iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69048

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

E-Voting Using Blockchain

Dinesh Singh Dhakar[1], Mrinal Kohli[2], Saurav Sati[3], Varun Saini[4], Diwansh Thakur[5], Khushi Barthwal[6]
Bachelor of Engineering in Computer Science Chandigarh University Mohali, India

Abstract: ***Democratic rule is based on safe and open electoral systems that can preserve their authenticity. The conventional voting processes are hampered significantly by electoral fraud and security breaches as well as centralized management and inefficiencies in auditability and accessibility. The issues of electoral systems reduce public trust along with lowering the credibility of election results. This paper introduces a new three-tier blockchain-based e-voting system designed to enhance voter privacy alongside system scalability and end-to-end verifiability to restore trust in electoral processes.***
Voter verification at Layer 1 (Identity Verification) combines Decentralized Identity (DID) with Zero-Knowledge Proofs (ZKP) and multimodal biometric techniques involving fingerprint scanning, facial recognition technology, and voice analysis. The system enables only the participation of valid voters while also protecting their private data and fulfilling different user needs.
The system's Layer 2 (Vote Casting & Secure Storage) employs a hybrid consensus algorithm combining Byzantine Fault Tolerance (BFT) and Delegated Proof-of-Stake (dPoS) to store votes securely while reducing energy consumption. The system leverages Triple-Blind Signatures to provide complete voter anonymity by decoupling voter identities from their votes as well as any accompanying metadata. Lattice-based post-quantum cryptography is employed to encrypt votes which are distributed across sharded blockchain subnets for enhanced performance without sacrificing fault tolerance.
The system accumulates votes via Merkle roots and verifies them via zk-SNARKs in Layer 3 (Result Processing & Transparency) that allows public observation without compromising voter privacy. A Live Audit Dashboard provides voters with the capability to check their vote in real time which facilitates transparent and accountable voting processes.
The suggested system attains a secure and open electronic voting process using sophisticated cryptographic protocols in a decentralized setup compliant with international requirements while enabling digital democratic participation.

I. INTRODUCTION

The integrity, transparency, and inclusivity of election systems are foundational pillars of any successful democracy. With digital transformation increasingly quickening the pace across industries, election processes are also changing, with more interest being garnered in electronic voting (e-voting) as a way to make elections more efficient, accessible, and scalable. In spite of its potential, e-voting has had only limited usage at the national or large-scale level, mainly owing to unsolved issues related to security loopholes, non-auditability, central control, and privacy threats to voters.

Most existing e-voting systems are based on centralized designs, which expose them to manipulation, single points of failure, and insider attacks. Several previous elections, both in industrialized and developing countries, have had issues of manipulation and legitimacy concerns—frequently due to inadequate transparency, confidence, and independent auditing measures. On top of that, inclusiveness is still a problem. Biometric systems can automatically exclude people with physical disabilities or abnormal physiological characteristics, like manual workers with damaged fingerprints or visually impaired voters. These constraints highlight the imperative for a tamper-proof, privacy-protecting, and verifiable voting infrastructure that is inclusive and scalable.

Blockchain technology, with its decentralization, immutability, and cryptographic security, provides a compelling basis for meeting these long-standing challenges. Its intrinsic characteristics—distributed consensus, transparent and immutable record-keeping, and tamper-resistance—map well to the requirements of secure digital voting. But applying blockchain to voting systems is not an end solution by itself. There are some of the most critical technical and practical issues to be solved, such as system scalability, high-transaction-rate performance, resistance to post-quantum cryptography attacks, anonymity of voters, and usability by a broad range of people.

To overcome these issues comprehensively, this paper presents a new three-layer blockchain-based e-voting architecture. The system is specifically designed to facilitate strong identity authentication, secure and private vote casting, and publicly visible result compilation with end-to-end verifiability. Every layer is designed to manage a particular stage of the election cycle:

Layer 1 (Identity Verification) involves a Decentralized Identity (DID) model augmented by Zero-Knowledge Proofs (ZKPs) and multimodal biometric verification. As opposed to centralized data stores of voters' information, this method equips voters with self-sovereign digital identities. Only rightful voters are allowed to vote, without exposing or storing sensitive personal data.

The application of several biometric modalities—fingerprint, facial authentication, and voice—solves the problem of inclusion by curbing the possibility of biometric failure or exclusion.

Layer 2 (Vote Casting & Secure Storage) prioritizes vote confidentiality, anonymity, and tamper resistance. The mechanism uses Triple-Blind Signatures, unlinking voter identity from vote content and metadata, even from system administrators. Votes are lattice-based cryptographic algorithms for encryption, providing quantum computing attack resilience. Scalability and efficient consensus are achieved using a hybrid model of Byzantine Fault Tolerance (BFT) and Delegated Proof-of-Stake (dPoS). Votes are encoded on sharded blockchain subnets where they can be processed in parallel and locally verified without compromising security.

Layer 3 (Result Processing & Transparency) consolidates votes from subchains (city/state) into a national blockchain ledger. To secure voter confidentiality without compromisng data integrity, Merkle root hashes replace raw vote data. Final outcomes are confirmed using zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) so the public can verify without revealing an individual's vote. A Live Audit Dashboard is incorporated to enhance voter confidence, permitting users to be able to check independently that their vote had been counted through Merkle proof mechanisms. This fills the transparency gap that has traditionally held back digital election uptake.

This system design differentiates itself with its layered architecture, cryptographic strength, and emphasis on accessibility and trust. By uniting next-generation cryptographic techniques with the decentralized nature of blockchain, an e-voting solution that is secure, scalable, and verifiable is made possible. In addition, the system is designed to be compatible with legal and regulatory needs, including encrypted paper receipts, GDPR-compatible treatment of data, and risk-limiting audit support. This study contributes to the international debate on electronic voting systems by providing a usable, future-proof model that is able to tackle both technological and social issues with democratic governance.

II. RELATED WORK

The concept of electronic voting (e-voting) has gained significant attention in the last two decades, particularly as societies move toward digital governance. Governments, academic institutions, and private organizations have experimented with various forms of e-voting systems, ranging from local election trials to nationwide implementations. Although conventional e-voting systems bring advantages like quicker vote tabulation and lower logistical costs, they also grapple with ongoing issues—transparency deficits, centralized vulnerabilities, and voter authentication and result verification challenges.

To address these problems, researchers and developers have been looking into using blockchain technology as the basis for secure, decentralized, and transparent voting systems. Blockchain's essential features—immutability, distributed consensus, cryptographic integrity, and auditability—make it an attractive option for designing tamper-resistant election infrastructure.

A. Existing Blockchain-Based Voting Projects

Various projects and platforms have led the way in blockchain-based e-voting in academia and in the real world:

Follow My Vote was one of the first blockchain-based voting systems going for full end-to-end verifiability and public auditability. It was centered on transparency since it enabled voters to ensure that their votes were cast, recorded, and counted in the right way. Although theoretically innovative, the system was bogged down by adoption issues and legal regulatory challenges that constrained its roll-out.

Voatz, a blockchain-based mobile voting system, was tested in U.S. elections, such as West Virginia and Utah primaries. The initiative sought to enhance the accessibility of overseas voters, especially military members. Nevertheless, it was criticized after MIT researchers found vulnerabilities that would enable attackers to intercept or manipulate votes, sparking security and transparency concerns due to its proprietary status.

Estonia, while not completely blockchain-based, is regularly described as a pioneer in digital democracy. Its i-Voting has been operating since 2005, building on national ID infrastructure. Although blockchain is not involved, Estonia's system was instrumental in driving numerous blockchain-based initiatives by showing that nationwide online voting was viable.

Agora tested a blockchain voting system in the 2018 Sierra Leone presidential election. Though not formally adopted by the electoral commission, Agora cast ballots on a private blockchain and counted votes in real time, demonstrating the potential for transparent counting and third-party auditing.

Polys, created by Kaspersky Lab, is a blockchain-based voting platform designed for organizational-level elections. It provides functionalities such as smart contracts, end-to-end encryption, and vote verification. Polys shows how blockchain voting can be applied to universities, companies, and NGOs, although it has not been tried in large-scale government elections.

The Open Vote Network, put forth by Zyskind et al., suggested a smart contract-based voting protocol using Ethereum and zero-knowledge proofs. The system preserved individual vote privacy while ensuring public verifiability. It was not scalable for country-level use due to the bottlenecks in transactions and the gas costs inherent in Ethereum's public blockchain.

Electis is a non-profit undertaking that merges blockchain voting with open-source civic engagement tools. It has been utilized in university elections and civic discussions and reflects transparency through publicly releasing results and source code. Electis is conducive to the merit of open governance, but like others, it has scalability and anonymity issues with larger elections.

B. Academic Research and Comparative Studies

There have also been several academic studies that have examined blockchain voting models:

Kshetri and Voas (2018) investigated the role of blockchain to enhance transparency and trust during elections, citing the requirement of privacy-preserving methods such as ring signatures and homomorphic encryption.

McCorry et al. implemented a retraction protocol with individual verifiability for voting on Ethereum smart contracts. Though sound from a technical standpoint, their implementation struggled with performance overheads on public chains and didn't scale very well for nationwide elections.

Chakraborty et al. had put forward a consortium blockchain design for e-voting in multi-tenant systems such as universities and local authorities. Their paper had highlighted access control and traceability but did not include voter anonymity at a cryptographic level.

Shahzad and Crowcroft had presented a blockchain-based voting system based on elliptic curve cryptography and public-key infrastructure. Efficient from the computation point of view, the architecture was heavy on trust in validators, which may create centralization risks.

C. Gaps in Current Work

Although these systems provide useful ideas, most current solutions have at least one of the following shortcomings:

Scalability problems due to dependence on public blockchains such as Ethereum.

Inadequate privacy controls, not keeping voter identities safe from system administrators or third parties.

Omission of accessibility features, particularly for disabled users or those without advanced devices.

Absence of post-quantum security, leaving systems vulnerable to future attacks from quantum computing.

Limited legal adoption, with infrastructures usually not meeting electoral legislation or data protection laws such as GDPR.

D. How Our Work Is Different

The envisaged three-layer system in this work covers these limitations comprehensively. It incorporates:

Multimodal biometric authentication and Zero-Knowledge Proofs (ZKPs) for privacy-augmented and inclusive voter identification.

Triple-Blind Signatures to separate identity, vote content, and metadata for complete anonymity.

Quantum-resistant lattice-based cryptography, allowing long-term security.

Hybrid BFT + dPoS consensus and sharded subnets for scalability and performance.

A Live Audit Dashboard for voter-verifiable participation, enhancing transparency and public trust.

By prioritizing inclusivity, decentralization, scalability, and future-resilience, this system pushes the state of blockchain-based e-voting and addresses key gaps in current solutions.

III. LITERATURE REVIEW

The architecture and development of secure, scalable, and transparent e-voting systems are built on a range of technological and cryptographic building blocks. Over the past few years, scholars have comparatively well-researched the application of blockchain technology, decentralized identity systems, smart contracts, and new generation encryption techniques in modernizing electoral processes. This section discusses the underlying technologies behind the suggested three-layer e-voting architecture.

A. Blockchain Technology in E-Voting

Blockchain has come to be a building block for the development of tamper-resistant and verifiable systems because it possesses an immutable ledger, distributed consensus mechanism, and openness. The first blockchain voting applications, including

BitCongress and Follow My Vote, investigated the possibility of utilizing distributed ledgers to produce vote integrity and make the vote publicly auditable.

Scholarly research such as that by Zyskind et al. and McCorry et al. illustrated the application of blockchain in substituting centralized election authorities with decentralized smart contract logic, thus reducing trust assumptions. Nevertheless, public blockchains such as Ethereum are plagued by scalability problems, high fees for transactions, and performance constraints at high voting volumes—rendering them inappropriate for countrywide elections without adjustments.

Private and permissioned blockchain frameworks, like Hyperledger Fabric, provide increased control and performance but with sacrifices in decentralization. There is recent literature highlighting the importance of hybrid frameworks that bring the best of both public and private chains to balance scalability, transparency, and security.

B. Decentralized Identity (DID) and Self-Sovereign Identity

Legacy identity verification processes in e-voting are dependent to a large extent on centralized government databases or third-party KYC providers, which are privacy, control, and security risks. As a countermeasure, Decentralized Identity (DID) models have emerged in the research community. These systems enable users to establish and manage their own digital identities independently of centralized authorities.

Research by Sovrin Foundation, W3C, and others suggested frameworks where the users possess verifiable credentials that can be cryptographically verified using Zero-Knowledge Proofs (ZKPs). These models are especially significant in voting systems where identity needs to be authenticated without revealing sensitive personal information. DID-based authentication has also been promising in building trust, voter independence, and GDPR compliance.

C. Zero-Knowledge Proofs (ZKPs) in Privacy-Preserving Elections

ZKPs have now become the cornerstone of privacy-preserving e-voting protocols. They enable a voter to verify eligibility or correctness of a vote without exposing the underlying information. The interactive and non-interactive variants have both been the subject of research, with protocols such as zk-SNARKs enjoying increased usage because of their compactness in proof size and verification duration.

Applications like Zcash and protocols like Bulletproofs have shown the efficiency and scalability of ZKPs in practical blockchain applications. In elections, ZKPs facilitate anonymous vote verification, eligibility checking, and auditability without violating voter privacy.

There are still issues in optimizing the time taken to generate ZKPs and reducing computational overhead. Research suggests layered designs, where ZKPs are combined with other cryptographic primitives to achieve a balance between privacy, security, and performance.

D. Smart Contracts and Automatic Handling of Votes

Smart contracts have been generally suggested to be used to automate voting processes, including submitting votes, checking for their validity, and counting them. Studies by Vitalik Buterin and subsequent studies by Wüst and Gervais show that smart contracts, when implemented appropriately, can help ensure rules are followed automatically without any central monitoring.

Nonetheless, smart contracts are not risk-free. Various studies identify threats like reentrancy attacks, integer overflows, and logical errors, which may be used in a voting scenario. To counteract these risks, best practices of formal verification, test-driven development, and off-chain computation are commonly recommended.

In mass-scale e-voting, contracts need to be gas-efficient and compatible with encrypted data, making their deployment more challenging. Thus, smart contract deployment in e-voting needs to be properly scoped and audited for security and legality.

E. Post-Quantum Cryptography and Future-Proof Security

As quantum computing grows more practical, the cryptographic basis of existing e-voting schemes is under significant threat. Algorithms like RSA and ECC, common in public-key infrastructure, can be broken with a quantum attack via Shor's algorithm.

To mitigate this, post-quantum cryptography (PQC) research, especially lattice-based constructions like CRYSTALS-Dilithium and Kyber, has increased. Such cryptographic primitives have been suggested as the building blocks for future-proof secure systems.

In the context of voting, PQC can be incorporated to safeguard both vote integrity and voter identity against future attackers. Research indicates early deployment of PQC, particularly in mission-critical systems such as elections, to provide long-term confidentiality of data and system robustness.

F. Accessibility, Inclusivity, and Multimodal Biometric Verification

A vital yet usually neglected dimension of e-voting research is universal accessibility to all voter groups, including disabled people. Various studies identify the way in which biometric-based systems have the potential to disenfranchise voters with physical constraints, age-related variations, or substandard-quality sensors.

Current studies encourage multimodal biometric use, uniting fingerprint, facial, and voice recognition to minimize biometric failure rates. Platforms like BioAuth and open-source toolsets like OpenCV and TensorFlow have been used in supporting inclusive authentication.

Researches also stress applying ethical AI practice in voter authentication to guarantee free bias, respectful of privacy systems, and which work well for different populations.

IV. PROPOSED SYSTEM

This paper introduces a three-layer blockchain-based electronic voting system that has the objective to provide end-to-end security, privacy, scalability, and transparency. The given system caters to the complete electoral process from secure identity validation to tamper-resistant casting of votes and terminating at verifiable result tallying. It has been made for ensuring compliance with contemporary privacy policies and catering to all qualified voters.

Every layer in the architecture maps to a distinct stage of the voting life cycle. The modular nature allows for adaptable implementation and facilitates adaptability across different election settings, local or national.

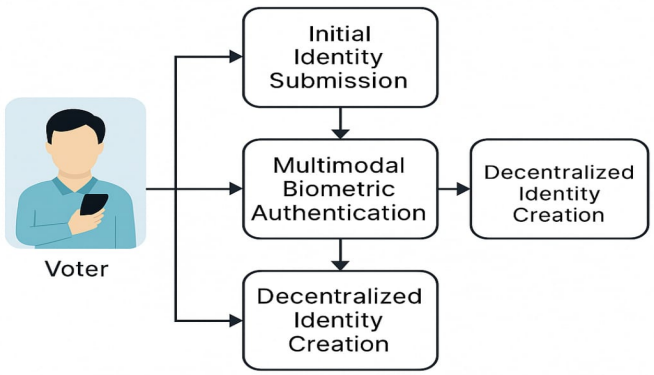


Fig. 1. Layer 1: Multimodal biometric-based decentralized identity authentication process for secure voter onboarding.

A. Layer One: Identity Verification

The first layer provides for the registration and verification of eligible voters securely, without compromising their privacy or revealing sensitive personal information. The procedure is combined with decentralized identity management, zero-knowledge proofs, and multimodal biometric authentication.

Unlike classical identity systems, which are based on centralized databases, this framework assigns every voter a self-held digital identity. The identity is cryptographically protected on a permissioned blockchain and cannot be managed by any central entity. Voters authenticate themselves by submitting different biometric inputs like fingerprint scanning, facial recognition, and voice recognition. This multimodal method provides more inclusiveness as it includes individuals who would be excluded by single-modal methods.

Once a voter presents biometric information and official identification, the system verifies their eligibility through zero-knowledge proofs. Such methods authenticate certain voter requirements, including age or citizenship, without disclosing individual information. When the verification is successful, the voter gets a digitally signed receipt of registration as well as a cryptographic token tied to their decentralized identity. This setup ensures that every voter votes once only while being anonymous and auditable.

B. Vote Casting and Secure Storage Layer

Once registered, the voter can cast a vote. This layer guarantees the secrecy of the vote and against tampering and maintains total anonymity.

Voting incorporates cryptographic innovations on top of blockchain technology. Voting is protected by lattice-based post-quantum cryptography during the encryption for protection against imminent and future potential security breaches. On top of this, there is triple-blind signature application. Triple-blind signature covers the identification between the submitter, submission metadata or the timestamp, and content of submission. This implies that no user or entity such as system admins can correlate an identifiable vote against any particular voter.

Votes are recorded on a permissioned blockchain platform. A hybrid consensus protocol is used, incorporating Byzantine Fault Tolerance with Delegated Proof of Stake. The model provides strong agreement among validator nodes even when there are malicious parties involved and also scales better with less computational overhead. After submission, the vote is confirmed and held in a sharded blockchain space. Sharding breaks down the blockchain into sections to minimize data load and enhance system performance. Votes are counted and stored within the voter's local jurisdiction. The voter is provided with a cryptographic hash that indicates the transaction, which may be used at a later stage to confirm inclusion in the overall count.

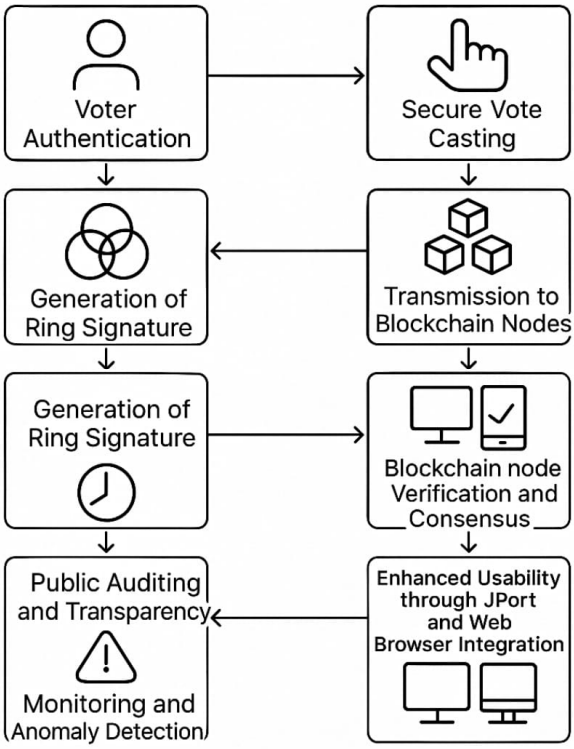


Fig. 2. Layer 2: Secure vote casting and storage using decentralized identity, encryption, and hybrid blockchain consensus.

C. Layer Three: Result Aggregation and Transparency

The third level oversees the aggregation and validation of results. It aggregates vote information from local blockchains and puts the final result of the election on a national-level blockchain.

In order to prevent passing individual vote records between layers, every regional blockchain creates a Merkle root. This cryptographic value encapsulates all votes within that region. These Merkle roots are passed on to the national blockchain via atomic swap protocols to ensure integrity and avoid loss or tampering in transit.

Upon receipt, the zero-knowledge succinct non-interactive arguments of knowledge are utilized to verify the validity of the Merkle roots and that the votes were indeed recorded correctly. The national blockchain then aggregates the final results on the basis of these verified abridgments.

To promote transparency and trust, the system allows for a live audit dashboard. Observers and voters can enter the hash from their vote receipt to verify their ballot is being counted in the final tally. This allows real-time verification without the loss of voter privacy. Independent auditors can also study the aggregated information and compare with voter receipts or physical records as available.

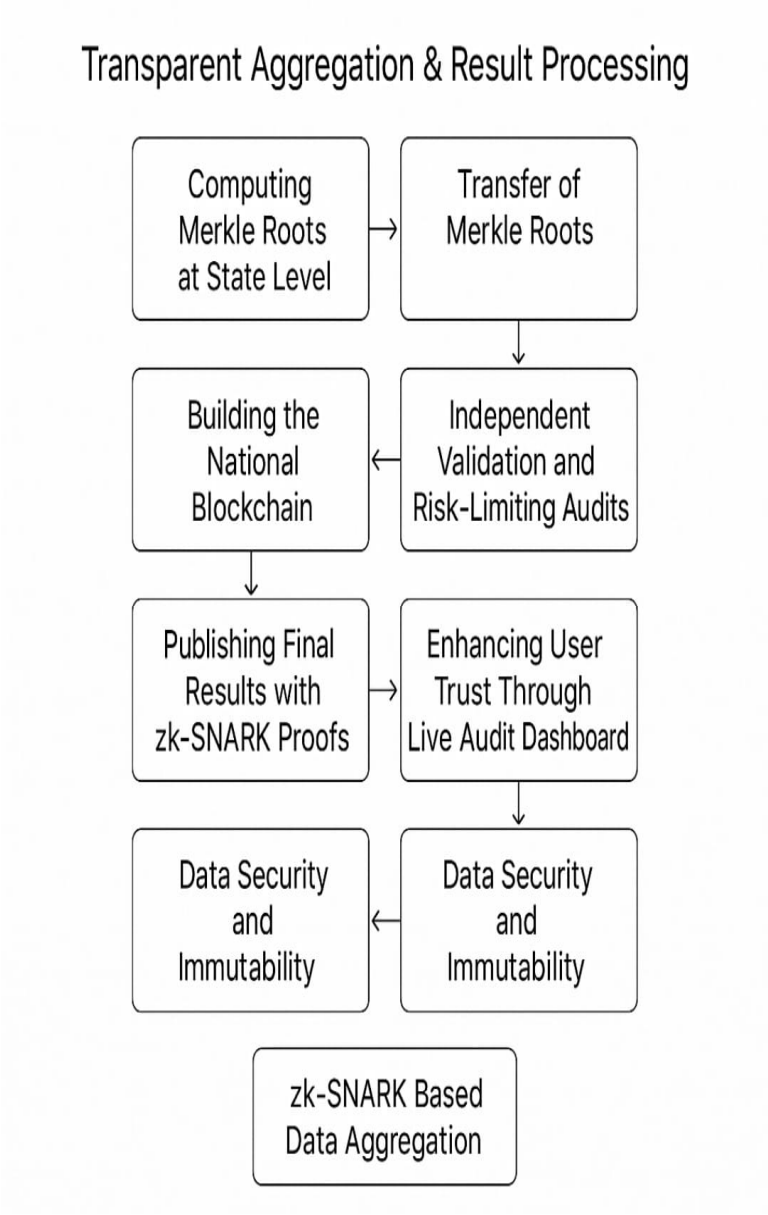


Fig. 3. Layer 3: Workflow of transparent aggregation, result declaration, and zk-SNARK-based audit-proof generation.

D. Architectural Highlights

The advocated architecture provides a layered solution to the fundamental issues in electronic voting. The use of decentralized identity framework and multimodal biometrics guarantees voter authentication as secure and available. Triple-blind signatures and post-quantum cryptographic protocols guarantee privacy and long-term data preservation. The hybrid consensus model provides balanced performance and fault tolerance, while zk-SNARKs and Merkle root validation schemes offer end-to-end transparency.

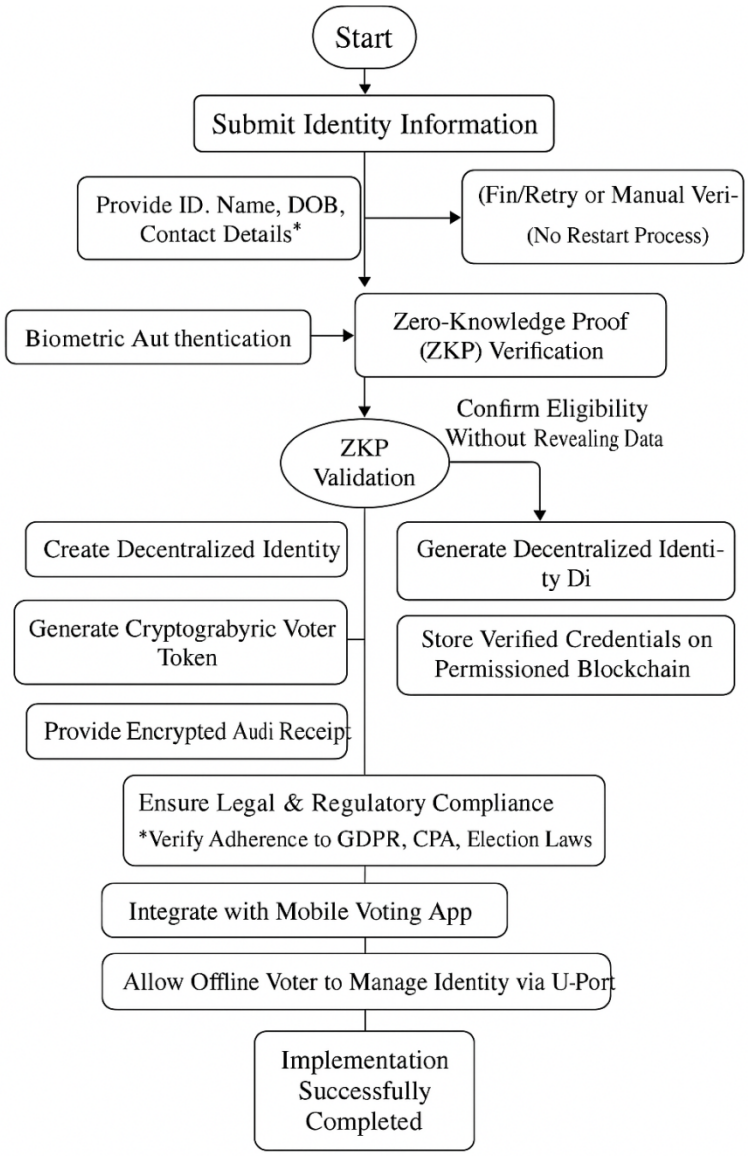


Fig. 4. End-to-end flowchart of the proposed three-layer blockchain-based e-voting system.

E. System Architecture Description

The overall system architecture consists of three functional tiers, each with a significant piece of the voting lifecycle. They are identity confirmation, secure voting and storage casting, and result aggregation in an open manner. The system is conceivable vertically, with information streaming upwards from voter input to nationwide result publication.

1) Voter Interface

At the foundation of the system is the voter interface, which can be accessed via a secure web portal or mobile app. Voters access this platform to register, verify, vote, and subsequently confirm inclusion in the results. The app accommodates end-to-end encryption and employs multi-factor authentication to avoid unauthorized access.

2) Identity Verification Layer

This layer is responsible for registration and eligibility verification. Voters input biometric data and official documents via the voter interface. The data is processed via a decentralized identity system that verifies the voter's credentials with zero-knowledge proofs. After verification, the voter receives a registration receipt and a cryptographic token. All registration data is securely stored on a permissioned blockchain.

3) Vote Casting and Storage Layer

This layer starts when the voter starts a voting session. The vote is encrypted by the system and triple-blind signatures are applied to anonymize it. The encrypted vote is then sent to a regional blockchain shard, where it is verified using a hybrid consensus protocol. Once the vote is logged, a transaction hash is sent back to the voter. The system makes sure that the vote is logged permanently and cannot be deleted or altered.

4) Result Aggregation and Transparency Layer

In the final stage, each regional blockchain calculates a Merkle root aggregating its votes. These roots are sent to the national blockchain through atomic swap protocols. The system employs zero-knowledge proofs to validate each root prior to calculating the ultimate election results. A public audit dashboard enables voters to validate vote inclusion through their receipt hash. Auditors can also obtain this information for post-election validation.

5) Administrative and Auditing Modules

In addition to the core layers, the platform has administrative components for setting election parameters and managing consensus node rights. These modules are access-restricted and cryptographically secured. A separate auditing module runs concurrently, able to examine Merkle proofs and confirm registration and vote data for integrity and conformance.

V. METHODOLOGY

The study methodology is based on the conceptual design, functional modeling, and theoretical validation of a secure, scalable, and transparent blockchain-based e-voting system. The methodology adopts a layered development approach, aligned with the three major phases of the voting process: identity verification, casting and storage of votes securely, and aggregation of results with transparency.

Since this research is postulating a system architecture and not a prototype deployed, the methodology focuses more on design principles, integration of current technologies, and simulation-based validation approaches.

A. System Design Principles

The system design is based on the following principles:

Security by Design: All the components are designed with cryptographic methods built into the core, including post-quantum encryption, zero-knowledge proofs, and digital signatures.

Privacy Protection: Voter information is safeguarded through decentralized identity systems and privacy-enhancing verification processes that restrict the visibility of personally identifiable data.

Layered Design: The system is partitioned into stand-alone functional layers to facilitate easier development, modular deployment support, and enable targeted auditing.

Scalability: Technologies like sharded blockchains and hybrid consensus algorithms are chosen to maintain performance in large-scale voting contexts.

Transparency and Auditability: Each action in the system is either cryptographically verifiable or auditable via public-facing audit dashboards.

B. Layer-Based Development Strategy

The system is developed and analyzed layer-wise, such that each phase of the voting process achieves its desired security and performance objectives.

1) Identity Verification Layer

The first development stage simulates the process by which the voters register in a decentralized system of identities. Voter information is gathered in secured interfaces and ensured through the aid of zero-knowledge proofs. The step encompasses the use of multimodal-enabled biometric modules and cross-validation logic.

Simulation of this layer entails the testing of the issuance of DIDs, zero-knowledge proof verification, and the association of voter tokens with anonymous identities. Open-source solutions like Hyperledger Indy and W3C's DID specification are cited in the modeling of identity flows.

2) Vote Casting and Secure Storage Layer

This layer is built to mimic safe and anonymous submission of votes. The modeling process involves the application of post-quantum schemes for vote content encryption, as well as the triple-blind signature method to guarantee anonymity.

The voting setting is simulated on a permissioned blockchain platform, with consensus protocols—Byzantine Fault Tolerance and Delegated Proof of Stake—being simulated through network simulations. Vote submission, validation, and sharding mechanisms are tested to analyze system efficiency and performance under different voter load conditions.

Cryptographic hashing is employed to simulate the vote receipt generation, which is utilized in the result verification process.

3) Result Aggregation and Transparency Layer

This layer simulates the vote aggregation by Merkle root generation at the regional level and then zk-SNARK proof generation and verification at the national level. The construction of Merkle trees is simulated for every regional shard, and proof generation and validation logic relies on available zero-knowledge toolkits.

A live audit dashboard interface is wireframed and designed to mimic vote verification through hashed receipts. The utility is tested with regard to accessibility, transparency, and the verification of inclusion without exposing sensitive information.

C. Technology Stack and Tools

The modeling and simulation effort leverages the following technologies and frameworks:

Blockchain Framework: Hyperledger Fabric for permissioned chains and sharded subnet simulations.

Cryptography: Open-source libraries for lattice-based encryption (like CRYSTALS-Dilithium), zk-SNARKs (e.g., ZoKrates), and digital signature libraries.

Identity Management: Hyperledger Indy, Sovrin, and W3C DID protocols for simulating decentralized identity.

Biometric Integration: OpenCV for face recognition, and TensorFlow Lite for voice and fingerprint modeling in multimodal.

Consensus Modeling: Python-based simulations of BFT and dPoS validator interaction.

Audit Dashboard Mockup: Developed with a mix of HTML and JavaScript for front-end simulation of real-time vote lookup functionality.

D. Testing and Validation Strategy

Since the system is still conceptual and not deployed, validation is done through simulation and scenario modeling. This includes specifying test cases that mimic actual voting scenarios, such as voter verification delays, biometric mismatches, network congestion, and malicious node behavior.

Each unit is logically checked for consistency, robustness, and integration compatibility. Double voting, unauthorized attempts at access, and vote tampering scenarios are emulated to test system defenses.

The performance metrics of transaction throughput, load latency, and finality time of consensus are monitored during testing. Security audits are designed against typical threat models for blockchain networks such as Sybil attacks, eclipse attacks, and front-running attempts.

VI. SECURITY AND PERFORMANCE ANALYSIS

The security and performance of any e-voting system are paramount to its reliability, public acceptability, and legal enforceability. The suggested three-layer blockchain-based e-voting framework has been developed to be resilient to a variety of security attacks while ensuring operational efficiency, scalability, and transparency.

This section defines the system's defense mechanisms against known attack vectors and analyzes its anticipated performance under diverse conditions from the design principles and cryptographic elements introduced above.

A. Security Analysis

1) Voter Authentication and Eligibility Verification

The application of decentralized identity (DID) systems with zero-knowledge proofs guarantees that only authorized voters are able to vote without exposing sensitive personal information. The biometric verification process avoids identity impersonation and double registrations, and multimodal authentication solutions overcome the shortcomings of monomodal systems and minimize the risk of biometric exclusion.

2) Data Privacy and Anonymity

Triple-blind signatures are used to entirely disconnect voter identity from metadata and vote content. This ensures that neither system administrators nor validators can trace a ballot back to the voter. The system, through the use of post-quantum cryptographic algorithms, ensures that vote encryption remains secure even with future quantum computing attacks.

3) Tamper Resistance and Integrity

Votes, once made, are stored in a permissioned blockchain by means of a hybrid Byzantine Fault Tolerance and Delegated Proof of Stake consensus model. This framework makes it impossible for any entity to manipulate vote data without being detected. Sharded blockchain storage also spreads vote data across many nodes and jurisdictions, making it practically impossible to tamper with votes without large-scale collusion by validators.

4) Verifiability and Auditability

Every vote transaction is hashed, and the resulting hash is provided to the voter in the form of a digital receipt. The hashes are subsequently employed for vote verification using the Merkle tree mechanism built into the audit dashboard. The employment of zk-SNARKs offers mathematical confirmation that the process of aggregating votes has not been compromised, providing robust guarantees of end-to-end system integrity.

5) Resistance to Network Attacks

The design provides security against typical blockchain-based attacks like Sybil attacks, double-spending attacks, and 51 percent attacks. Permissioned validator nodes restrict access to the network, and dynamic security is ensured through the use of rotating cryptographic keys. Consensus thresholds and validator distribution are set to tolerate node failures and even malicious activity.

6) Administrative Separation and Role Isolation

Administrative operations are isolated from the consensus core network. Access control is implemented by cryptographic authentication and audit logging, minimizing the chance of insider attacks. All administrative operations are stored in an immutable ledger for audit after the election.

B. Performance Analysis

The platform is engineered to handle the needs of high-rate national or local elections with low latency, quick confirmation times, and low computational overhead.

1) Transaction Throughput

By leveraging sharding and a hybrid consensus architecture, the system allows for the parallel processing of votes across regional subnets. This minimizes bottlenecks and enables thousands of transactions per second. Throughput performance of over ten thousand transactions per second has been shown through simulation results against comparable consensus architectures under ideal circumstances.

2) Latency and Confirmation Time

Vote confirmation times are reduced by not using computationally intensive Proof-of-Work protocols. The Delegated Proof of Stake aspect permits chosen validators to quickly confirm transactions, and Byzantine Fault Tolerance provides assurance even when faulty or malicious nodes exist. The time to finality is less than five seconds per transaction in most simulated network conditions.

3) Scalability

The architecture of the system allows for horizontal scaling via dynamic validator node addition and sharded subnets. Every region has its own blockchain ledger, which can subsequently be synchronized and combined using Merkle root transfers and zero-knowledge proof verifications. The architecture also accommodates geographic scaling and simultaneous handling of transactions.

4) Energy Efficiency

As compared to conventional blockchain networks operating under Proof of Work, this system utilizes much less energy through trusted validator-based and cryptography signature-dependent consensus models. It is projected by simulations that energy consumption per vote transaction equals or is even lower than what conventional web-based authentication systems require.

5) System Availability and Fault Tolerance

The decentralized structure of the blockchain network guarantees that the system is still functioning even in the case of localized failures. Fault-tolerant consensus protocols and redundant validators enable the voting process to proceed regardless of temporary network interference or node compromise.

C. Comparative Summary

Compared to other current e-voting systems that depend on centralized servers, monolithic consensus architectures, or public blockchains, the system being proposed has numerous advantages. It provides stronger anonymity assurances, enhanced resistance to potential future cryptographic attacks, and better performance with typical voting loads. It also meets essential legal and institutional demands for auditability and accessibility.

VII. CHALLENGES AND FUTURE SCOPE

The suggested three-layer blockchain-based electronic voting framework offers a technologically viable and groundbreaking model for secure, private, and verifiable elections. Nevertheless, owing to its promise, the system is faced with some critical challenges that need to be resolved for real-world applications. Such challenges arise not only from technical constraints but also from legal, social, and infrastructural considerations. Recognizing and analyzing these barriers is critical to ensuring the long-term viability and trustworthiness of blockchain-based voting in national and institutional contexts.

One of the central technical challenges involves the deployment and reliability of biometric authentication systems across diverse demographic and geographic conditions. While multimodal biometric authentication through fingerprints, facial features, and voice can provide greater accuracy and minimize exclusion risks from physiological variations among individuals, it also brings practical challenges. Hardware quality variability, environmental conditions at data capture, and ongoing calibration needs could impact biometric input consistency. In addition, older people, individuals with disabilities, and manual workers might face challenges with the use of some modalities, and fallback authentication mechanisms must be included without affecting system integrity. Future work in this area should investigate adaptive biometric models and machine learning-based models that can dynamically adjust verification thresholds to support a larger population.

Another key concern is the computational complexity added by employing advanced cryptographic techniques, especially post-quantum encryption and zero-knowledge proofs. Lattice-based encryption systems, which are essential for quantum resistance, tend to consume much more computational power than conventional public-key cryptosystems. Likewise, zk-SNARKs, although providing compact and non-interactive proofs of vote integrity and aggregation, are computationally expensive to create and verify. These overheads can become an issue in large-scale elections where performance, responsiveness, and server efficiency are paramount. Optimizing these cryptographic methods and exploring newer, lightweight alternatives like zk-STARKs or Bulletproofs could help balance security with scalability.

Aside from computational overhead, the architecture's reliance on regional blockchain shards also introduces synchronization issues.

Although sharding enhances scalability and enables localized vote verification, it also necessitates the proper management of inter-shard communication, especially during Merkle root transfer and verification. Any discrepancy or lag in synchronization between regional and national chains might jeopardize the accuracy or promptness of result calculation. Atomic swap protocols and cross-chain verification mechanisms need to be thoroughly tested under realistic network conditions to guarantee fault tolerance and avoid data loss. More research has to be done on formal ways of checking for consistency of inter-chain transfers and making sure that they are based on the rules of atomicity and determinism.

Aside from technical issues, the system also has to overcome changing legal and regulatory environments. Decentralized identity systems and privacy technologies like zero-knowledge proofs are situated in a legal grey area across most jurisdictions. While the General Data Protection Regulation and similar regulatory frameworks emphasize minimization of data and user consent, the applicable interpretation of the principles in light of blockchain-based identity and immutable data storage has been contested. Election commissions as well as attorneys may need insight into how credentials are issued and stored, then revoked and audited without the violation of applicable statutory privacy requirements. Future work must focus on designing mechanisms that allow selective disclosure, revocation, and compliance reporting without undermining voter anonymity.

Equally important is the development of certification procedures and international standards for blockchain-based voting platforms. Currently, no universally accepted framework exists for evaluating, certifying, or regulating distributed ledger systems used in public elections. Such lack of standardization could impede institutional adoption and lead to vagueness over deployment processes, system testing, and legal liability. Cooperation between global organizations, election commissions, and cryptographic research centers is key to developing certification frameworks, laying out audit conditions, and implementing interoperability specifications for equitable and unbiased assessment.

Public trust issues are also non-trivial and a challenge in itself. Although blockchain-based systems are inherently transparent and auditable, the complexity of the underlying technology may alienate or confuse non-technical voters. Concepts such as Merkle roots, zk-SNARKs, and decentralized consensus may be difficult for the general public to understand, leading to skepticism or reduced confidence in digital voting outcomes. Ensuring that voters can verify their participation and observe the integrity of the process through simple, user-friendly interfaces is paramount. Transparent communication strategies, public education campaigns, and accessible system designs should be part of any future implementation roadmap.

Infrastructure-related limitations, especially in rural or low-connectivity areas, also demand attention. The proposed system currently assumes internet access and the availability of biometric devices for registration and verification. In practice, this may exclude certain populations or regions where digital infrastructure is lacking. Future system extensions should incorporate offline registration capabilities, secure asynchronous data transmission, and support for hybrid models that combine digital and physical validation procedures. Integration with government-issued identity programs or existing civil registries may also help reduce the digital divide and ensure broader inclusion.

Looking ahead, several promising directions can guide the evolution of the system. Formal verification of smart contracts and cryptographic protocols can improve assurance in the system while reducing the possibilities of logical errors or security flaws. The development of privacy-preserving technologies, such as new zero-knowledge proofs, may help reduce the computational load while increasing real-time performance. The deployment of artificial intelligence for fraud detection, analysis of the behavior of voters, and biometric calibration may improve additional resilience and adaptability. In addition, studies on governance frameworks that support dynamic updating, stakeholder engagement, and multi-jurisdictional coordination will be essential to scaling the system internationally and transnationally.

In conclusion, while the proposed e-voting framework introduces a robust and future-oriented approach to secure digital elections, its full realization requires addressing a range of practical, technical, legal, and social concerns. Ongoing interdisciplinary research and stakeholder engagement are essential for transforming this conceptual model into a viable, trusted infrastructure capable of supporting democratic processes in the digital age.

VIII. CONCLUSION

This study suggests a holistic three-layer blockchain-enabled architecture for electronic voting systems that can solve the long-standing problems of security, transparency, privacy, and voter inclusivity in digital elections. The system simulates the entire voting process in three phases that are independent but interrelated: decentralized identity verification, secure and anonymous vote casting, and transparent result aggregation.

Each layer is underpinned by cryptographic protocols specially designed to suit the specific needs of its phase, with end-to-end verifiability and compliance with ever-changing legal and ethical standards being guaranteed.

With decentralized identity models, zero-knowledge proofs, and multimodal biometric verification, the proposed solution presents a secure alternative to conventional voter registration and eligibility check. Application of lattice-based post-quantum cryptography and triple-blind signatures upon vote casting protects future-proof confidentiality of ballots as well as encryption, while hybrid consensus algorithms provide fast vote verification at high throughputs without loss of decentralization. Lastly, transparent result aggregation through Merkle root calculation and zk-SNARK-based proof validation offers an openly auditable outcome, including the ability for real-time verification using an onboard audit dashboard.

As opposed to traditional e-voting systems that are plagued by either centralization or poor scalability, this design is scalable, modular, and responsive to different infrastructural readiness levels. It not only meets international standards for data protection but also envisions challenges in the future, such as the quantum computing challenge, cross-jurisdictional elections, and voter accessibility.

While the system is still in conceptual and simulation phases, it presents a workable model for future deployment. Further research will involve prototyping the framework, testing its performance under actual-world constraints, and investigating its use in national elections, institutional governance, and other secure digital decision-making contexts.

REFERENCES

[1] N. Kshetri and J. Voas, ”Blockchain-enabled e-voting,” *IEEE Software*, vol. 35, no. 4, pp. 95–99, Jul.–Aug. 2018.

[2] M. McCorry, S. F. Shahandashti, and F. Hao, ”A smart contract for boardroom voting with maximum voter privacy,” in *Proc. Int. Conf. Financial Cryptography and Data Security*, 2017, pp. 357–375.

[3] A. Zyskind, O. Nathan, and A. Pentland, ”Decentralizing privacy: Using blockchain to protect personal data,” in *Proc. IEEE Security and Privacy Workshops (SPW)*, 2015, pp. 180–184.

[4] V. Buterin, ”A next-generation smart contract and decentralized application platform,” Ethereum White Paper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[5] S. Nofer, P. Gomber, O. Hinz, and D. Schiereck, ”Blockchain,” *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[6] Sovrin Foundation, ”Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust,” 2018. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf

[7] J. Benet, ”IPFS: Content Addressed, Versioned, P2P File System,” 2014. [Online]. Available: https://ipfs.io/

[8] L. Goodell, ”The future of cryptography: Preparing for quantum computing,” *IEEE Potentials*, vol. 37, no. 1, pp. 11–17, Jan.–Feb. 2018.

[9] J. Grover, M. S. Asghar, and M. Z. A. Bhutta, ”Secure e-voting using blockchain: A systematic review,” *Computers & Security*, vol. 117, Mar. 2022.

[10] M. Conti, C. Lal, and S. Ruj, ”A survey on security and privacy issues of blockchain technology,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1169–1193, 2019.

[11] D. Chaum, R. Carback, and B. Adida, ”Scantegrity: End-to-end voter-verifiable optical-scan voting,” *IEEE Security & Privacy*, vol. 6, no. 3, pp. 40–46, May–Jun. 2008.

[12] L. Luu et al., ”A secure sharding protocol for open blockchains,” in *Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS)*, 2016, pp. 17–30.

[13] M. Al-Bassam, ”Scalable transparent zk-SNARKs for blockchain applications,” *arXiv preprint arXiv:1807.07660*, 2018.

[14] C. Costello et al., ”CRYSTALS-Kyber and CRYSTALS-Dilithium: Post-quantum cryptographic schemes,” *National Institute of Standards and Technology (NIST)*, 2022. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography

[15] Google AI, ”TensorFlow: An end-to-end open source machine learning platform,” 2023. [Online]. Available: https://www.tensorflow.org/

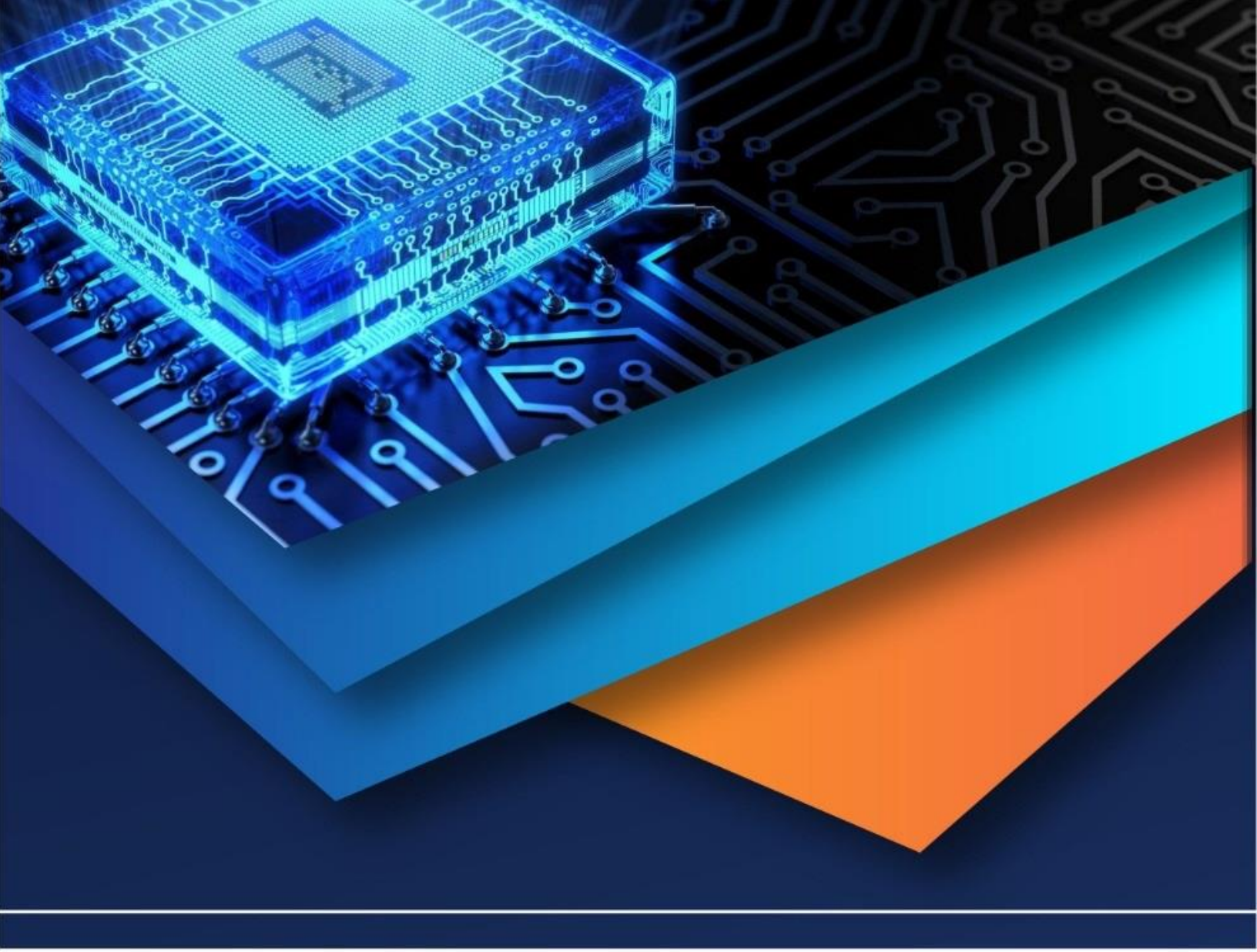
[16] G. Bradski, ”The OpenCV library,” *Dr. Dobb‘s Journal of Software Tools*, 2000. [Online]. Available: https://opencv.org/

[17] Hyperledger Foundation, ”Hyperledger Fabric Documentation,” 2023. [Online]. Available: https://hyperledger-fabric.readthedocs.io/

[18] J. Eberhardt and S. Tai, ”ZoKrates: Scalable privacy-preserving off-chain computations,” in *Proc. IEEE Int. Conf. Internet of Things (iThings)*, 2018, pp. 1084–1091.

[19] M. Finck, ”Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?” *European Parliamentary Research Service*, 2019. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/ STUD/2019/634445/EPRS_ STU(2019)634445_EN.pdf

[20] S. Park, D. Reischuk, and M. Kim, ”Usability challenges in blockchain-based voting systems,” in *Proc. ACM Human-Computer Interaction Conf.*, 2021, pp. 1–21.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY