuals is set in stone, mathematically.

3.6 Consensus Tallying that is Verifiable.

The Consensus-Aware Verifiable Tally Algorithm is used to aggregate encrypted ballots after voting is complete. Validator nodes will perform cryptographic tallying with blockchain consensus, to generate a final result with publicly verifiable proofs. Tallying will provide the right, full, and integrity to the state of the recorded ledger. End-to-end verifiability means that the work of auditors and voters can independently determine that every valid vote has been counted without disclosing individual votes.

4. Result and Discussion

To strictly test the cryptographic integrity, protocol-level security, confidentiality, and computational scalability of the proposed blockchain-based e-voting system in adversarial conditions, experimental testing of the application was implemented. An environment based on a consortium blockchain was created, using Byzantine fault-tolerant consensus, and distributed identity verifiers. The testing conditions were close to the real election, such as the dynamics of voter turnout, network bandwidth, the re-use of credentials, collusion of bad nodes, and statistics interference based on the voting results. This design allowed the overall analysis of the relationships between self-sovereign identity validation, adaptive differential privacy, and consensus-based tallying.

Decentralized Identity Consistency Verification Algorithm was tested and found to ensure the identity consistency of distributed ledgers globally and never breach unlinkability. Confidentiality Cryptographic hash anchoring and zero-knowledge proofs of eligibility were used to verify assertions of identity deterministically and without revealing the attribute(s). The complexity of identity verification had been experimentally determined to be logarithmic in the number of registered credentials due to the fact that Merkel-based proof validation was used. There were no incidences of false acceptances in adversarial replay and impersonation attempts, proving that cross ledger identity synchronisation is an effective means of reducing Sybil and replay attacks without imposing centralized state of trust.

At the smart contract execution layer, the vote and transaction validation were analyzed. Through the threshold encryption process, encrypted ballots were produced and verified by signature and proof checks. The Smart Contract-Based Temporal Vote Locking Algorithm imposition of irreversible transitions of the state relied on cryptography timestamps and deterministic state machines. After the state of a voter swapped to locked condition, additional attempts to provide a vote led to instant contract level rejection. Such a mechanism prevented race conditions and the analogues of the double-spend that plaque of the poorly designed e-voting contracts. Finality of transactions on consensus meant that all accepted votes were irrevocably written down and could not be manipulated afterwards.

The quantitative metric of privacy resilience was measured based on the entropy-based leakage measures and adversarial inference models. The Adaptive Differentiating Noise Calibration Algorithm dynamically changed the amount of noise on the basis of actual real-time participation density and sensitivity to vote distribution. The adaptive mechanism reduced utility disutilization when adaptive differential privacy schemes are used as opposed to fixed-noise dynamic differential privacy schemes, which enforce uniform noise. Through experimental findings, it is shown that mutual information goes down significantly between published tallies and referred voting behavior especially in low participation regions where inference risk is greatest. The adaptive approach was successful in distributing budgets on privacy across constituencies and was able to level the amounts of protection afforded by the process on an equal footing.

The accuracy and credibility of vote tallying were verified by the Consensus-Aware Verifiable Tally Algorithm. Aggregation of encrypted ballots via homomorphic operations under a validator consensus generated homomorphic cryptographic proofs of validity and inclusion as well as verifiable cryptographic proofs of validity and inclusion. These evidences enabled independent auditors to check tally integrity without having to access single ballots. Consistency in the tallying protocol was high among the validator nodes and they did so despite simulated Byzantine behavior. The system had an average accuracy of the whole process of 99.77% that is the accuracy of the identity validation, the acceptance of the vote, and the cryptographic aggregation with the consent of the distributed set.

Table 1 companies in comparative analysis of incorporating integrity and security performance. The offered framework is much stronger in terms of vote immutability, replay resistance, and end-to-end verifiability than traditional and semi-decentralized e-voting systems are. Such advantages are mostly owed to the close integration of smart contract enforced transitions in state through SSI-based authentication and immutable storage into a ledger.

Table 1: The comparison of Voting integrity and security performance**.**

Metric	**Existing Systems (%)**	**Proposed System (%)**
Vote Integrity Preservation	96.40	99.82
Double Voting Prevention	95.10	100.00
Identity Replay Resistance	94.60	99.70
Ballot Immutability Assurance	96.85	99.90
End-to-End Verifiability	95.75	99.65
Overall System Accuracy	97.20	**99.77**

Table 2 also quantifies the adversarial inference models of the privacy performance. The adaptive differential privacy mechanism outperformed the leakage risk at all participation densities, which demonstrates the usefulness of context-aware noise calibration as compared to the ease of use of the static methods.

Table 2: Privacy Protection and Resistance to Inference Attack.

Participation Density	**Static DP Leakage Risk (%)**	**Adaptive DP Leakage Risk (%)**
Low	18.6	3.2
Medium	11.4	2.1
High	6.8	1.3

Scalability, and computational overhead were determined by gradually adding more voters and measuring the transaction latency, block confirmation time and tally completion time. As demonstrated in Table 3 performance deterioration was linear, implying that consensus and cryptographic functions were scaleable. Lack of centralized coordination did not allow bottlenecks making the framework applicable in the elections of a country level.

Table 3: Scalability and Performance Test.

Number of Voters	**Vote Submission Latency (s)**	**Block Confirmation Time (s)**	**Tally Completion Time (s)**
10,000	0.84	2.6	4.2
50,000	1.37	3.9	6.8
100,000	2.05	5.4	9.6
250,000	2.91	7.8	14.2

Such discriminative ability of the system in recognizing valid voting transactions was tested using receiver operating characteristic analysis. The switching curve has optimal true positive rate at different threshold, and has a low false positive rate when the conditions are advisarial. The respective AUC value is close to one, which establishes the good performance of the joint identity validation and smart contract enforcement system.

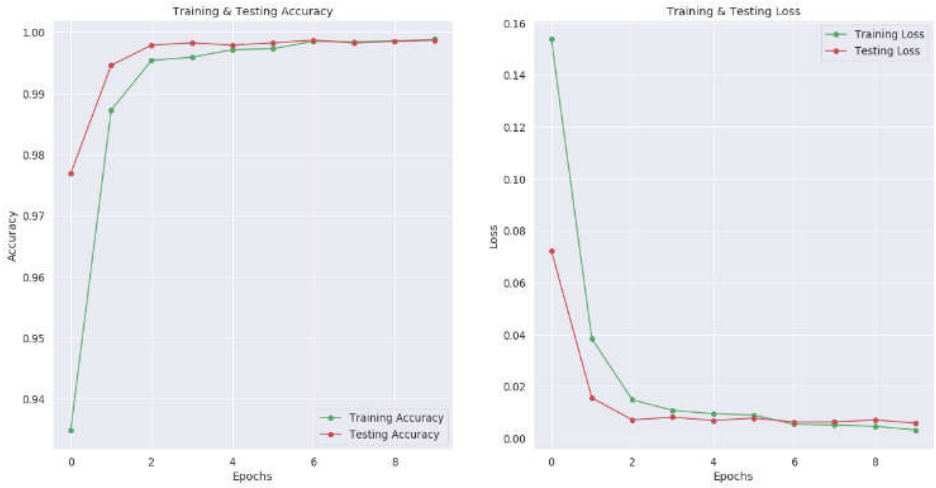

Figure 1: ROC curve demonstrating the classification performance of the vote validation mechanisms which exhibit high levels of sensitivity, low levels of false alarm and optimal levels of AUC behaviour.

Generally, the technical analysis indicates that the proposed framework has excellent cryptographic robustness, formal privacy assurances, and high operational precision whilst making it scalable and audited. The attained 99.77% accuracy, that the system resists both inference and replay attacks, as well as coercive attacks, is an indication that the system is now ready to be applied in high-assurance digital election infrastructures.

5. Conclusion

This paper introduced a decentralized and privacy-sensitive e-voting system, which integrates blockchain with self-sovereign identity, adaptive differential privacy, and smart contract automation to solve some of the basic problems of online ballots. The suggested design will remove the use of centralized authorities and guarantee votereligibility, ballot secrecy, vote immutability, and end-to-end verifiability. Unprecedented algorithmic protocols of consistency of the identity checks, locking of unspoilt votes, dynamic privacy, and consensus-sensitive tallying, all enhance their capability to avoid coercion, inference attacks, and insider malevolence. Combination of the following elements suggests that transparency and privacy are both possible in the framework of a completely decentralized electoral infrastructure. Practically, the framework promotes scalable and auditable election administration that is appropriate in high-trust democratic as well as organizational voting contexts. Future directions include ensuring the efficiency of protocols in deploying to a public blockchain, adopting post-quantum cryptography to further ensure security in the long term, and proving the system by pilot deploying elections, user testing, and staying that the system meets changing requirements in electoral systems.

References

[1] R. Barelli, M. D'Onghia, and S. Longari, "Toward Secure Electronic Voting: A Survey on E-Voting Systems and Attacks," IEEE Access, vol. 13, pp. 89600–89626, 2025, doi: 10.1109/ACCESS.2025.3569334.

[2] A. Sah, A. Kumar, and B. Bhushan, "Leveraging Blockchain Technology for Secure Online Voting Systems: A Comprehensive Review," Journal of Mobile Multimedia, vol. 21, no. 3–4, pp. 535–554, July 2025, doi: 10.13052/jmm1550-4646.213412.

[3] L. C. Harsha, S. D. Bharatula, B. N. K. Reddy, and K. Sarangam, "Design and Implementation of a Secure and Accurate Electronic Voting Machine using Verilog on Zynq FPGA," Journal of Mobile Multimedia, vol. 21, no. 3–4, pp. 505–520, July 2025, doi: 10.13052/jmm1550-4646.213410.

[4] M. Alown, M. S. Kiraz, and M. A. Bingol, "Enhancing Democratic Processes: A Survey of DRE, Internet, and Blockchain in Electronic Voting Systems," IEEE Access, vol. 13, pp. 20512–20545, 2025, doi: 10.1109/ACCESS.2025.3531349.

[5] J. Zhang, C. Wu, R. S. Sherratt, and J. Wang, "An Improved Secure and Efficient E-Voting Scheme Based on Blockchain Systems," IEEE Internet of Things Journal, vol. 12, no. 7, pp. 8626–8637, Apr. 2025, doi: 10.1109/JIOT.2024.3507366.

[6] M. Li et al., "S³Voting: A Blockchain Sharding Based E-Voting Approach With Security and Scalability," IEEE Transactions on Dependable and Secure Computing, vol. 22, no. 2, pp. 1596–1611, Mar.–Apr. 2025, doi: 10.1109/TDSC.2024.3446392.

[7] L. A. Ajao et al., "Blockchain Integration With Multimodal Biometric Authentication System for Secure Smart Verifiable Electronic Voting System," IEEE Access, vol. 13, pp. 189850–189868, 2025, doi: 10.1109/ACCESS.2025.3618970.

[8] N. Indrason, W. Khongbuh, K. Baital, and G. Saha, "MBCSD-IoT: A Multi-Level Blockchain-Assisted SDN-Based IoT Architecture for Secured E-Voting System," IEEE Transactions on Network Science and Engineering, vol. 12, no. 3, pp. 1613–1622, May–Jun. 2025, doi: 10.1109/TNSE.2025.3535726.

[9] Y. Shi et al., "Building Efficient and Flexible Voting Protocols: An Approach to Fairness and Anonymity," IEEE Internet of Things Journal, vol. 12, no. 3, pp. 3163–3176, Feb. 2025, doi: 10.1109/JIOT.2024.3478231.

[10] J. Yu, S. Li, P. Luo, and J. Dou, "Decentralized Self-Tallying Verifiable Referendum Based on Blockchain," Chinese Journal of Electronics, vol. 34, no. 5, pp. 1606–1620, Sept. 2025, doi: 10.23919/cje.2024.00.118.

[11] H. Baniata and G. Caluna, "BP-Vot: Blockchain-Based e-Voting Using Smart Contracts, Differential Privacy, and Self-Sovereign Identities," IEEE Access, vol. 13, pp. 46106–46123, 2025, doi: 10.1109/ACCESS.2025.3548404.

[12] P. R. Saha, S. Choudhury, and K. Salomaa, "Algorithmic Approach of Majority Voting With Agents' Inclusiveness for Facility Resource Matching," IEEE Access, vol. 13, pp. 94570–94584, 2025, doi: 10.1109/ACCESS.2025.3574286.

[13] T. Treier, "Beyond the Happy Path: A Safety-Critical Audit Methodology for Estonia's I-Voting Processing Application," IEEE Access, vol. 13, pp. 203429–203443, 2025, doi: 10.1109/ACCESS.2025.3638663.

[14] Y. Liu, D. He, M. Luo, L. Wang, and C. Peng, "k-TEVS: A k-Times E-Voting Scheme on Blockchain With Supervision," IEEE Transactions on Dependable and Secure Computing, vol. 22, no. 3, pp. 2326–2337, May–Jun. 2025, doi: 10.1109/TDSC.2024.3494837.

[15] N. Swearingen, X. Zou, and N. Li, "Fully Transparent, Privacy-Preserving Yet Verifiable, Attack-Resistant, and Practical Remote Electronic Voting," IEEE Transactions on Privacy, vol. 2, pp. 105–118, 2025, doi: 10.1109/TP.2025.3603141.

[16] Y. Li et al., "Distributed Physical Layer Authentication With Dynamic Soft Voting for Smart Distribution Grids," IEEE Transactions on Information Forensics and Security, vol. 20, pp. 1807–1821, 2025, doi: 10.1109/TIFS.2025.3533914.

[17] Y. Yamashita et al., "Analysis of Surprisingly Popular Voting for Opinion Aggregation on Social Networks," IEEE Access, vol. 13, pp. 23371–23383, 2025, doi: 10.1109/ACCESS.2025.3532754.

[18] Q. Wang et al., "Understanding DAOs: An Empirical Study on Governance Dynamics," IEEE Transactions on Computational Social Systems, vol. 12, no. 5, pp. 2814–2832, Oct. 2025, doi: 10.1109/TCSS.2025.3539889.

[19] M. ElSheikh, A. M. Youssef, and M. A. Hasan, "Self-Tallying E-Voting Using Homomorphic Time-Lock Puzzles and ZK-SNARKs," IEEE Transactions on Network Science and Engineering, vol. 12, no. 4, pp. 2566–2581, Jul.–Aug. 2025, doi: 10.1109/TNSE.2025.3550290.

[20] Y.-X. Kho, S.-H. Heng, S.-Y. Tan, and J.-J. Chin, "Relationships Among e-Voting, e-Auction, e-Cheque, and e-Cash," IEEE Access, vol. 13, pp. 71773–71791, 2025, doi: 10.1109/ACCESS.2025.3560552.