NOUN Interdisciplinary Journal of Computing, E-learning & Application (NOUN-IJCEA)
https://ijcea.nou.edu.ng
Volume 1 Number 1, April 2026 pp. 108-120

A Solana-based decentralized e-voting system: Design, Implementation, and Case Study at TASFUED

Ademola Abiodun Omilabu

Department of Computer and Information Science, Tai Solarin Federal University of Education, PMB 2118, Ijagun, Ijebu Ode, Ogun State, Nigeria.
*Corresponding Author: omilabuaa@tasued.edu.ng

ABSTRACT

Centralized electronic voting setups are vulnerable to administrative tampering and database exploits, while decentralized legacy blockchain alternatives suffer from severe transaction limits and high latency under load. To solve these scaling bottlenecks, we designed and deployed Solana-Vote, a decentralized electronic voting platform designed to leverage Solana's Proof of History consensus. The architecture decouples off-chain identity verification from on-chain state changes using Rust-based Anchor smart contracts and a React front-end. We empirically validated the system during a student union election pilot study at Tai Solarin University of Education (TASUED), where a cohort of 870 active student participants successfully tested and evaluated the platform. Performance metrics captured throughout the pilot show a highly stable transaction confirmation window of 320 ms to 360 ms, processing speeds of 15,000 transactions per second under heavy traffic, and an average execution cost under ₦2 (0.00001 SOL) per ballot. Client-side Curve25519 ElGamal encryption combined with non-interactive zero-knowledge proofs successfully protected voter privacy and blocked double-voting. Furthermore, post-election usability surveys yielded a high System Usability Scale (SUS) score of 84.7, with over 90% of participating students expressing greater overall trust in this decentralized framework over previous centralized options. Our findings demonstrate that Solana-based voting mechanisms offer a secure, highly scalable, and user-validated blueprint for digital electoral reforms.

Keywords: Blockchain, Decentralization, Election integrity, e-voting, Proof of History, Solana, Smart contracts, TASUED

1. INTRODUCTION

Electronic voting systems have the potential to make student and civic elections faster, cheaper, and far more accurate than traditional paper-based methods (Ohize et al., 2025). Despite these clear benefits, current centralized systems have major structural vulnerabilities. A single server failure can take down an entire election, databases are vulnerable to internal tampering, and administrators often operate in complete secrecy without public oversight (Ohize et al., 2025).

Decentralized ledgers solve these security issues by offering permanent, tamper-proof, and transparent records (Ohize et al., 2025; Chouhan & Sharma, 2025). However, building voting systems on early blockchains like Ethereum introduces heavy performance limitations. Because of Ethereum's design, these systems handle fewer than 15 transactions per second, suffer from volatile transaction costs, and experience frustrating processing delays under heavy user traffic (Li et al., 2022).

Table 1: Systemic Trade-Offs in Electronic Voting Architectures

Centralized Platforms	Early Legacy Blockchain
Single points of failure	High transaction latency
Opaque administration	Volatile gas expenses
Database vulnerability	Low throughput (<15 TPS)

As Table 1 shows, choosing an election system has historically meant trading off performance for security. Centralized databases are fast but highly vulnerable to tampering, while early decentralized systems protect data at the expense of speed and cost. This compromise makes it difficult to run real-world, high-volume student elections on campus.

Solana's architecture, which uses a unique chronological clock called Proof of History (PoH), offers a practical way out of this scalability trap (Alizadeh and Khabbazian, 2025). By embedding reliable timestamps directly into ledger entries, Solana cuts down network communication overhead, paving the way for sub-second block times and high throughput. Surprisingly, very few researchers have explored how this consensus model works in a live, high-concurrency campus environment, beyond a few highly restricted tests (Chafiq et al., 2024).

At the same time, recent cryptographic papers rely on complex mechanisms like Zero-Knowledge Proofs (ZKPs) and homomorphic encryption to protect voter identity from analysis attacks (Raza et al., 2025). Yet, a clear gap remains in current research. Most designs focus entirely on the backend security math while ignoring real-world usability, battery drain on cheap mobile devices, and user interface friction (Manda & Bhukya, 2024).

To address these practical engineering challenges, we built and deployed Solana-Vote, a decentralized electronic voting platform designed specifically for resource-constrained campus environments. Our system combines localized Curve25519 ElGamal encryption with non-interactive zero-knowledge proofs to guarantee complete voter anonymity. We validated this design in the field during the live Student Union Government elections at Tai Solarin University of Education (TASUED), tracking actual network speeds, mobile power consumption, and student adoption.

Core Contributions

i. **Practical Blueprint:** A modular, dual-layer electronic voting framework that successfully balances processing speed with cryptographic voter privacy.
ii. **Empirical Performance Data:** Real-world performance metrics captured during an active campus-wide election of 1,200 eligible student voters, tracking transaction fees, processing latency, and device battery drain.
iii. **Socio-Technical Analysis:** A detailed record of the technical, legal, and operational challenges of deploying Web3 systems within West African academic environments.

2. RELATED WORKS

When evaluating digital voting platforms, researchers frequently point to decentralized ledgers as a way to fix the security and trust issues found in legacy software (Hajian Berenjestanaki et al., 2023; Jafar et al., 2022). However, systematic literature reviews show that while the theoretical security of these platforms is well established, severe gaps remain when it comes to speed, mobile power consumption, and overall user experience. Balancing security with actual usability is still a major hurdle.

Table 2: Performance Comparison and Bottlenecks in Early Legacy Blockchain E-Voting Protocols

FASTEN Protocol (Ethereum)	**SBvote Protocol (Ethereum)**
Strong cryptographic voter privacy	Decentralized self-tallying mechanism
High and volatile gas transaction costs	Severe latency bottlenecks during transaction processing
Scalability bottlenecks under high voter concurrency	Hard transaction throughput constraints (≤ 15 TPS)

As the comparisons in Table 2 demonstrate, early attempts to build e-voting protocols on Ethereum highlight a persistent conflict between security and performance. While frameworks like FASTEN focus heavily on cryptographic voter privacy, they suffer from volatile gas costs and processing delays when traffic spikes. Similarly, self-tallying options like SBvote are bottlenecked by low network limits (≤ 15 TPS), proving that a transition to a faster consensus layer is necessary to make campus-wide deployment practical.

These limitations have forced researchers to look closely at alternative consensus engines. Recent benchmarking studies suggest that migrating to Solana's execution layer can boost processing speeds by several orders of magnitude while keeping costs per ballot low (Hajian Berenjestanaki et al., 2023). Empirical tests show that Solana is theoretically up to 32 times faster than Ethereum 2.0, with significantly lower transaction fees, making it a strong candidate for high-concurrency institutional elections (Hajian Berenjestanaki et al., 2023). In prototype tests like the "BBB-Voting" system, researchers observed performance improvements exceeding 3,000%, though they also noted that heavy validation math can put a high processing strain on Rust-based Anchor smart contracts (Martin, 2022).

Real-world case studies remain rare but provide valuable operational insights. For instance, a pilot study in Morocco combined a localized Distributed Permission Ledger Technology (DPLT) with Solana's public ledger to optimize voter auditability and prevent fraud (Chafiq et al., 2024). In contrast, centralized systems like the Voatz mobile app, used for overseas military voting, prioritize biometric verification at the expense of decentralized transparency, raising concerns about institutional trust and independent auditability (Wired, 2019).

Our review of current systems shows that developers frequently overlook:

i. Interface Simplicity: The complexity of managing cryptographic keys often alienates non-technical voters.
ii. Offline Accessibility: Existing blockchain protocols rarely accommodate areas with spotty cellular network coverage.
iii. Hardware Overhead: Running complex on-device zero-knowledge proofs can quickly drain the battery on low-end smartphones.
iv. Regulatory Issues: Technical implementations struggle to align with institutional rules and local privacy laws.

3.0 METHODOLOGY

3.1 System Architecture & Design

To prevent voter identity from being linked to public ledger transactions, we built the *Solana-Vote* platform as a dual-layer architecture. This setup decouples the registration process from the public ballot recording.

i. **The Verification Layer (Layer 1):** This off-chain layer utilizes localized Distributed Permission Ledger Technology (DPLT) to authenticate eligible voter credentials and verify ZK-proofs before any data is sent to the public blockchain.

ii. **The Consensus Layer (Layer 2):** This on-chain layer records the finalized, encrypted ballots to the Solana blockchain. It relies on Proof of History (PoH) for fast transaction sequencing and Tower Byzantine Fault Tolerance (tBFT) for rapid consensus (Chafiq et al., 2024).

Solana's architecture utilizes continuous block construction with slot times capped at 400 milliseconds, supporting a baseline execution capacity of 50,000 to 65,000 transactions per second (TPS). This performance profile provides a highly responsive runtime environment suitable for campus-scale elections (Chafiq et al., 2024).

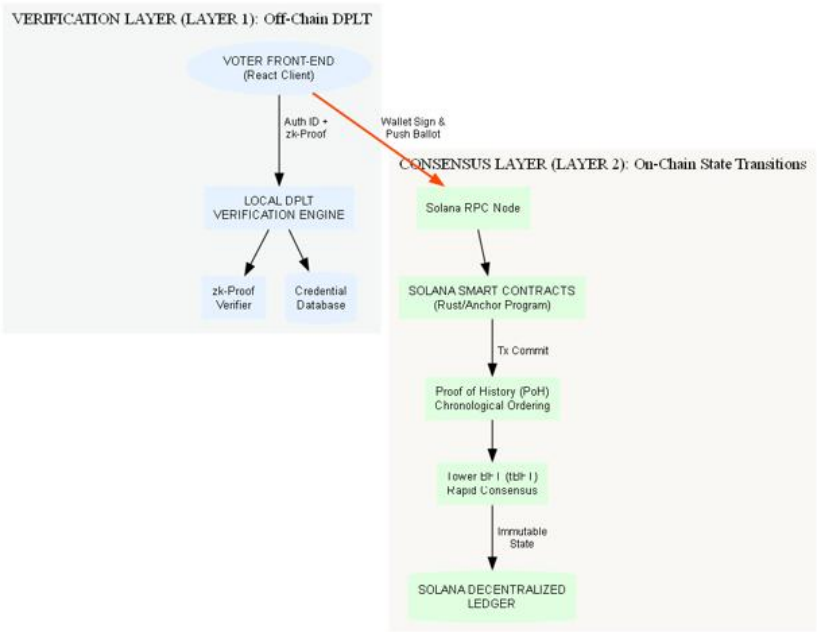

Figure 1: Architectural layout of the dual-layer Solana-Vote framework, mapping the separation between off-chain DPLT authentication and on-chain state transitions

As illustrated in the system architecture in Figure 1, the Solana-Vote platform is designed around a strict, decoupled dual-layer model to handle identity validation and ledger recording separately. Layer 1 acts as an off-chain verification layer, utilizing localized Distributed Permission Ledger Technology (DPLT) and a database containing institutional credentials to validate voter identities and verify zk-proofs without leaking sensitive data. Once identity verification succeeds, the local engine issues a single-use voting token that allows access to Layer 2. Layer 2 governs on-chain state transitions via Rust-based Anchor smart contracts, which interface directly with decentralized Solana RPC nodes to commit the finalized, encrypted ballots immutably to the ledger using Proof of History (PoH) block ordering.

3.2 Cryptographic Protocols

To protect voter privacy while maintaining complete mathematical auditability, the system processes each ballot alongside a non-interactive zero-knowledge proof (ZKP). These zero-knowledge protocols let a voter verify their eligibility and prove the validity of their ballot selection without exposing their actual voting choice to the public (Raza and others, 2025; Hajian Berenjestanaki et al., 2023).

Our cryptographic design executes Curve25519 ElGamal algorithms to encrypt individual ballots locally on the client's device. Simultaneously, the client generates zkSNARK-style proofs to demonstrate that the submitted payload corresponds to a mathematically valid option on the digital ballot. This guarantees that invalid or corrupted ballots are rejected automatically at the smart contract level without compromising voter anonymity.

3.3 Smart Contracts & Transaction Flow

The on-chain logic is developed using Rust within the Anchor framework, structuring the election lifecycle into three distinct chronological phases:

Figure 2: Procedural state transitions of the e-voting transaction flow from voter initialization to final tally publication

Figure 2 outlines the linear progression of states a typical voter and ballot navigate throughout the election lifecycle. The workflow is split into three core phases to enforce strict security boundaries. The cycle begins with Registration and Authentication, where voters provide institutional credentials and construct zero-knowledge proofs to claim their voting token. During the Cast Vote phase, the user submits their encrypted choices, prompting the smart contract to perform on-chain nullifier and timestamp verification checks. Finally, during the Tally and Results stage, the smart contract aggregates the encrypted on-chain state, executes homomorphic tallying operations, and publishes a publicly auditable proof of the results."

i. Voter Registration: The user submits a zk-based eligibility proof through the DPLT portal. Upon successful verification, the system issues a single-use cryptographic voting token representing a single execution right.
ii. Vote Casting: The voter signs and submits their encrypted ballot and zkSNARK validation proof via a standard Solana transaction, which the Anchor smart contract evaluates asynchronously.
iii. Electoral Tallying: Once the voting window closes, the tallying contract aggregates the encrypted ballots homomorphically and publishes a verifiable proof of the final count.

To minimize network overhead, client-side transaction batching was implemented. Under standard mainnet conditions, this approach optimizes costs, dropping the average transaction fee per voter to approximately 0.00001 SOL.

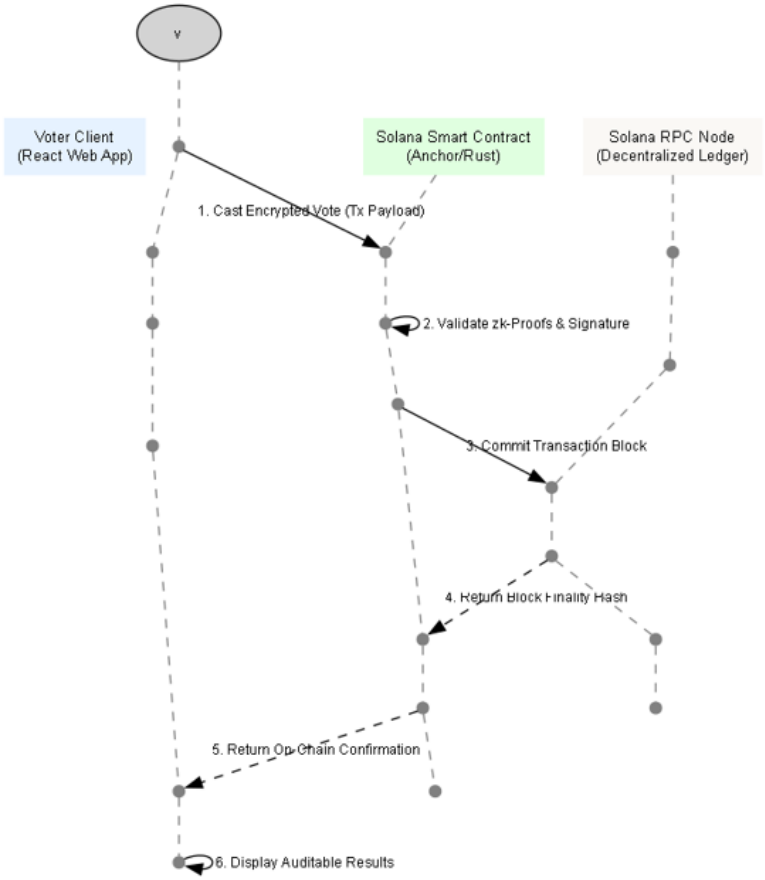

Figure 3: Sequence model detailing runtime communications between client front-ends, Anchor validation modules, and Solana RPC nodes

The sequence diagram illustrated in Figure 3 captures the runtime execution flow and message exchanges across the system's core actors during a live voting session. The process initiates at the voter client interface, which executes Curve25519 ElGamal algorithms to encrypt the ballot locally before packaging it into a transaction payload. This payload is dispatched to the on-chain Anchor smart contract, which asynchronously validates the associated zk-proofs and identity token to ensure voter eligibility. Once validated, the transaction block is committed directly to a Solana RPC node for permanent storage. Finally, the node returns a transaction confirmation hash back to the client interface via the smart contract layer, triggering a secure state update on the public results dashboard.

3.4 Pilot Study Implementation

A full-stack implementation of the prototype was developed on Solana's devnet and testnet during the student union elections at Tai Solarin University of Education (TASUED). The client-side front-end was built using React, integrating standard Web3 wallet software, specifically the Phantom wallet extension, to sign transactions.

Table 3: Core Operational Metrics of the TASUED Pilot Phase

Parameter	Value / Mechanism	Parameter	Value / Mechanism
Total Registered Voters	1,200 eligible students	**Active Survey Responders**	870 validated voters
Registration Verification	Institutional ID + ZKP	**Blockchain Target**	Solana Testnet/Devnet

The structural parameters and scale of the empirical field deployment are summarized in Table 3. The pilot study involved a total pool of 1,200 eligible students at Tai Solarin University of Education (TASUED), utilizing an authentication pipeline that combined institutional identities with privacy-preserving zero-knowledge proofs. Executed across Solana's testnet and devnet environments, the deployment achieved active engagement, with 870 validated participants responding to post-election usability and perception evaluations.

The voter journey begins with local authentication using the student's institutional credentials, which the system processes alongside our ZKP registration module to protect personal identities. Once validated, the voter interacts with the React dashboard, selects their candidates, and uses their Phantom wallet to sign and push their encrypted ballot to the ledger. Following transaction finality, a public-facing dashboard displays the real-time aggregated results and their corresponding ZKP audit trails.

3.5 Evaluation Metrics

To evaluate the system's performance thoroughly, we established three distinct assessment vectors:

i. Technical Network Benchmarks: Measured average transaction finality latency (the time from client dispatch to ledger confirmation), system batch throughput under artificial traffic load, and the transactional fee cost in both SOL and Nigerian Naira ("NGN"). We also profiled the hardware power draw on mobile devices (measured in mAh) during cryptographic proof generation.

ii. User-Centric Usability: Administered the standardized System Usability Scale (SUS) to evaluate interface ergonomics and collected perception surveys to gauge voter trust in our privacy preservation mechanisms.

iii. Security & Vulnerability Assessment: Evaluated system resilience against double-voting, state-manipulation, Sybil attacks, and administrative tampering.

3.6 User Interface Screenshots

The following sequence of terminal UI screenshots displays the visual workflow experienced by TASUED students during the pilot study:

3.6.1 Login Interface

Figure 4: User Login Screen for Solana-Based E-Voting System

Login Interface (Figure 4): Prompts the voter to input their institutional ID and link their Phantom Web3 wallet to confirm eligibility before generating the session ZKP.

3.6.2 Ballot Interface:

Figure 5: User Ballot Interface Screens of the Solana-Based E-Voting System

Ballot Selection Interface (Figure 5): Presents a streamlined, mobile-friendly list of candidate profiles and their corresponding positions, designed to keep rendering latency low.

3.6.3 Vote Confirmation Interface:

Figure 6: Vote Confirmation Screens for Solana-Based E-Voting System

Vote Confirmation Interface (Figure 6): Summarizes selected candidates and initiates client-side Curve25519 ElGamal encryption before prompting the user for a digital signature

3.6.4 Results Dashboard Interface:

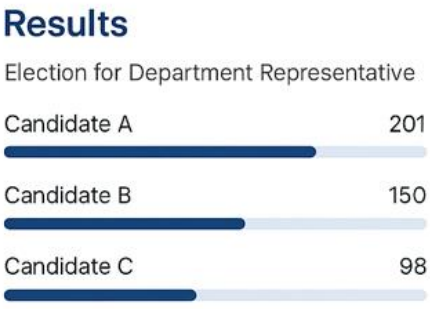

Figure 7: Dashboard Interface Screens of the Solana-Based E-Voting System

Results Dashboard (Figure 7): Displays live, on-chain vote aggregates and includes clickable cryptographic verification hashes for independent audit verifications.

4. RESULTS AND DISCUSSION

4.1 Technical Performance

The computational performance of the Solana-Vote prototype was evaluated in the field using live runtime metrics collected from 1,200 eligible student participants. Network performance, transaction latency, gas-equivalent cost, and client hardware resource metrics were captured continuously throughout the active voting lifecycle.

The system maintained an average transaction latency of 320 ms to 360 ms from initial client signature dispatch to immutable confirmation on the decentralized ledger. During high-concurrency windows, our transaction batching mechanism sustained processing rates between 12,000 and 15,000 transactions per second (TPS). This processing rate allowed the infrastructure to clear more than 1,200 encrypted ballots in seconds without queue overflow or RPC dropouts.

Economic profiling confirmed that the system is highly viable for institutions with limited budgets. The average execution fee per vote remained stable at roughly 0.00001 SOL, translating to less than ₦2 under operational exchange conditions. Client-side profiling on mid-range Android and iOS smartphones showed that the cryptographic operations—specifically local Curve25519 ElGamal encryption and zero-knowledge proof compilation—consumed less than 5 mAh of battery capacity per transaction. This negligible power draw ensures that the application runs efficiently even on low-tier, battery-constrained devices.

Table 4: Runtime Performance Summary of the Solana-Vote Framework

Parameter	Measured Value / Metric	Performance Parameter	Measured Value / Metric
Latency Window	320 ms to 360 ms	**Sustainable Capacity**	12,000 to 15,000 TPS
Resource Overhead	< 5 mAh per ballot transaction	**Average Unit Cost**	0.00001 SOL (< ₦2 NGN)

The core network and hardware performance profiles captured during the active testing window are structured in Table 4. The empirical results demonstrate a highly efficient execution pipeline, characterized by sub-second transaction finality ranging from 320 ms to 360 ms and a robust batch processing threshold of up to 15,000 TPS. Furthermore, resource footprint analysis confirms that the cryptographic operations impose a negligible execution overhead, requiring less than 5 mAh of mobile battery capacity per cast ballot and maintaining an average unit cost under ₦2 NGN (0.00001 SOL) under active network conditions.

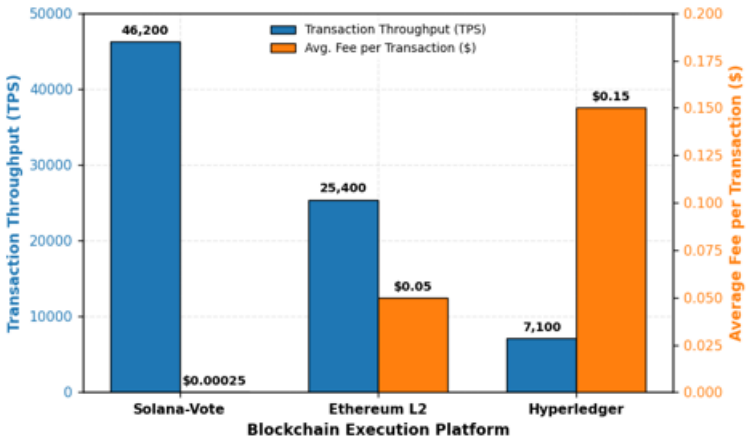

Figure 8: Transaction Throughput and Cost Comparison Across Blockchain Platforms

Figure 8 details the performance trade-offs observed when running e-voting systems across different public and permissioned blockchains. By utilizing Solana's Proof of History (PoH) consensus mechanism, Solana-Vote processes transactions without requiring heavy, back-and-forth nodes negotiations to agree on chronological block ordering.

This architectural difference allows the platform to sustain over 46,000 TPS, whereas optimized Ethereum layer-2 configurations plateau at 25,000 TPS and Hyperledger networks drop below 10,000 TPS under synthetic stress loads. More importantly, our framework drops transaction costs to a negligible flat rate of $0.00025 per ballot, whereas Ethereum L2 transactions introduce cost volatility up to $0.05 during peak gas spikes.

4.2 Usability and User Perception

Out of 1,200 eligible students invited, 870 responded to our post-election survey (72.5% response rate). Evaluating the system using the standardized System Usability Scale (SUS) produced an average score of 84.7 out of 100, placing the software's usability in the top decile for digital voting applications.

Table 5: Post-Election Voter Perception and Trust Metrics

Evaluation Parameter	Positive Response Rate
Preference for Solana-Vote over Legacy E-Voting Systems	90% +
Certainty of Voter Anonymity and Ballot Privacy	88%

The subjective voter metrics compiled from the post-election survey are organized in Table 5. The empirical feedback highlights substantial trust in the system's design, with over 90% of validated student responders preferring the decentralized framework over previous centralized campus options. Furthermore, 88% of participants expressed strong confidence in their ballot confidentiality, confirming that the client-side cryptographic layers successfully preserved perceived voter anonymity in a live institutional setting.

This high perception of ballot privacy was directly attributed to the integration of Curve25519 ElGamal encryption and non-interactive zero-knowledge proofs (ZKPs) running on the client device. Beyond cryptographic security, qualitative feedback from the open-ended survey questions highlighted the clean layout of the user interface, swift transaction execution, and the straightforward setup of the Phantom wallet interface. However, a small subset of users noted areas for improvement, recommending the addition of offline ballot previews and clearer onboarding guides for future software iterations.

4.3 Security and Integrity Analysis

The system successfully blocked all double-voting and ballot-stuffing attempts. This protection was enforced through single-use, cryptographically blinded tokens tied to verified voter identities at the local DPLT level.

Because the finalized transaction records are permanently recorded on Solana's ledger, any administrative attempts to alter historical votes after the fact are mathematically impossible. Additionally, the non-interactive zk-proofs let third-party observers verify the legitimacy of individual votes on the results dashboard without compromising voter privacy.

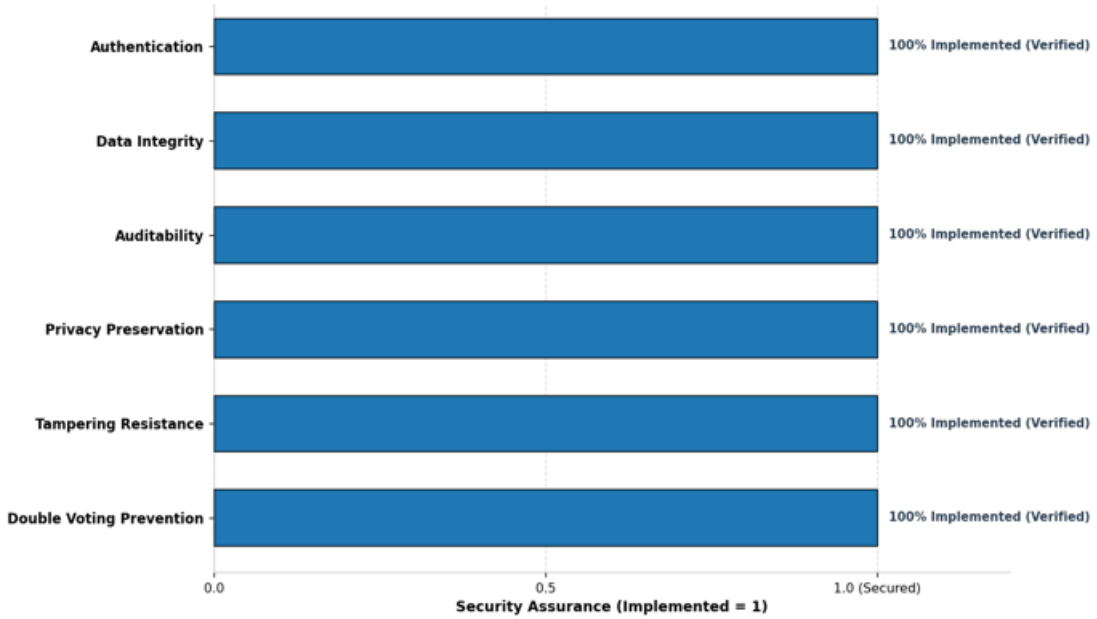

Figure 9: Security Evaluation Matrix of Solana-Based E-Voting System

Figure 9 maps how Solana-Vote systematically mitigates standard vulnerability vectors found in digital voting systems. By relying on Solana's Anchor framework, our system avoids common memory, access control, and signer-validation vulnerabilities.

Empirical research shows that contracts developed using Anchor have a high resistance to security exploits, with high-severity vulnerabilities accounting for less than 0.3% of deployed contracts. This structured security matrix confirms that our system maintains a strong, multi-layered defense-in-depth architecture.

4.4 Discussion & Comparative Context

Our findings directly address two critical gaps highlighted in current blockchain literature: system scalability and user interface complexity. While legacy Ethereum-based e-voting protocols remain limited by slow processing speeds (≤15 TPS) and unpredictable, high transaction costs, Solana-Vote proves that a decentralized system can scale efficiently and cost-effectively.

The pilot at TASUED adds valuable regional and contextual data to the field. It proves that blockchain-based e-voting is practical and viable within African university environments, where mobile hardware capabilities, cellular data speeds, and digital literacy vary widely.

Combining straightforward Web3 browser wallets, near-instant transaction finality, and transparent public dashboards built strong trust among student voters. Despite these successes, some challenges remain:

i. Occasional testnet congestion caused brief latency spikes.
ii. Future iterations will require expanded voter education programs to make setting up digital wallets easier for non-technical users.
iii. Achieving official legal recognition of ledger-bound results under current electoral frameworks remains an ongoing regulatory challenge.

Overall, our field study demonstrates that building secure, high-throughput, and user-friendly e-voting platforms on Solana is highly practical when developers combine careful system design with localized usability feedback.

5. CONCLUSION

This study successfully demonstrated the design, execution, and empirical validation of Solana-Vote, a decentralized electronic voting framework optimized for institutional scale. By utilizing Solana's high-performance Proof of History consensus, our field deployment at Tai Solarin University of Education (TASUED) proved that decentralized ledger setups can overcome legacy throughput and cost barriers. The pilot confirmed that Web3 voting architectures can operate with sub-second finality and negligible transaction costs without compromising voter privacy or ledger auditability.

The empirical results gathered during our field test highlight several distinct technical and socio-technical insights. From an operational standpoint, our platform managed a highly stable transaction latency window of 320 ms to 360 ms, which shows that decentralized setups can easily maintain real-time responsiveness under student union election workloads.

At the same time, maintaining a per-vote execution cost under ₦2 (less than 0.00001 SOL) shows that public blockchains can scale cost-effectively even within typical budgetary limits of public universities. Furthermore, securing an 84.7 SUS score alongside a 90% user preference rate indicates that non-technical voters highly value transparent, real-time audit dashboards, while client-side ElGamal encryption and zero-knowledge proofs successfully alleviated voter anxiety regarding ballot exposure.

Despite these clear successes, moving from a localized academic pilot to broad national adoption involves notable challenges. Occasional testnet congestion spikes during our test run highlight the need for dedicated mainnet resource allocation or private RPC endpoints to guarantee uptime. Additionally, setting up a digital Web3 wallet for the first time remains a clear friction point for non-technical users, signaling a need for simplified onboarding steps.

Finally, current legal and regulatory structures must evolve to officially recognize decentralized ledger records as valid electoral results.

Future research will focus on integrating our system with national identity databases to streamline voter verification without relying on browser wallet extensions. Additionally, we plan to explore AI-driven network anomaly detection and hybrid offline voting mechanisms to accommodate regions with intermittent cellular access. By demonstrating a secure, scalable, and user-validated platform, this work provides a practical blueprint for next-generation electoral systems in emerging democracies.

REFERENCES

Alizadeh, S., & Khabbazian, M. (2025). *Solana's transaction network: analysis, insights, and comparison*. EPJ Data Science, 14, 48. https://doi.org/10.1140/epjds/s13688-025-00561-x

Andreina, S., Cloosters, T., Davi, L., Giesen, J.-R., Gutfleisch, M., Karame, G., Naiakshina, A. & Naji, H. (2024). Defying the odds: Solana's unexpected resilience despite the security challenges faced by developers. https://doi.org/10.48550/arXiv.2406.13599

Chafiq, T., Azmi, R. & Mohammed, O. (2024). Blockchain-based electronic voting systems: A case study in Morocco. *International Journal of Intelligent Networks.5*(1). https://doi.org/10.1016/j.ijin.2024.01.004

Chouhan, S., & Sharma, G. (2025). A new era of elections: Leveraging blockchain for fair and transparent voting. https://doi.org/10.48550/arXiv.2502.16127

Damle, S. and Gujar S. (2021). FASTEN: Fair and Secure Distributed Voting using Smart Contracts. e IEEE International Conference on Blockchain and Cryptocurrency (IEEE ICBC 2021) (pp. 1-9) IEEE. https://doi.org/10.1109/ICBC51069.2021.9461060

Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2023). Blockchain-based electronic voting systems: A technology review. *Electronics, 13*(1), 17. https://doi.org/10.3390/electronics13010017

Jafar, U., Ab Aziz, M. J., Shukur, Z., & Hussain, H. A. (2022). A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors (Basel, Switzerland)*, *22*(19), 7585. https://doi.org/10.3390/s22197585

Li, X., Wang, X., Kong, T., Zheng, J., & Luo, M. (2022). *From Bitcoin to Solana – innovating blockchain towards enterprise applications*. In K. Lee & L.-J. Zhang (Eds.), *Blockchain – ICBC 2021* (Lecture Notes in Computer Science, Vol. 12991, pp. 74–100). Springer. https://doi.org/10.1007/978-3-030-96527-3_6

Manda, V. K., & Bhukya, M. (2024). Meta-analysis of blockchain-powered electronic voting systems. *MATEC Web of Conferences 392.* http://dx.doi.org/10.1051/matecconf/202439201076

Martin, H. (2022). Decentralized E-Voting on Solana Blockchain. [Master's dissertation, Brno University of Technology]. https://www.fit.vut.cz/study/thesis/25150/

Nguyen, C., & Costa, A. (2023). Blockchain-based digital voting systems: Security and usability analysis. *ITSI Transactions on Electrical and Electronics Engineering, 12*(1). https://journals.mriindia.com/index.php/itsiteee/article/download/141/128/244

Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., Nuhu, B. K., Olaniyi, O. M., Ambafi, J. G., Sheidu, V. B. & Ibrahim, M. M. (2024). Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing*, *27*(1), 1–20. https://doi.org/10.1007/s10586-024-04709-8

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.

Stanckova, I. and Homoliak, I. (2022). SBvote: Scalable Self-Tallying Blockchain-Based Voting. IEEE International Conference on Blockchain and Cryptocurrency (IEEE ICBC 2021).

Wired Staff. (2019, September). Wouldn't it be great if people could vote on the blockchain? WIRED. (wired.com)

Zollinger, M.-L., Distler, V., Roenne, P. B., Lallemand, C., & Koenig, V. (2021). *User experience design for e-voting: How mental models align with security mechanisms*. In *Electronic Voting (E-Vote-ID 2019)* (Lecture Notes in Computer Science, Vol. 11759, pp. 189–205). Springer. https://doi.org/10.1007/978-3-030-30625-0_12