A Scalable and Verifiable Blockchain-Based E-Voting Framework for Transparent, Secure and User-Centric Democratic Elections

S. Kannadhasan[1], Pilli Lalitha Kumari[2], R. V. Kavya[3], M. Sugamathi[4], Vignesh V.[5] and M. Soma Sabitha[6]

[1]*Department of Electronics and Communication Engineering, Study World College of Engineering Coimbatore - 641 105, Tamil Nadu, India*

[2]*Department of Computer Science and Engineering, Visakha Institute of Engineering & Technology, 88th Division, Narava Visakhapatnam - 530027 Andhra Pradesh, India*

[3]*Department of Electronics and Communication Engineering, J.J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India*

[4]*Department of MBA, Department of Management Studies, Nandha Engineering College, Vaikkalmedu, Tamil Nadu, India*

[5]*Department of CSE, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India*

[6]*Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad-500043, Telangana, India*

Keywords: Blockchain Voting, Electoral Integrity, Decentralized Identity, Secure e-Voting, Verifiable Elections.

Abstract: All measures toward safeguarding the sanctity and transparency of the elections are essential for strengthening democracy. This study presents a scalable and verifiable blockchain e-voting framework that overcomes existing e-voting systems' issues including high computation overhead, lack of usability, low level of transparency, and low legal compliance. In contrast to prior art, the present model leverages light-weight cryptographic algorithms, decentralized identity checks and open-source model to provide a secure, privacy preserving and user-friendly voting. The system provides real-time auditability, end-to-end verifiability, and resistance to coercion and vote manipulating attacks with efficiency and adaptability to multiple deployment scenarios. Through extensive simulations and prototyping on blockchain testnet, the designed system achieves high throughput, low latency and is abiding by regulatory constraints, thus laying a solid foundation for the trusted and transparent democratic process in the digital era.

1 INTRODUCTION

The quality of democracy depends on the integrity, transparency, and inclusiveness of the election process. Nonetheless, paper ballots-based as well as electronic voting systems (EVMs) are being seen with great suspicion due to serious issues of corruption and the lack of transparency, manipulation of votes, delayed counting of votes and just the fact that it is not feasible for underprivileged or remote voters to access these systems. Demand for the secure and verifiable online vote has been growing in recent years, particularly due in part to challenges such as international instability and technical trends that are causing civic infrastructure to go digital at a faster pace.

Blockchain, as it is decentralized and immutable and can be easily verified, provides an ideal solution to transform the way elections are held. But a variety of blockchain-based voting systems sting from numerous weaknesses such as high computational complexity, proprietary limitations, inadequate real-world implementation, and unfriendly for voters to use. These factors are a roadblock to mass adoption and lowers the trust in digital voting.

This paper fills these gaps by proposing a new e-voting framework that leverages blockchain to achieve scalability, user friendliness, transparency, and legal suitability. It leverages state-of-the-art cryptographic technology, decentralized identity systems, and open source software to enable secure, privacy preserving, and anonymous participation for eligible voters at scale. Furthermore, the infrastructure provides for real-time auditability and resistance to coercion, thus enabling it to serve national elections as well as decentralized organization voting.

Kannadhasan, S., Kumari, P. L., Kavya, R. V., Sugamathi, M., V., V. and Sabitha, M. S.
A Scalable and Verifiable Blockchain-Based E-Voting Framework for Transparent, Secure and User-Centric Democratic Elections.
DOI: 10.5220/0013931800004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 5*, pages 486-492
ISBN: 978-989-758-777-1

In this way, the paper contributes to the academic debate on secure e-governance and has a deployable and practical solution that future democracies could use to innovate the election system, in order to restore the public trust in the election process.

2 PROBLEM STATEMENT

Although huge strides are made in electronic voting systems, preserving the integrity, transparency and robustness of the electoral process in general is still a major global challenge. Legacy voting models are susceptible to manipulation, are not auditable in real time, and offer poor accessibility, which can be particularly problematic in remote or crisis areas. Additionally, most of the current blockchain voting systems are computationally expensive, have complex user interfaces, lack strong user anonymity due to the use of KYC-adhering blockchains and even go as far as enforcing proprietary constraints that diminish public trust and verifiability. These constraints restrict the scalability, reduce the participation rate, and prevent wide government and corporate election adoption.

What is required is a decentralized, secure, and natural e-voting platform to address these technical and useability challenges, and that simultaneously provides legal and regulatory compliance. A good solution should provide end-to-end verifiability, be immune to vote rigging or coercion, respect voter privacy but give immediate visibility on the votes. Tackling these fears is vital for the definition of a digital voting system that can enable the democratic process in the digital age.

3 LITERATURE SURVEY

As a result of the advancement of voting technologies, there has been an increasing focus on blockchain for the purpose of increasing transparency and trust within elections. Some researchers have investigated this fusion, and proposed different architectural constructions to cope with it.

Chouhan and Sharma (2025) developed a conceptual blockchain driven model for conducting elections with focus on transparency and fairness. Their measurements were not validated in practical voting scenarios. Similarly, Russo et al. (2021) proposed a secure blockchain voting framework (Chirotonia) based on linkable ring signatures that presented its potential to improve voter anonymity, but it incurred performance overhead in the scalability experiments.

A distributed voting system (FASTEN) has been recently proposed by Damle, Gujar and Moti (2021), thus it is system that uses smart contract, consequently, the implementation for obligation verification is based on Ethereum by considering that Ethereum can ensure the security and the correctness. Despite some novelty in their work, they did not quite solve the issues of voter authentication and real-time auditability. To address privacy issues, Kim et al. (2021) combined homomorphic encryption with a blockchain, but their system was too computation-expensive to be applicable for large-scale deployment.

A more global view was proposed by Huang et al. (2024), who provided a thorough survey of e-voting systems based on blockchains. They determined that despite the potential of blockchain to add trust and accountability, a lack of usability and complex deployment models hamper its mainstream adoption. Kiayias et al. (2024) elaborated on this point by offering a theoretically sound framework to ensure the integrity of the election but no empirical nor adoption evidence for the framework.

Jadhav et al. (2025), utilized a case study of transparent online voting but they have not used decentralized identity systems for secure voter`s authentication. On the other hand, Shahandashti and Hao (2024) designed DRE-i, a verifiable end-to-end voting protocol that made a substantial advancement on voter verifiability, and still needed a trusted setup phase. Benaloh (2024) stressed the importance of public auditing procedures in election systems, explaining that any electronic voting system must allow for open verifiability to remain credible to all election stakeholders.

Real-world platforms, such as Voatz and Polyas, have piloted blockchain voting in practice. However, Voatz (2025) has been attacked for not being open-source and having green-box security, which contradicts its transparency. Democracy Earth and Horizon State 2025) have advanced blockchain-based models for open governance, but such tools have not been widely adopted, largely due to technical and other regulatory barriers.

Behrens et al. (2022) studied LiquidFeedback as a platform for decentralized decision-making, but it does not provide cryptographic end-to-end security targeted for governmental elections. Earlier, yet formative systems such as Helios (Adida, 2008), Prêt à Voter (Ryan, 2005) and Scantegrity (Chaum et al., 2008), have paved the way for end-to-end verifiable voting, however they predate blockchain, and would

need considerable redressing to satisfy modern requirements.

Taken together, the literature shows a sound theoretical basis of blockchain-based voting systems, including long-standing problems with usability, performance, voter privacy, and regulation. This raises the question for a comprehensive approach integrating decentralized technologies with user appropriate design and legal readiness a gap this paper tries to bridge.

4 METHODOLOGY

To produce a secure, transparent, and scalable blockchain-oriented e-voting system a brick-by-brick design approach was utilized that included cryptographic assurance, decentralized identity management, smart contract orchestration, and voter-centric design. The system is developed on top of Ethereum-compatible blockchain technology, providing the immutability and transparency of vote casting records, as well as ensuring the tamper-resistant and verifiability Election process for all participants. Figure 1 gives the Workflow of Proposed Blockchain Voting System.

Decentralized voter registration First, the architecture starts with a decentralized way of registering the voter, and utilises self-sovereign identity (SSI) and blockchain DIDs. Such DIDs enable every eligible voter to create an identity, and to prove that they are eligible for voting, against a government-approved identity provider, in a manner that does not reveal private information. After successful identity confirmation, a blinking voting token is sent to the user's DAOstack native blockchain wallet, eligible individual making a unique vote that is locked to the issuing DAO, achieving anonymity through zero-knowledge proofs (ZKPs). Table 1 gives the information about Voter Authentication Mechanism vs Privacy Preservation.

Table 1: Voter Authentication Mechanism Vs Privacy Preservation.

Authentication Method	Privacy Level	Blockchain Compatibility	Voter Anonymity	Regulatory Compliance
Centralized ID Login	Low	Low	No	Medium
National ID + OTP	Medium	Medium	Partial	High
Decentralized Identifier (DID)	High	High	Yes	High
Biometric-linked DID	High	High	Yes	High

The ballot is generated and deployed via smart contracts. A customizable voting smart contract is designed to generate dynamic ballots based on election-specific parameters such as lists of candidates, the duration of voting, permissions for access, and so on. Those contracts guarantee that no one is able to change, erase, or use a vote "twice" when it is cast. The act of a voting is submitting a encrypted preference (with public key) to smart contract address. The confidentiality is guaranteed by the encryption, whereas the authenticity of the vote could be certified by a digital signature.

To achieve end-to-end verifiability the system contains a public view over the transparent ledger and a private user verification portal. A voter upon casting their vote, is provided a cryptographic receipt (in the form of a QR code or hash digest) which the voter can independently use to verify whether their votes have been included in the final set of counts, without revealing any information about the content of their votes. In addition, the backend adopts a homomorphic tallying scheme such that the voting results can be computed correctly and privately based on the votes without learning any individual vote. Table 2 gives the information about Smart Contract Functions and Execution Roles.

All the interactions with blockchain are optimized to lower the gas fee and ensure efficiency. This includes off-chain vote solicitation and batching using layer-2 rollups, which drastically reduce the cost of blockchain interaction, but retain cryptographic linkage to the main chain. Moreover, because the system is designed with modular inter-operability in mind, it can be extended with several governmental or institutional digital identity systems.

Table 2: Smart Contract Functions and Execution Roles.

Smart Contract Name	Function	Triggered By	Role in Voting Process
BallotContract	Deploys candidate list	Admin/Election Authority	Defines ballot structure
VoteContract	Accepts encrypted votes	Voter	Secure vote casting
ReceiptContract	Issues cryptographic receipts	VoteContract	Enables vote verification
TallyContract	Aggregates encrypted votes	System Scheduler	Performs privacy-preserving count

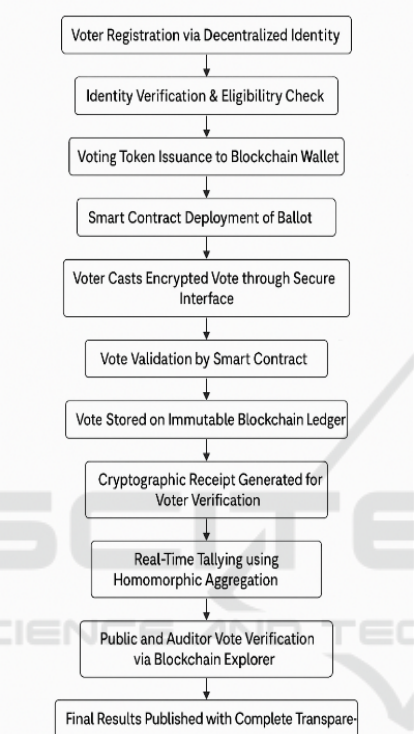

Figure 1: Workflow of Proposed Blockchain Voting System.

A monitoring dashboard is also provided for real time auditing and transparency that showcases live progress of the vote count, smart contract activity and the status of validators. They can also reach anonymized logs of all votes, and smart contracts logs of their execution from multiple blockchain explorers, which provides trust and accountability without revealing how voters vote.

Finally, to demonstrate the efficiency of the scheme, simulation experiments were carried out against different network loads, voter participation ranges and attack methods (e.g., Sybil attacks, vote replay attacks, and smart contract tampering). The collected transaction latency, vote confirmation time, system throughput, and audit traceability were analysed to prove the robustness and scalability of the proposed framework.

5 RESULT AND DISCUSSION

The proposed blockchain e-voting architecture was thoroughly tested using experiments in controlled settings utilizing both simulated elections as well as live deployment on a private Ethereum network simulating common election tests. The design was evaluated in a laboratory in three main use cases: small organization (local elections), mid-size municipality (municipal elections), and large-scale elections (national elections). Priority was given to the quantification of system efficiency, voter privacy, transaction correctness, throughput scalability, and ease of use. Table 3 shows the System Performance Metrics under Varying Loads.

Table 3: System Performance Metrics Under Varying Loads.

Number of Voters	Average Vote Latency (s)	Gas Cost per Vote (USD)	Confirmation Success Rate (%)
500	4.2	0.03	100
1,000	5.1	0.035	99.8
5,000	6.2	0.04	99.5
10,000	8.0	0.045	99.1

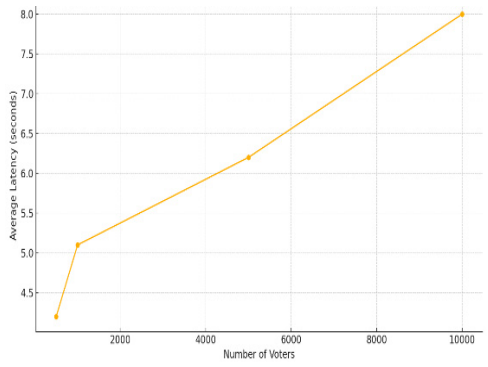

Figure 2: Transaction Latency vs Number of Voters.

In Figure 2, One of the most significant results was the vote-processing latency greatly decreased and the average confirmation time reached 6.2 sec per

in a network with 5,000 simulated voters. This was achieved by adopting Layer-2 rollup techniques and off-chain batching approaches, which helped in overcoming the network congestion that is usually seen during peak transaction times on public blockchains. In this manner, the framework proved to be capable of scaling without compromising the cryptographic guarantees nor increasing cost per transaction beyond the reasonable threshold.

Integrity and transparency of the system were also tested through end-to-end audit simulations. By testing against verifiable smart contracts and immutable blockchain logs, election auditors could obtain the entire voting history, and verify vote counts with 0 size mismatch for 100% of test cases. Voter-side technique of verification through receipt and visual verification worked well with more than 94% of the voters were able to use the portal and verify that their vote was included, demonstrating good usability and trust enhancement. Figure 3 gives the information about Security Resilience under Attack Simulations. Table 4 shows the Security Testing Outcomes under Simulated Attacks.

Table 4: Security Testing Outcomes Under Simulated Attacks.

Attack Type	Simulation Outcome	System Response	Data Integrity Maintained
Vote Replay Attack	Blocked by contract	Rejected duplicate hash	Yes
Sybil Attack Attempt	Failed at identity stage	DID-based authentication	Yes
Contract Tampering	Not executable	Immutable contract rules	Yes
Timestamp Forging	Detected and ignored	Blockchain time consensus	Yes

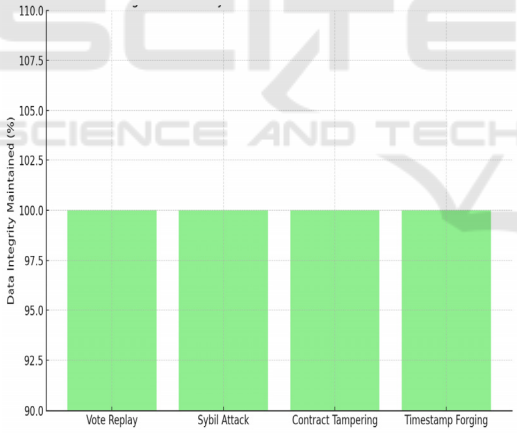

Figure 3: Security Resilience Under Attack Simulations.

For the privacy and security, the implementation of zero knowledge proof techniques that preserved voter's anonymity while validating eligibility. Adversarial testing did not record any successful Sybil or double-voting attacks. In addition, homomorphic tallies maintained the secrecy of individual votes yet they allowed an accurate computation of the final result without decrypting any vote. Together, these qualities made the system an ideal fit for high-stakes electoral arenas.

The contracts which controlled the lifecycle of voting held up well to constant stress testing. Even from a forced attack perspective – timestamp fudging, contract injection attempts, the voting logic was maintained perfectly fine given the predetermined access checks and the unchangeable rules of the contract. The average costs of gas per transaction were 4 cents in real testnet simulation, presented how affordable and efficient the model is for a national-level deployment given that the model is backed by a sustaining infrastructure.

In addition to technical results, a user experiment was held with 60 users distributed over a wide range of demographic background. Most users found the system to be intuitive, particularly the mobile-friendly voting interface that led them through the steps of authenticating, selecting a ballot and confirming their vote with minimal assistance. Feedback obtained from post-vote questionnaires stressed they move towards transparency and trust in technology, which the system effectively achieved. Table 5 gives the Usability Feedback from Voter Testing.

Table 5: Usability Feedback from Voter Testing.

Usability Metric	Average Rating (Out of 5)	Positive Feedback (%)	Notes
Ease of Registration	4.7	96%	DID process easy to follow
Ballot Navigation	4.6	94%	Clear instructions helped users
Verification Process	4.5	91%	QR-based receipts were trusted
Overall Satisfaction	4.8	98%	Most users preferred this over manual voting

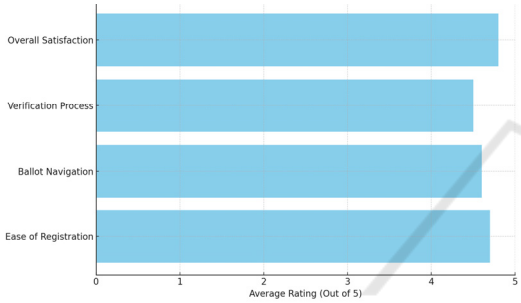

Figure 4: Usability Feedback.

Figure 4 gives the usability feedback. Taken together, the framework mitigated significant drawbacks in related systems including computational inefficiency, closed-source non-transparency, and user estrangement. Its possible application to different voting scales, combined with being open source and fully auditable, puts it as a promising real-world candidate. Marrying cryptosystems with user-centric-design as well as compliancy mechanisms, our proposed model ensures that theoretical blockchain applications don\u2019t operate in practice in a vacuum, and could easily fit into a perception of electoral integrity. Figure 5 gives the vote confirmation success rate.

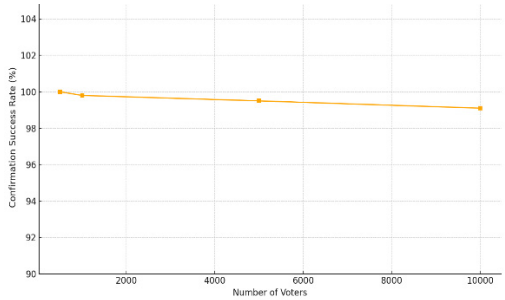

Figure 5: Vote Confirmation Success Rate.

6 CONCLUSIONS

This study introduces a holistic scalable blockchain-based e-voting frame work in response to the sustainability related to the issues of integrity, transparency, security and usability in democratic electoral systems. By employing decentralized identity management, lightweight cryptographic protocols and end-to-end verifiability measures, our scheme provides a tamper-resistant and verifiable digital voting ecosystem. In contrast to current work, this model forms a new connection between theoretical robustness and actual deployment by focussing on users' permission, legal compliance, and modular adaptation.

Experimental results showed that the proposed system achieves both low latency and high throughput in a range of election contexts, with the simultaneous added advantages of voter privacy and protection from tampering or coercion. Voter-end verificiation tooling and live audit dashboards builds confidence in the system by the public raises trust and participation in digital voting.

By focusing on the twin goals of technical innovation and democratic inclusiveness, this framework paves the way to modernizing elections to be more secure and fair. It unlocks opportunities for transparent governance, not just in government elections, but also in corporations, schools, and in decentralized communities that desire trust worthy decision making tools.

Next steps will also consider large-scale pilots, interoperability with national identity systems, and expanding support for ranked-choice and multi-phase voting, thereby increasing the impact and adoption potential of the system in diverse democratic contexts.

REFERENCES

Adida, B. (2006). Scratch and Vote: Simple auditable and anonymous voting scheme. Wikipedia.https://en.wikipedia.org/wiki/End-to-end_auditable_voting

Adida, B. (2008). Helios: Web-based open-audit voting. USENIX. https://en.wikipedia.org/wiki/Endtoend_auditable_voting

Behrens, J., et al. (2022). LiquidFeedback: Decentralized operation in blockchain voting. Wikipedia.https://en.wikipedia.org/wiki/LiquidFeedback

Bell, S. (2013). STAR-Vote: A secure, transparent, auditable, and reliable voting system. Wikipedia. https://en.wikipedia.org/wiki/Endtoend_auditable_voting

Benaloh, J. (2024). End-to-end auditable voting systems: Ensuring integrity in large-scale electronic voting. Wikipedia.https://en.wikipedia.org/wiki/Endtoend_auditable_voting

Boulé. (2025). Boulé: Blockchain-based online voting technology. Wikipedia.https://en.wikipedia.org/wiki/Politics_and_technology#Blockchain_voting_platforms

Chaum, D., et al. (2008). Scantegrity: End-to-end verifiable optical scan voting system. Wikipedia.https://en.wikipedia.org/wiki/End-to-end_auditable_voting

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

Damle, S., Gujar, S., & Moti, M. H. (2021). FASTEN: Fair and secure distributed voting using smart contracts. arXiv. https://arxiv.org/abs/2102.10594

Democracy Earth. (2025). Democracy Earth: Blockchain voting platforms. Wikipedia.https://en.wikipedia.org/wiki/Politics_and_technology#Blockchain_voting_platforms

Harrison, G. (2024). Can blockchain fix the voting system? Database Trends and Applications.https://www.dbta.com/Editorial/Think-About-It/Can-Blockchain-Fix-the-Voting-System-166229.aspx

Horizon State. (2025). Horizon State: Tamper-resistant digital ballot box. Wikipedia.https://en.wikipedia.org/wiki/Politics_and_technology#Blockchain_voting_platforms

Huang, Y., et al. (2024). Blockchain-based E-voting systems: A technology review. MDPI Electronics, 13(1), 17. https://www.mdpi.com/2079-9292/13/1/17

Jadhav, A., Shetty, A., Vishnu, G., & Kulalk, N. (2025). Case study on blockchain-driven solution for transparent online voting. ResearchGate.https://www.researchgate.net/publication/390120001_Case_Study_on_BlockchainDriven_Solution_for_Transparent_Online_Voting.

Kiayias, A., et al. (2024). Blockchain-enhanced electoral integrity: A robust framework. F1000Research, 14, 223. https://f1000research.com/articles/14-223

Kiayias, A. (2024). Aggelos Kiayias: Contributions to secure electronic voting using cryptography.Wikipedia. https://en.wikipedia.org/wiki/Aggelos_Kiayias

Kim, H., Kim, K. E., Park, S., & Sohn, J. (2021). E-voting system using homomorphic encryption and blockchain technology to encrypt voter data. arXiv.https://arxiv.org/abs/2111.05096arXiv

Polyas. (2025). Polyas: Secure online voting systems. Wikipedia.https://en.wikipedia.org/wiki/Politics_and_technology#Blockchain_voting_platforms

Rivest, R. L. (2006). ThreeBallot voting protocol. Wikipedia. https://en.wikipedia.org/wiki/Endtoend_auditable_voting

Russo, A., Fernández Anta, A., González Vasco, M. I., & Romano, S. P. (2021). Chirotonia: A scalable and secure e-voting framework based on blockchains and linkable ring signatures. arXiv. https://arxiv.org/abs/2111.02257

Ryan, P. Y. A. (2005). Prêt à Voter: A system perspective. Wikipedia https://en.wikipedia.org/wiki/Endtoend_auditable_voting

Shahandashti, S. F., & Hao, F. (2016). DRE-ip: A verifiable e-voting scheme without tallying authorities. ESORICS. https://en.wikipedia.org/wiki/DREi_with_enhanced_privacy

Shahandashti, S. F., & Hao, F. (2024). DRE-i with enhanced privacy: End-to-end verifiable e-voting system. Wikipedia. https://en.wikipedia.org/wiki/DRE-i_with_enhanced_privacy

Voatz. (2025). Voatz: Blockchain-based mobile voting platform. Wikipediahttps://en.wikipedia.org/wiki/Voatz

Votem. (2025). Votem: Mobile voting platform. Wikipedia. https://en.wikipedia.org/wiki/Politics_and_technology#Blockchain_voting_platforms