Blockchain based e-voting system

Prof. Manjula Sandirigama
Department of Computer Engineering
University of Peradeniya
Peradeniya, Sri Lanka
manjula.sandirigama@eng.pdn.ac.lk

Silva N. H. D. U.
Department of Computer Engineering
University of Peradeniya
Peradeniya, Sri Lanka
e19375@eng.pdn.ac.lk

Senevirathne T. N.
Department of Computer Engineering
University of Peradeniya
Peradeniya, Sri Lanka
e19363@eng.pdn.ac.lk

Kaushalya N.V.K.
Department of Computer Engineering
University of Peradeniya
Peradeniya, Sri Lanka
e19193@eng.pdn.ac.lk

***Abstract*—Voting is a fundamental pillar of democracy, ensuring security, integrity, and transparency. While traditional paper ballot systems remain widely used due to their simplicity, they face challenges such as vote tampering, inefficiencies in counting, high labor costs, and absentee voting difficulties. To address these issues, electronic and internet-based voting systems have been introduced, offering improved efficiency and accessibility. However, these systems are vulnerable to cyber threats and often lack verifiability, raising concerns about voter trust and election transparency.**

Blockchain technology has emerged as a promising solution, leveraging decentralization, cryptographic security, and transparency to enhance key voting properties such as anonymity, privacy, verifiability, and fairness. This paper provides a comparative analysis of existing blockchain-based e-voting systems, examining their advantages and limitations. By identifying key research gaps and challenges, we aim to contribute to the advancement of secure, scalable, and transparent digital voting solutions, offering insights for future research and real-world implementation.

***Index Terms*—blockchain, voting, ethereum, hyperledger**

I. Introduction

Voting is a cornerstone of democracy, allowing citizens to influence governance. Over time, various voting methods have been used, including paper ballots, mechanical lever machines, punch cards, direct recording electronic (DRE) systems, and internet-based voting (i-voting) [1]. While paper-based voting remains the most common due to its simplicity, it has significant drawbacks such as vote tampering, ballot mismanagement, environmental concerns, and manual counting inefficiencies. Malicious actors could manipulate election outcomes, particularly in close races, by discreetly altering or destroying ballots.

To improve efficiency and accessibility of the voting process, electronic and internet-based voting systems were introduced. However, these methods bring new challenges, including cybersecurity threats, auditability issues, and software vulnerabilities that could alter results without detection. Ensuring that votes are recorded, stored, and counted correctly is crucial for election integrity [2].

Blockchain technology offers a potential solution by enhancing security, transparency, and trust in e-voting. Its decentralized, tamper-resistant nature addresses many of the weaknesses in both traditional and electronic voting systems. By leveraging cryptographic techniques and smart contracts, blockchain can ensure verifiable, private, and coercion-resistant elections, ultimately paving the way for a more robust and trustworthy voting process.

A. Importance of Secure and Transparent Voting

A voting system's credibility depends on its ability to ensure security, transparency, and fairness. Voters must trust that their ballots are cast as intended, recorded accurately, and protected from tampering. Traditional voting methods often lack full transparency, while electronic systems, though improving efficiency, introduce risks like hacking, fraud, and centralized control. Addressing these vulnerabilities is essential to maintaining public trust and safeguarding democratic integrity.

Transparency plays a key role in secure voting. Even well-designed security-critical software can have vulnerabilities, and insider threats, such as compromised developers, pose additional risks. To counteract these issues, open-source development is a widely recommended practice, as seen in cryptocurrency systems. Open-source implementations allow independent experts to review and verify security mechanisms, reducing the risk of hidden flaws or malicious backdoors [2].

A secure and trustworthy voting system must balance transparency and security, ensuring its cryptographic protocols and software are verifiable without compromising election integrity. Achieving this balance is crucial for creating a tamper-resistant, verifiable voting process that upholds public confidence in election outcomes.

B. Role of Blockchain in E-Voting

Blockchain technology enhances e-voting security through decentralization, transparency, and tamper resistance. Unlike traditional digital voting, which faces cyber threats and centralization risks, blockchain ensures vote integrity using cryp-

tographic techniques, distributed consensus, and immutability [3].

Smart contracts automate voting rules, reducing reliance on intermediaries and minimizing fraud. Blockchain's transparency enables public verification while protecting voter privacy, fostering trust in elections. Different implementations, such as permissioned and public blockchains [4], offer trade-offs in security, efficiency, and scalability.

Despite challenges like scalability, cost and regulatory concerns, blockchain holds promise for secure, verifiable, and transparent voting systems.

C. Objective and Scope of the Paper

This paper aims to analyze and compare existing blockchain-based e-voting implementations, evaluating their strengths and weaknesses. By examining different approaches, we aim to identify key challenges, potential improvements, and research gaps in the field. The study focuses on aspects such as security, scalability, usability, integrity, and auditability to provide a comprehensive understanding of the current landscape.

D. Layout of the Paper

The remainder of this paper is structured as follows: Section II discusses the problem definition, highlighting challenges in traditional and electronic voting systems. Section III outlines the fundamental properties of a secure voting system. Section IV presents a study of various blockchain-based e-voting implementations. Section V provides a comparative analysis of these systems. Section VI explores research gaps and future directions, followed by the conclusion in Section VII.

II. Problem Definition

A. Challenges in traditional voting systems

Voting is one of the most important aspects of a country's democracy, giving people the power to choose their leaders and shape the future. However, traditional paper-based elections come with a lot of challenges, especially when it comes to security, privacy, and fairness. Since these elections are managed by a central authority, there's always a risk of fraud, human error, or even intentional manipulation [5]. Paper ballots can be lost, tampered with, or miscounted, making the process less trustworthy. These issues highlight the need for a more secure and transparent voting system that ensures every vote truly counts [6]. Visualization of a traditional voting system is given in Fig 1.

B. Issues in electronic and internet-based voting

The shift to an online voting system did not fully resolve the issues faced by traditional elections. While it made voting more accessible and convenient to users, many concerns surrounding security, privacy, and fairness still persisted. The transition to online voting sparked the development of new technologies designed to address these challenges. Although this change streamlined the election process, security and privacy issues remained. Risks such as cyberattacks, vote tampering, and system failures continued to threaten the integrity of the system. To truly improve the voting process, it became essential to create a solution that tackled the weaknesses of both traditional and online voting. The focus was on developing technologies that prioritized security, safeguarded voter privacy, and prevented fraud, ensuring the system's integrity.

C. Need for blockchain-based solutions

Blockchain technology has emerged as a promising solution for addressing security and transparency challenges in digital systems, particularly in electronic voting. It operates as a decentralized, immutable ledger that stores a continuous sequence of blocks, each containing transaction data and a header [7]. Unlike traditional centralized systems that rely on a central authority, blockchain eliminates the need for third-party validation by leveraging distributed consensus mechanisms, reducing the risk of manipulation and single points of failure.

By instantly validating transactions that cannot be altered or reversed once verified, blockchain ensures data integrity and prevents unauthorized modifications. Additionally, it enhances privacy, as users interact using cryptographic addresses rather than personal identities. Blockchain also facilitates transaction monitoring and verification, as seen in the Bitcoin blockchain's unspent transaction output (UTXO) model, which improves traceability and transparency.

Furthermore, blockchain employs cryptographic hash functions and consensus mechanisms to ensure transaction authenticity. The hash-linking technique makes altering past transactions nearly impossible without affecting the entire chain, reinforcing data immutability [6]. These features make blockchain a reliable framework for applications such as supply chain management, financial transactions, and online voting. By adopting blockchain, organizations can enhance security, prevent fraud, and build trust in decentralized digital ecosystems.

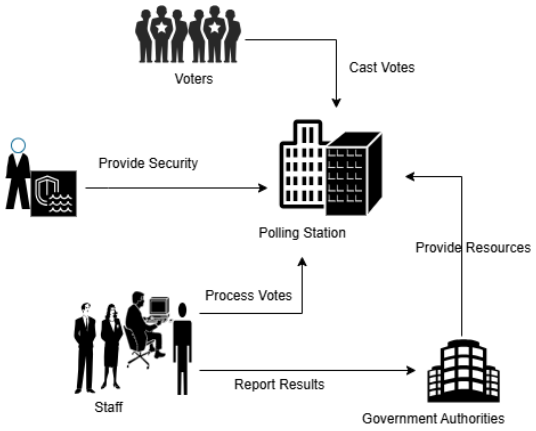


Fig. 1. Traditional voting system.

III. Fundamental Properties of a Voting System

A reliable voting system must meet several essential properties to ensure security, fairness, and accessibility. Adhering to these principles fosters public trust and establishes the system as a credible voting method. Below are the key properties that a trustworthy voting system should uphold [1], [8] :

- **Security** – The system must safeguard against fraud, unauthorized access, and manipulation. It should ensure that votes are cast, recorded, and counted accurately without interference.
- **Transparency** – The voting process should be open to public scrutiny while maintaining voter confidentiality. Transparent systems enable independent verification of election integrity.
- **Anonymity and Privacy** – Voters must be able to cast their votes without fear of retaliation. The system should protect voter identities while ensuring that votes remain unlinkable to individuals. [9]
- **Verifiability** – A reliable voting system should allow voters and independent auditors to verify that votes were recorded and counted correctly without compromising privacy. End-to-end verifiability ensures trust in the process.
- **Scalability** – The system should efficiently handle large voter populations without performance degradation. It must support high turnout while maintaining security and usability.
- **Coercion Resistance** – Voters should be able to vote freely without external pressure or influence. The system must prevent vote buying, intimidation, or any form of undue coercion.
- **Affordability** – The system should be cost-effective, ensuring accessibility while minimizing operational and infrastructure costs. It must balance security, efficiency, and financial feasibility.

IV. Study of Existing Blockchain-Based E-Voting Systems

A. ECC-EXONUM-eVOTING [10]

- **Features**: The ECC-EXONUM-eVOTING system ensures a secure, transparent, and efficient e-voting experience. It integrates elliptic curve cryptography (ECC) and the Exonum blockchain framework to guarantee vote immutability and security. Anonymity and privacy are achieved through Idemix technology, allowing voters to cast votes without revealing personal details. Transparency is ensured as each validated vote is permanently recorded and cannot be altered or deleted. The system is designed to be scalable and affordable, making it suitable for elections of any size. It also prevents double voting and incorporates coercion resistance to protect voter choices. Secure communication is maintained using the Elliptic Curve Diffie-Hellman (ECDH) protocol [11], which encrypts data exchanges to prevent interception and tampering.
- **Implementation**: The system employs a smart contract on the Exonum private blockchain, utilizing a hybrid consensus algorithm that combines RAFT and PBFT to enhance security and reduce overheads. Idemix technology, based on Zero-Knowledge Protocol (ZKP) and a blind signature scheme, ensures voter anonymity while maintaining integrity. It facilitates secure transactions through a communication model for decentralized applications (DApps) and leverages the IBM Blockchain-as-a-Service (BaaS) [12] model for backend security. The system undergoes formal security analysis using the Random Oracle Model (ROM) and informal analysis to ensure robustness. The blockchain structure permanently links each vote to the previous one, preventing tampering and ensuring transparency. Secure communication is further reinforced using the ECDH protocol.
- **Limitations**: Despite its advanced security features, the ECC-EXONUM-eVOTING system faces several limitations. The use of sophisticated cryptographic techniques, such as zero-knowledge proofs and blind signatures, adds complexity to the system, requiring expert knowledge for management and maintenance. Running a decentralized network with multiple validators and auditors demands significant computing power and storage, which may hinder widespread adoption. Another challenge is the lack of a verifiability mechanism for voters to check their cast votes, which could raise concerns about trust and election integrity. These challenges highlight areas for potential improvement in the system.

B. A Framework to Make Voting System Transparent Using Blockchain Technology [13]

- **Features**: The system supports multiple consensus algorithms, with Proof of Work (PoW) as the default. Other algorithms like Ripple, Proof of Vote, and Proof of Stake (PoS) can be selected at deployment for optimized performance and security. Blockchain ensures transparency by storing transaction hashes and election results immutably. Voter data is secure, and results are publicly accessible through a dashboard. Proof of Stake (PoS) validates transactions by randomly selecting nodes. If a node validates a false transaction, it loses its stake. The Voting Coin given for one time use prevents double voting.
- **Implementation**: The system uses a single-chain blockchain with security algorithms and cryptographic hashing to ensure secure transactions. Smart contracts automate the voting process, and flexible consensus algorithms improve scalability. Voter registration is linked to a National ID, ensuring voter integrity. Blockchain records each voter's transaction and stores election results, ensuring transparency and immutability. Results can be accessed through a user dashboard for verification. Before voting, the system verifies the voter's nationality and checks if they have already voted. If they still have a voting coin, they can vote. Voter details, including

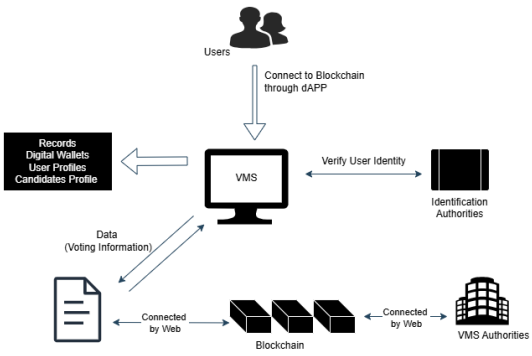


Fig. 2. Voting system architecture.

identifier, vote choice, and timestamp, are securely stored on the blockchain. Fig 2 shows the architecture of the voting system.

- **Limitations**: Centralized voter databases could introduce privacy concerns, and scalability challenges may arise when dealing with a very large voter base. Proof of Work (PoW) requires significant computational power, which may reduce system efficiency and scalability in large-scale elections. The system's security depends on the health of its nodes. If a large number of nodes become compromised, the voting process may be affected despite decentralization. Verification of voter eligibility through National ID can be complex and time-consuming, especially if database access is slow or unavailable, potentially affecting system speed.

C. Decentralized and Automated Online Voting System using Blockchain Technology [14]

- **Features**: The system ensures security through facial recognition for logins, preventing unauthorized access. Blockchain technology records votes and transactions in an encrypted ledger, ensuring transparency and public accessibility. Fault tolerance is maintained using the Ethereum network and Ganache, allowing the system to function even if some nodes fail. MongoDB efficiently stores user, candidate, and election data for quick retrieval. An admin component handles voter verification, election scheduling, and notifications.This system enables secure wallet management and transactions.It also uses smart contracts to manage the voting process.
- **Implementation**: The Ethereum blockchain is utilized to maintain vote integrity, Votes are recorded on the blockchain and kept traceable without revealing individual voting choices. The system uses facial recognition for voter authentication, ensuring secure logins. Blockchain technology encrypts and stores votes and transactions in a distributed ledger for transparency. Ethereum and Ganache distribute blocks across nodes, ensuring fault tolerance. In database management system, stores user, candidate, and election data for efficient retrieval. An admin panel manages voter verification, election scheduling, and result notifications. MetaMask enables secure wallet management and transactions.
  Truffle is used for developing, compiling, and deploying smart contracts on the private blockchain, ensuring seamless system interaction with Ethereum.
- **Limitations**: Facial recognition may be inaccurate under certain conditions, such as poor lighting or facial obstructions, leading to authentication failures. The system's dependence on Ethereum and Ganache for fault tolerance may reduce flexibility in handling network issues or ecosystem changes, affecting stability. While MongoDB efficiently manages data, high-traffic elections could cause performance slowdowns and delays in data retrieval. Managing wallets with MetaMask may be challenging for non-technical users, potentially reducing accessibility. Truffle simplifies smart contract deployment but requires technical expertise for migration and compilation, which may be difficult for administrators unfamiliar with Ethereum development. Privacy concerns surrounding facial recognition technology and the potential scalability issues with the Ethereum blockchain could limit the system's widespread adoption, especially in large elections. [15]

D. e-Voting on Ethereum Blockchain [16]

- **Features**: The Ethereum-based e-voting system ensures security, transparency, and tamper resistance by leveraging blockchain technology. Voter anonymity is preserved through the use of public and private addresses and zero-knowledge proofs. The system guarantees transparency by allowing the voting network to be publicly accessible through platforms like *ropsten.etherscan.io*, enabling real-time verification of transactions. Additionally, the system prevents double voting by assigning each voter one unit of Ether, which is used to cast a vote, making it impossible to vote more than once. Each vote is linked to a unique transaction ID for verifiability, allowing voters to confirm their votes have been accurately recorded.
- **Implementation**: The system features two primary interfaces: one for administrators to create elections and manage candidates, and another for voters to cast their votes securely. Smart contracts are used to enforce election rules, ensuring the integrity of the voting process. The system is built using the Truffle Framework, which facilitates the writing, testing, and deployment of Solidity-based smart contracts on the Ethereum blockchain. Voter authentication is achieved by verifying the wallet ID, and the Ethereum blockchain's decentralized nature guarantees the immutability and security of the votes cast.
- **Limitations**: One of the main challenges faced by the system is scalability, as Ethereum's current infrastructure may struggle to support elections with large numbers of voters. Solutions such as Layer 2 scaling techniques [17], including sidechains [18] and state channels [19], can help alleviate congestion by offloading transactions from the main blockchain. Sharding [20] can also be

implemented to divide the blockchain into smaller sections that can independently process transactions, thereby improving scalability. Another limitation is the lack of strong voter authentication, which could lead to unauthorized access or identity theft, potentially undermining the integrity of the voting process. The implementation of biometric authentication or cryptographic keys can mitigate this risk. Additionally, Ethereum's transaction fees (gas fees) could hinder large-scale adoption due to the high costs involved, making it less feasible for widespread implementation of blockchain-based voting systems.

E. Iraqi Paradigm E-Voting System Based on Hyperledger Fabric Blockchain Platform [21]

- **Features**: The Hyperledger Fabric E-Voting system ensures security, transparency, and scalability. It offers voter verifiability, allowing voters to authenticate, cast, and verify their votes before and after the election, enhancing trust in the process. Data security and immutability are maintained using SHA-256 cryptographic hashing, preventing any alteration of recorded votes. The system ensures voter anonymity while displaying election results transparently. Additionally, it is scalable, allowing the inclusion of more organizations, polling stations, or voters as needed. A user-friendly interface makes it accessible to all participants without requiring advanced IT skills.
- **Implementation**: The system is built on the Hyperledger Fabric platform, utilizing a Raft ordering service for secure transaction processing. It is configured with two organizations, each comprising a committer node and an endorser node, while CouchDB serves as the state database for efficient data management. SHA-256 cryptographic hashing ensures vote immutability and security. Voters authenticate using their voter ID and fingerprint or PIN through a web interface. After successful verification, the Certificate Authority registers their identity and generates a unique wallet, granting them access to the blockchain network to cast votes. The system updates their "has-voted" status upon casting a vote and enables real-time vote verification. To maintain transparency, authorized polling center users can view election results displaying vote counts per candidate without compromising voter identities. The system upholds election integrity by requiring participants to audit ballots and election activities, promoting transparency and accountability. These implementations contribute to a secure, transparent, and scalable e-voting solution using Hyperledger Fabric.
- **Limitations**: Despite its advantages, the Hyperledger Fabric E-Voting system has some limitations. As more organizations join the network, the system may experience reduced efficiency due to the increased number of transactions and nodes participating in consensus. The high computational power and memory requirements may pose challenges in regions with limited technological infrastructure. Additionally, the system lacks coercion resistance, meaning it does not prevent voters from being influenced or pressured by external parties during the voting process because the voters can view their ballots after the election ends. These limitations highlight areas that require further enhancements to improve the system's overall robustness.

F. DVTChain: A Blockchain-Based Decentralized Voting System [22]

- **Features**: DVTChain utilizes a decentralized ledger to ensure vote immutability. Each vote is encrypted before being sent to the blockchain, and a small node server, known as the crypto server, is responsible for managing the public and private keys. The system operates with three smart contracts: the voter contract, candidate contract, and voting contract. The voter contract hashes the voter's information to secure it and provide anonymity. It also prevents double spending through a vote coin system. The system provides transparency by allowing users to examine the blockchain and verify that vote counting is done correctly, and verifiability is achieved by allowing voters to use a transaction ID to confirm their votes.
- **Implementation**: The DVTChain system operates in four main phases:
  1) **Registration**: Voter credentials are hashed and stored on the blockchain to ensure voter anonymity and security.
  2) **Voting Setup**: The election commission generates key pairs for voters and initializes candidate details.
  3) **Voting**: Voters authenticate using hashed credentials, receive a vote coin, encrypt their votes, and submit them to the blockchain.
  4) **Result**: The election commission decrypts the votes, transfers vote coins to candidates, and securely publishes the results.

  The system is built on the Ethereum blockchain using Solidity and Truffle for smart contract management. To address scalability and performance concerns, the system suggests integrating Ethereum Layer 2 technologies like sidechains or state channels to improve transaction speed and reduce gas costs. A high level overview can be seen in Fig 3.
- **Limitations**: Despite the strengths of the system, it faces several limitations. High voter turnout can cause performance issues due to Ethereum's limited scalability, with transactions often taking longer to execute and incurring high gas fees. The use of cryptographic operations adds computational overhead, and while the system provides voter anonymity and transparency, it could lead to vote selling since voters can verify their votes post-election. A central crypto server stores the public and private keys used for encryption, creating a single point of failure. If this server is compromised, the integrity of the entire system could be jeopardized. Additionally, the system's high energy consumption remains a concern,

TABLE I
COMPARISON OF BLOCKCHAIN-BASED VOTING SYSTEMS

	SE	TR	AP	VE	SC	CR	AFF
[10]	✓	✗	✓	✗	✓	✓	✓
[13]	✗	✓	✗	✓	✗	✗	✓
[14]	✗	✓	✗	✗	✗	✓	✗
[16]	✗	✓	✓	✓	✗	✗	✗
[21]	✗	✗	✓	✓	✓	✗	✓
[22]	✗	✓	✓	✓	✓	✗	✗

SE: Security
TR: Transparency
AP: Anonymity & Privacy
VE: Verifiability
SC: Scalability
CR: Coercion Resistance
AFF: Affordability

though switching from proof-of-work to proof-of-stake may reduce its environmental impact.

V. COMPARATIVE ANALYSIS OF EXISTING SYSTEMS

A. Strengths and Weaknesses

Each blockchain-based e-voting system has distinct strengths and weaknesses. Some systems excel in security and transparency by leveraging cryptographic techniques and smart contracts, while others focus on scalability and accessibility. However, limitations such as vote selling risks, auditability issues, scalability constraints, high computational costs [23], and storage overhead. remain common concerns.

Table I presents a comparative analysis of existing blockchain-based e-voting systems, evaluating key factors such as security, transparency, anonymity, privacy, verifiability, scalability, coercion resistance, and affordability. Additionally, Table II and Table III provides reasoning for why certain properties may or may not be available.

B. Common Trends and Limitations

The analysis highlights recurring trends across blockchain-based e-voting systems:

- **Security and Privacy:** Most systems prioritize encryption, smart contracts, and cryptographic techniques to secure votes and voter identities.
- **Scalability Concerns:** Systems relying on Ethereum face high gas fees, while private blockchains have limited transaction throughput. [24]
- **Authentication Challenges:** Some implementations use facial recognition and national ID verification, but OTP-based authentication is not widely used.
- **Storage Overhead:** Storing encrypted votes on-chain increases costs and requires efficient data management strategies.

Despite advancements, achieving an optimal balance among security, transparency, anonymity, privacy, verifiability, scalability, coercion resistance, and affordability remains a significant challenge for blockchain-based e-voting systems.

VI. RESEARCH GAPS AND FUTURE DIRECTIONS

A. Unresolved Challenges in Blockchain-Based Voting

Despite significant advancements, blockchain-based e-voting systems still face key challenges, including scalability limitations, coercion resistance, cost efficiency, and user accessibility. Addressing these issues is crucial to ensuring widespread adoption and practical implementation.

B. Potential Areas for Improvement

Several improvements can enhance the effectiveness of blockchain-based e-voting systems:

- **Scalability**: Implementing private blockchains, sharding technologies [20] and Hyperledger Fabric [25] to improve performance and handle large-scale elections efficiently.
- **Coercion Resistance**: Enabling mechanisms such as allowing multiple voting attempts [26] or utilizing cryptographic techniques [27], [28] to enable voters to verify their votes while preventing external influence or vote selling [29]. Additionally, hybrid approaches can be explored, such as generating a physical paper ballot upon vote submission and depositing it in a secure ballot box. This method adds an extra layer of verification and mitigates the risks of vote selling.
- **Cost Reduction**: Utilizing off-chain implementations [30], [31] where necessary to minimize computational and storage expenses, along with research on optimizing system costs [32], [33].
- **User Accessibility**: Designing an intuitive and user-friendly UI to accommodate voters with limited technological literacy, ensuring ease of use in real-world election scenarios.

C. Future Research Opportunities

Future research should focus on developing novel solutions to address these challenges. This includes designing blockchain architectures optimized for large-scale voting, integrating cryptographic techniques for secure yet anonymous voting, and enhancing the usability of blockchain-based systems to ensure equitable access for all voters. Additionally, research into hybrid blockchain models that combine digital and physical verification methods could further strengthen election integrity.

VII. CONCLUSION

Blockchain-based e-voting offers significant improvements in security, transparency, and verifiability through decentralized ledgers and cryptographic techniques. However, several challenges remain, including scalability limitations, coercion resistance, high costs, and user accessibility. Public blockchains often face high transaction fees, while private blockchains struggle with limited throughput. Additionally, risks such as vote selling, auditability issues, and storage overhead hinder widespread adoption.

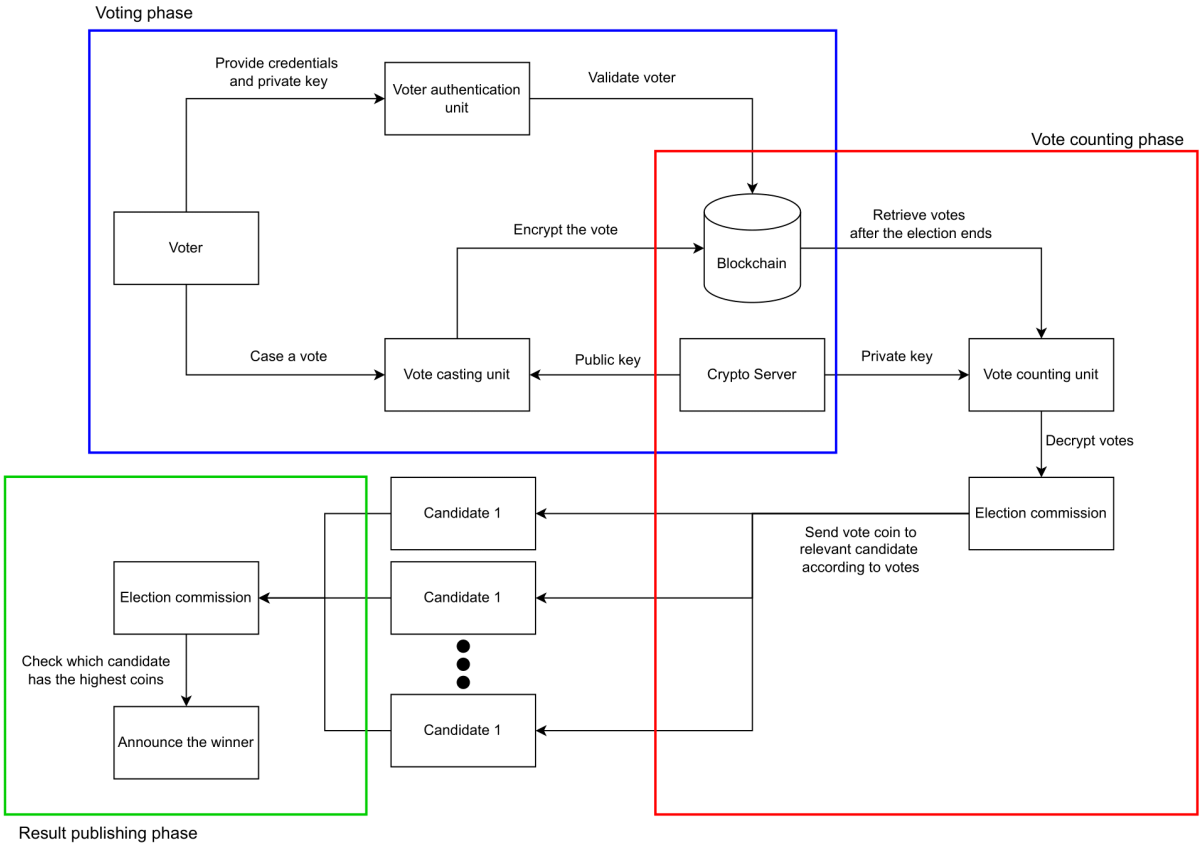


Fig. 3. DVTChain high level overview

TABLE II
REASONING FOR DIFFERENT PROPERTIES IN BLOCKCHAIN-BASED VOTING SYSTEMS (PART 1)

	SE	TR	AP
[10]	Hybrid consensus, private blockchain for security	Private blockchain lacks transparency	Zero-knowledge protocol for anonymity
[13]	Centralized database may be compromised	Results publicly available via dashboard	Privacy risks from compromised database
[14]	Centralized database may be compromised	Public blockchain enables voter verification	Privacy concerns from facial recognition
[16]	Lacks authentication, allowing unauthorized access	Public blockchain enables voter verification	Public and private addresses, zero-knowledge proofs for privacy
[21]	Centralized database may be compromised	Private blockchain lacks transparency	Data hashed for privacy
[22]	Centralized crypto server, compromised keys affect security	Public blockchain enables voter verification	Data encrypted and hashed for privacy

To address these challenges, off-chain solutions, sharding techniques, and hybrid blockchain models can improve scalability and reduce costs. Coercion resistance can be strengthened by allowing re-voting mechanisms or integrating cryptographic techniques like zero-knowledge proofs. Ensuring a balance between transparency and voter privacy remains crucial to gaining public trust.

Future research should explore innovative blockchain architectures optimized for large-scale elections while maintaining security and efficiency. Additionally, cost-effective implementations and user-friendly interfaces are essential for widespread adoption. Interdisciplinary collaboration between blockchain researchers, cryptographers, and policymakers is necessary to address regulatory concerns and ensure practical deployment.

Despite its challenges, blockchain-based e-voting has the potential to revolutionize electoral processes by enhancing trust, security, and accessibility. Continued advancements, pilot implementations, and rigorous testing will determine whether blockchain can become a viable, scalable, and widely accepted solution for future elections.

TABLE III
REASONING FOR DIFFERENT PROPERTIES IN BLOCKCHAIN-BASED VOTING SYSTEMS (PART 2)

	VE	SC	CR	AFF
[10]	Not mentioned	Scalable due to private blockchain	Voter can't verify votes. Vote selling is not possible	Lower cost with private blockchain
[13]	Results accessible for verification	High computational power affects scalability	Vote selling risk due to user verification	No details on cost differences
[14]	Not mentioned	Ethereum blockchain scalability issues	Voter can't verify votes. Vote selling is not possible	Higher costs due to transaction fees
[16]	Votes verified via transaction ID	Ethereum blockchain scalability issues	Votes verified via transaction ID. Vote selling is possible	Higher costs due to transaction fees
[21]	Voters verify ballots after election ends	Scalable due to private blockchain	Voters verify ballots after election ends. Vote selling is possible	Lower cost with private blockchain
[22]	Votes verified via transaction ID after election	Ethereum Layer 2 boosts scalability	Votes verified via transaction ID. Vote selling is possible	High energy consumption resulting higher costs

REFERENCES

[1] S. E. Kafhali, "Blockchain-based electronic voting system: Significance and requirements," *Mathematical Problems in Engineering*, vol. 2024, pp. 1–17, 2 2024.

[2] S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: from internet voting to blockchain voting," *Journal of Cybersecurity*, vol. 7, 2 2021.

[3] B. Shrimali and H. B. Patel, "Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, pp. 6793–6807, 10 2022.

[4] P. Paul, P. Aithal, R. Saavedra, and S. Ghosh, "Blockchain technology and its types—a short review," *International Journal of Applied Science and Engineering (IJASE)*, vol. 9, no. 2, pp. 189–200, 2021.

[5] P. M. Pathak, A. Suradkar, A. Kadam, A. Ghodeswar, and P. Parde, "Blockchain based e-voting system," *International Journal of Scientific Research in Science and Technology*, pp. 134–140, 5 2021.

[6] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, "E-voting system based on blockchain technology: A survey," pp. 200–205, 7 2021.

[7] M. An, Q. Fan, H. Yu, B. An, N. Wu, H. Zhao, X. Wan, J. Li, R. Wang, J. Zhen, Q. Zou, and B. Zhao, "Blockchain technology research and application: A literature review and future trends," *Journal of Data Science and Intelligent Systems*, 10 2023.

[8] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital voting: A blockchain-based e-voting system using biohash and smart contract," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 228–233, IEEE, 8 2020.

[9] M. H. Jumaa and A. C. Shakir, "Iraqi e-voting system based on smart contract using private blockchain technology," *Informatica*, vol. 46, pp. 87–94, 8 2022.

[10] S. Majumder, S. Ray, D. Sadhukhan, M. Dasgupta, A. K. Das, and Y. Park, "Ecc-exonum-evoting: A novel signature-based e-voting scheme using blockchain and zero knowledge property," *IEEE Open Journal of the Communications Society*, 2023.

[11] R. Haakegaard and J. Lang, "The elliptic curve diffie-hellman (ecdh)," *Online at https://koclab. cs. ucsb. edu/teaching/ecc/project/2015Projects/Haakegaard+ Lang. pdf*, 2015.

[12] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "Nutbaas: A blockchain-as-a-service platform," *Ieee Access*, vol. 7, pp. 134422–134433, 2019.

[13] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A framework to make voting system transparent using blockchain technology," *IEEE Access*, vol. 10, pp. 59959–59969, 2022.

[14] P. Sanjeeva, M. S. Sathwik, G. S. Prasad, G. P. Reddy, V. Sajwan, and B. Ganesh, "Decentralized and automated online voting system using blockchain technology," *E3S Web of Conferences*, vol. 430, p. 01046, 10 2023.

[15] M. Ibrahim, K. Ravindran, H. Lee, O. Farooqui, and Q. H. Mahmoud, "Electionblock: An electronic voting system using blockchain and fingerprint authentication," in *2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C)*, pp. 123–129, IEEE, 3 2021.

[16] M. H. Razali, A. A. Jamal, S. A. Fadzli, M. D. Zakaria, W. N. S. W. Nik, and H. Hassan, "e-voting on ethereum blockchain," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 50, pp. 186–194, 8 2025.

[17] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020.

[18] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K. K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," 1 2020.

[19] L. D. Negka and G. P. Spathoulas, "Blockchain state channels: A state of the art," *IEEE Access*, vol. 9, pp. 160277–160298, 2021.

[20] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14155–14181, 2020.

[21] S. H. Saeed, S. M. Hadi, and A. H. Hamad, "Iraqi paradigm e-voting system based on hyperledger fabric blockchain platform," *Ingénierie des systèmes d information*, vol. 27, pp. 737–745, 10 2022.

[22] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "Dvtchain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, pp. 6855–6871, 10 2022.

[23] Y. Ucbas, A. Eleyan, M. Hammoudeh, and M. Alohaly, "Performance and scalability analysis of ethereum and hyperledger fabric," *IEEE Access*, vol. 11, pp. 67156–67167, 2023.

[24] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, vol. 105, pp. 13–26, 4 2020.

[25] S. Shalaby, A. A. Abdellatif, A. Al-Ali, A. Mohamed, A. Erbad, and M. Guizani, "Performance evaluation of hyperledger fabric," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp. 608–613, IEEE, 2 2020.

[26] P. Ehin, M. Solvak, J. Willemson, and P. Vinkel, "Internet voting in estonia 2005–2019: Evidence from eleven elections," *Government Information Quarterly*, vol. 39, p. 101718, 10 2022.

[27] L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, p. 103678, 2 2024.

[28] W. Jamroga, *Pretty Good Strategies for Benaloh Challenge*, vol. 14230 LNCS, pp. 106–122. Springer Science and Business Media Deutschland GmbH, 2023.

[29] K. Ye, D. Zheng, R. Guo, J. He, Y. Chen, and X. Tao, "A coercion-resistant e-voting system based on blockchain technology," *Int. J. Netw. Secur*, vol. 23, pp. 791–806, 2021.

[30] R. Mühlberger, S. Bachhofner, E. C. Ferrer, C. D. Ciccio, I. Weber, M. Wöhrer, and U. Zdun, *Foundational Oracle Patterns: Connecting Blockchain to the Off-Chain World*, pp. 35–51. 7 2020.

[31] C. Xu, C. Zhang, J. Xu, and J. Pei, "Slimchain," *Proceedings of the VLDB Endowment*, vol. 14, pp. 2314–2326, 7 2021.

[32] K. Nelaturu, S. M. Beillahi, F. Long, and A. Veneris, "Smart contracts refinement for gas optimization," in *2021 3rd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*, pp. 229–236, IEEE, 9 2021.

[33] L. Marchesi, M. Marchesi, G. Destefanis, G. Barabino, and D. Tigano, "Design patterns for gas optimization in ethereum," in *2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pp. 9–15, IEEE, 2 2020.

……

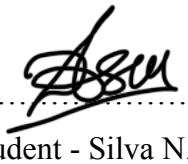
Supervisor - Prof. Manjula Sandirigama

……

Student - Kaushalya N. V. K. (E/19/193)

……

Student - Senevirathne T. N. (E/19/363)



……

Student - Silva N. H. D. U. (E/19/375