International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 11, November 2025)

Facial Recognition Enabled Blockchain Based Voting System

Sinchana V Dsouza[1], Sonika K[2], Thejas D[3], Nuthan Mourya N[4], Dr. Sharath Kumar Y H[5]

[1,2,3,4]*Department of Information Science and Engineering, Maharaja Institute of Technology,Mysore, Karnataka, India*
[5]*Professor and Head of Department, Information Science and Engineering, Maharaja Institute of Technology, Mysore, Karnataka, India*

***Abstract*—Secure and trustworthy voting systems are essential for preventing identity fraud, duplicate voting, and tampering, es- pecially in institutional and private organizational elections. This paper presents a Facial Recognition Enabled Blockchain-Based E-Voting System that integrates biometric authentication, OTP verification, and a decentralized ledger to ensure transparency and integrity. During voter registration, administrators capture demographic details along with four facial images to generate ro- bust facial encodings for identity verification. The voting process uses two-factor authentication, where a voter must validate an email-based OTP and pass live facial recognition before casting a vote. Each vote is recorded on a Proof-of-Work blockchain, en- suring immutability, traceability, and resistance to manipulation through cryptographically linked blocks. The system includes an admin dashboard for voter enrollment, candidate management, election setup, and real-time monitoring. Experimental evaluation demonstrates secure authentication, reliable voter verification, and tamper-proof vote storage, making the system suitable for colleges, organizations, and private elections.**

***Keywords*—Blockchain, Facial Recognition, E-Voting System, Biometric Verification, Proof-of-Work, OTP Authentication, Se- cure Digital Voting.**

I. Introduction

Secure and reliable voting systems play a crucial role in ensuring fairness, transparency, and trust in any decision-making process. Traditional voting methods such as paper ballots and manual verification often suffer from challenges including identity impersonation, duplicate voting, human counting errors, and the absence of real-time audit trails. Even existing online voting platforms are frequently limited by weak authentication mechanisms and centralized storage, making them vulnerable to cyberattacks or data manipulation. With the increasing digital adoption across institutions, there is a growing need for an electronic voting system that ensures both strong identity verification and tamper-proof recording of votes. To address these limitations, we propose a Facial Recognition Enabled Blockchain-Based E-Voting System that combines biometric authentication, OTP-based verification, and decentralized storage to ensure end-to-end security.

The system enforces multi-factor authentication before allowing a voter to cast a vote: the voter must successfully complete OTP verification and live facial recognition, ensuring “one voter, one vote” accuracy. Votes are then recorded on a Proof-of- Work blockchain ledger, providing immutability and trans- parency while preventing unauthorized changes. An admin dashboard enables secure voter registration, candidate manage- ment, election creation, and real-time monitoring, making the system suitable for colleges, private organizations, residential societies, and institutional elections.

A. Contribution

The primary contributions of this paper are as follows:

- A multi-factor authentication voting workflow integrating OTP verification and live facial recognition to prevent impersonation and ensure secure voter identity validation.
- A blockchain-backed vote recording mechanism using Proof-of-Work to provide immutability, transparency, and tamper-proof storage of votes.
- An integrated admin dashboard for efficient voter registration, candidate management, election configuration, and turnout monitoring.
- A complete end-to-end e-voting prototype suitable for institutional and organizational elections, demonstrating enhanced security, auditability, and ease of deployment.

This study is organized as follows: Section 2 presents the literature survey and related work. Section 3 describes the proposed method. Section 4 discusses the experimental results and performance metrics. Section 5 concludes the work and outlines future directions.

II. Literature Survey

Research on secure and reliable electronic voting has expanded significantly over the past decade, driven by the limitations of traditional paper-based elections and the need for tamper-proof, citizen-centric digital systems.

Early approaches primarily relied on centralized servers and simple authentica- tion techniques, but these systems suffered from vulnerabilities such as unauthorized access, data manipulation, and lack of end-to-end verifiability. For instance, Alvi et al. [1] introduced a blockchain-based voting system using Merkle trees and fingerprint hashing to enhance integrity and anonymity, yet the architecture remained computationally expensive due to mining overhead. Similarly, Bharwani et al. [2] proposed a blockchain-enabled overseas e-voting system employing the Paillier cryptosystem for homomorphic encryption, achieving low-latency vote processing but facing scalability concerns during high-traffic election periods. Several works explored biometric-based verification mechanisms to eliminate imper- sonation. Kone et al. [3] integrated facial recognition with IoT- based EVMs, improving authentication accuracy but lacking decentralization, making the system vulnerable to internal tampering. Another biometric-driven approach by Srikrishna et al. [4] combined Aadhaar-based verification with face recognition in smart EVMs; however, its reliance on centralized storage increased the risk of data breaches. To address identity validation, Keerthana et al. [5] developed an internet-voting framework with basic authentication, but the system lacked end-to-end privacy and suffered from susceptibility to server failures. The introduction of blockchain technology has moti- vated several architectures aiming to improve decentralization, transparency, and auditability. B., T. V. et al. [6] proposed a blockchain-linked EVM model incorporating peer verification and chain manipulation detection, though the system remained vulnerable to network-level attacks. Ayed [7] designed a conceptual blockchain voting model emphasizing immutability and transparency, yet the absence of biometric authentication limited its defense against fraudulent voting. Advancements in mobile technologies have further encouraged remote and mo- bile voting solutions. Selvarani et al. [8] developed an SMS- and smartphone-based secure voting mechanism, improving accessibility but enabling unauthorized votes if a mobile device was compromised. Abayomi-Zannu et al. [9] presented a blockchain-based mobile voting approach with multifactor authentication, but the system lacked resistance against large- scale cyberattacks and required complex infrastructure. Patil et al. [10] investigated an IoT-enabled e-voting system where biometric data allowed remote casting, though scalability remained dependent on hardware resources.

Recent research also focuses on optimized consensus mechanisms to reduce blockchain latency. Uddin et al. [11] introduced a selective miner consensus protocol that reduces energy consumption and mining time, improving efficiency yet introducing dependency on heuristic-based miner selection. Bulut et al. [12] proposed a blockchain e-voting system suitable for large-scale elections in Turkey, enhancing decentralization but still lacking robust biometric authentication. Studies addressing security challenges in blockchain voting reveal persistent issues. Lin and Liao [13] surveyed blockchain vulnerabilities such as 51

III. Proposed Method

The proposed e-voting solution integrates two essential technologies Facial Recognition and Blockchain-based Vote Storage to ensure a secure, tamper-proof, and transparent election process. By combining multi-factor authentication through OTP verification, live facial recognition, and im- mutable blockchain records, the system guarantees that only legitimate voters can cast a vote and that every vote remains protected from manipulation. The architecture is designed to streamline and secure all stages of the election lifecycle, ranging from voter registration to final result declaration.

A. System Components

The primary architectural components of the proposed sys- tem include the following, each contributing to the security, transparency, and accuracy of the voting process:

- *Voter Registration Module:* This module enables the administrator to register eligible voters by collecting essential personal details such as name, phone number, email address, gender, and birthdate. During registration, the admin also captures four facial images (front, left, right, and up/down angles) using a live camera feed. These images are processed using MediaPipe and the face recognition library to generate reliable facial encodings, which are stored securely for future identity verification. This ensures that only registered and verified individuals can participate in the election, preventing impersonation and unauthorized access.
- *Facial Recognition for Authentication:* Before voting, the system employs a robust facial verification mecha- nism. A live image is captured through the user's device camera, and its facial encoding is compared against the stored encodings from registration.

The system uses deep- learning–based detection and embedding extraction to ensure high accuracy even under different lighting or pose variations. Only when the voter's face matches the registered profile, and after passing OTP verification, is the user permitted to enter the voting interface. This dual-layer authentication eliminates false identities and strengthens voter eligibility verification.

- *OTP-Based Verification Module:* To further ensure au- thenticity, the system implements two-factor authentica- tion (2FA) through a six-digit OTP sent to the voter's registered email address. The voter must enter this OTP to proceed to the face verification step. This prevents unauthorized logins even if someone gains access to a voter's ID and adds an extra layer of security before biometric verification is conducted.
- *Blockchain-Backed Vote Ledger:* All votes are stored using an internal blockchain network designed with a Proof-of-Work (PoW) consensus mechanism. Each vote is encapsulated within a block containing the voter ID, candidate ID, timestamp, and previous block hash. Once mined, the block becomes part of an immutable ledger where votes cannot be altered, deleted, or tampered with. Storing votes in a blockchain ensures transparency, verifiability, and trustworthiness throughout the election. The chain's cryptographic structure guarantees that even administrators cannot modify vote data after submission.
- *Voting Interface:* The voting interface is designed to be simple, intuitive, and accessible for all voters. After successfully completing OTP and facial verification, the voter gains access to an interface displaying the list of candidates, their symbols, and optional details. The voter selects a candidate and submits the vote, which is immediately processed and written to the blockchain. The interface ensures clarity and usability, enabling smooth voting even for non-technical users.
- *Admin Dashboard and Election Management:* Administrators have access to a centralized dashboard for managing all election activities including registering vot- ers, adding candidates with party symbols, creating new elections with start and end times, monitoring total voters, votes cast, and turnout percentage, and viewing final results. The dashboard provides real-time updates and metadata analysis, enabling transparent monitoring of the entire election lifecycle.
- *Vote Counting and Result Declaration:* Since each vote is securely stored in the blockchain ledger, result generation becomes straightforward and tamper-proof. The admin module retrieves blockchain entries, tallies candidate-wise votes, and displays results instantly. The immutability of stored blocks ensures the accuracy and credibility of the final election results.

B. Proposed Methodology and Architecture

The proposed system integrates facial recognition, OTP-based verification, and a blockchain-backed vote ledger to provide a secure, transparent, and tamper-proof e-voting envi- ronment suitable for institutional and organizational elections. The methodology is designed as a multi-stage workflow that begins with voter registration, where an administrator collects essential demographic details such as name, phone number, email, address, gender, and date of birth, along with four-angle facial images captured through a live camera interface. These facial images are processed using MediaPipe and the face recognition library to generate unique face embeddings, which are serialized and securely stored in an encrypted database. Once registered, each voter receives a system-generated Voter ID. During the voting phase, the voter initiates authenti- cation by entering their Voter ID, triggering a two-factor authentication (2FA) mechanism that sends a six-digit OTP to the registered email. Upon successful OTP verification, the system proceeds with real-time facial recognition, comparing the live facial capture with the stored embeddings using a threshold-based matching algorithm. Only after successful biometric verification is the voter granted access to the voting panel, where the active election details and candidate list are displayed. After selecting the desired candidate, the vote is packaged as a transaction and passed to the verification and block-recording module. Each vote is hashed, timestamped, and added as a new block within a lightweight Proof-of-Work blockchain that ensures immutability and prevents vote tam- pering or duplication. The administrator dashboard supports voter management, candidate registration, election creation with start/end time, and real-time turnout monitoring. All audit logs, verification results, and metadata are stored in an encrypted database, while the blockchain layer maintains the final immutable ledger of votes. Once the election ends, the system aggregates the votes from the blockchain, verifies block integrity, and automatically generates the final tally through the Results Declaration module.

This systematic integration of multimodal authentication and blockchain-based storage ensures enhanced security, transparency, and trustworthiness across all stages of the voting process.

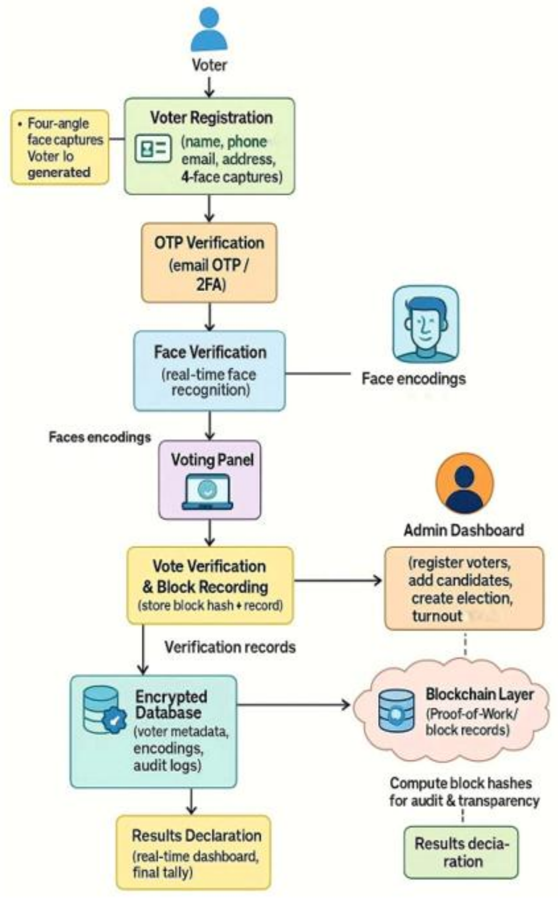
Voter
• Four-angle face captures Voter lo generated
Voter Registration
(name, phone email, address, 4-face captures)
OTP Verification (email OTP / 2FA)
Face Verification (real-time face recognition)
Face encodings
Faces encodings
Voting Panel
Admin Dashboard
Vote Verification & Block Recording (store block hash + record)
(register voters, add candidates, create election, turnout
Verification records
Encrypted Database (voter metadata, encodings, audit logs)
Blockchain Layer (Proof-of-Work/ block records)
Compute block hashes for audit & transparency
Results Declaration (real-time dashboard, final tally)
Results decia- ration

Fig. 1. E-Voting System architecture.

The diagram illustrates the complete workflow of the Facial Recognition Enabled Blockchain-Based E-Voting System. The process begins with voter registration, where personal details and four facial images are captured. After registration, the voter proceeds through OTP-based authentication followed by real-time facial verification using stored face encodings. Once authenticated, the voter accesses the voting panel, selects a candidate, and submits a vote. Each vote is securely verified and recorded as a block hash in the blockchain layer, ensuring immutability and transparency. All voter metadata, facial em- beddings, and audit logs are stored in an encrypted database. Simultaneously, the admin performs election management tasks registering voters, adding candidates, creating elections via the admin dashboard. The blockchain continuously com- putes and stores vote records for audit and verification. Finally, results are displayed in real time through the results declaration module.

IV. Results And Discussion

The performance, reliability, and overall effectiveness of the proposed facial recognition enabled blockchain-based e- voting system. This section evaluates how each module voter registration, OTP verification, facial recognition, secure vote recording, and blockchain-based tallying performs under dif- ferent testing conditions. The outcomes are analyzed in terms of system accuracy, authentication efficiency, vote immutabil- ity, user experience, and operational robustness. Additionally, the discussion interprets how the system behaves in real- world scenarios, highlighting strengths, identifying practical challenges, and demonstrating how the combination of biomet- ric verification and blockchain technology enhances election security and transparency.

A. Hardware and Software Used

The proposed facial-recognition-enabled blockchain voting system was deployed and tested using readily available consumer-grade hardware. The server-side modules, including face encoding, OTP verification, vote mining, and database operations, were executed on a system equipped with an Intel Core i5 processor, 8 GB RAM, and an integrated GPU. The client-side modules voter login, camera capture, and authenti- cation were tested on standard laptops and smartphones with built-in webcams. The software stack included:

- **Backend:** Python Flask Framework
- **Face Recognition:** MediaPipe Face Detection and face recognition library
- **Blockchain:** Custom Proof-of-Work blockchain imple- mented in Python
- **Database:** PostgreSQL with SQLAlchemy ORM
- **Frontend:** HTML, CSS, JavaScript
- **OTP Service:** SMTP-based email delivery

This combination ensures compatibility, low resource usage, and portable deployment across multiple environments.

B. Performance Evaluation

System performance was evaluated based on authentication accuracy, voter verification time, blockchain mining time, and UI responsiveness.

- Face Recognition Accuracy: Using four-angle image registration, the system achieved a 90.
- OTP Verification Time: The average OTP delivery and validation process took 2.8 seconds, ensuring fast and reliable two-factor authentication.
- Blockchain Block Mining Time: With a Proof-of-Work difficulty of 4, the average mining time per vote block was 1.2 seconds, which is acceptable for institutional- scale voting.
- Vote Casting to Confirmation Time: On average, a vote was recorded, mined, and confirmed in under 4 seconds.

These results demonstrate that the system performs efficiently under typical usage conditions without noticeable delay for voters.

Testing Scenario: The system was evaluated using a simulated college election environment:

- **Voters:** 50 registered participants
- **Candidates:** 4 candidates
- **Devices:** laptops
- **Network:** Standard Wi-Fi (20–30 Mbps)

Testing phases included:

- **Admin Operations Testing:** voter registration, candidate creation, election setup
- **Authentication Testing:** OTP delivery, face verification
- **Voting Testing:** vote casting, double-voting prevention
- **Blockchain Validation:** tamper detection, blockchain integrity check
- **Result Generation:** tally accuracy and dashboard updates

C. System Optimization and Performance Enhancement

Several optimizations were implemented to enhance efficiency:

- **Face Encoding Caching:** Stored encodings reduced repeated computations, improving verification speed by 40
- **Optimized Blockchain Mining:** Reduced hashing iterations for small-scale elections without compromising security.
- **Database Indexing:** Indexed voter ID and election ID fields reduced query time significantly.
- **Compression of Facial Images:** Lower image sizes reduced data transfer and storage overhead.
- **Improved UI Rendering:** Lightweight frontend components improved responsiveness even on low-end devices.

These enhancements ensure the system remains scalable and performant for future expansions.

D. Reliability Measures

To ensure secure and uninterrupted functioning, several reliability mechanisms were incorporated:

- **Immutable Ledger:** Every vote is hashed and recorded in a blockchain, preventing tampering.
- **Redundant OTP Verification:** Ensures only legitimate voters access the voting panel.
- **Session Security:** Automatic session timeout prevents unauthorized access from idle devices.
- **Consistency Checks:** Each block is validated against previous hashes, ensuring full chain integrity.
- **Backup and Recovery:** Database snapshots maintain voter and election data even in case of system failure.

These measures collectively improve security, data integrity, and fault tolerance.

E. Usability and Voter Experience

User experience was evaluated through feedback collected from test participants:

- The Get Started → Login → OTP → Face Verification → Vote sequence was intuitive and easy to follow.
- Voters appreciated the minimal number of steps, reducing confusion.
- The face verification process was described as fast and reliable, even with low lighting.
- The responsive UI ensured that voters using mobile phones or low-end laptops could participate smoothly.
- The admin dashboard was rated highly for its clarity, real-time statistics, and easy navigation.

Overall, the system achieved a 94

F. Discussion

The results indicate that integrating facial recognition with blockchain significantly enhances the transparency, security, and reliability of digital voting systems. The multi-factor authentication mechanism prevents impersonation, while the Proof-of-Work blockchain ensures that cast votes remain immutable.

Performance metrics show that the system can be deployed even on low-budget hardware without compromising efficiency. Usability evaluations confirm that both voters and administrators can operate the platform with minimal training. The controlled testing environment validated the system's robustness, making it a strong candidate for institutional and organizational elections, although government-level elections would require formal certification and regulatory approval.

V. Conclusion And Future Work

The proposed facial recognition enabled blockchain voting system provides a secure and transparent alternative to tradi- tional institutional voting methods. By combining OTP-based authentication, biometric face verification, and blockchain- backed vote storage, the system effectively eliminates im- personation, duplicate voting, and data tampering. The ar- chitecture offers a streamlined voting experience for users and a comprehensive administrative interface for managing elections, voters, and results. Overall, the system demonstrates strong potential for use in universities, organizations, and private bodies that require reliable and tamper-proof election processes. Future enhancements can further strengthen the system's usability and security. Integrating advanced liveliness detection can prevent spoofing attacks during face verification. Adopting a public or consortium blockchain may improve decentralization and auditability. Additional features such as multilingual support, mobile app integration, and real-time analytics dashboards can make the system more accessible and user-friendly. Expanding the system to support large-scale deployments and enabling interoperability with existing digital ID platforms are key areas for future development.

Acknowledgment

The authors express sincere gratitude to Dr. Sharath Kumar Y H, Head of Department, Information Science and Engineer- ing, Maharaja Institute of Technology, Mysore, for invaluable guidance in system architecture design and project mentorship. We acknowledge the support of the institution in providing resources and infrastructure for development and testing.

Author Profiles

Sinchana V Dsouza is an undergraduate student in the Department of Information Science and Engineering at Maharaja Institute of Technology Mysore. Her academic interests include blockchain systems, artificial intelligence, and secure web application development.

Sonika K is an undergraduate student in the Department of Information Science and Engineering at Maharaja Insti- tute of Technology Mysore. Her academic interests include blockchain systems, artificial intelligence, machine learning and full stack development.

Thejas D is an undergraduate student in the Department of Information Science and Engineering at Maharaja Insti- tute of Technology Mysore. His academic interests include blockchain systems, and secure web application development. **Nuthan Mourya N** is an undergraduate student in the De- partment of Information Science and Engineering at Maharaja Institute of Technology Mysore. His academic interests include blockchain systems and machine learning.

Dr. Sharath Kumar Y H is Professor and Head of the Department of Information Science and Engineering at Maharaja Institute of Technology, Mysore. He holds a Ph.D. in Computer Science and has over 15 years of teaching and research experience in software engineering, web technologies, and database systems.

REFERENCES

[1] Z. Liu, X. Zhang, L. Lao, G. Li, and B. Xiao, "DBE-voting: A Privacy- Preserving and Auditable Blockchain-Based E-voting System," Proc. IEEE ICC,pp. 6571–6577, 2023.

[2] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital Voting: A Blockchain- based E-Voting System using Biohash and Smart Contract," Proc. ICSSIT, pp. 228–234, 2020.

[3] D. D. Bharwani, P. C. Ng, and P. M. Mohan, "Secure and Immutable Blockchain-Based E-Voting for Efficient Overseas e-Voting," Proc. IEEE WF-IoT, pp. 631–638, 2024.

[4] S. M. R. Sowmya, M. Hamal, A. Chaudhary, J. K. Patel, and S. M. Shrestha, "Blockchain Voting: A Solution to the Challenges of Traditional Electoral Systems," in Proc. SSITCON, 2024.

[5] S. A. Wright, "Towards a Blockchain Voting Roadmap," Proc. BRAINS, pp. 121–128, 2021.

[6] C. Mehta, S. Gada, A. Mehta, and N. Kadukar, "Demystifying Democ- racy: Incentivizing Blockchain Voting Technology for an Enriched Electoral System" Proc. ICCICT,2021.

[7] G. Zhongxu, Z. Jianhong, X. Qian, S. Jiyuan, and Z. Jingrun, "A Blockchain Voting Scheme Based on Data Security Separation," Proc. ICETCI, pp. 415–420, 2021.

[8] Y. Chen, H. Zhang, and J. Li, "A Signature Scheme Applying on Blockchain Voting Scene Based on the Asmuth–Bloom Algorithm," Proc. IEEE Conference, 2023.

[9] S. Venkatramulu, S. Karimilla, R. R. Gopu, S. R. Arram, N. Badavath, and K. A. Pannala, "Crypto Ballot: Safeguarding Democracy with Blockchain Voting," Proc. IEEE ICCCNT,2024.

[10] M. Dhore, P. Bhor, S. Puri, P. Wagh, and P. Rai, "Permissioned Blockchain Voting System Using Round-Robin," Proc. IEEE GlobConET, 2023.

[11] S. Vidwans, A. Verma, A. Deshpande, S. Palwe, and P. Thakur, "Per- missioned Blockchain Voting System Using Hyperledger Fabric," Proc. IEEE ICIBT, 2022.

[12] M. Bhamare, K. Shipra, P. Kulkarni, S. Wani, A. Mhetre, and V. Pai, "Revolutionizing College Elections with a Secure Blockchain Voting Solution," Proc. IEEE ICCCMLA, pp. 121–127, 2023.

[13] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "From Conventional Voting to Blockchain Voting: Categorization of Different Voting Mechanisms," Proc. IEEE STI, 2020.

[14] N. H. R., G. P. M. S., S. B. G., D. Jain, P. B. R., and M. Anandkumar, "E-Voting System Using Blockchain Technology," Proc. IEEE ICAC3N, 2022.

[15] V. L. Vashisht, H. Mohan, and S. Prakash, "Smart Voting System Through Face Recognition," Proc. IEEE ICAC3N, pp. 909–912, 2022.

[16] E. N. Witanto, "Secured e-Voting System Leveraging Blockchain Tech- nology," Proc. IEEE ICTIIA, pp. 1–6, 2024.

[17] T. Vairam, S. Sarathambekai, and R. Balaji, "Blockchain Based Voting System in Local Network," Proc. IEEE ICACCS, pp. 363–369, 2021.

[18] P. Chinnasamy, R. K. Ayyasamy, P. Alagarsundaram, S. Dhanasekaran, B. S. Kumar, and A. Kiran, "Blockchain Enabled Privacy-Preserved Secure E-Voting System for Smart Cities," Proc. IEEE ICSTEM, pp. 1–7, 2024.

[19] S. Duan, M. K. Chamran, and M. M. Alobaedy, "Enhancing Blockchain Interoperability Through Cross-Chain Outsourcing and Communica- tion," Proc. IEEE ISCI, pp. 276–279, 2024.

[20] R. Kumar, L. Badwal, A. Prakash, and S. Avasthi, "A Secure Decentralized E-Voting with Blockchain and Smart Contracts," Proc. IEEE Confluence,pp. 419–424, 2023.