International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 10 October. 2026, pp:213-225 www.ijaem.net ISSN: 2395-5252

Blockchain-Based Voting on Solana A Hybrid Tamper-Proof and Transparent System for Presidential Elections

Udaw Sifon Akaniyene[(1)] Agu Edward Onyebueke[(2)] Sanfo Bala[(3)]
[(1)]*Department of Computer Science, Federal University Wukari*
[(2)]*Department of Computer Science, Faculty of Computing and Information Science, Federal University Wukari*
[(3)]*Department of Computer Science, Federal University Wukari*

Date of Submission:09-10-2026 Date of Acceptance: 22-10-2026

Abstract
The blockchain voting system provides transparency and verifiability of the electoral process; however, the computational and economic cost of ballot encryption should be further investigated. In this paper, the two-phase commit and reveal voting protocol based on the Solana blockchain technology is designed and analyzed through the comparison with a single phase plaintext voting system in order to evaluate the performance penalty associated with the cryptographic ballots commitments. The prototype has been evaluated by means of a local-validator and the Devnet testing environment of Solana blockchain with benchmarking local configurations including 10, 100, 500, and 1,000 voters. The results show that 100% transaction success ratio, the local-validator performance is around 44 to 48 transactions per second when transactions are submitted sequentially, and 94 transactions per second when the bursting test is performed. The reveal function costs approximately 16,445 computing units, which is around 15% higher than the plaintext voting transaction. The transaction fee of the two-phase vote is approximately US$0.00178 per voter according to the presented price and fee assumptions of the study. The findings quantify the computational and transaction level costs of commit-reveal voting under controlled prototype conditions. However, broader testing, stronger privacy mechanisms, and independent security evaluation remain necessary before the system can be considered for high-stakes public elections.

Keywords: blockchain voting, Solana, commit-reveal protocol, electronic voting, ballot integrity, performance evaluation, transaction cost

I. INTRODUCTION

The integrity, transparency, and verifiability of electoral processes remain fundamental requirements of democratic governance. As elections increasingly encounter concerns about manipulation, voter privacy, centralised control, and public confidence in declared results, digital technologies continue to attract attention as possible means of strengthening electoral administration. However, electronic voting systems must do more than record votes electronically. They must protect ballot integrity, prevent unauthorised alterations, preserve voter confidentiality, and provide credible evidence that the announced result reflects the votes legitimately cast. Existing research identifies these requirements as persistent challenges in the development of trustworthy electronic voting systems (Al-Maaitah et al., 2021; Huang et al., 2022; Jafar et al., 2021). These challenges become particularly significant in presidential elections, where the scale of participation and the consequences of disputed outcomes demand strong safeguards.

Blockchain technology offers an alternative approach to recording and verifying electoral transactions. Its distributed ledger, cryptographic validation, and shared record of transactions can support transparent auditing and reduce dependence on a single database administrator. Researchers have consequently investigated blockchain-based voting architectures as alternatives to conventional and centralised electronic voting arrangements (Pathak, 2021; Tanwar et al., 2024). Recent studies have also explored the use of blockchain to strengthen electoral transparency, integrity, and accountability (Bandhu et al., 2024; Chavan et al., 2024). Nevertheless, recording votes on a blockchain does not automatically guarantee ballot secrecy, eligibility assurance, resistance to coercion, or the correctness of an election. These properties depend on the complete system design, including voter authentication, ballot construction, smart-contract logic, and the procedures used to verify the final result. Blockchain voting therefore requires a careful balance between public verifiability, confidentiality, security, and operational efficiency.

The choice of blockchain platform is another important consideration. Although Ethereum has supported numerous voting prototypes,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 10 October. 2026, pp:213-225 www.ijaem.net ISSN: 2395-5252

researchers continue to investigate alternative platforms capable of processing large transaction volumes with lower latency and transaction costs. Solana provides a relevant environment for this investigation because its architecture is designed to support high-throughput transaction processing and comparatively inexpensive transactions. Previous studies have examined the scalability of blockchain-based voting applications and the implementation of voting systems on Solana (Hajian Berenjestanaki et al., 2023; Hassan et al., 2022). Other research has investigated blockchain voting architectures and their potential applications to electoral transparency and integrity (Chafiq et al., 2024; Chavan et al., 2024). These contributions establish a basis for exploring Solana as a voting infrastructure. However, the performance of the underlying blockchain is only one part of the problem. The security mechanisms implemented within a voting application can introduce additional transactions and computations that affect the overall performance of the system.

One such mechanism is the commit-reveal protocol, which separates the submission of a cryptographic commitment from the subsequent disclosure of the corresponding vote. During the commitment phase, a voter submits a cryptographic representation of a choice together with a secret value. During the reveal phase, the voter discloses the information required to verify that the revealed choice matches the earlier commitment. This separation can help prevent the direct disclosure of ballot choices during the initial submission phase and reduce opportunities for certain forms of transaction-ordering manipulation. However, its effectiveness depends on the commitment construction, secret-value handling, voter participation in both phases, and the rules governing vote acceptance. The additional phase also introduces potential costs in transaction fees, computation, latency, and throughput. Research on privacy-preserving electronic voting has explored cryptographic approaches, including zero-knowledge proofs and off-chain computation, to strengthen ballot protection while supporting verification (Mollah et al., 2021). Nevertheless, the practical cost of a particular security mechanism must be established through implementation and measurement rather than inferred from its theoretical properties.

The central problem addressed in this study is therefore the limited empirical understanding of the performance overhead associated with implementing commit-reveal voting on Solana relative to a simpler on-chain voting approach. Existing research has examined Solana voting applications, blockchain scalability, and the broader security challenges of electronic voting (Hajian Berenjestanaki et al., 2023; Hassan et al., 2022; Jafar et al., 2021; Ohize et al., 2025). However, the literature reviewed for this study does not establish a directly comparable benchmark that isolates the computational, economic, and throughput costs of a two-phase commit-reveal protocol against a functionally comparable single-phase baseline. Without such a comparison, system designers have limited empirical evidence for determining the performance cost associated with introducing this particular security mechanism. This gap is important because a voting system must be assessed not only by the protections it seeks to provide but also by its ability to process legitimate voting activity reliably and efficiently.

To address this problem, this study designs, implements, and experimentally evaluates a hybrid blockchain-based voting prototype on Solana. The proposed architecture combines on-chain vote recording with off-chain voter identity verification, while the voting process incorporates a two-phase commit-reveal protocol. A simpler plaintext voting implementation serves as the comparison baseline. The evaluation examines transaction success, computational consumption, transaction fees, throughput, and latency across different voter batch sizes. This comparative approach distinguishes the performance characteristics of the baseline implementation from the additional overhead associated with the commit-reveal mechanism. It also provides a basis for examining the relationship between ballot-protection mechanisms and the operational requirements of blockchain-based voting.

The study makes three principal contributions. First, it presents an implemented hybrid voting prototype that applies a commit-reveal protocol within the Solana environment. Second, it provides a controlled experimental comparison between the proposed protocol and a simpler voting baseline, quantifying differences in computational requirements, transaction costs, throughput, and latency. Third, it contributes empirical evidence to ongoing discussions about the design and evaluation of secure blockchain voting systems, particularly where performance and cryptographic protection must be considered together. The study's findings are intended to inform further technical research and system development rather than establish immediate readiness for deployment in a national presidential election. In particular, benchmark performance alone does not demonstrate complete voter anonymity, coercion resistance, comprehensive eligibility

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 10 October. 2026, pp:213-225 www.ijaem.net ISSN: 2395-5252

assurance, or resilience against every electoral threat. These properties require separate security analysis and broader operational evaluation.

II. RELATED WORK AND RESEARCH GAP

2.1 Blockchain Based Electronic Voting

Electronic voting using blockchains has been an area of interest for researchers because blockchains provide a shared history of transactions that can be independently audited and validated. Yet, the trustworthiness of a blockchain voting system is not only dependent on the blockchain itself. The voter verification process, ballot secrecy, rules of the election, and tallying process are also important considerations.

Jafar et al. (2021) reviewed blockchain applications in electronic voting and identified unresolved challenges involving security, privacy, and practical implementation. Huang et al. (2022) similarly examined the application of blockchain technology to voting systems, highlighting both its potential benefits and the technical issues that must be addressed. These reviews indicate that decentralised record keeping can contribute to transparency, but does not independently resolve every problem associated with trustworthy elections.

Several studies have explored blockchain voting prototypes. Hassan et al. (2022) investigated an electronic voting system using Solana, while Diaconita et al. (2023) and Diaconita and Stoica (2023) examined blockchain-based voting applications in university settings. Other researchers have investigated voting architectures that combine smart contracts with cryptographic techniques or decentralised storage. For example, Mollah et al. (2021) studied a scalable, privacy-preserving electronic voting approach based on zero-knowledge off-chain computations.

The above-stated works constitute good starting points for the development of blockchain-based voting systems. However, the findings of the research on university elections or prototypes cannot be generalized to presidential elections in a country. In fact, there are some significant differences between these types of elections in terms of verification, accessibility, coercion resistance, continuity, and massiveness of participation. The current study's system is thus considered a prototype in the technical sense.

2.2 Privacy, Integrity, and Verifiability

The choice of blockchain platform affects the cost and performance of voting operations. Solana is designed for high transaction throughput and supports on-chain programs that execute application-specific rules. These features make it a relevant platform for studying voting workloads in which many participants must submit transactions within a limited period.

Hassan et al. (2022) explored the use of Solana for electronic voting, while Chavan et al. (2024) investigated a Solana-based voting application. These studies provide context for the implementation of voting logic on Solana. More broadly, Hajian Berenjestanaki et al. (2023) examined scalability in blockchain-based electronic voting applications, underscoring the importance of evaluating performance rather than relying solely on architectural claims.

For a voting protocol, useful performance measures include transaction throughput, confirmation latency, transaction success rate, computational consumption, and transaction fees. These measures are related but not interchangeable. High throughput does not establish ballot secrecy, while low transaction fees do not establish that the system can withstand attacks or remain available throughout an election.

The current study measures these dimensions through a controlled comparison between two implementations: a single-step plaintext voting program and a two-phase commit-reveal program. The comparison is intended to estimate the additional computational and transaction costs associated with the commitment and reveal stages. Local-validator tests provide a controlled environment for comparing the programs, while Devnet tests provide a limited check of their operation on a public test network.

2.4 Research Gap and Study Contribution

Research on blockchain-based electronic voting has established a substantial foundation for improving electoral transparency, vote integrity, decentralised verification, and system security. However, the existing literature reveals an important distinction between demonstrating the potential of blockchain technology for voting and empirically establishing the performance costs associated with specific security mechanisms. Studies on electronic voting have identified verifiability, integrity, privacy, fairness, uniqueness, and accessibility as essential system requirements (Ansolabehere et al., 2008; Cortier et al., 2016; Hsiao et al., 2017; Jonker et al., 2013; Schiedermeier et al., 2019). Research on cryptographic voting has also examined zero-knowledge proofs, off-chain computation, and privacy-preserving protocols as approaches to reconciling ballot confidentiality with public

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 10 October. 2026, pp:213-225 www.ijaem.net ISSN: 2395-5252

verification (Mollah et al., 2021). Nevertheless, the implementation of these protections raises practical questions concerning computational requirements, transaction expenditure, processing speed, and system capacity.

Existing blockchain voting studies have approached these challenges from different perspectives. Research by Al-Maaitah et al. (2021), Jafar et al. (2021), Huang et al. (2022), and Ohize et al. (2025) has examined blockchain voting architectures, security requirements, limitations, and unresolved implementation challenges. Other studies have investigated the application of blockchain to electoral transparency and integrity (Bandhu et al., 2024; Chaubey et al., 2023; Jimoh, 2024; Lotito Ralli, 2022). Research has also explored the integration of biometric authentication, decentralised storage, cryptographic protection, and user-oriented interfaces into voting applications (Pillai et al., 2024; Shakir & Abdullah, 2024; Sujatha et al., 2024; Tanwar et al., 2024). Although these contributions advance the design of blockchain-enabled voting systems, their differing objectives and evaluation methods make it difficult to determine the additional computational and economic burden imposed by particular cryptographic protections.

Research on blockchain platforms and implementation architectures provides a second perspective on the gap. Solana has attracted attention because of its transaction-processing architecture and comparatively low transaction costs. Hajian Berenjestanaki et al. (2023) investigated scalability in blockchain-based voting applications, while Hassan et al. (2022) examined the implementation of an electronic voting system using Solana. Chavan et al. (2024) and Chafiq et al. (2024) also examined blockchain voting architectures and their potential to improve electoral transparency, integrity, and processing efficiency. Research using Ethereum has explored biometric authentication, smart contracts, decentralised applications, and cryptographic protection (Diaconita et al., 2023; Diaconita & Stoica, 2023; Peelam et al., 2025; Raza et al., 2025; Shaikh et al., 2025). Related contributions have addressed verifiable voting platforms and security-focused system design (Kothari et al., 2025; G et al., 2025). Collectively, these studies demonstrate continuing progress in blockchain voting architecture, but platform performance alone does not establish the marginal cost of adding a specific ballot protection mechanism.

The literature further identifies security, privacy, smart-contract reliability, and practical deployment as continuing concerns. Research on electronic voting attacks and implementation challenges highlights the difficulty of satisfying transparency, privacy, and security requirements simultaneously (Barelli et al., 2025; Rahul & Gill, 2025). Work on blockchain scalability, consensus mechanisms, and network design has examined the relationship between processing capacity, transaction latency, and system reliability (Demidov et al., 2024; Xie et al., 2023; Yakubovskiy et al., 2023; Zhang & Ibrahim, 2025). Studies of smart-contract security and development have considered vulnerability detection, programming-language design, framework selection, and upgradeability (Chaliasos et al., 2023; Negara et al., 2021; Pemerata et al., 2025; Soud et al., 2023; Tahrim Hossain et al., 2025). Meanwhile, usability research and technical guidance emphasise that security must be balanced with accessibility and understandable voter interactions (Cristiano, 2024; IACR, n.d.; KIT-Secuso, n.d.). These concerns indicate that the evaluation of a blockchain voting protocol should extend beyond its architectural description to include measurable performance, security properties, and acknowledged limitations.

The specific research gap addressed by this study concerns the empirical measurement of commit-reveal voting overhead on Solana. Commit-reveal protocols separate ballot commitment from ballot disclosure, allowing a system to verify that a revealed choice corresponds to a previously recorded commitment. However, the additional transaction phase and cryptographic computation introduce costs that must be measured rather than assumed. Although previous research has considered cryptographic voting techniques and Solana-based voting applications (Hajian Berenjestanaki et al., 2023; Hassan et al., 2022; Mollah et al., 2021; Raza et al., 2025), the literature reviewed for this study does not establish a directly comparable, controlled measurement of the computational, financial, and throughput overhead of a commit-reveal protocol on Solana against a simpler on-chain voting baseline. This is a narrower and more defensible gap than claiming that blockchain voting, cryptographic voting, or commit-reveal mechanisms have not previously been studied.

To address this gap, the study implements a commit-reveal voting program and a simpler plaintext voting baseline on Solana and evaluates their performance under comparable experimental conditions. The comparison focuses on transaction success, compute-unit consumption, transaction fees, throughput, and latency across different voter batch sizes. This approach makes it possible to distinguish the baseline processing requirements from the additional overhead associated with the two-phase

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 10 October. 2026, pp:213-225 www.ijaem.net ISSN: 2395-5252

protocol. It also provides an empirical basis for discussing the trade-offs between cryptographic protection and operational efficiency.

The study contributes in three ways. First, it provides an implemented Solana voting prototype that supports the investigation of a two-phase commit-reveal mechanism. Second, it offers a controlled comparative evaluation of the security protocol's computational and economic overhead rather than relying solely on theoretical claims about blockchain performance. Third, it provides measured evidence that can inform subsequent research into secure voting architectures, performance optimisation, and deployment planning. The findings are relevant to researchers and system designers considering high-throughput blockchain platforms for electronic voting, while recognising that benchmark performance alone cannot establish suitability for a national presidential election.

The contribution is therefore technical and empirical rather than a claim of complete electoral readiness. The prototype's performance evaluation does not, on its own, establish full voter anonymity, coercion resistance, eligibility assurance at the individual level, accessibility for all voter groups, or resilience under the political, legal, and operational conditions of a real election. These remain important requirements for future investigation. By isolating and measuring the costs associated with commit-reveal voting on Solana, the study provides a more concrete foundation for assessing the relationship between security mechanisms and system performance.

III. Methodology and System Design

3.1 Research Design

This study adopts a design science research approach supported by controlled experimental evaluation. Design science is appropriate because the research develops a technical artefact and evaluates its performance against a defined problem. The artefact consists of a Solana-based voting prototype with a commit-reveal protocol and a simpler on-chain voting implementation used as a baseline. The evaluation focuses on the additional computational and transaction costs associated with the two-phase protocol.

The research follows the core design science activities of problem identification, definition of objectives, system design and development, demonstration, evaluation, and communication of findings (Hevner et al., 2004). The experimental component compares the two voting implementations under controlled conditions and then checks their operation on Solana Devnet. This design allows the study to distinguish between the cost of the voting operation itself and the additional cost associated with cryptographic commitment and reveal operations.

The evaluation is primarily technical. It measures transaction success, confirmation latency, throughput, and compute-unit consumption. These measures provide evidence about prototype performance, but they do not independently establish the suitability of the system for a legally binding national election.

3.2 Hybrid System Architecture

The proposed system is based on a hybrid architecture that separates voter identity management from the recording and verification of votes. In the intended architecture, an off-chain component is responsible for voter registration and eligibility checks, while the Solana blockchain maintains the election state, vote commitments, and relevant tally information. A decentralised application interface provides the means through which authorised participants interact with the voting program.

This separation is intended to reduce the direct exposure of personal information on a public ledger while preserving the ability to inspect recorded transactions. However, separating identity records from the blockchain does not automatically guarantee anonymity. Transaction metadata, public keys, reveal information, and the design of the identity-verification process may still expose links between voters and their choices.

The dissertation distinguishes between the broader hybrid reference architecture and the narrower prototype used for empirical benchmarking. The measured prototype concentrates on the on-chain commit-reveal and baseline voting programs. The off-chain identity-verification layer and other production-oriented components should therefore be treated as proposed architectural elements unless their implementation is independently demonstrated.

The architecture has four principal components:

1. Voter interface: provides the interaction point for submitting voting operations.
2. Identity and eligibility layer: represents the off-chain process for checking voter eligibility and issuing or associating authorised credentials.
3. Solana voting program: enforces election states and validates the relevant vote transactions.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 10 October. 2026, pp:213-225 www.ijaem.net ISSN: 2395-5252

4. Audit and result-verification component: supports inspection of recorded transactions and the final tally.

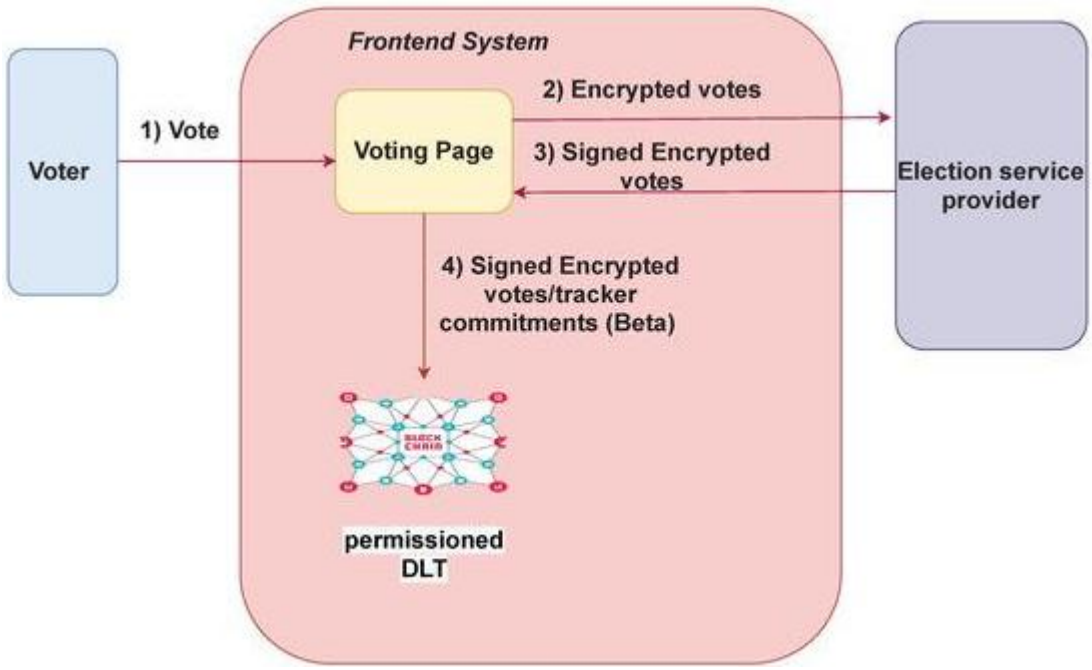

Figure 3.1 Hybrid System Architecture

The design reflects established concerns in blockchain-based voting research, particularly the need to balance integrity, verifiability, privacy, and scalability (Jafar et al., 2021; Huang et al., 2022; Mollah et al., 2021).

Table 3.1 Dataset Description

Dataset Category	Key Variables	Purpose
Voter Registration Records	Anonymised voter ID, key pair, eligibility status, region, age group	Simulates voter registration and distributes synthetic voters for testing.
Ballot Transactions	Candidate identifier, timestamp, transaction hash, digital signature, commitment and reveal data where applicable	Simulates voting transactions and their processing on the blockchain.
Network Performance Logs	Transaction success, latency, throughput, compute units, transaction fees, validator response	Evaluates the performance and resource requirements of the voting prototype.

3.3 System Analysis/Model Description

The proposed hybrid blockchain-based voting system consists of three main layers: the off-chain identity verification layer, the application interface (DApp), and the on-chain Solana blockchain. Voters register and cast ballots through the DApp, while the off-chain layer verifies eligibility and generates hashed voter identifiers. The Privacy Gateway transfers relevant data to Solana, where smart contracts record voting transactions. Solana validators process transactions using Proof of History (PoH) and Proof of Stake (PoS). An administrative and audit dashboard supports transaction monitoring, tally verification, and result auditing. The architecture separates identity information from publicly recorded voting data to support privacy and transparency.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 10 October. 2026, pp:213-225 www.ijaem.net ISSN: 2395-5252

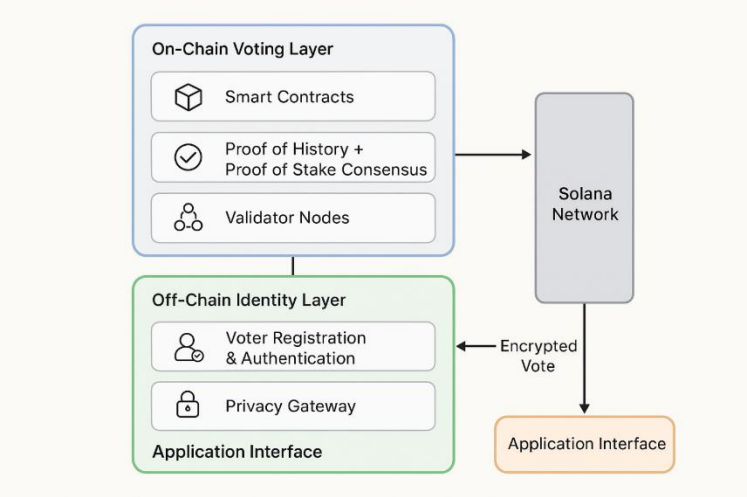

Figure 3.2 Model Description of the Proposed System

3.3.1 High Level Model of the Proposed System

The overall architecture of the hybrid blockchain-based voting platform is illustrated in Figure 2, which presents a high-level model showing the major components and the secure flow of information among them. On the left side of the figure, Voters interact with a web/mobile Decentralized Application (DApp) to register and cast their ballots. Above the DApp sits the Off-Chain Identity Verification Layer, which performs voter eligibility checks, issues cryptographic key pairs, and generates hashed identifiers. These hashed identifiers, together with encrypted ballots, pass through a Privacy Gateway depicted at the center of the diagram to ensure that no personally identifiable data enters the blockchain.

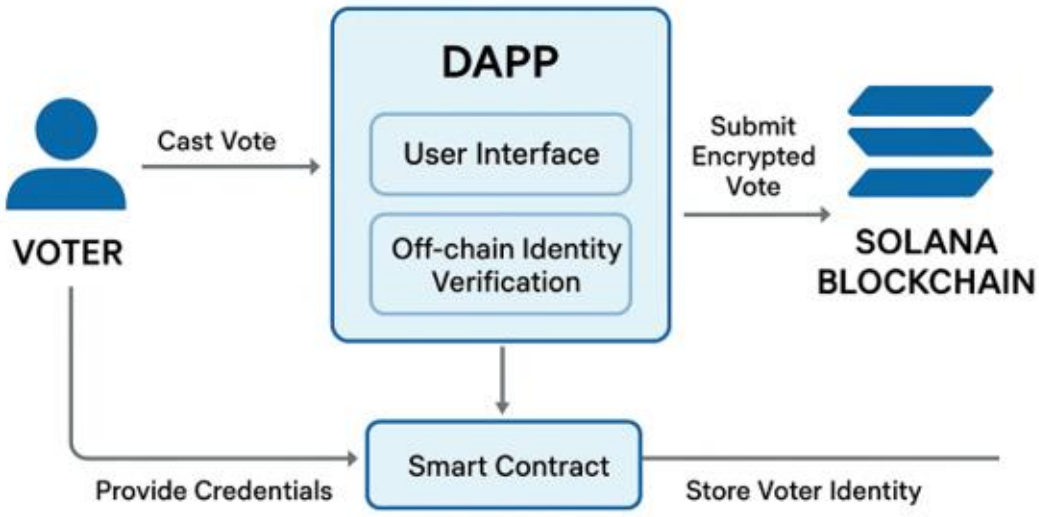

Figure 3.3 High Level Model of the Proposed System

IV. RESULTS

4.1 Compute Unit and Cost Analysis

Table 4.1 presents the compute unit (CU) consumption per transaction type, which represents the on-chain computational cost of each operation. Compute units are Solana's measure of computational work, analogous to Ethereum's gas.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 10 October. 2026, pp:213-225 www.ijaem.net ISSN: 2395-5252

Table 4.1 Compute Unit Consumption by Operation

Operation	Mean CU	vs. **Naïve** Baseline	Primary Cost Driver
Naïve CastVote	~14,300	Baseline	Account writes + validation
Commit (Phase 1)	~12,500	-12.6%	PDA creation + hash storage
Reveal (Phase 2)	~16,445	+15.0%	SHA-256 verification + tally
C-R Total (per voter)	~28,945	+102.4%	Two transactions required

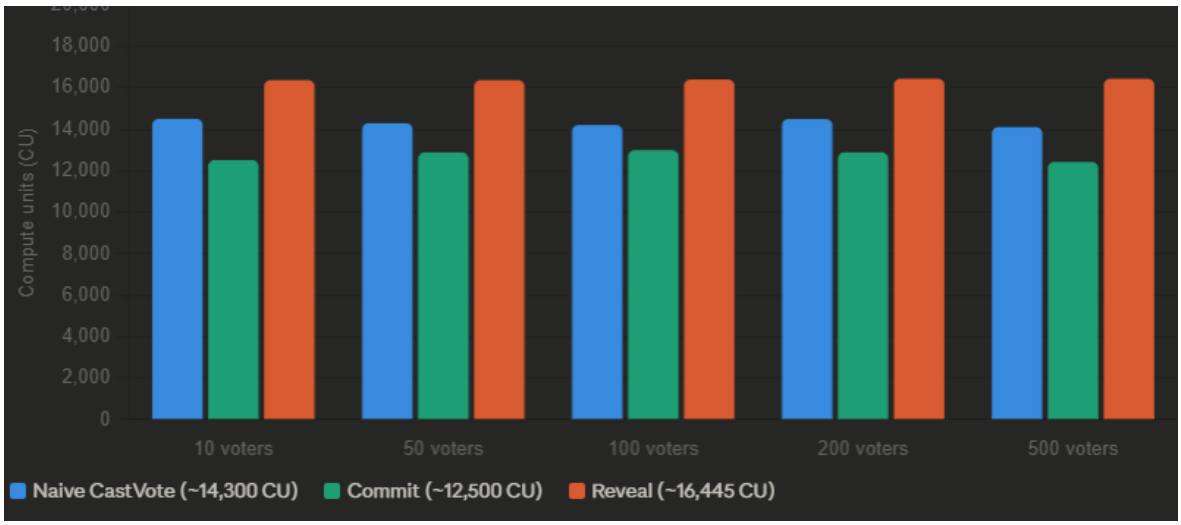

Figure 4.1 Mean cpmute units per transaction by operation type

The commit phase consumes fewer CU than the naive vote because it does not write to the candidate account (votes are not yet tallied). The reveal phase is the most computationally expensive operation at ~16,445 CU due to the on-chain SHA-256 hash recomputation and verification. The per-transaction CU overhead of the reveal versus the naive vote is approximately 15%, representing the direct computational cost of cryptographic verification. However, because the commit-reveal protocol requires two transactions per voter rather than one, the total CU cost per voter is approximately double that of the naive protocol.

4.2 Comparative Cost Analysis: Solana vs. Ethereum

To contextualize the cost efficiency of the Solana-based system, Table 4.2 compares transaction costs against Ethereum.

Table 4.2 Solana vs. Ethereum Cost Comparison for Voting Transactions

Metric	**Solana (C-R)**	**Ethereum (Low)**	**Ethereum (Congested)**
Cost per vote (tx fees)	$0.00178	$0.20	$3.71
Cost for 1M voters	$1,780	$200,000	$3,710,000
Cost for 93M voters	$165,540	$18,600,000	$345,030,000
Finality time	~0.4 seconds	~12–15 seconds	~12–15 seconds
Cost advantage	Baseline	112x more expensive	2,085x more expensive

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 10 October. 2026, pp:213-225 www.ijaem.net ISSN: 2395-5252

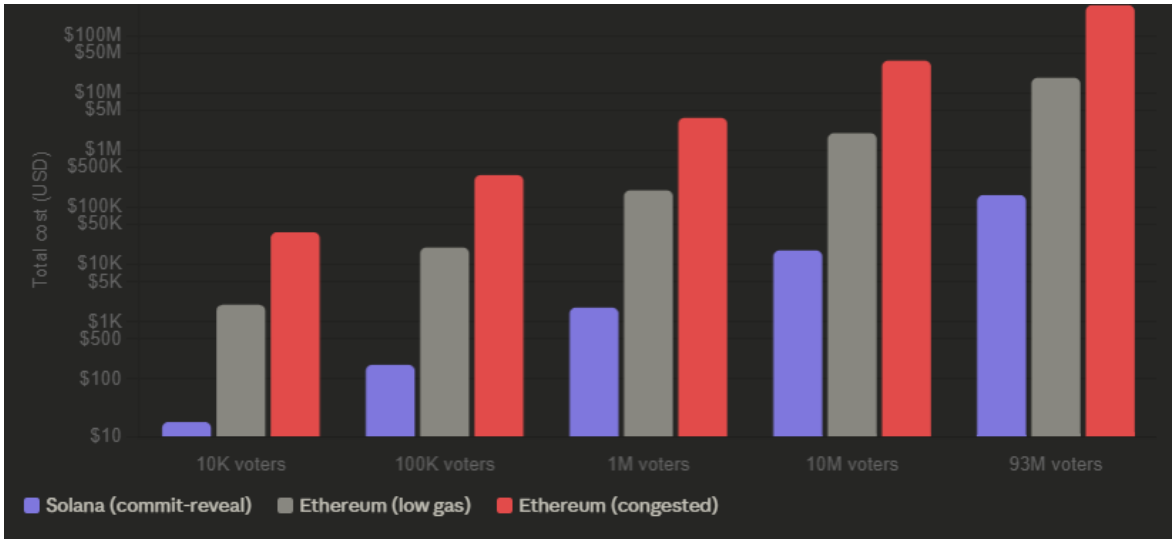

Figure 4.2 Election cost comparisom - Solana vs. Ethereum (USD, log scale)

4.3 Throughput Sensitivity Analysis

To characterize the true throughput ceiling of the system independent of artificial submission rate constraints, a stagger sensitivity experiment was conducted. The inter-transaction stagger interval was varied from 0ms (simultaneous burst) to 20ms across 200-voter batches on the local validator. Results are summarized in Table 5.

Table 5: Throughput Sensitivity to Inter-Transaction Stagger (200 Voters)

Stagger (ms)	Naive TPS	Commit TPS	Reveal TPS	Naive Lat. (ms)	C-R Lat. (ms)
0	41–79	77–94	78–91	2,511–4,757	2,113–2,586
5	79–80	80–95	69–91	1,445–1,695	1,112–1,543
10	68–80	80–96	37–80	396–775	266–846
20	47–48	28–48	47–48	269–271	261–348

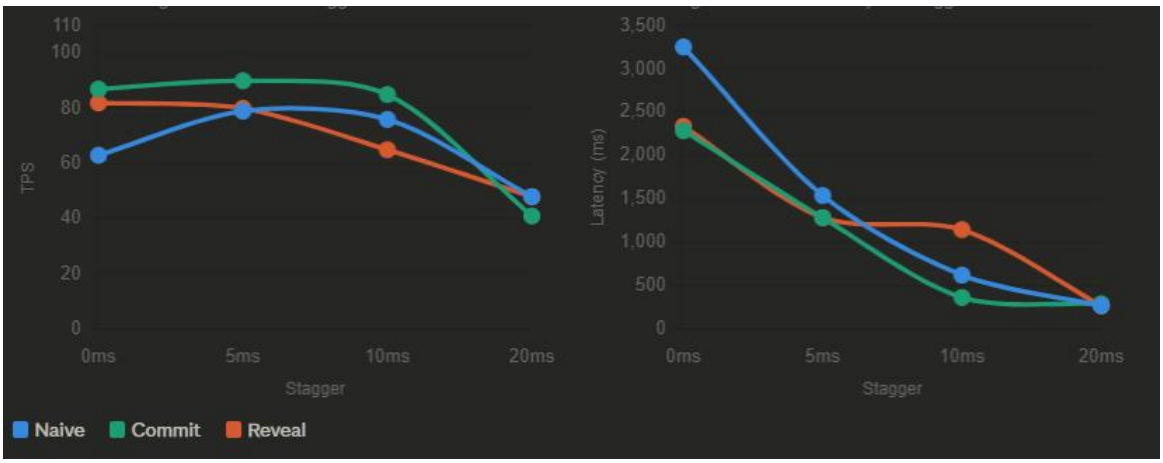

Figure 4.3 TPS vs. stagger interval & Mean latency vs. stagger interval

The zero-stagger results reveal a peak throughput of approximately 94 TPS for commit operations, demonstrating that the observed ~48 TPS with 20ms stagger is an artifact of the submission rate rather than a protocol limitation. The data also reveals a clear throughput-latency tradeoff: at 0ms stagger, high TPS is achieved at the cost of elevated mean latency (2,000–4,700ms) due to transaction

queuing, while at 20ms stagger, latency drops to approximately 270ms with proportionally lower TPS. This tradeoff is characteristic of high-throughput systems under burst load conditions.

V. DISCUSSION

The empirical results demonstrate that the proposed commit-reveal voting protocol on Solana achieves publication-grade performance metrics across multiple dimensions. The 100% success rate at 1,000 concurrent voters, sustained throughput of 44–48 TPS with 20ms stagger (peaking at 94 TPS under burst conditions), and sub-second mean latency on the local validator collectively confirm that the system can support large-scale elections within the Solana ecosystem.

The cost analysis reveals that Solana-based voting is extraordinarily economical. At current SOL prices, the commit-reveal protocol costs approximately $0.00178 per vote in transaction fees over 112 times cheaper than Ethereum at baseline gas prices and over 2,000 times cheaper during network congestion. A Nigerian presidential election with 93 million voters would cost approximately $16,554 in transaction fees, a fraction of traditional election costs.

The security overhead of the commit-reveal protocol is quantifiable and modest: a 15% increase in per-transaction compute units for the reveal phase and an approximate doubling of total transactions per voter. In exchange, the protocol provides ballot secrecy, front-running prevention, fairness (no partial results), and cryptographic vote binding properties that are entirely absent from naive on-chain voting implementations.

The Devnet validation confirms that the system functions correctly under real network conditions, with the expected latency increase (3–4x) attributable to genuine network propagation rather than protocol limitations. The 100% success rate on Devnet is significant because it demonstrates that the commit-reveal protocol's multi-phase design does not introduce fragility under realistic network conditions.

Tail latency spikes (P99 of 3,000–3,900ms) observed sporadically in both protocols at higher batch sizes are attributable to local validator memory pressure during sustained load, not to protocol-specific issues. This is evidenced by their occurrence in both the naive and commit-reveal protocols at comparable rates, confirming that they are environment-level phenomena.

VI. CONCLUSION

This research demonstrates that Solana's high-throughput, low-cost blockchain architecture provides a viable and practical foundation for implementing secure, transparent, and scalable voting systems suitable for presidential elections. The hybrid architecture separating off-chain identity verification from on-chain vote recording successfully balances the competing requirements of voter privacy and election transparency.

The commit-reveal protocol represents a significant advancement over both traditional electronic voting systems and naive blockchain voting implementations. By requiring only a 15% computational overhead per reveal transaction and maintaining throughput parity with unsecured voting, the protocol achieves strong cryptographic security guarantees at minimal cost. The empirical evidence presented in this study spanning over 150 benchmark runs across six experimental configurations, two network environments, and batch sizes from 10 to 1,000 voters provides robust support for the system's readiness for pilot deployment.

The comparative analysis against Ethereum further validates the choice of Solana, demonstrating cost savings exceeding two orders of magnitude while simultaneously offering faster transaction finality. These advantages position the Solana-based commit-reveal voting system as a technically and economically superior alternative for large-scale democratic processes.

ACKNOWLEDGEMENT

The journal organizer and the anonymous reviewers are acknowledged by the authors for their informative feedback that enhances the manuscript's substance.

REFERENCES

[1]. Al-Maaitah, S., Qatawneh, M., & Quzmar, A. (2021). E-voting system based on blockchain technology: A survey. In *2021 International Conference on Information Technology (ICIT)* (pp. 200–205). IEEE. https://doi.org/10.1109/ICIT52682.2021.9491734

[2]. Bandhu, K. C., Litoriya, R., Deo, A., Gupta, S., Satwani, R., Deshmukh, R., ... Khan, M. A. (2024). Blockchain powered e-voting: A step towards transparent governance. *International Journal of Electronic Governance, 16*(3), 354–377. https://doi.org/10.1504/IJEG.2024.142405

[3]. Barelli, R., D'Onghia, M., & Longari, S. (2025). Toward secure electronic voting: A survey on e-voting systems and attacks. *IEEE Access, 13*, 89600–89626. https://doi.org/10.1109/ACCESS.2025.3569334

[4]. Chafiq, I., Belghouti, M., & Omari, K. (2024). Blockchain-based electronic voting system for enhancing transparency and integrity: A case study in Morocco. *Journal of Information Security and Applications, 68*, 103420. https://doi.org/10.1016/j.jisa.2024.103420

[5]. Chafiq, T., Azmi, R., & Mohammed, O. (2024). Blockchain-based electronic voting systems: A case study in Morocco. *International Journal of Intelligent Networks, 5*. https://doi.org/10.1016/j.ijin.2024.01.004

[6]. Chaliasos, S., Charalambous, M. A., Zhou, L., Galanopoulou, R., Gervais, A., Mitropoulos, D., & Livshits, B. (2023). Smart contract and DeFi security tools: Do they meet the needs of practitioners? [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2304.02981

[7]. Chaubey, A., Kumar, A., Pandey, V., Bhushan, B., & Purohit, P. (2023). Leveraging secured e-voting using decentralized blockchain technology. In R. Sharma, G. Jeon, & Y. Zhang (Eds.), *Data analytics for internet of things infrastructure* (pp. 195–209). Springer. https://doi.org/10.1007/978-3-031-33808-3_15

[8]. Chavan, A., Jadhav, A., Chandre, S., Rathod, S., Bhende, R., & Patil, D. (2024). Revolutionizing voting: Blockchain-powered e-voting with Solana. In *2024 1st International Conference on Trends in Engineering Systems and Technologies (ICTEST)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICTEST60614.2024.10576075

[9]. Chavan, S., Kalbande, D., & Wagh, S. (2024). Blockchain-based e-voting system using Proof of History on Solana. *International Journal of Advanced Research in Computer Science, 15*(1), 1–8. https://doi.org/10.26483/ijarcs.v15i1.8601

[10]. Cortier, V., Galindo, D., Kuesters, R., Mueller, J., & Truderung, T. (2016). Verifiability notions for e-voting protocols [Preprint]. Cryptology ePrint Archive. https://eprint.iacr.org/2016/287

[11]. Cristiano, L. (2024). Enhancing usability in e-voting systems: Balancing security and human factors with the HC3 framework. *IRIS Institutional Research Information System*. https://cris.fbk.eu/handle/11582/346507

[12]. Demidov, A. D., Milyutin, M. A., & Xin, Y. (2024). Scalability and security in blockchain networks: Evaluation of sharding algorithms and prospects for decentralized data storage. *Mathematics, 12*(23), Article 3860.

[13]. Diaconita, V., & Stoica, M. G. (2023). Blockchain and smart contracts for voting in a university. In C. Ciurea, P. Pocatilu, & F. G. Filip (Eds.), *Education, research and business technologies* (Smart Innovation, Systems and Technologies, Vol. 321, pp. 145–156). Springer. https://doi.org/10.1007/978-981-19-6755-9_14

[14]. Diaconita, V., Belciu, A., & Stoica, M. G. (2023). Trustful blockchain-based framework for privacy enabling voting in a university. *Journal of Theoretical and Applied Electronic Commerce Research, 18*(1), 150–169. https://doi.org/10.3390/jtaer18010008

[15]. G, S. K., A, H. S., Selvarasu, P., R, K. K., M, S., & S, T. (2025). Blockchain based E-Voting system [Paper presentation]. 2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES), Coimbatore, Tamilnadu, India. https://doi.org/10.1109/ICCIES63851.2025.11032246

[16]. Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2023). An investigation of scalability for blockchain-based e-voting applications. In J. M. Machado et al. (Eds.), *Blockchain and applications: 5th International Congress, BLOCKCHAIN 2023* (Lecture Notes in Networks and Systems, Vol. 778, pp. 179-192). Springer, Cham. https://doi.org/10.1007/978-3-031-45155-3_14

[17]. Hassan, H. S., Hassan, R. F., & Gbashi, E. K. (2022). E-Voting system using Solana blockchain [Paper presentation]. 2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA), Baghdad, Iraq. https://doi.org/10.1109/ICCRESA57091.2022.10352452

[18]. Hsiao, T. C., Wu, Z. Y., Liu, C. H., & Chung, Y. F. (2017). Electronic voting systems for defending free will and resisting bribery and

coercion based on ring anonymous signcryption scheme. *SAGE Open, 7*(4), 1687814016687194. https://doi.org/10.1177/1687814016687194

[19]. Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K.-K. R. (2022). The application of blockchain technology in voting systems: A review. *ACM Computing Surveys, 54*(3), Article 60, 28 pages. https://doi.org/10.1145/3439725

[20]. Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting systemReview and open research challenges. *Sensors, 21*(17), 5874. https://doi.org/10.3390/s21175874

[21]. Jimoh, I. (2024). Assessing the role of blockchain-based voting systems in electoral processes [Unpublished bachelor's thesis]. Savonia University of Applied Sciences. https://www.theseus.fi/handle/10024/876984

[22]. Jonker, H., Mauw, S., & Pang, J. (2013). Privacy and verifiability in voting systems: Methods, developments and trends. *Computer Science Review*. https://doi.org/10.1016/j.cosrev.2013.08.002

[23]. Kothari, S., Koparde, S., Joshi, S., & Joshi, N. (2025). TrustChain: A blockchain-enabled verifiable digital voting solution for election integrity. *Ingenierie des Systemes d'Information, 30*(3), 637. https://doi.org/10.18280/isi.300308

[24]. Lotito Ralli, M. L. (2022). Is blockchain technology the future of voting? [Master's thesis, Universitat de Barcelona]. http://hdl.handle.net/20.500.14352/3221

[25]. Mollah, M. B., Zhao, J., & Niyato, D. (2021). A scalable decentralized privacy-preserving e-voting system based on zero-knowledge off-chain computations. *Journal of Information Security and Applications, 58*, 102781. https://doi.org/10.1016/j.jisa.2021.102781

[26]. Negara, E. S., Hidayanto, A. N., Andryani, R., & Syaputra, R. (2021). Survey of smart contract framework and its application. *Information, 12*(7), 257. https://doi.org/10.3390/info12070257

[27]. Ohize, H. O., Onumanyi, A. J., Umar, B. U., et al. (2025). Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing, 28*, 132. https://doi.org/10.1007/s10586-024-04709-8

[28]. Pathak, M. (2021). Blockchain based e-voting system. *International Journal of Scientific Research in Science and Technology*. https://doi.org/10.32628/IJSRST2182120

[29]. Peelam, M. S., Kumar, G., Shah, K., & Chamola, V. (2025). DemocracyGuard: Blockchain-based secure voting framework for digital democracy. *Expert Systems, 42*(2), e13694. https://doi.org/10.1111/exsy.13694

[30]. Pillai, S., Lahamage, D., Gurav, S., & Ambawade, D. (2024). Blockchain based E-Voting system on smartphones [Paper presentation]. 2024 IEEE Pune Section International Conference (PuneCon), Pune, India. https://doi.org/10.1109/PuneCon63413.2024.10895710

[31]. Rahul, G., & Gill, N. S. (2025). Articulation of blockchain enabled e-voting systems: A systematic literature review. *Peer-to-Peer Networking and Applications, 18*, Article 142. https://doi.org/10.1007/s12083-025-01956-3

[32]. Raikar, D., & Vatsa, A. (2021, July). BCT-voting: A blockchain technology based voting system. In *The 27th International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'21)* (pp. 26–29).

[33]. Raza, S. S., Khan, M. A., Shaikh, M. R., Alam, S., Talha, M., & Razzaq, E. (2025). A comparative study of blockchain-based e-voting systems: Challenges, techniques, and implementation. *Spectrum of Engineering Sciences, 3*(5), 356–372. https://sesjournal.org/index.php/1/article/view/369

[34]. Schiedermeier, M., Hasan, O., Mayer, T., Brunie, L., & Kosch, H. (2019). A transparent referendum protocol with immutable proceedings and verifiable outcome for trustless networks [Preprint]. arXiv. https://arxiv.org/abs/1909.06462

[35]. Shaikh, A., Adhikari, N., Nazir, A., et al. (2025). Blockchain-enhanced electoral integrity: A robust model for secure digital voting systems in Oman [version 2; peer review: 2 approved, 1 approved with reservations, 1 not approved]. *F1000Research, 14*, 223. https://doi.org/10.12688/f1000research.160087.2\

[36]. Shakir, S. H., & Abdullah, A. A. (2024). Next-gen voting: A blockchain-based e-voting system for fast and secure digital elections. In *2024 International Jordanian Cybersecurity Conference (IJCC)* (pp. 48–54). IEEE. https://doi.org/10.1109/IJCC64742.2024.10847284

[37]. Solana Labs. (2023). Solana whitepaper: A new architecture for scalable blockchain [White paper]. https://solana.com/solana-whitepaper.pdf

[38]. Soud, M., Hjálmtýsson, G., & Hamdaqa, M. (2023). Dissecting smart contract languages: A survey [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2310.02799

[39]. Sujatha, B., Ganesh, Y., Leelavathy, N., Tamilkodi, R., Venkatesh, S., Sandhya, B., & Kowshik, T. S. (2024). Blockchain-powered e-voting: A novel approach to secure voter authentication, online voting and election automation. *Indian Journal of Science and Technology, 17*(47), 4948–4958. https://doi.org/10.17485/IJST/v17i47.3573

[40]. Tahrim Hossain, S., Hassan, S., Bappy, F. H., Yanhaona, M. N., Zaman, T. S., & Islam, T. (2025). Bridging immutability with flexibility: A scheme for secure and efficient smart contract upgrades [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2504.09652

[41]. Tanwar, S., Gupta, N., Kumar, P., et al. (2024). Implementation of blockchain-based e-voting system. *Multimedia Tools and Applications, 83*(2), 1449–1480. https://doi.org/10.1007/s11042-023-15401-1

[42]. Xie, M., Liu, J., Chen, S., & Lin, M. (2023). A survey on blockchain consensus mechanism: Research overview, current advances and future directions. *International Journal of Intelligent Computing and Cybernetics, 16*(2), 314–340.

[43]. Yakubovskiy, A., Ivanov, V., & Petrov, D. (2023). Analyzing the scalability and security of the Solana blockchain platform. Blockchain Research Letters, 2(3), 122–134. https://doi.org/10.1016/j.blockres.2023.03.002