E-VOTING SYSTEM BLOCK CHAIN

Prof. Divya K
Assistant Professor.
Department of E&CE
S J M Institute of Technology,
Chitradurga,Karnataka, India
divyaechappy@gmail.com

Aishwarya C K
UG Student
Department of E&CE
S J M Institute of Technology,
Chitradurga ,Karnataka, India
aishwaryakudapali2@gmail.com

Akash S Kademane
UG Student
Department of E&CE
S J M Institute of Technology,
Chitradurga,Karnataka, India
akashkademane89@gmail.com

Dileep R Pawar
UG Student
Department of E&CE
S J M Institute of Technology,
Chitradurga,Karnataka, India
darusladileep@gmail.com

Likhith K J
UG Student
Department of E&CE
S J M Institute of Technology,
Chitradurga ,Karnataka, India
likhithneelvala@gmail.com

Abstract

Modern substitute for conventional voting systems, electronic voting (e-voting) has benefits including faster counting, better accessibility, and less logistical expenses. Still, issues with security, voter privacy, vote tampering, and openness keep its general acceptance hampered. Blockchain technology, referred to as for its distributed, unchangeable, open character, offers a likely answer to these problems. This paper uses a thorough review of the literature and system analysis to investigate, via blockchain-based e-voting systems, their viability and fit. Blockchain is used in the suggested system to improve vote integrity, stop illegal access, and enable real-time auditability, even if advanced cryptographic methods guarantee voter anonymity. Review of case studies and implementations shows that blockchain can greatly raise confidence in digital voting systems.

1 INTRODUCTION

The demand for safe, open, and effective voting systems is more urgent in the digital era than it was years ago. Although dependable in theory, traditional paper-based voting systems suffer many difficulties including logistical complexity, high running expenses, delayed results, and vulnerability to human error or tampering. Although electronic voting (e-voting) systems have become a substitute, they too generate serious questions about vote integrity, voter privacy, and system openness. Conventional e-voting systems' trust and scalability have been limited by problems including centralized control, lack of verifiability, and vulnerability to cyberattacks.

Originally intended as the basis for cryptocurrencies, blockchain technology presents special qualities including decentralization, immutability, openness, and cryptographic security. These characteristics make it a perfect candidate to solve the restrictions of conventional and electronic voting systems. Blockchain could improve trust in the voting process, guarantee vote authenticity, and let safe remote participation by spreading control over a peer-to--peer network and tracking votes in an unchangeable ledger.The feasibility and fit of including blockchain into e-voting systems is investigated in this paper. It analyses its possible advantages and drawbacks, suggests a safe architecture for blockchain-based voting, and offers a thorough literature review. The aim is to assess whether blockchain can really offer a fair and inclusive venue for contemporary democratic voting. During democratic procedures vote-tampering and a lack of transparency in real time. This project presents a Blockchain-Based Voting System that uses blockchain technology and biometric authentication to provide a safe, transparent, and impenetrable voting platform in order to overcome these issues.This technology makes sure that every vote is cast just once, verified biometrically, and recorded irrevocably by combining an ESP32 microcontroller, an R307 fingerprint sensor, and a private Ethereum Proof of Authority (Po A) blockchain. The "one person, one vote" principle is upheld by using smart contracts, which also make results instantly accessible.

2 LITERATURE CHECK-IN

So, there's been a bunch of peeps looking into how we could use this fancy blockchain stuff for e-voting. They've found some cool things and some not-so-cool things. Let's hit the highlights:

[1] **Cabuk and their pals (2002)** did a deep dive into whether blockchain could be a good fit for e-voting. They saw that it could totally make our votes more see-through, keep the data safe, and stop any funny business. But, they pointed out that we'd need some super strong secret codes and spread out computer systems to make sure everyone's trust isn't broken. Plus, blockchain could be like a vote vault that keeps our democracy safe and sound for ages.

[2] Ryan et al. (2009) came up with this cool thing called Prêt à Voter, which is basically a super safe way to vote using some fancy tech stuff called cryptography. It's like a secret code that makes sure everyone's vote is kept private while still making sure everything's on the up and up. It's kind of like the OG for the blockchain systems we've got going on now.

The good part is that voters can totally check that their vote went through and got counted the way they wanted it to, all thanks to these cool math-y proofs. It's like a receipt for your vote, but way more secure.

But here's the catch: because it's all mixed with paper ballots and secret codes, it's a bit of a headache to get it all to work together. It needs some serious tech know-how and more gadgets than a usual voting booth. So while it's a pretty neat idea, it's not as simple as just slapping a sticker on a ballot and calling it a day.

[3] Ben-Nun and their team came up with this cool idea in 2012. They thought, "Why not mix old-school paper voting with some fancy cryptography?" And boom, we've got a dual voting system! It's like having the best of both worlds, right? You get the solidness of paper and the security of some techy digital stuff.The main perk of this system is that you, the voter, can totally make sure your vote counts without anyone knowing who you voted for. It's like having a secret vote that's also totally legit.But, like with anything that tries to be two things at once, there are some downsides. For folks who aren't tech-savvy or are new to this whole voting game, the way the ballots are set up and the whole receipt process can get a bit tricky. It's kind of like when you're at a buffet and you don't know how the dessert section works, but you really want that slice of cake. It's cool when you get it, but it might take a bit of explaining first.

[4] Bell et al. came up with STAR-Vote back in 2013, which is basically a fancy online way to vote that keeps everything super safe and lets everyone check if the count is on the up and up. It's like having your cake and eating it too, but for voting. They used some cool tech stuff like homomorphic encryption and digital signatures to make sure no one messes with your vote.The upsides are that it's pretty high-tech with all the latest security bells and whistles to keep your vote locked down tight. But here's the catch: some folks might get confused by all the cryptography mumbo jumbo and the receipts you get. They might not get why they're important or how to use them to make sure everything's on the level. So, that could mean people either don't trust it or just don't get it, and that's not exactly ideal for something as serious as voting.

[5]Gibson and some folks (2016) took a look at how e-voting has changed over the years, from when it first started to what we've got going on today with the digital stuff. They talked about some problems early systems had, like making sure no one bullies you into voting a certain way and keeping it all hush-hush so you can't be traced. They threw out the idea that blockchain might be the cool new thing to fix those issues.Now, let's chat about the good stuff: e-voting lets you vote from your couch, which is a big deal if you're not so mobile or you're chilling on the other side of the planet. It's pretty handy for those in the boonies, too.But, there's the not-so-fun part: making sure it's totally anonymous so no one can peek at your vote is still a head-scratcher for the techies out there. They're working on it, though!

[6] Then there's Adeshina and Ojo from 2019. These two were all about keeping our votes on the up-and-up with blockchain. They talked about how blockchain is like having no bosses in our voting system, which could stop it from breaking down and make everyone trust it more. But, they also said that if everyone's using blockchain, like for big ol' national elections, it might get as slow as a sloth on a lazy Sunday.the upside of e-voting is that it lets folks vote from anywhere, even if they're not close to a polling place or they can't leave their couch. But, the tricky part is keeping it totally anonymous so no one can track or mess with your vote. And blockchain can totally help with that trust thing because it keeps a clear record without giving away who you voted for. But, we gotta figure out how to make it work fast enough for when a bazillion people want to vote at once.Those are the main points from these studies, folks. Just remember, while blockchain could be the future of voting, it's not gonna be perfect out of the gate. We've got some kinks to work out before it can handle the big leagues**.**

3 METHODOLOGY

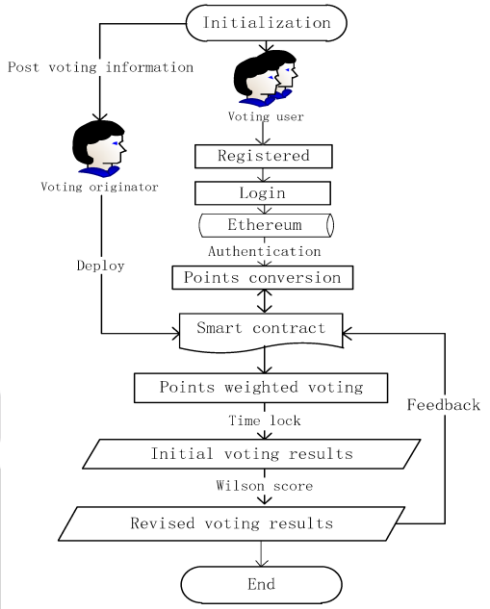

Figure: Flow Chart for Blockchain on E-Voting System

This blockchain-based fingerprint voting system is like the superhero of keeping things legit. It uses a method that's all about combining the power of blockchain with the uniqueness of our fingerprints to make sure each vote is counted and no one tries to cheat the system. It's like giving each vote a secret handshake that only the rightful owner knows, keeping everything on the up and up.follows a structured process, ensuring secure, reliable, and transparent elections. Below are the key steps:

1) FINGERPRINT ENROLLMENT

- Users begin by registering their fingerprints through the ESP32 microcontroller and the R307 fingerprint sensor.
- The fingerprint is captured and converted into a template that is stored on the ESP32's memory.

2) VOTING PROGRESS

- To cast a vote, the user must authenticate by scanning their fingerprint via the R307 sensor.
- If the fingerprint matches the enrolled template, the system confirms the user's identity.
- The ESP32 microcontroller then triggers the web interface, where the user can select their vote

3) VOTE VALIDATION

- After receiving the vote information, the backend server confirms that the user hasn't cast a ballot yet.
- The Ethereum Po A blockchain is contacted by the server to guarantee the integrity and immutability of the vote.
- The blockchain's smart contract logs the vote and modifies the user's status to "voted" if it is legitimate.

4) VOTE STORAGE ON BLOCKCHAIN

- Votes are recorded in an unchangeable ledger on the block chain for Ethereum.
- The Solidity-written smart contract makes sure that votes cannot be removed or changed once they have been submitted.
- The voting results' security, traceability, and transparency are ensured by this procedure.

5) RESULT VEIWING

- Users can view real-time vote tallies via the web interface after voting is finished.
- The backend receives a GET request from the ESP32 and searches the Ethereum blockchain for votes counts.

6) SECURITY AND PRIVACY

- HTTPS encryption is used for all communications, including data exchanges between the ESP32 and the backend server.
- To protect privacy, fingerprint data is kept in an encrypted and secure format.

7) SYSTEM MAINTENANCE

- Up to 10,000 concurrent users can be supported by the system's scalable design.
- To keep the system safe and effective, regular updates and security patches can be applied.

3.1 Design and Implementation Introduction

- The goal of designing and implementing a blockchain-based electronic voting system is to overcome the drawbacks of both conventional and electronic voting methods by establishing a digital voting environment that is safe, transparent, and impenetrable. The main objective is to guarantee that every vote is cast by an authorized voter, that it is permanently recorded, and that it is accurately counted without jeopardizing voter privacy.
User registration, authentication, safe voting, blockchain-based storage, and vote tallying via smart contracts are just a few of the integrated modules that make up the system architecture. Every vote is recorded as a transaction in the decentralized, immutable ledger that is blockchain, guaranteeing data transparency and integrity. To safeguard voter identities and guarantee the confidentiality and legitimacy of every vote, cryptographic techniques like digital signatures, hashing, and encryption are used.

Depending on the required degree of decentralization and performance, this system can be implemented using either public or permissioned blockchain platforms, such as Ethereum or Hyperledger Fabric. Without the need for centralized authority intervention, smart contracts securely tally the results, automate the voting logic, and handle vote validation.
Voter anonymity, end-to-end verifiability, fraud risk reduction, and boosting confidence in digital electoral processes are the main goals of the design and implementation process.

System Design

- The blockchain-based electronic voting system's architecture is set up to guarantee high security, verifiability, transparency, and voter privacy throughout the entire voting process. Several essential parts of the modular architecture cooperate in a decentralized setting. Every module in the voting process is made to manage a particular task, and blockchain serves as the central ledger that ensures integrity and auditability.

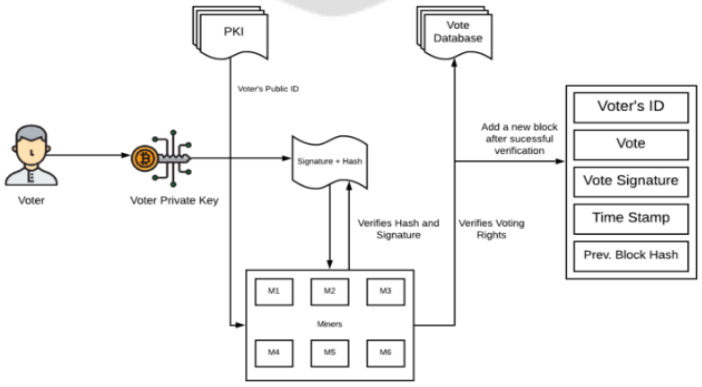

Figure :Block Diagram Of Blockchain On e voting system.

1. User Interface Layer

- **Platform:** Web or Mobile Application
- **Function:** Allows voters to register, log in, cast their votes, and verify their participation.
- **Design Goal:** Simple, secure, and user-friendly interface that can guide even non-technical users through the voting process.

2. Voter Registration Module

- **Function:** Collects voter details and verifies identity using government-issued IDs or biometric authentication.
- **Security Feature:** Once verified, each voter is issued a unique cryptographic key pair (public and private key).

3. Authentication Module

- **Function:** Handles login and session management using secure multi-factor authentication.
- **Techniques Used:** OTP verification, biometric check, and password-based login.
- **Goal:** Prevent unauthorized access and impersonation.

4. Voting Module

- **Function:** permits the voter to use a computer to cast their ballot.
- **Procedure:** Before being submitted, the vote is encrypted and signed with the voter's private key.
- **Goal:** Maintain vote confidentiality and authenticity.

5. Blockchain Layer

- **Platform Options:** Ethereum (public), Hyperledger Fabric (permissioned)
- **Function:** Stores each vote as a transaction in an immutable ledger.
- **Smart Contracts:** Implement rules for vote validation and result tallying automatically.
- **Consensus Mechanism:** PBFT or PoA for permissioned systems; PoW or PoS for public systems.
- **Goal:** Ensure vote immutability, transparency, and eliminate tampering.

6. Result Tallying Module

- **Function:** Automatically counts the votes through smart contract logic.
- **Goal:** Eliminate manual counting and human errors.

7. Audit and Verification Module

- **Function**: Enables voters and officials to confirm that votes were accurately cast without disclosing specific selections.
- **Methods Employed:** hash-based verification and end-to-end verifiability.
- **Objective**: Boost election process transparency and confidence.

✓ **Security Features**

- End-to-End Encryption
- Immutable Ledger
- Anonymity through Cryptographic Techniques
- Tamper Detection via Hash Functions

✓ **Technology Stack (Example)**

- **Frontend:** HTML, CSS, JavaScript (React/Angular)
- **Backend:** Node.js, Python (Flask/Django)
- **Blockchain:** Ethereum / Hyperledger Fabric
- **Smart Contracts:** Solidity (Ethereum) / Chain code (Hyperledger)

3.2 Software and Hardware Requirements Hardware Requirements:

1.ESP32 MICRO CONTROLLER : A key component of the blockchain-based fingerprint voting system is the ESP32 microcontroller. With its integrated Wi-Fi and Bluetooth capabilities, this high-performance, low-power gadget allows for wireless communication with the blockchain and backend server. The ESP32's dual-core processor allows it to perform several tasks at once, including voting, fingerprint scanning, and server communication. It securely authenticates users before they cast their votes by interacting directly with the R307 fingerprint sensor. The user interface for choosing voting options and viewing results is also provided by the ESP32, which securely transmits data via HTTPS to the backend server. Its large memory (RAM and flash) allows voting data and fingerprint templates to be stored, and its low power consumption makes it perfect for

Figure: ESP32 Micro Controller

2. R307 Fingerprint Sensor: A crucial part of the blockchain-based fingerprint voting system, the R307 Fingerprint Sensor is in charge of taking and confirming user fingerprints to guarantee safe and trustworthy authentication. This optical fingerprint sensor scans, processes, and compares fingerprint patterns using sophisticated minutiae extraction and template matching algorithms. The R307 scans a user's fingerprint and compares it to templates that have been stored before the user tries to cast their ballot. The sensor verifies the user's identity if a match is discovered, enabling them to continue with the voting process. The ESP32 microcontroller manages the user interface and data exchange in conjunction with the R307 sensor. It ensures that only registered users are able to vote by providing quick and precise fingerprint recognition. Up to 1000 fingerprint templates can be locally stored by the sensor.

Figure : R307 Fingerprint Sensor

3.BATTERY: One kind of rechargeable battery that is frequently found in electric cars, consumer electronics, and renewable energy systems is the lithium-ion (Li-ion) battery. Lithium ions are the essential element for energy storage and transfer in its operation. An electrolyte separates the two electrodes that make up the battery: the positive cathode and the negative anode. Lithium ions transfer from the anode to the cathode during battery discharge, releasing energy. The ions store energy as they travel in the opposite direction during charging. Because of their high energy density, long lifespan, and lightweight design, lithium-ion batteries are recommended for use in electric vehicles and portable electronics like tablets, laptops, and smartphones.

Figure:Lithium Ion(Li-ion) Battery

4. Switch : It is a commonly used electrical component designed to control the flow of current in a circuit. It features a red actuator marked with the standard symbols “I” for ON and “O” for OFF, making it easy for users to identify its current state. When the switch is pressed on the “I” side, it completes the electrical circuit, allowing current to flow; pressing the “O” side breaks the circuit, stopping the flow of electricity. Rocker switches typically come with two or more metal terminals (pins) for easy connection in electronic circuits and are often mounted into panels of devices. These switches are widely used in applications such as home appliances, power supplies, and DIY electronics due to their durability, ease of use, and clear operational status.

Figure: Switch

Software Requirements:

1.Arduino IDE

- **Purpose**: Used to write and upload code to the ESP32 microcontroller.
- **Features**:
  - Open-source development platform.
  - Supports C/C++ programming for ESP32.
  - Allows integration with other libraries and sensors.

2.ESP32 Libraries

- **Purpose**: Libraries to facilitate communication and control between the ESP32 and various components.
- **Libraries**:
  - ESP32 Wi-Fi: Handles Wi-Fi communication between ESP32 and backend server.
  - **Fingerprint Sensor Library**: For interacting with the R307 Fingerprint Sensor to capture and match fingerprints.
  - **HTTP Client Library**: Allows the ESP32 to send HTTP requests to interact with backend servers and APIs.

3.Ethereum (Solidity)

- **Purpose**: creation of smart contracts for the Ethereum network.
- **Features**:
  - Solidity: The main programming language for Ethereum smart contract development.
  - Smart Contract: Manages voting logic, vote recording, and ensures one-vote-per-person logic.

4.Truffle Suite

- Purpose: Development framework for Ethereum-based applications.
- **Features**:
  - Used for compiling, deploying, and testing smart contracts.
  - Integrates with the Ethereum PoA (Proof of Authority) network to deploy and interact with the blockchain.

5.Node.js (Backend Server)

- **Purpose**: Backend server to manage data flow between the ESP32 and Ethereum blockchain.
- **Features**:
  - Express.js: Framework for building RESTful APIs.
  - Handles HTTP requests from the ESP32, validates votes, and interacts with the Ethereum blockchain.

6. Flask (Alternative Backend)

- ✓ **Purpose**: a thin backend framework for managing blockchain communications and API requests.
- ✓ **Features**:
  - Python-based framework for rapid API development.
  - Can interact with Ethereum blockchain via Web3.py library.

7.Web3.js

- **Purpose**: The Ethereum blockchain can be accessed through a JavaScript library.
- **Features**: Enables transactions to be sent to the Ethereum blockchain from the backend.

4 Results And Discussion

4.1 The core processing unit of the biometric blockchain-based electronic voting system is a central microcontroller, usually an ESP32. As the main means of voter authentication, the system starts with a fingerprint scanner module that is conspicuously mounted on the casing. The gadget takes a picture of the user's fingerprint when they place their finger on the scanner, then transmits it to the ESP32 for processing. The voter legitimacy is then ascertained by the microcontroller by comparing the recorded data with pre-registered templates.

The system moves on to the voting phase after authentication is successful. Voters can cast their ballots using a straightforward user interface, which may include a touchscreen or, if used, a button-based display. In the meantime, visual feedback is provided by indicator LEDs, which turn red or off when authentication is successful and green otherwise.

Figure 4.1: Fingerprint Voting Machine

The model on display is a realistic depiction of a Blockchain-Based E-Voting System (EVS), which combines digital and physical elements to mimic a voting procedure in the real world. The setup consists of a box structure that has been decorated and labeled "Blockchain on EVS." It has components like a laptop, hammer, and voting elements, as well as visual indicators like symbolic icons for candidates. This structure, which is supported by blockchain security, visually leads viewers through the voting process and represents the shift from traditional to digital voting. A fictitious "polling booth" with cultural decorations at the center makes for an interesting and instructive experience.
A laptop running the voting system's front-end interface, which includes a login portal where verified voters can safely access the electronic voting platform, is located to the left of the model. This

Figure 4.2: Model of the voting booth

5 Conclusion:

An alternative to conventional voting techniques that is safe, transparent, and impenetrable is the blockchain-based fingerprint voting system. Each vote is guaranteed to be authentic and irrevocable by combining biometric authentication with blockchain technology's immutability, greatly lowering the possibility of fraud and manipulation. Even in remote or resource-constrained locations, cost-effective deployment is made possible by the ESP32 microcontroller and R307 fingerprint sensor. With one-person-one-vote enforcement and real-time result viewing, this system provides a reliable and innovative way to hold elections in local government bodies, organizations, and campuses. This system could expand and change how democratic processes are carried out around the world as technology develops. One potential remedy for the persistent issues is the incorporation of blockchain technology into electronic voting systems.

6 Reference:

[1] S. M. T. Toapanta, G. A. C. Pacheco, D. W. B.Valencia, and
L. E. M. Gallegos, ‘‘Optimization of an electronic signature scheme in a voting system in a distributed architecture,’’ in *Proc. 2nd Int. Conf. Saf. Produce Informatization (IICSPI)*, Nov. 2019, pp. 593–596.

[2] S. Heiberg, K. Krips, J. Willemson, and P. Vinkel, ‘‘Facial recognition for remote electronic voting–missing piece of the puzzle or yet another liability?’’ in *Proc. Int. Workshop Emerg. Technol. Authorization Authentication*. Switzerland: Springer, 2021, pp. 77–93.

[3] A. A. Monrat, O. Schelén, and K. Andersson, ‘‘A survey of blockchain from the perspectives of applications, challenges, and opportunities,’’ *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[4] V. Vijayalakshmi and S. Vimal, ‘‘A novel P2P based system with blockchain for secured voting scheme,’’ in *Proc. 5th Int. Conf. Sci. Technol. Eng. Math. (ICONSTEM)*, Mar. 2019, pp. 153–156.

[5] U. Jafar, M. J. A. Aziz, and Z. Shukur, ‘‘Blockchain for electronic voting system—Review and open research challenges,’’ *Sensors*, vol. 21, no. 17,
p. 5874, 2021.

[6] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, ''E-voting system based on blockchain technology: A survey,'' in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Jul. 2021, pp. 200–205.
[7] Y. Abuidris, R. Kumar, and W. Wenyong, ''A survey of blockchain based on E-voting systems,'' in *Proc. 2nd Int. Conf. Blockchain Technol. Appl.*, Dec. 2019, pp. 99–104.
[8] K. T. Sri, K. R. Sri, and N. Pedamallu, ''E-voting system using blockchain,'' *J. Xi'an Univ. Archit. Technol.*, vol. 13, no. 5, pp. 527–533, 2021.
[9] V. Anilkumar, J. A. Joji, A. Afzal, and R. Sheik, ''Blockchain simulation and development platforms: Survey, issues and challenges,'' in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICCS)*, May 2019, pp. 935–939.
[10] T. Moura and A. Gomes, ''Blockchain voting and its effects on election transparency and voter confidence,'' in *Proc. 18th Annu. Int. Conf. Digit. Government Res.*, Jun. 2017, pp. 574–575.
[11] S. Salam and K. P. Kumar, ''Survey on applications of blockchain in E-governance,'' *Revista Gestão Inovação e Tecnologias*, vol. 11, no. 4, pp. 3807–3822, Jul. 2021.
[12] I. Kubjas, ''Using blockchain for enabling internet voting,'' Inst. Comput. Sci., Univ. Tartu, Tartu, Estonia, Tech. Rep. MTAT.03.323 Fall 2016, 2017. [Online]. Available: https://courses.cs.ut.ee/MTAT.03.323/ 2016_fall/uploads/Main/004.pdf
[13] Y. Abuidris, A. Hassan, A. Hadabi, and I. Elfadul, ''Risks and opportunities of blockchain based on E-voting systems,'' in *Proc. 16th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process.*, Dec. 2019, pp. 365–368.
[14] V. Neziri, R. Dervishi, and B. Rexha, ''Survey on using blockchain technologies in electronic voting systems,'' in *Proc. 25th Int. Conf. Circuits, Syst., Commun. Comput. (CSCC)*, Jul. 2021, pp. 61–65.
[15] F. Rabia, A. Sara, and T. Gadi, ''A survey on e-voting based on blockchain,'' in *Proc. 4th Int. Conf. Netw., Inf. Syst. Acad. Manage. Perspect. Security.*, Apr. 2021, pp. 1–8.
[16] S. Kadam, K. Chavan, I. Kulkarni, and A. Patil, ''Survey on digital E- voting system by using blockchain technology,'' *Int. J. Advance Sci. Res. Eng. Trends*, vol. 4, no. 2, pp. 5–8, Feb. 2019.
[17] S. Sayyad, M. Pawar, A. Patil, V. Pathare, P. Poduval, S. Sayyad, M. Pawar, A. Patil, V. Pathare, and P. Poduval, ''Features of blockchain voting: A survey,'' *Int. J.*, vol. 5, pp. 12–14, Feb. 2019.
[18] A. Khandelwal, ''Blockchain implimentation on E-voting system,'' in *Proc. Int. Conf. Intell. Sustain. Syst. (ICISS)*, Feb. 2019, pp. 385–388.
[19] M. Rezvani and H. Khani, ''E-voting over blockchain platforms: A survey,'' *J. Netw. Secur. Data Mining*, vol. 2, no. 3, pp. 1–14, 2019.
[20] Y. Rosasooria, A. K. Mahamad, S. Saon, M. A. M. Isa, S. Yamaguchi, and M. A. Ahmadon, ''E-voting on blockchain using solidity language,'' in *Proc. 3rd Int. Conf. Vocational Educ. Electr. Eng. (ICVEE)*, Oct. 2020, pp. 1–6.
[21] O. Cetinkaya and D. Cetinkaya, ''Verification and validation issues in electronic voting,'' *Electron. journal E-Government*, vol. 5, no. 2, pp. 117–126, 2007.
[22] N. Kshetri and J. Voas, ''Blockchain-enabled E-voting,'' *IEEE Softw.*, vol. 35, no. 4, pp. 95–99, Jul./Aug. 2018.
[23] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, ''Analysis of blockchain solutions for E-voting: A systematic literature review,'' *IEEE Access*, vol. 10, pp. 70746–70759, 2022.
K. Patidar and S. Jain, ''Decentralized E-voting portal using blockchain,'' in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–4.
[24] E. Yavuz, A. K. Koc, U. C. Cabuk, and G. Dalkilic, ''Towards secure E- voting using ethereum blockchain,'' in *Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Mar. 2018, pp. 1–7.
[25] M. A. Cheema, N. Ashraf, A. Aftab, H. K. Qureshi, M. Kazim, and A. T. Azar, ''Machine learning with blockchain for secure E-voting sys- tem,'' in *Proc. 1st Int. Conf. Smart Syst. Emerg. Technol. (SMARTTECH)*, Nov. 2020, pp. 177–182.
[26] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, ''Decentralized voting platform based on ethereum blockchain,'' in *Proc. IEEE Int. Multidisciplinary Conf. Eng. Technol. (IMCET)*, Nov. 2018, pp. 1–6.
[27] S. Khan, A. Arshad, G. Mushtaq, A. Khalique, and T. Husein, ''Implementation of decentralized blockchain E-voting,'' *EAI Endorsed Trans. Smart Cities*, vol. 4, no. 10, Jun. 2020, Art. no. 164859.
[28] F. Sheer Hardwick, A. Gioulis, R. Naeem Akram, and K. Markantonakis, ''E-voting with blockchain: An E-voting protocol with decentralisation and voter privacy,'' in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1561–1567.
[29] A. M. Al-madani, A. T. Gaikwad, V. Mahale, and Z. A. T. Ahmed, ''Decentralized E-voting system based on smart contract by using blockchain technology,'' in *Proc. Int. Conf. Smart Innov. Design, Environ., Manage., Planning Comput. (ICSIDEMPC)*, Oct. 2020, pp. 176–180.

[30] K. Kost'al, R. Bencel, M. Ries, and I. Kotuliak, ''Blockchain E-voting done right: Privacy and transparency with public blockchain,'' in *Proc. IEEE 10th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Oct. 2019, pp. 592–595.
[31] B. Ahn, ''Implementation and early adoption of an ethereum-based electronic voting system for the prevention of fraudulent voting,'' *Sustainability*, vol. 14, no. 5, p. 2917, Mar. 2022.
[32] H. Yi, ''Securing E-voting based on blockchain in P2P network,'' *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–9, Dec. 2019.
[33] C. K. Adiputra, R. Hjort, and H. Sato, ''A proposal of blockchain- based electronic voting system,'' in *Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS4)*, Oct. 2018, pp. 22–27.
[34] M. Pawlak, A. Poniszewska-Marańda, and N. Kryvinska, ''Towards the intelligent agents for blockchain E-voting system,'' *Proc. Comput. Sci.*, vol. 141, pp. 239–246, Jan. 2018.
[35] A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam, and A. Islam, ''Towards blockchain-based E-voting system,'' in *Proc. Int. Conf. Innov. Sci., Eng. Technol. (ICISET)*, Oct. 2018, pp. 351–354.
[36] T. M. Roopak and R. Sumathi, ''Electronic voting based on virtual ID of aadhar using blockchain technology,'' in *Proc. 2nd Int. Conf. Innov. Mech. for Ind. Appl. (ICIMIA)*, Mar. 2020, pp. 71–75.
[37] M. Doost, A. Kavousi, J. Mohajeri, and M. Salmasizadeh, ''Analysis and improvement of an E-voting system based on blockchain,'' in *Proc. 28th Iranian Conf. Electr. Eng. (ICEE)*, Aug. 2020, pp. 1–4.
[38] R. Hanifatunnisa and B. Rahardjo, ''Blockchain based E-voting recording system design,'' in *Proc. 11th Int. Conf. Telecommun. Syst. Services Appl. (TSSA)*, Oct. 2017, pp. 1–6.
[39] F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, ''Crypto- voting, a blockchain based E-voting system,'' in *Proc. 10th Int. Joint Conf. Knowl. Discovery, Knowl. Eng. Knowl. Manage.*, 2018, pp. 221–225.
[40] S. T. Alvi, M. N. Uddin, and L. Islam, ''Digital voting: A blockchain- based E-voting system using biohash and smart contract,'' in *Proc. 3rd Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Aug. 2020, pp. 228–233.
[41] J. Goyal, M. Ahmed, and D. Gopalani, ''A privacy preserving E-voting system with two-phase verification based on ethereum blockchain,'' *Preprint Res. Square*, pp. 1–33, Jun. 2022.
[42] K. Teja, M. Shravani, C. Y. Simha, and M. R. Kounte, ''Secured voting through blockchain technology,'' in *Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI)*, Apr. 2019, pp. 1416–1419.
+