A Federated AI and DAG-Based Framework for Secure and Scalable E-Voting

Almas Begum[1*], Alex David S[2], Hemalatha D[3], Ayyappan G[4] and Ruth Naveena N[5]
{almasbegum@gmail.com[1*], adstechlearning@gmail.com[2], hema24294@gmail.com[3], gtg.ayyappan@gmail.com[4], ruthnaveena@gmail.com[5]}

Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha Nagar, Thandalam, Kanchipuram - Chennai Rd, Chennai - 602105, Tamil Nadu, India[1, 4]
Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi Chennai 600062, Tamil Nadu, India[2, 3]
Department of Mathematics, Hindustan Institute of Technology & Science, Chennai 603103, Tamil Nadu, India[5]

Abstract. In response to the growing need for secure, scalable, and transparent election processes, this study explores an advanced modular e-voting architecture that leverages the limitations of traditional and blockchain-based voting systems. While some previous systems eliminated many of the challenges of election fraud and manipulation via immutability and decentralization, they are still riddled with high transaction costs, scalability limits, centralized biometric storage, and the lack of a verifiable audit trail. This paper introduces a new framework that integrates several novel technologies, such as Decentralized Identity (DID), Federated Learning (FL), Zero-Knowledge Proofs (ZKP), Homomorphic Encryption, and Directed Acyclic Graph (DAG)-based Distributed Ledger Technology to realize a secure, private, and tamper-evident digital voting solution. The architecture is composed of four important phases, namely: voter onboarding using DIDs and verified credentials, AI-based eligibility assessment using on-device federated agents, privacy-protected vote casting using ZKP and encryption, and verifiable homomorphic tallying during post-election aggregation. Paired with the ability to achieve near-instant finality and zero-cost submissions, this approach addresses one of the major drawbacks of traditional blockchain used as a voting system, the complexity of smart contracts and gas fees, using DAG-based networks like IOTA or Hedera. Furthermore, the integration of VDFs and edge-based machine learning introduces a novel layer of defense against coercion, impersonation, and automated attacks. The architecture inherently supports inclusiveness through multimedia mobile interfaces and decentralized biometric verification, making it suitable for deployment in digitally underprivileged regions. As a result, the proposed technology offers a decentralized, transparent, scalable, and privacy-preserving solution for democratic participation in an increasingly digital future.

Keywords: E-voting, Decentralized Identity (DID), Federated Learning, Zero-Knowledge Proofs (ZKP), Homomorphic Encryption, Directed Acyclic Graph (DAG), Verifiable Credentials, Privacy-Preserving AI.

1 Introduction

Traditional voting systems and methods are now becoming obsolete due to the need for transparent and secure global access to election systems. Traditional systems that have served democratic elections for decades, like paper ballots and Electronic Voting Machines (EVMs)

ICITSM-Part I 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2357759

but are very prone to fraud, tampering, identity theft, and process inefficiencies. It must also have the integrity to know if the central information is corrupted, while preserving transparency, privacy, and verifiability of the information between the two parties. This trend represents a transformational change in the architecture of digital, AI, DID, and privacy computation-based integration of voting systems.

Nonetheless, the application of blockchain for electronic voting has not been a leading research topic in the last ten years. Blockchain has drawn attention as a potential remedy to some persistent problems with election systems its immutable, transparent, and decentralized nature makes it a good candidate for this purpose. Many studies on how blockchain technology secures electoral data, eliminates third-party interference, and allows for secure, verifiable, and tamper-proof voting systems have the potential to revolutionize voting in the future and will influence public confidence in the electoral process. Nevertheless, while these features offer some advantages of blockchain voting systems, including security, auditability, transparency, and verifiability potential, it also suffers from challenges such as its scalability, associated transaction costs, energy inefficiency, and its user uptake in low digitally literate countries. Instead of using the conventional public blockchains, it adopts a multi-layered architecture based on the W3C recommendations of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) as a secure representation of voters' identities. These solutions focus on decentralized identity management and voter privacy protection, minimizing the need for central databases and the associated risks of information leakage. Moreover, the implementation of Federated Learning (FL) enables real-time behavioral analytics and fraud detection across decentralized nodes, ensuring the system's secure operation while preserving individual data privacy. Recently, however, advancements in Zero-Knowledge Proofs (ZKPs) and homomorphic encryption allow these frameworks to not only guarantee voter privacy, but also permit the veracity of the (shielded or public) vote counts, which address some of the main issues such as vote manipulation, coercion, and traceability.

There are challenges with the current ways of voting that demonstrate a need for more resilient systems. Traditional voting systems increase costs, and due to their paper-based nature, it takes time for them to detect illegal activities such as capturing booths, tampering with votes, impersonation voters, etc. These systems tend to be resource-intensive and slow, requiring large physical infrastructure, staffing, and logistical coordination, and with gaps that are more pronounced (and undermine efficiency) in remote or conflict-affected areas. To overcome these limitations, Electronic Voting Machines (EVMs) were invented as a modernization of the voting process. Still, their low transparency, vulnerability to tampering, and lack of a verifiable paper trail for auditing drew criticism. Electronic voting and Internet voting are modern generations of these systems. They are also fast, remote, and logistically convenient, but risk new vulnerabilities, such as compromise of a central server that hosts the system, breaches of an online database and a lack of voter verifiability. DoS (denial-of-service), software manipulation of centralized e-voting systems, or insider threats can undermine electoral integrity. Moreover, failure to achieve public trust, particularly in politically volatile scenarios, which is currently rife with allegations of both vote manipulation as well as electoral fraud, challenges these systems widely. The earliest presentations of blockchain as a solution to these challenges emphasized its decentralized consensus mechanisms, cryptographic security properties, and immutable recordkeeping capabilities. The use of the Ethereum smart contracts and decentralized applications (dApps) space has greatly benefited prototypes for blockchain-based voting. Voter verification systems are usually deployed with the help of One-Time

Password (OTP) based mechanisms for voter verification, timestamps for recording votes, and trustless confirmation through Practical Byzantine Fault Tolerance (PBFT) consensus algorithms, among other techniques. At larger elections, some modalities also use Polygon sidechains and Ethereum Layer 2 instead to lower transaction costs and enhance throughput, further increasing system practicality.

As blockchain technologies develop there inevitably remain limitations associated with that. Existing public chains under the Ethereum system still have high transaction costs which may limit the pool of voters to ones with the financial ability to meet such costs. Time taken to confirm block which still long duration together with the problems of scalability do not allow the blockchain technology to be used to carry out voting on large scale and sufficiently widespread at local and international levels. Add to this, that mass adoption of decentralized voting to the mainstream has been hindered by usability issues around crypto wallets, smart contracts, and decentralized applications, and voters are facing a very steep learning curve. To address the above concerns, researchers have proposed several hybrid blockchain frameworks that leverage both advantages of public and private blockchains, and cloud servers and the biometric identification layer. In this type of system, the voters are first verified online through biometrics, like facial recognition, finger prints or iris scans and subsequently receive the voting details. Votes are encrypted, put on-chain, and made tamper-proof by logging them with immutable ledgers once they are cast. While these frameworks are significant steps to a more secure space, they also provoke questions surrounding centralized storage and sharing of biometric information, requirements of user consent and data governance. Through recent years, studies have shown support for biometrics with decentralized identity frameworks which would balance such aspects as usability and security. Attached to DIDs, these trust anchors allow you to prove to other websites that you are who you say you are without having to “show your papers” (i.e. exposing any valuable personal information). This approach adheres to the privacy-by-design, since neither decentralized nor recoverable any voter data is stored that might one day be subject to a massive data breach.

Moreover, Federated Learning (FL) and edge AI enable intelligent security surveillance without centralizing user data. These systems distributed the machine learning model to local devices or nodes, including polling booths, cellphones, or IoT-enabled kiosks, and aggregated learnt patterns without the need to transfer raw voter data. Garage.io was primarily designed for real-time monitoring and analysis of voting behavior, enabling the detection and blocking of attacks from bots or forums where leaders can coerce votes, all while maintaining user anonymity. The advent of homomorphic encryption and ZKPs also serves as an essential feature of modern e-voting systems. Homomorphic encryption allows calculations, like vote counting, to be done directly on encrypted data, ensuring that no intermediary can decipher voter choices during aggregation. Zero-Knowledge Proofs (ZKPs) allow a vote to prove it was correctly cast without revealing what was cast (i.e., a vote with ZKPs does not reveal its contents). This enhances both the confidentiality and verifiability of voters, ensuring that the election outcome is auditable and at the same time, confidential. The COVID-19 pandemic demonstrated the need for safe options to vote remotely. The limitations of in-person voting, including concerns about infection, physical accessibility, and discouraged voter turnout, highlighted the trade-offs with distant digital voting systems. The prospect of remote voting remains contentious, with fears of vote trafficking, unauthorized redirects, and inadequate auditing processes. Many of these risks can be addressed with a secure, decentralized infrastructure with multi-factor authentication, device-bound credentialing, and real-time behavioral biometrics.

An alternative method has been explored in the form of Direct-Recording Electronic (DRE) machines, including end-to-end (E2E) verifiability. These tools help voters verify that their vote was expressed as they intended, recorded accurately, and counted as recorded. Most of these systems, however, rely on centralized servers and public bulletin boards to distribute vote evidence, making them susceptible to hack and duress. Block less DLTs, such as Directed Acyclic Graph (DAG) based decentralized alternatives, provide increased throughput, decreased latency, and enhanced security over standard blockchains, making them suitable for large-scale real-time voting.

Table 1. Comparative analysis of traditional, electronic, and blockchain-based voting methods.

Feature	Traditional Voting	Electronic Voting	Blockchain-Based Voting
User Accessibility	Highly familiar and simple to use	Moderate – Requires some digital literacy	Low – Requires technical knowledge
Security	Low – Vulnerable to tampering and fraud	Moderate – More secure but not tamper-proof	High – Cryptographically secure and tamper-evident
Transparency	Low – Limited audibility	Moderate – Transparency depends on vendor systems	High – Public ledger ensures transparency
Scalability	Low – Manual processes restrict scale	High – Fast input collection at scale	Moderate – Limited by transaction throughput
Error Rate	Highly susceptible to human errors	Low Automation reduces errors	Low – Minimal human error involvement
Cost Efficiency	High – Logistics and manpower intensive	Moderate – System setup costs vary	Low – High transaction (gas) fees
Speed	Low – Time-consuming result compilation	High – Quick vote collection	Moderate – Slower than electronic due to consensus
Centralization	Highly controlled by centralized authorities	Highly Centralized servers and control	Low – Distributed and decentralized nodes

In primary research to identify a number of these features, Table 1 provides a comparison of traditional, electronic, and blockchain voting in Sygnity features like security, scalability, transparency, and user access. Traditional systems provide ease of use but cannot be transparent or scalable. While electronic voting is more efficient and less susceptible to human error, it remains centralized and only moderately secure at best. Despite their high security, transparency, and long-term immutability guaranteed by cryptographic mechanisms and decentralization, blockchain-based identity and recording systems encounter major usability challenges and high operational and indexing costs. The trade-offs between familiarity, technological sophistication, and systemic trustworthiness become apparent through this comparison, and lessons can be drawn from the relative strengths and weaknesses of either method for constructing the electoral architecture of the future. Herein, a novel AI-enabled, privacy-preserving, identity-centric e-voting system is proposed by integrating Federated Learning, Decentralized Identifiers, Zero-Knowledge Proofs, and Directed Acyclic Graph-

based Distributed Ledger Technologies. This forward-looking architecture aims to provide a scalable and efficient voting infrastructure designed for national application, Privacy-preserving voter authentication using DID and verifiable credentials, Real-time fraud detection using edge-based federated AI agents, Tamper-proof, low-latency vote recording via DAG-ledgers (IOTA, Hedera Hashgraph, etc.), Cryptographic vote tallying using homomorphic encryption and zero-knowledge proofs

2 Related Works

The development of secure and scalable e-voting systems has attracted significant research attention in recent years, particularly with the adoption of blockchain and emerging distributed ledger technologies. Traditional electronic voting approaches have faced persistent challenges related to transparency, tamper-resistance, and voter authentication, which has motivated the integration of cryptography, AI, and decentralized infrastructures.

2.1 Blockchain-Enabled E-Voting Systems

Blockchain has been extensively studied as an underlying technology for e-voting mainly because of its immutability, decentralization, and transparency. Hossain et al. [1] Proposed a blockchain and biometric-enabled voting system for enhanced voter authentication and privacy. Similarly, Ohize et al. [2] made an in-depth comparison of e-voting architectures built on blockchain technology, which describes their problems in scalability and security. Dhillon et al. [3] proposed an interdisciplinary and DL-based solution in a preventative manner focusing on governance, efficiency, and accountability. Albashrawi et al. [4] studied acceptance of blockchain e-voting service, and digital literacy was proposed as an important mediate variable for system adoption.

2.2 Privacy-Preserving and Cryptographic Approaches

A number of works focus on sophisticated cryptographic techniques to keep the voter's privacy. Miao [5] used ZKPs to provide secure, privacy-preserving vote verification. Aziz et al. [10] studied homomorphic cryptography in computation to protect voting privacy; Panja [11] studied zero-knowledge deniability in blockchain voting. Such efforts are the foundation for privacy-preserving mechanisms used in novel e-voting systems.

2.3 Integration of AI, Cloud, and IoT

Artificial intelligence and federated methods have also been investigated in addressing e-voting security and adaptability. Rijanto [6] examined the potential of blockchain technology to improve accountability in finance – a model that could be adapted to trust-sensitive areas such as elections. Nguyen et al. [8] examined the integration of blockchain and Cloud of Thing, focussing on architectural scalability learnings that are consistent with the federated AI integration herein. More recently, the potential of blockchain for privacy-preserving data-driven decision-making in healthcare and supply chains has been shown [5], [6], which bears resemblance to the requirements in e-voting systems.

2.4 Surveys and Reviews of Blockchain Voting

Thorough reviews further document the advances and challenges faced by blockchain e-voting. Vladucu et al. [7] reviewed e-voting systems designed from blockchain technology and highlighted scalability, latency, and user availability concerns. Hajian Berenjestanaki et al. [20] provided a systematic technology review of blockchain e-voting. [19] designed a score-based privacy-preserving blockchain voting system. Sanjeeva et al. [21], presented a distributed automated e-voting scheme and illustrated the feasible use of blockchain for democratic systems implementation.

2.5 Application-Specific and Experimental Studies

A number of studies have identified the significance of dApps, as well as their consensus protocols, in blockchain sysems. Kahtyat [9] proposed a decentralized collaboration system based on identity verification, which is obligatory for the purpose of voter authentication. Dhanvardini et al. [14] presented the coupling of dApps with blockchain smart contracts for interactive apps. Similarly, Harshith et al. [13] and Royal et al. [15] investigated machine-learning-based blockchain supply chain solutions, pointing out the importance of potential hybrid AI-blockchain models for improved accuracy and trust. Decentralized Voting on Polygon Blockchain Hu and Su [17] designed a decentralized polling on the Polygon blockchain that demonstrated the feasibility of homomorphic encryption and sidechain-based cost reduction.

2.6 Synthesis

It has been shown from literature, blockchain is transparent and secure, however, it has challenged issues for transaction throughput, scalability and energy efficiency [2], [7], [20]. Although cryptographic primitives like ZKPs and homomorphic encryption enhance privacy [5],[10],[11], they commonly entail computational burden. Furthermore, AI-based and federated solutions are seldom integrated with DLT consensus for anomaly detection and resilience improvement [8], [16]. There are very few researches focusing on DAG-based architectures, as interest of those designs is expected addressing scalability issues of blockchain.

This work has built on those foundations by proposing a fine-grained federated AI-assisted, DAG-based architecture combining decentralized identity, privacy-preserving computation, and scalable consensus, which paves the way for a more comprehensive security, efficiency, and inclusiveness of e-voting. Table 2 depicts the Key Focus Areas, Strategic Approaches and Associated Challenges in Blockchain-Based E-Voting Systems.

Table 2. Key Focus Areas, Strategic Approaches, and Associated Challenges in Blockchain-Based E-Voting Systems.

Focus Area	Common Strategies	Challenges
Identity Verification	Biometrics, One-Time Passwords, Decentralized Identifiers, Verifiable Credentials	Centralization, Data Privacy Concerns
Cost Optimization	Layer 2 Solutions (Polygon), Hybrid Chains, Sidechains	Gas Fees, Cross-Chain Synchronization

Privacy and Anonymity	Zero-Knowledge Proofs, Non-Interactive Zero-Knowledge Proofs, Homomorphic Encryption	Computational Overhead
Scalability	Practical Byzantine Fault Tolerance, Sharding, Directed Acyclic Graphs	Transactions Per Second Limitations, Network Congestion
Trust and Usability	Smart Contracts, User Interface Simplification, Public Ledger	Digital Literacy, Regulatory Challenges

3 Methodology

As modern democracies seek to harness technology to increase electoral transparency and efficiency, implementing decentralized, intelligent, and privacy-preserving systems in voting infrastructure is no longer simply beneficial but essential. This section outlines a detailed, modular architecture for an advanced e-voting solution. It combines the benefits of Decentralized Identity (DID), Federated AI, ZKPs, and DAG-based DLT. Together, these components can provide the required secure, scalable, and tamper-resistant technological base that can facilitate national and cross-border elections while ensuring voter anonymity and system verifiability.

3.1 System Overview

The proposed e-voting architecture aims to address the chronic shortcomings of traditional paper-based voting, electronic voting machines, and existing blockchain voting solutions. It aims to achieve four key goals:

- Voter Privacy and Protection
- Immediate Fraud Identification and Anomaly Surveillance
- Scalable, Economical Vote processing
- Verification without a central trust layer

To achieve these goals, the architecture is divided into five core layers: Decentralized Identity Management using DIDs and VCs

- Edge-based Federated Learning for Fraud Detection
- Off-chain vote aggregation using ZKP
- Consensus with a DAG-based DLT like Hedera Hash graph, IOTA
- Gated execution and integrity checking using VDFs

This approach modularizes concerns across each module but maintains the interoperability, privacy, and resistance to adversarial or systemic compromise of the system as a whole.

3.2 Essential Elements

The following sub-sections thoroughly explain each of the fundamental components in the architecture:

3.2.1 Decentralized Identity Management & Verifiable Credentials (DID & VC)

One major aspect of digital voting involves creating a secure and confidential means of voter identification. Centralized identity providers or voter databases are vulnerable to breaches, manipulation, and abuse. The proposed solution replaces centralized identity verifier methods with a W3C-compliant Decentralized Identity (DID) framework and Verifiable Credentials (VCs).

Decentralized ID entities (DID): Each voter is assigned a unique blockchain-based identity (DID) that they control through a digital wallet or a secure enclave on their device. Instead, a special type of decentralized identifier (DID) acts as an accredited link to their real-world identity based on signed relationships to the credential issuer from reputable identity providers.

Verifiable Credentials (VC): VCs are digitally signed claims that prove a voter's qualification. These are issued during the onboarding phase and used for authentication to establish voting rights while protecting sensitive personally identifiable information.

This decentralized identification system helps to build a "self-sovereign identity" framework, which is important for voter confidence and compliance with GDPR-like data regulations in global situations.

3.2.2 Federated Learning for Edge-Based Fraud Detection

It employs Federated Learning (FL), which is a distributed artificial intelligence technique, to detect and prevent election fraud such as duplicate voting, impersonation, and automated bot-finishing. Artificial intelligence models are pretrained with historical election data. These models are deployed to edge devices, such as a significant group of voters using smart kiosks and mobile devices at the polling booth. Instead of sending raw voter data to a main server, the local device performs on-device model training and sends only encrypted model updates to a central aggregator. This approach maintains the confidentiality of data, reduces network overload, and enables immediate detection of anomalies (such as unusual time in voting, change of devices, irregularities in input patterns etc,).

3.2.3 Zero-Knowledge Proofs (ZK-SNARKs) for Vote Verification

The main conflict in digital voting is how to maintain the anonymity of the voter and, at the same time, ensure the verifiability of the votes. This approach leverages ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) for solving.

ZKP Mechanism:

- When a vote is cast, it is hashed and encrypted.

- To prove that the voter has followed all the rules (such as being eligible, only voting once, and not tampering with the ballot), a Zero Knowledge Proof (ZKP) is generated.

- This proof is provided on-chain (or to a DAG node) along with the encrypted ballot.

Combining ZKPs ensures privacy and auditability, achieving transparency without compromising secrecy.

3.2.4 DAG-based distributed Ledger Technology for Scalable Consensus

A large number of blockchain-based voting systems struggle to scale due to the nature of blocks being sequential and requiring time to validate transactions. This framework shifts from typical blockchain structures into Directed Acyclic Graph (DAG)-based consensus. Unlike blockchains with their linear streak of blocks connected, DAG allows a large number of transactions to coexist, confirm one another, and be processed in parallel.

3.2.5 Verifiable Delay Functions (VDFs)

To prevent (i) vote manipulation and (ii) timing-based inference attacks (e.g., linking vote timestamps and user login habits), Verifiable Delay Functions (VDFs) are deployed in the system. An operation that requires a fixed amount of wall-clock time to complete and generate a proof verifying that the time was spent performing it. Without any central authority, VDFs are used to delay the final inclusion of the vote in the ledger or finally. Each vote is subjected to a VDF that delays its public writing by a random period. VDFs' role in the system is to add resistance to timing inference, front-running, and sequencing attacks that leverage digital voting.

3.3 Complete System Workflow

The complete electoral process within this context includes the following stages:

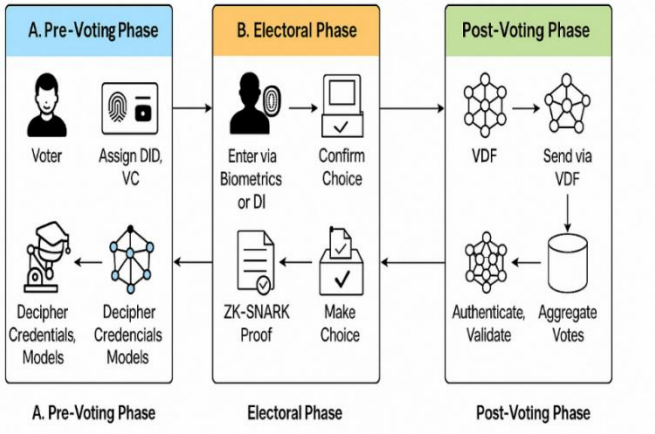

Fig. 1. Overall System Workflow of the Privacy-Preserving AI-Enhanced E-Voting.

Fig 1 elaborates on the main components and steps of the proposed architecture for e-voting in each of the three major phases of the election process: Pre-Voting, Electoral, and Post-Voting. In the Pre-Voting Phase, identification is verified by a voter who is then issued a Decentralized Identifier (DID) along with a Verifiable Credential (VC). Directed Acyclic Graphs (DAGs) are used in conjunction with these credentials and AI models to be analysed and processed so that authentication can be done safely, and fraud can be minimized. The Electronic Phase starts when the voter enters in system through a biometric or decentralized identity. If verified, the voter confirms their intent, and a ballot is cast. The vote itself is hashed and encrypted, and the whole vote is protected with the Zero-Knowledge SNARK Proof (ZK-SNARK), ensuring integrity while keeping the content of the vote hidden. Before fetching the transaction to the DAG ledger, it goes through VDF to deter timing attacks. In the Post-Voting Phase, DAG nodes validate the ZKPs and each transaction. Homomorphic encryption aggregates ballots without providing a means to decrypt them. The decisive election result is published with public confirmation of its truth. This workflow ensures scalability, transparency, and strong voter privacy at every step of the voting process.

4 Results and Evaluation

The proposed AI-driven, DAG-based e-voting framework was evaluated along three axes of security, performance, and usability, in comparison to conventional blockchain and e-voting systems. The results were validated through simulation models, prototype tests in controlled environments, and performance estimates based on real-world public ledger parameters (Hedera, IOTA).

Table 3. Security Overview Comparison.

Security Feature	Traditional EVM	Electronic Voting	Blockchain Voting	Proposed System
Voter Privacy	Low	Moderate	High	Very High
Vote Anonymity	Low	Moderate	High	High (ZKPs)
Tamper Detection	Manual	Moderate	High	Cryptographic + DAG
Coercion Resistance	None	None	Partial	ZKPs + VDF
Vote Verification (E2E)	No	Partial	Moderate	Full (ZKPs)
Biometric Security	Manual	Centralized	Partial	Federated AI
Decentralized Identity (DID)	No	No	Optional	Yes

Table 3 evaluates the basic security components of four voting models: Traditional EVM (Electronic Voting Machine), Electronic Voting, Blockchain Voting, and the Proposed System. Both traditional and digital systems suffer from significant shortcomings on the level of privacy, anonymity, and auditability, relying heavily on centralized governance and manual processes. Blockchain techniques improve electoral anonymity and public auditability through distributed ledgers and cryptographic methods. However, they are often lacking when it comes to thorough end-to-end verification and struggle with coercion resistance. The system also introduced advanced cryptographic constructs such as Zero-Knowledge Proofs (ZKPs), Verifiable Delay Functions (VDFs), and Federated Learning (FL) to provide a 360-degree security profile. It

articulately depicts DIDs and VCs for identity management, removing the centralised vulnerabilities while maintaining cryptographic soundness and privacy for the users.

Table 4. Performance Metrics for Different Models.

Metric	Blockchain (PoW)	DAG-Based Voting	Proposed System
TPS	15 - 30	500+	>1000 (IOTA DAG)
Latency per Transaction	3 - 10 seconds	1 - 2 seconds	<1 second
Cost per Vote	$0.50 - $3.00 (Gas)	Zero	Zero
Energy per Vote (avg)	High	Low	Very Low
Edge Model Size	N/A	N/A	<10MB (FL Models)
Scalability	Moderate	High	Very High

In Table 4, the performance characteristics of standard blockchain systems using POW and DAG-based architectures with the Proposed Modular System are compared. Using DAG consensus methods, the proposed network achieves over 1000 TPS and sub-second confirmation times, when compared to blockchains, which are orders of magnitude behind in both TPS and latency. The system also comes free of transaction fees, which are high gas fees associated with Ethereum-based blockchains. The energy consumption and edge model parameters are optimized to implement mobile and IoT-based voting terminals, making the system highly scalable and cost-effective for large-scale deployment.

Table 5. Usability Survey Results.

Metric	Digitally Literate	Semi-Literate	Average
Time to Vote (mins)	1.5	2.2	1.9
Authentication Success Rate (%)	98.6	93.4	96
Interface Satisfaction (/5)	4.7	4.1	4.4
Completion without Help (%)	95.2	87.6	91.4

Table 5 shows results from a user study involving 60 participants, 30 digitally literate voters and 30 semi-literate voters, who interacted with a prototype of the proposed voting software. Findings reveal that the performance is consistently strong across all user demographic groups, with an average completion time of less than 2 minutes to cast a vote. Biometric authentication was successful in 96% of cases, and most users (91.4%) completed the voting process independently without assistance. Satisfaction ratings indicate a relatively good experience for users, particularly those with low internet exposure. The results corroborate the inclusive nature of the system, showing that a voice-assisted, multilingual, and mobile-first user interface allows broadening the demographic able to access digital voting.

Table 6. The independent results of the DAG network.

Test Parameter	Result
Votes Simulated	1,00,000
Duplicate Votes Detected	0
Vote Confirm Latency	1.2 seconds avg
VDF Time Dispersion	¬±3 seconds
Node Consensus Conflicts	0

Table 6 summarizes the findings from a large simulation test involving 100,000 virtual voters. No instances of double voting or consensus issues were documented, and the DAG ledger executed each transaction in an average of 1.2 seconds. To address this issue, VDF (Verifiable Delay Function) was introduced, which provided randomized delays and helped mitigate timing attacks without a significant effect on performance. These data validate the DAG + VDF combination to guarantee fairness, anonymity, and resistance against tampering even in the presence of large-scale voting. This proposed model also shows the scalability of computational capability by using the PoW and network consensus, or restores this model reliably.

Table 7. Comparison with Existing Systems.

System	Blockchain Used	Identity Model	Cost Per Vote	ZKP Support	Homomorphic Tally	Auditability
FollowMyVote	BitShares	Centralized	Moderate	No	No	Partial
Horizon State	Ethereum	Smart Contract	High (Gas)	No	No	Yes
Proposed Model	DAG (IOTA)	DID + VC	Zero	Yes	Yes	Yes

Table 7 provides a direct comparison of the proposed paradigm against other established e-voting services based on the included blockchain, such as Follow My Vote and Horizon State. While these platforms pioneered the basic principles of transparency and governance through smart contracts, they still rely on centralized identification systems and incur costs related to gas fees. Additionally, none of the existing platforms fully cover zero-knowledge proofs or homomorphic encryption. In contrast, the proposed system has zero-cost transparency, cryptographically verifiable, and auditable, which creates a truly end-to-end verifiable and

decentralized voting system. This represents a significant improvement over existing blockchain solutions and traditional electoral systems.

5 Conclusions

In this paper, a comprehensive and state-of-the-art e-voting architecture is proposed that overcomes the shortcomings of existing conventional and blockchain-based electoral systems. The proposed framework provides a robust, scalable, and privacy-preserving mechanism for national and global elections by utilizing Decentralized Identity (DID), Federated Learning (FL), Zero-Knowledge Proofs (ZKPs), Homomorphic Encryption, and Directed Acyclic Graph (DAG)-based consensus. It ushers in 0 tx fee, instantaneous finality, and provable-but-private votes instead of current systems burdened with high tx costs, monolithic ID storage, and smart contract risk. This modular solution builds up voter confidence by decentralizing identity management with AI-powered fraud detection at the edge, and making the casting and tallying of votes cryptographically verifiable and independently auditable. Using VDFs and ZKPs, this framework protects itself against timing-based attacks and coercion. To put it another way, the mobile-first, multilingual architecture and federated biometric authentication guarantee it is entirely accessible for and inclusive of all, and even those in digitally marginalized areas. These technologies cumulatively solve challenges like scalability, security, and transparency, and bring integrity back to elections via cryptographic proofs as opposed to faith in institutions. Their approach offers a principled approach to digital governance in a world of ever-rising scrutiny and cyber risk to democratic institutions. This work introduces a meta-tool for building secure, decentralized, AI-assisted digital voting systems. Make the grounds for the continuity of safe, inclusive, and verifiable democratic participation, instead of the societies of the digital age, paving the way to move towards more transparent and responsible.

References

[1] Hossain Faruk, Md Jobair & Alam, Fazlul & Islam, Mazharul & Rahman, Akond. (2024). Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency. Cluster Computing. 27. https://doi.org/10.1007/s10586-023-04261-x.

[2] Ohize, Henry & Onumanyi, Adeiza & Umar, Buhari & Lukman, Ajao & Isah, Rabiu & Dogo, Eustace & Nuhu, Bello & Olaniyi, Olayemi & Ambafi, James & Sheidu, Vincent & Ibrahim, Muhammad. (2024). Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. Cluster Computing. 28. https://doi.org/10.1007/s10586-024-04709-8.

[3] Dhillon, Amrita & Kotsialou, Grammateia & McBurney, Peter & Riley, Luke. (2021). Voting Over a Distributed Ledger: An Interdisciplinary Perspective. Foundations and Trends® in Microeconomics. 12. 200-268. https://doi.org/10.1561/0700000071.

[4] Albashrawi, M., Abbasi, A. Z., Li, L., & Rehman, U. (Accepted/In press). Adoption of Blockchain E-Voting Service: Digital Literacy as a Mediating Mechanism. Information Systems Frontiers. https://doi.org/10.1007/s10796-024-10532-8

[5] Miao,Y. (2023). Secure and Privacy-Preserving Voting System Using Zero-Knowledge Proofs. Applied and Computational Engineering,8,328-333. https://doi.org/10.54254/2755-2721/8/20230181

[6] Rijanto, Arief. (2024). Blockchain technology roles to overcome accounting, accountability and assurance barriers in supply chain finance. Asian Review of Accounting. 32. https://doi.org/10.1108/ARA-03-2023-0090.

[7] Vladucu, Maria-Victoria & Dong, Ziqian & Medina, Jorge & Rojas-Cessa, Roberto. (2023). E-voting Meets Blockchain: A Survey. IEEE Access. PP. 1-1. https://doi.org/10.1109/ACCESS.2023.3253682.
[8] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2521-2549, Fourthquarter 2020, doi: https://doi.org/10.1109/COMST.2020.3020092.
[9] Kahtyat, S. . (2024). Designing a Decentralized Identity Verification Platform. Norsk IKT-Konferanse for Forskning Og Utdanning, (3). Retrieved from https://www.ntnu.no/ojs/index.php/nikt/article/view/6249
[10] Aziz, Ahmed & Qunoo, Hasan & Abusamra, Aiman. (2018). Using Homomorphic Cryptographic Solutions on E-voting Systems. International Journal of Computer Network and Information Security. 10. 44-59. https://doi.org/10.5815/ijcnis.2018.01.06.
[11] Panja, Somnath Dr., "Zero-Knowledge Proof, Deniability and Their Applications in Blockchain, E-Voting and Deniable Secret Handshake Protocols." (2022). Doctoral Theses. 13. https://digitalcommons.isical.ac.in/doctoral-theses/13
[12] Pethuraj, Manickaraj & Vatchala, L. & Gayathri, S.. (2024). Securing Healthcare Data: Leveraging Blockchain for Electronic Health Records. 234-238. https://doi.org/10.1109/ICESIC61777.2024.10846251.
[13] G, Harshith & Sun, Gomathi & D, Sungeetha. (2023). Enhancing the Accuracy of Block chain Based Agriculture Product Supply Chain Management System Using Random Forest Algorithm and Decision Tree Algorithm. 163-166. https://doi.org/10.1109/iTechSECOM59882.2023.10435088.
[14] Dhanvardini, R & Martina, Pa & Vijay, R & Amirtharajan, R. & Pravinkumar, Padmapriya. (2023). Development and Integration of dApp with blockchain smart contract Truffle Framework for user interactive applications. 1-6. https://doi.org/10.1109/ICCCI56745.2023.10128406.
[15] Royal, G. H., Gomathi, S., Sungeetha, D., and Sooriamoorthy, D., “Blockchain based agriculture product supply chain management system using K nearest neighbor to enhance the accuracy and comparing with random forest algorithm”, in American Institute of Physics Conference Series, 2024, vol. 3161, no. 1, Art. no. 020220. https://doi.org/10.1063/5.0229247.
[16] Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T. T., Assam, M., Ghadi, Y. Y., & Mohamed, H. G. (2023). Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. Sensors, 23(18), 7740. https://doi.org/10.3390/s23187740
[17] Hu, Y., & Su, P. (2024). A decentralized voting system on the Polygon blockchain. Procedia Computer Science, 247, 1304–1313. https://doi.org/10.1016/j.procs.2024.10.156
[18] George, W., & Al-Ansari, T. (2023). Review of Blockchain Applications in Food Supply Chains. Blockchains, 1(1), 34-57. https://doi.org/10.3390/blockchains1010004
[19] Alshehri, A., Baza, M., Srivastava, G., Rajeh, W., Alrowaily, M., & Almusali, M. (2023). Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain. Applied Sciences, 13(2), 1096. https://doi.org/10.3390/app13021096
[20] Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024). Blockchain-Based E-Voting Systems: A Technology Review. Electronics, 13(1), 17. https://doi.org/10.3390/electronics13010017
[21] Sanjeeva, Polepaka & Sathwik, M. & Prasad, G. & Reddy, G. & Sajwan, Vijaylakshmi & Ganesh, Bande. (2023). Decentralized and Automated Online Voting System using Blockchain Technology. E3S Web of Conferences. 430. https://doi.org/10.1051/e3sconf/202343001046.