INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

International Journal of Electronic Governance

ISSN online: 1742-7517 - ISSN print: 1742-7509
https://www.inderscience.com/ijeg

Blockchain powered e-voting: a step towards transparent governance

Kailash Chandra Bandhu, Ratnesh Litoriya, Arpit Deo, Sanket Gupta, Ravish Satwani, Rishee Deshmukh, Rohit Kumar Lavvanshi, Mubeen Ahmed Khan

DOI: 10.1504/IJEG.2024.10067195

Article History:

Received:	13 May 2024
Last revised:	24 May 2024
Accepted:	12 August 2024
Published online:	29 October 2024

Blockchain powered e-voting: a step towards transparent governance

Kailash Chandra Bandhu*, Ratnesh Litoriya, Arpit Deo, Sanket Gupta, Ravish Satwani, Rishee Deshmukh, Rohit Kumar Lavvanshi and Mubeen Ahmed Khan

Department of Computer Science and Engineering,
Medi-Caps University,
Indore, 453331, India
Email: kailashchandra.bandhu@gmail.com
Email: litoriya.ratnesh@gmail.com
Email: deo.arpit33@yahoo.com
Email: sanket.jec@gmail.com
Email: ravishsatwani.work@gmail.com
Email: rishee.rsd@gmail.com
Email: rohitlavvanshi07@gmail.com
Email: makkhan0786@gmail.com
*Corresponding author

Abstract: Elections hold immense significance in shaping the leadership of a nation or organisation, serving as a pivotal moment that influences the trajectory of the entity involved. Despite their centrality to modern democratic systems, elections face a significant hurdle: widespread mistrust in the electoral process. This pervasive lack of confidence poses a substantial threat to the democratic framework, even in the case of prominent democracies such as India and US, where inherent flaws persist in the electoral system. Issues such as vote rigging, electronic voting machine (EVM) hacking, election manipulation, and polling booth capturing remain prominent concerns within the current voting paradigm. Leveraging blockchain for electronic voting systems offers an effective solution to alleviate the prevailing apprehensions associated with e-voting. By incorporating blockchain into the electoral process, the integrity and security of the system could be significantly strengthened, addressing the current vulnerabilities and fostering trust in democratic elections.

Keywords: blockchain; e-voting system; secured; ethereum; decentralised; digitalising.

Reference to this paper should be made as follows: Bandhu, K.C., Litoriya, R., Deo, A., Gupta, S., Satwani, R., Deshmukh, R., Lavvanshi, R.K. and Khan, M.A. (2024) 'Blockchain powered e-voting: a step towards transparent governance', *Int. J. Electronic Governance*, Vol. 16, No. 3, pp.354–377.

Biographical notes: Kailash Chandra Bandhu is the Academic Head and Professor in the Department of Computer Science and Engineering at Medi-Caps University, Indore. He holds a BE from Mandsaur Institute of

Technology, an MTech from Medi-Caps Institute of Technology and Management, and a PhD from Bhagwant University. With over 18 years of academic experience, he has held key roles, including Dean at Shivajirao Kadam Institute of Technology and Management. His research interests include machine learning, big data, wireless networks, and blockchain. He has supervised multiple doctoral theses and contributed to patents in IoT, mental health tracking, and road safety.

Ratnesh Litoriya is a Distinguished Academic and Researcher serving as the Professor and Head of the Department of Computer Science and Engineering at Medi-Caps University, Indore, India. He received his BTech (Information Technology), ME (Computer Engineering), and PhD (Computer Engineering) degrees from different reputed Universities of India in 2004, 2007, and 2015, respectively. His research interests include machine learning, blockchain technology, artificial intelligence, and their applications in healthcare, agriculture, and electronic health records. Notably, he has contributed to various high-impact projects, such as the development of applications for elderly care, blockchain-based frameworks for healthcare during the COVID-19 pandemic, and machine learning-driven solutions for Indian agriculture. With over 18 years of experience, he supervises numerous PhD students and continues to contribute to cutting-edge research, bridging the gap between academic theory and practical solutions that benefit society.

Arpit Deo is associated with Medi-Caps University in Indore as an Assistant Professor, India. He is known for his significant contributions to the academic and administrative sectors of the university. His role at Medi-Caps University highlights his dedication to fostering academic excellence and innovation within the institution.

Sanket Gupta is working as an Assistant Professor at Medi-Caps University in Indore, India. He is known for his significant contributions to the academic and administrative sectors of the university. His expertise in machine learning, blockchain and server administration.

Ravish Satwani is a BTech Student specialising in Computer Science and Engineering at Medi-Caps University in Indore, India. As an Aspiring Engineer, he is actively engaged in acquiring both theoretical knowledge and practical skills in various domains of computer science, including programming, algorithms, data structures, and software development.

Rishee Deshmukh is a BTech student specialising in Computer Science and Engineering at Medi-Caps University in Indore, India. As an Aspiring Engineer, he is actively engaged in acquiring both theoretical knowledge and practical skills in various domains of computer science, including programming, algorithms, data structures, and software development.

Rohit Kumar Lavvanshi is a BTech student specialising in Computer Science and Engineering at Medi-Caps University in Indore, India. As an aspiring engineer, he is actively engaged in acquiring both theoretical knowledge and practical skills in various domains of computer science, including programming, algorithms, data structures, and software development.

Mubeen Ahmed Khan is an accomplished academic serving as an Assistant Professor in the Department of Computer Science and Engineering at Medi-Caps University, Indore. He holds an MTech in Computer Science and

Engineering and is his PhD in the same field. With over 18 years of experience in both academia and research. His expertise includes machine learning, big data analysis, and network security. His research focuses on areas such as wireless communication, IoT, and artificial intelligence, with an emphasis on their practical applications in enhancing communication networks and data security. He has contributed to various scholarly publications and is actively involved in guiding students in research projects, particularly in emerging technologies.

1 Introduction

Elections serve as essential foundations of a democratic system, providing the general public with the opportunity to voice their opinions through the act of voting. Given their pivotal role in shaping society, it is imperative that the election process upholds transparency and reliability to maintain the trust and credibility of all participants. Within this framework, the methodology of voting continuously evolves to adapt to changing needs and circumstances (Jafar et al., 2021). Our research centers on leveraging ICT advancements through electronic machines within polling stations, particularly during public votes like the General Election in the UK. The primary objective is to explore the challenges associated with this approach and identify potential solutions to mitigate them. We aim to understand and address the complexities that arise when integrating electronic technology into the voting process, especially in the context of a widespread electoral event such as a General Election. By examining these challenges and proposing solutions, our research contributes to the ongoing discourse on enhancing the efficiency, security, and overall effectiveness of electronic voting systems within the democratic framework (Cohen and Fischer, 1985).

Ensuring electoral integrity is imperative not only for the functioning of democratic nations but also for fostering trust and accountability among state voters. The choice of political voting methods plays a pivotal role in this regard. From a governmental perspective, the adoption of electronic voting technologies has the potential to enhance voter participation and instil confidence, thereby reigniting interest in the electoral process (Zachariadis et al., 2019). Elections, as a fundamental mechanism for democratic decision-making, have long been a societal priority. With the growing volume of votes being cast, citizens are increasingly recognising the significance of the electoral system. Essentially, the voting system serves as the mechanism through which individuals determine their representatives in both political and corporate governance. Democracy, fundamentally, revolves around voters selecting representatives through the act of voting.

In 2008, an individual or group using the pseudonym Nakamoto introduced a new digital currency known as Bitcoin. This currency was built on blockchain technology, which was seen as potentially groundbreaking in various sectors like finance and governance. Blockchain, in essence, is a system of interconnected blocks forming a chain-like data structure (Nakamoto, 2009). These blocks are stored across a network of nodes, where they are collectively validated and updated through a specific algorithm. This technology allows for secure and transparent record-keeping without the need for a

central authority, making it highly versatile and impactful in numerous fields (Poniszewska-Maraundefinedda et al., 2020).

Blockchain has garnered substantial attention due to its widespread applications in finance, healthcare, and supply chain management systems (Davor and Sajter, 2019). Conceptually, a blockchain functions as a data structure that continuously records and shares all transactions starting from its inception. It operates as a decentralised, distributed database, ensuring the security of data records against unauthorised manipulation. Users can connect to the network, submit new transactions, verify existing transactions, and contribute to the creation of new blocks. Each block is associated with a cryptographic hash, essentially a fingerprint, which remains valid unless the block's data is altered. Any changes to the data result in an immediate alteration of the cryptographic hash, serving as an indicator of potential malicious activity (Zhang et al., 2018). With its robust cryptographic foundations, blockchain is increasingly utilised to counteract unauthorised transactions across diverse domains.

Enhanced transparency facilitated by open and distributed ledgers. Inherent anonymity of voters. Improved security and reliability, especially in guarding against Denial-of-Service attacks. Immutability, ensuring the integrity of the voting process and individual ballots (Chondros et al., 2019). By distributing vote information across thousands of computers, blockchain makes it virtually impossible to alter or erase votes once cast, fostering greater trust between voters and governments by safeguarding their data. Blockchain enables voters to cast their ballots conveniently via smartphones or computers using dedicated applications, eliminating the need for long queues at polling stations (Benítez-Martínez et al., 2021). Importantly, implementing blockchain does not necessarily require governments to overhaul their existing systems; instead, they can adapt their current platforms accordingly. One notable limitation of blockchain is its capacity to handle only small text strings that record balance transfers between parties.

To ensure a fair and transparent voting process, certain security properties must be met, including authentication, transparency, anonymity, integrity, security, privacy, mobility, fairness, and verifiability. However, implementing these properties in an Ethereum-based application can be costly (Bandhu et al., 2023a; Hanifatunnisa and Rahardjo, 2017). Thus, our focus is on discussing how the proposed system satisfies these security requirements while minimising compute and storage costs. Furthermore, there are several benefits associated with utilising blockchain technology. Here are some of them (Bandhu et al., 2023b; Vaigandla et al., 2023):

1 *Decentralisation*: In e-voting systems, decentralisation ensures that no single entity has control over the voting process. Instead, the voting data is distributed across multiple nodes in the network, reducing the risk of manipulation or fraud. Each node in the network holds a copy of the voting ledger, and changes to the ledger must be agreed upon by a consensus of the network participants, ensuring the integrity of the voting process.

2 *Transparency*: Transparency in e-voting systems ensures that all participants, including voters, candidates, and election officials, have access to the same information about the voting process. This transparency helps build trust in the system by allowing stakeholders to verify the integrity of the voting results. With blockchain technology, every transaction or vote cast is recorded on the blockchain and is visible to all participants, ensuring transparency and accountability.

3 *Immutability*: Immutability ensures that once a vote is recorded on the blockchain, it cannot be altered or deleted. This property is crucial for maintaining the integrity of the voting process and preventing tampering or manipulation of votes. In e-voting systems, immutability ensures that the voting results are final and cannot be changed after the fact, providing assurance to voters that their votes will be counted accurately.

4 *Accessibility*: Blockchain-based e-voting systems can increase accessibility for voters, especially those who are unable to physically attend polling stations. Through secure digital platforms, voters can cast their ballots from anywhere with an internet connection.

5 *Auditability*: Every transaction on the blockchain is timestamped and linked to previous transactions, creating a transparent audit trail. This auditability is crucial in ensuring the accuracy and fairness of election results.

6 *Reduced fraud*: The combination of cryptographic security, transparency, and immutability makes blockchain-based e-voting systems highly resistant to fraud. It significantly reduces the risk of unauthorised access, tampering, or manipulation of votes.

7 *Faster results*: With traditional voting systems, it can take time to count and verify votes manually. Blockchain technology enables real-time vote counting and result verification, leading to faster and more accurate election outcomes.

8 *Trust and confidence*: Ultimately, the benefits of blockchain in e-voting contribute to building trust and confidence in the electoral process. When voters have faith in the security and fairness of the system, they are more likely to participate and accept the outcome of elections.

2 Literature review

Initially, voting was conducted using paper-based methods, involving manual voting and counting processes. Subsequently, paper punch cards were introduced, where votes were manually punched and counted electronically. This method was later replaced by mark sense and digital pen voting, requiring voters to queue up to cast their votes using machines. Currently, electronic voting systems are in use, employing the modular square root and blind signature system to ensure voter secrecy. These systems prioritise voter confidentiality, ballot secrecy, anonymity, and minimal computational costs to enhance the integrity and security of the voting process (Selvarani et al., 2017).

Many researchers and professionals are working on solving the issues related to casting votes. Traditional voting systems encounter challenges like human errors in manual ballot counting, causing inaccuracies and delays in result announcements. Digital voting system minimise trust in central authorities and enhance voting process fairness. The system employs a Solidity smart contract, two NodeJS servers, and an Angular framework interface, demonstrating its functionality on the Sepolia testnet. It ensures ballot privacy, individual verifiability, eligibility, fairness, accuracy, uniqueness, robustness, and universal verifiability. Notably, it leverages blockchain to secure and

transparently broadcast ballot results, allowing public audits for result verification (Khan et al., 2020).

Extensive research has been conducted on electronic voting systems, which allow voters to vote from their mobile phones, computers, or other electronic devices. However, these technologies have not been widely adopted due to security worries about their potential impact on vote integrity. This study explores a blockchain-based electronic voting system that is secure, transparent, and robust (Abayomi-Zannu et al., 2019).

The exploration of challenges and opportunities of blockchain for e-voting revealed a multifaceted landscape. Identified challenges included addressing scalability concerns to accommodate high transaction volumes during elections, ensuring privacy and anonymity while maintaining transparency, mitigating the risk of cyberattacks, and overcoming regulatory hurdles. Additionally, accessibility issues were noted to be crucial in ensuring all voters, regardless of technological proficiency or access to resources, could participate in the e-voting process securely. However, the literature also highlighted numerous opportunities for revolutionising e-voting through blockchain. Its immutable ledger was found to ensure the integrity of voting records, reducing the risk of fraud and manipulation. Smart contracts were recognised for their potential to automate and streamline voting processes, improving efficiency and reducing costs. Decentralisation was noted to foster trust by eliminating reliance on centralised authorities, while cryptographic techniques secured data transmission and storage. Furthermore, blockchain enabled real-time verification of voting results, enhancing transparency and public trust in the electoral process. Despite challenges, the literature indicated that the potential of blockchain to transform e-voting was significant, promising greater inclusivity, integrity, and efficiency in democratic practices (Taş et al., 2020).

The groundbreaking decentralised voting platform built on the Ethereum Blockchain, with a key focus on curbing multiple votes per mobile (MSISDN). The platform's innovation extends its applicability to national government elections, suggesting enhancements through fingerprint authentication or specialised devices in voting centers. Emphasising adaptability, the user interface and results visualisation can be tailored to meet diverse customer requirements. Positioned as a viable alternative to centralised systems reliant on SMS polling, this platform has the potential to streamline voting processes for governments, competitions, and expositions. Beyond its technological implications, the paper introduces a transformative business model for voting service providers, engaging key stakeholders such as voting event organisers, service providers, and voters (Khoury et al., 2018).

Blockchain technology offers a secure solution for electoral system challenges by employing hash values to link and safeguard voting records at each polling station. The addition of digital signatures enhances reliability, ensuring a tamper-resistant process. Unlike Bitcoin, this electoral blockchain sequence eliminates the need for mining due to the clarity and non-duplicative nature of voter data. The proposed sequence establishes legal connections between nodes, reducing the risk of data collisions during transmission. In essence, this application of blockchain principles fortifies voting process security, fostering transparency and trust in the electoral system (Sridharan, 2013).

The significant role of hash functions in cryptography, such as MD5, SHA, RIPEMD-160, CBC-MAC, and MD5-MAC, have demonstrated their versatility beyond encryption, finding applications in authentication, virus checking, and digital signatures. Surprisingly, despite advancements in machine capabilities, performance tests reveal

modest improvements in hash function processing speeds, emphasising the resilience of established algorithms like SHA-1. Importantly, within the dynamic landscape of blockchain technology, the significance of hash functions echoes, as they underpin the security and integrity of distributed ledgers. As cryptography navigates the quantum era, the intersection with blockchain technology amplifies the need for resilient hash functions as foundational elements in ensuring the continued trustworthiness of decentralised systems (Yi, 2019).

Using a consortium blockchain emerges as a compelling option for e-voting systems due to its unique features. Unlike public blockchains, consortium blockchains (like: Hyperledger, Contour, Quorum and Corda) are permissioned, providing controlled access to a pre-selected group of participants. This attribute ensures heightened privacy and security, essential for sensitive voting information. Consortium blockchains enable customisation based on specific voting requirements, allowing for the implementation of tailored smart contracts. The governance structure is typically shared among the consortium members, promoting collaboration while maintaining a level of control. This makes consortium blockchains well-suited for scenarios where a trusted group of entities, such as government agencies or election authorities, collaborates to facilitate secure, transparent, and efficient e-voting processes (Elisa et al., 2019).

Choosing between Hyperledger and Ethereum for an e-voting system involves weighing distinct features. Hyperledger's permissioned structure ensures controlled access, enhancing privacy, and its Byzantine fault tolerance mechanism ensures security, ideal for enterprise applications. Ethereum's public blockchain promotes decentralisation but grapples with scalability issues and gas fees. While Ethereum's standardised smart contract approach facilitates rapid development, it may limit customisation. The decision depends on factors like use case, participant dynamics, flexibility, scalability, and transaction costs, all influencing the selection for a secure, transparent, and efficient e-voting system. Despite scalability challenges, Ethereum's decentralisation makes it preferable for public e-voting scenarios (Díaz-Santiso and Fraga-Lamas, 2021).

Implementation of smart contracts through blockchain transactions, emphasising their role in decentralised networks, interaction with cryptocurrency, and user input. Written in the Solidity language, a blend of C++ and JavaScript, these contracts are governed by Ethereum peers, requiring validation from at least two users for activation. The focus is on leveraging blockchain for comprehensive e-voting solutions, addressing transparency, validation, and security concerns. Ensuring the legitimacy of participants and maintaining the integrity of credentials is crucial, achieved by collecting and analysing signed, timestamped election data. The deployment of self-executable smart contracts on the blockchain establishes rules and data models, ensuring the immutability of the election process. Ethereum's decentralised network, particularly its private version, provides a cost-effective testing ground for new smart contracts, eliminating the need for significant resource expenditure on the actual network. In the context of e-voting, blockchain systems offer advantages over traditional methods, saving time, energy, and costs, and preventing invalid votes (Fusco et al., 2018).

Ethereum employs a proof of work (PoW) consensus algorithm to secure its blockchain, including its application in e-voting systems. In PoW, miners compete to solve complex puzzles, validating and adding transactions to the blockchain. In the context of e-voting, each vote is treated as a transaction, and the PoW mechanism ensures the secure and tamper-resistant recording of votes on the Ethereum blockchain. This decentralised process prevents single-entity control and enhances the overall

trustworthiness of the e-voting system. It's essential to note that Ethereum is transitioning to proof of stake (PoS) with Ethereum 2.0, a more environmentally friendly consensus mechanism that aims to maintain the security and integrity of transactions while reducing energy consumption compared to PoW (Alsunaidi and Alhaidari, 2019).

This study introduces an innovative e-voting protocol on a blockchain platform, featuring an inherent audit function. To fortify the system against potential quantum attacks, we've implemented the Niederreiter algorithm, known for its resilience against such threats. Within this scheme, the Key Generation Center (KGC) is incorporated as a regulatory entity within a certificateless cryptosystem. This dual role ensures voter anonymity while also enabling auditability through the integration of the traceable ring signature algorithm. Essentially, these measures aim to maintain the integrity, fairness, and accuracy of the entire electoral process. Upon closer examination of our protocol, it becomes evident that it offers certain advantages in terms of security and efficiency, particularly in scenarios involving a smaller number of voters, making it well-suited for elections on a more modest scale. However, in cases with a larger voter base, the protocol leans towards emphasising heightened security, albeit at a slight expense of efficiency (Sun et al., 2019).

Solana, renowned for its scalability and speed in blockchain technology, was explored as a potential solution to the scalability challenges encountered by e-voting systems. The study found that Solana's innovative architecture allowed it to process thousands of transactions per second, making it well-suited for managing the substantial volume of voting transactions during elections. By leveraging Solana's efficient consensus mechanism and low latency, e-voting platforms were able to ensure swift and reliable voting processes, even amidst high demand. The scalability provided by Solana not only improved the efficiency of the voting system but also enhanced accessibility for voters, as they could participate without experiencing delays or congestion. Additionally, the study revealed that Solana's robust security features provided resilience against potential threats, thereby safeguarding the integrity and trustworthiness of the e-voting process. Overall, the findings suggested that integrating Solana into e-voting systems led to smoother operations, increased voter participation, and enhanced confidence in the electoral process (Pierro and Tonelli, 2022).

Main role of blockchain technology in e-voting systems is data security was assured within the blockchain network through various mechanisms inherent to blockchain technology. The immutability of blockchain ensured that once data was recorded, it could not be altered or deleted without network consensus, thereby maintaining the integrity of voting records. Decentralisation eliminated reliance on a single central authority, reducing the risk of manipulation or censorship. Cryptographic techniques secured data by hashing transactions and linking them, making it challenging for malicious actors to alter data undetected. Consensus mechanisms validated transactions, ensuring only valid entries were added to the blockchain. The transparency of blockchain allowed all network participants to verify transactions in real-time, enhancing trust in the voting process. By leveraging these features, e-voting systems were able to ensure the security, integrity, and transparency of voting data (Kumari and Farheen, 2020).

Improving authentication in an e-voting system was crucial for ensuring the integrity and security of the electoral process. The study identified robust authentication methods such as biometric identification, multi-factor authentication, or cryptographic techniques as effective means of enhancing the accuracy and reliability of verifying voters' identities. Biometric authentication, such as fingerprint or iris scanning, was noted for its

high level of security by uniquely identifying individuals based on their biological traits. Multi-factor authentication required users to provide multiple forms of verification, such as a password combined with a one-time code sent to their mobile device, thereby adding an extra layer of protection against unauthorised access. Additionally, cryptographic techniques, such as digital signatures, were highlighted for securely authenticating voters' identities while preserving anonymity. Through the implementation of these advanced authentication measures, the literature indicated that e-voting systems could bolster trust, prevent fraudulent activities, and uphold the democratic principles of fairness and transparency (Rexha et al., 2012). Table 1 gives literature summary in brief.

Table 1 Literature summary

S. no.	*Work done*	*Technologies used*	*Result*	*Limitations*	*Research gap*
1	The paper advocates for the utilisation of mobile phone voting for commercial purposes. It addresses the issue of double voting by maintaining databases in encrypted formats (Selvarani et al., 2017)	NIC, Sim Card, Mail ID	More efficient, reliable, and useful remote voting process	User profiles are dependent on Sim Card/Mail Id which allows to create fake voter profiles	Lack of authentication of voter profiles
2	The paper outlines our endeavours to bridge the existing literature gap by conducting a thorough examination of parameters crucial for attaining scalable solutions through blockchain technology. However, a literature gap exists regarding performance constraints across broader application domains (Khan et al., 2020)	Ethereum chain	Decrease in network delay can double the transaction speed	Fully dependent on network delay, available miners and network traffic	Dose not solves the scalability issues of blockchain network
3	The paper introduces a mobile voting framework that employs blockchain technology and multifactor authentication to create a voting system that is easily accessible while also securely safeguarding cast votes and verifying voters' eligibility to cast their votes (Abayomi-Zannu et al., 2019)	Blockchain network, multifactor authentication	Cost effective as it requires less resources, prevents illegible votes	Indispensability of mobile devices	Challenging for individuals residing in remote areas

Table 1 Literature summary (continued)

S. no.	*Work done*	*Technologies used*	*Result*	*Limitations*	*Research gap*
4	The paper reviews blockchain-based voting systems in electronic voting research. It maps current e-voting systems, explains blockchain fundamentals, and explores its potential for improving e-voting. It identifies system gaps, discusses current blockchain solutions, and suggests future research paths for blockchain-based e-voting systems (Taş et al., 2020)	–	–	Major security risks, malware attacks	Vulnerable to identity theft and cyber-attacks
5	This paper introduces a decentralised voting platform using Ethereum Blockchain, emphasising its innovation in limiting multiple votes per mobile (Khoury et al., 2018)	MSISDN, Oraclise	Reduces avg. voting time to 40 sec	Dependent on Oraclise, an external service	Cost Considerations Scalability
6	This research has developed a comprehensive voting system that includes configuring voting terminals with ballot definitions before elections, utilising smart cards for voter authentication and voting, and employing biometric identification for security (Sridharan, 2013)	Smart cards, biometrics verification	Streamlines voting processes, enhances security, Prevent duplicate voting	Lack of Specific Results related to cost	Time efficiency and hardware cost considerations
7	The study presents a blockchain-based e-voting scheme, combining DLT for vote record security, ECC for user authentication, and a withdrawal model. Our scheme is public, auditable, decentralised, and ensures data security, addressing key e-voting needs (Yi, 2019)	DLT, ECC, SHA, consensus algorithms	Anonymous voting, non-repudiation of votes	High implementation cost	Quantum-resistant cryptography

Table 1 Literature summary (continued)

S. no.	*Work done*	*Technologies used*	*Result*	*Limitations*	*Research gap*
8	This research introduces a secure e-government architecture using consortium blockchain, demonstrating its viability through performance evaluation. Minimising validators enhances its suitability for efficient information sharing in e-government systems (Elisa et al., 2019)	Consortium blockchain P2P network	Scalable, High data integrity, minimal risk against 51% attack	–	Real-time cyber attacks
9	The study concludes that blockchain, particularly Hyperledger, fulfils key e-voting requirements. While effective, areas like concurrency management and complementary frameworks remain to be further developed (Díaz-Santiso and Fraga-Lamas, 2021)	Hyperledger fabric	Fabric nodes can handle 2500 concurrent transactions	Highly complex integration challenges	Robustness on large scale
10	The paper introduces the Crypto-voting system, based on permissioned blockchain technology and Smart Contracts. It enhances voting efficiency, anonymises consensus nodes, and addresses issues like voting abroad and secure identification integration (Fusco et al., 2018)	Sidechain, consensus nodes	–	The challenge privacy of voter	A research gap exists in implementation of cybersecurity tool on sidechain
11	The paper presents a classification of these algorithms, conducts a comprehensive comparison of common consensus algorithms, and offers a detailed discussion with an analysis of the main factors affecting these algorithms (Alsunaidi and Alhaidari, 2019)	Consensus algorithms	Votes verification speed is < 10s	Limitations may involve low throughput	A research gap in extendible and scalability

Table 1 Literature summary (continued)

S. no.	*Work done*	*Technologies used*	*Result*	*Limitations*	*Research gap*
12	The paper introduces an active voting protocol on Quantum Blockchain, guaranteeing anonymity, binding, non-reusability, verifiability, eligibility, fairness, and self-tallying. It employs quantum secure communication and bit commitment, achievable with current technology (Sun et al., 2019)	Quantum Blockchain	–	–	There is a research gap concerning real-time implementation
13	The study collects and analyses data from the Solana blockchain, revealing an average transaction throughput and lower user fees compared to similar blockchains. This showcases Solana's potential for scalable, decentralised, and secure operations (Pierro and Tonelli, 2022)	Solana blockchain	High transaction speed, Low gas cost	Partially decentralised Security risks	One potential research gap could be an in-depth investigation into the long-term sustainability
14	The paper emphasises the importance of blockchain and IoT networks and presents a survey on IoT network security. It addresses security issues by introducing authentication for IoT systems and enhancing blockchain security, contributing to improved security in blockchain-based IoT setups (Kumari and Farheen, 2020)	IOT network	–	Limitations is high deployment cost	A research gap exists in authentication using biometric and preventing IoT security breaches
15	The paper concludes that e-Voting implementation boosts voter turnout and offers cost advantages over paper voting, highlighting its potential for enhancing accessibility and efficiency in electoral procedures (Rexha et al., 2012)	Digital Signatures	Increase in voter participation and a reduction in voting expenses	–	A research gap exists in malware security issues

3 Proposed methodology

In the proposed method, the system utilises blockchain technology for its backend, specifically smart contracts written in Solidity for the Ethereum network. Solidity is a programming language specifically designed for building secure and tamper-proof smart contracts on the Ethereum blockchain. Running these smart contracts and using their functions requires paying a fee called "gas". Think of gas like fuel for the blockchain – it's what powers the computations needed to execute the terms of the smart contract. The amount of gas needed depends on the complexity of the contract and the functions being called. This fee structure helps maintain the security and efficiency of the blockchain network.

E-voting systems require a user interface that prioritises both security and ease of use. This is where ReactJS and CSS shine. ReactJS allows for building the voting interface as secure, reusable components. Imagine separate components for candidate information, casting votes, and confirming selections. This modular approach makes it easier to implement security features within each component. Additionally, ReactJS utilises a Virtual DOM, ensuring efficient updates when users interact with the system. This minimises the risk of exposing sensitive information during the voting process.

CSS plays a vital role in creating a transparent and accessible voting experience. By using distinct colours and highlighting selections, voters can clearly understand the information presented and review their choices before submitting their vote. Furthermore, following accessibility guidelines in CSS allows developers to create interfaces that work seamlessly for users with disabilities. This includes features like proper colour contrast, keyboard navigation, and screen reader compatibility. In conclusion, ReactJS and CSS work together to build a user interface for the e-voting system that is both secure and user-friendly, fostering trust and confidence in the entire process.

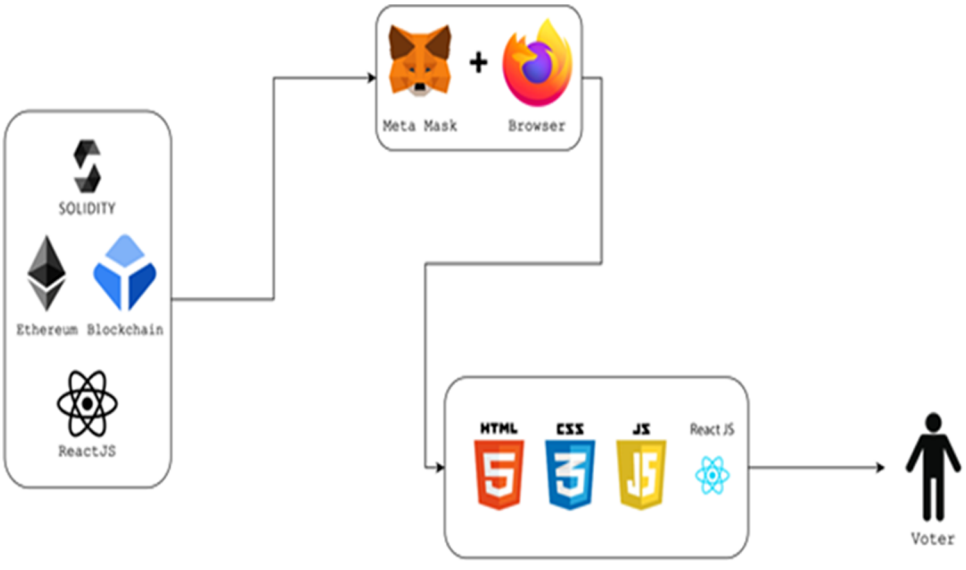
E-voting demands a user interface that prioritises both security and user-friendliness. ReactJS and CSS play crucial roles in achieving this. ReactJS allows building the voting interface with secure, reusable components, facilitating the implementation of security features within each section. Additionally, it utilises a Virtual DOM for efficient updates, minimising the risk of exposing sensitive information during voting. CSS ensures transparency and accessibility by using distinct colours, highlighting selections, and following accessibility guidelines for users with disabilities.

Figure 1 outlines the proposed system for an electronic voting system enabled by blockchain technology and smart contracts.

However, the user interface and the blockchain infrastructure are currently separate components. To bridge this gap and establish a secure connection, the system utilises Metamask, a Chrome extension that facilitates communication between the user's browser and the blockchain. Metamask relies on a hashed string provided by Infura to securely connect to the network. Once connected, users can log in to Metamask with their blockchain credentials, ensuring only authorised users can cast votes. With a successful login, the user-friendly interface, built with ReactJS and CSS, guides voters through the process of casting their ballots for their preferred candidate. This combined approach creates a secure and user-friendly e-voting experience that fosters trust in the entire process. Upon connecting with MetaMask, voters encounter an advanced authentication phase involving a QR code scanner. This process adds an extra layer of security by linking the unique QR code presented digitally to voters with the identical code found on their physical voter IDs. The scanner seamlessly integrates into the e-voting interface,

guiding users to align their device cameras with the QR code for verification. Successful scans grant access to the voting screen, ensuring only authorised users proceed, while failed attempts prompt an 'invalid voter' notification. QR code authentication enhances security, leveraging widely available technology without requiring specialised hardware. It instils trust by digitally verifying voters' physical identities, minimising the risk of unauthorised access or fraud. This user-friendly approach aligns with modern digital practices, prioritising security and accessibility in the e-voting experience.

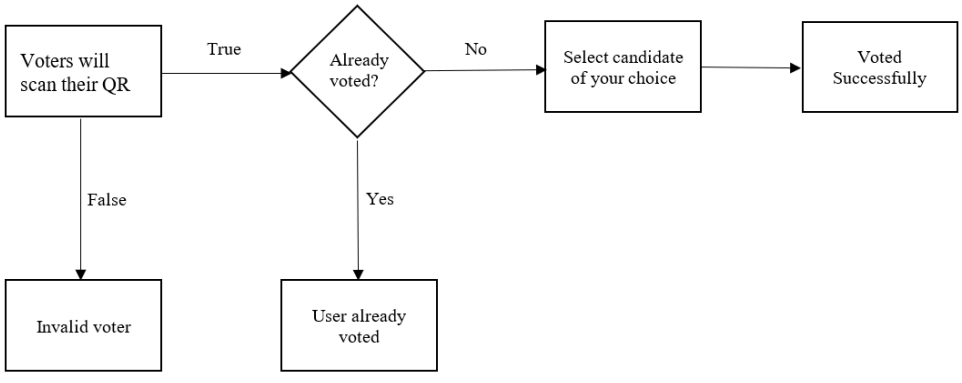
Figure 1 Decentralised application (DAPP) architecture (see online version for colours)



To cast a vote, the procedure begins with voter verification using a QR code scan. When voters access the e-voting platform, they are prompted to authenticate themselves. This authentication process involves scanning the QR code on their physical voter IDs using the system's QR code scanner feature. If the scan is successful and matches the voter's identity, the system redirects them to the voting screen. However, if the QR code scan is invalid or does not match the voter's identity, the system displays an 'Invalid Voter' message and denies access to the voting screen, ensuring that only authorised individuals participate in the voting process. Once on the voting screen, voters can proceed to cast their votes by selecting their choices and submitting the ballot. The system then conducts a validation check to determine if the voter has already cast their vote in the ongoing election. This validation process involves querying the blockchain ledger to verify the voter's voting status. If the voter has not yet voted in the current election, their vote is recorded as valid on the blockchain. However, if the system detects that the voter has already cast their vote, it displays a message indicating that their vote has already been recorded and prevents any further attempts to submit duplicate votes.

This comprehensive voting procedure ensures the integrity of the electoral process by verifying voter identities, preventing duplicate voting, and maintaining accurate records on the blockchain ledger. Figure 2 illustrates the visual representation of the voting procedure.

Figure 2 The process for casting a vote



Algorithm 1 Creating data structures for candidate registration

Step 1: The smart contract receives the Candidate Name, Age and Wallet Address as input and uses this information to generate a candidate structure, storing the provided name, age and wallet address.

```
struct Candidate
{
string name;                    // Candidate Name
uint age;                       // Candidate Age
address candidateAddress;       // Wallet Address
}
```

Step 2: A constructor is called with the candidate's name, which calls a function registerCandidates. This function requires three parameters: _name (a string), _age (an unsigned integer), and _candidateAddress (an address).

```
constructor()
{
owner = msg.sender;
eventName = _eventName;
totalVote = 0;
votingStarted=false;
}

function registerCandidates(string memory _name, uint _age, address _candidateAddress) public
{
// Creation of an object with the provided details
Candidate memory candidate = Candidate({
name: _name,
age: _age,
candidateAddress: _candidateAddress
});

// After that the object is pushed to the Candidates array/list
if(candidateList.length == 0){
candidateList.push();
}
[_candidateAddress] = candidateList.length;
.push(candidate);
}
```

Algorithm 1 Illustrates the smart contract, manages candidate registration for an event or election. It defines a Candidate structure with fields for name, age, and wallet address. Upon deployment, the constructor initialises contract details like the owner, event name, and voting status. The registerCandidates function enables adding new candidates by creating Candidate objects and storing them in the candidateList array. If no candidates exist, a new entry is made; otherwise, the new candidate is appended. This process ensures a structured and transparent approach to managing candidate information within the contract, enhancing reliability and accountability for the event or election.

4 Results and discussions

The practical application of an electronic voting (e-voting) system is demonstrated through the utilisation of a smart contract within blockchain technology. An assessment of the system's efficacy is conducted based on factors such as the gas cost for voting by users, the system's speed in successful or rejecting votes, and its overall accuracy. This evaluation encompasses various aspects of the e-voting process, including cost efficiency, transaction speed, and the system's ability to ensure the integrity and correctness of votes cast.

4.1 Smart contract

The Candidate contract is pivotal in an e-voting system, comprising attributes like name, age, registration status, wallet address, and vote count. These attributes serve distinct purposes within the system: name and age verify candidate eligibility, registration status tracks their participation, wallet address serves as their unique Candidate ID and linked with the votes they get, and vote count tallies received votes. This structured data management ensures accurate candidate identification, eligibility verification, and real-time vote tracking.

Figure 3 illustrates the structure of candidate information within the smart contract.

Figure 3 Candidate smart contract (see online version for colours)

```
1   // SPDX-License-Identifier: GPL-3.0
2
3   pragma solidity ^0.8.0;
4
5   contract Voting {
6
7       struct Candidate{
8           string name;
9           uint age;
10          bool registered;
11          address candidateAddress;
12          uint votes;
13      }
14
```

Algorithm 2 Vote cast function

```
if(voter is not admin && Voting is started ){
   if( isValidVoter ){
      if(user already voted){
         alert(User already voted !!)
      }
      else{
         Transaction successfull alert(Voted successfull)
      }
   }
   else{
      Transaction Rejected alert( Invalid voter !!)
   }
}
else{
   Transaction Rejected alert(admin cannot cast vote or voting is not started.)
}
```

Before casting a vote, each voter must be on the whitelist and for that purpose we have defined whiteListAddress function. The whiteListAddress function is a crucial component of the smart contract, enabling the whitelisting of addresses for voting purposes. It imposes necessary checks to uphold the integrity of the process. Firstly, it ensures that the address being whitelisted is not the owner's address, preventing self-voting. Additionally, only the contract owner can execute this function, safeguarding against unauthorised access. Furthermore, the function verifies that the address is not already registered, preventing duplicate entries. Upon successful validation, the function registers the address as a voter and emits a success event. You can see the visual representation in Figure 4.

Figure 4 Voter registration function (see online version for colours)

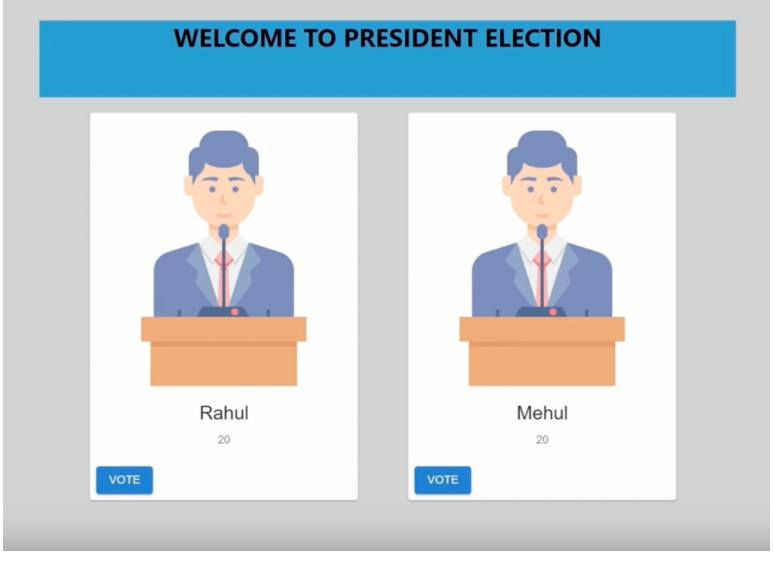
```
58
59      function whiteListAddress(address _voterAddress) public {   57743 gas
60
61          require(_voterAddress != owner, "Owner can not vote!!");
62
63          require(msg.sender == owner, "Only owner can whitelist the addresses!!");
64
65          require(voterList[_voterAddress].registered == false, "Voter already registered!!");
66
67          Voter memory voter = Voter({
68              registered: true,
69              voted: false
70          });
71
72          voterList[_voterAddress] = voter;
73
74          emit success("Voter registered!!");
75      }
76
```

Figure 5 displays the QR verification process for validating a voter in an e-voting system. A person is seen holding a smartphone with the e-voting app open, ready to scan the QR code provided at the voting station. The QR code is generated uniquely for each voter and contains encrypted data to authenticate their identity and ensure a secure voting process.

Figure 5 QR validation of voter (see online version for colours)

Figure 6 depicts the user interface for the voting process. Once a voter completes their QR validation, they will be directed to this interface. It is crucial for voters to confirm that they are connected to their corresponding Metamask wallet before proceeding to cast their vote.

Figure 6 Voting interface (where user can caste vote) (see online version for colours)



4.2 Gas cost estimation

Table 2 shows an overview of the gas costs associated with various operations conducted on the blockchain. These operations include Contract Deployment, Candidate Registration, Voter Registration, Start/Stop Voting, and Cast Vote. Gas costs are a measure of ether required for each operation, reflecting the resources consumed by the blockchain network.

Table 2 Gas cost for all operation performed on blockchain

Operation performed	*Gas used* (Gwei)	*Actual cost* (ETH)
Smart contract deployment	614,032	0.01228064
Registration of voter	185,390	0.00018539
Registration of candidate	136,934	0.0027387
Start/stop voting	220,190	0.00022019
Casting vote	7,500,070	0.00750007

The gas cost is directly proportional to the number of gas units consumed, (GasUsed × PricePerUnit). So, the cost to process a transaction on the network is measured in units of Ether (ETH).

where,

$$1ETH = 10^{18}\,Gwei \; or \; 10^{18}\,Gwei = 1ETH$$

Total GC for contract deployment $= 614032$ Gwei

Avg. GC for registration of 2 candidate $= \dfrac{113998+159870}{2} = 273868\,Gwei$

Avg. GC for registration of 5 voters $= \dfrac{926,950}{5} = 185,390\,Gwei$

Avg. GC for start and stop of voting $= \dfrac{220,190}{2} = 110,095\,Gwei$

Avg. GC for casting 5 vote $= \dfrac{37,500,350}{5} = 7,500,070\,Gwei$

For above, GC = Gas Cost, Avg. = average.

4.3 Time efficiency

The e-voting system underwent rigorous testing for deployment on the Ethereum mainnet via Infura. Smart contracts were deployed successfully, achieving a high-test coverage of 95%. Integration with Infura allowed seamless interaction with the blockchain, while security audits and gas optimisation ensured efficient and secure transactions.

Comprehensive testing covered critical functions like voter registration and result tallying, all functioning without errors. User acceptance testing (UAT) with fifty participants yielded positive feedback on usability and performance. Documentation and

monitoring tools were set up for future reference and ongoing maintenance, culminating in a successful deployment on the Ethereum mainnet through Infura endpoint. Table 3 shows the time taken by miners to validate transactions. Table 4 shows the time taken for casting vote.

Table 3 Time taken by miners to validate transactions

Operations performed	*Average time taken for confirmation of transaction made* (in seconds)
Smart contract deployment	6
Registration of candidate	4
Registration of voters	3
Start/stop of voting	5
Get results	3

Table 4 Time taken for casting vote

voter's wallet address	*Time taken for acceptance/rejection of vote* (in seconds)
0xb1ee9815d5dd4588d518a47adf1e6ed994300286	5
0x7309D8669E5Ff646b8066933f67A3E4F68ac812b	4
0x10904fDd7D9D7194e16fD022057fbfD7c2632A0B	9
0x6eF4a862e20aA57B1d6c0504A24149D0B41bBcD6	3
0x981cc9D11e651c5434f0f8f73757bAA8365990E8	6

5 Discussion and implications

The proposed approach in the paper demonstrates significant superiority over other methods, particularly in terms of performance and security. By leveraging blockchain technology, the system ensures the immutability, transparency, and decentralisation of voting records, which greatly enhances the overall security of the electoral process. The use of cryptographic techniques and distributed ledgers makes it nearly impossible for unauthorised entities to alter or manipulate the votes, thereby safeguarding the integrity of the election. In terms of performance, the system's ability to handle real-time vote counting and verification leads to faster and more accurate results, which is a marked improvement over traditional voting methods (Everett et al., 2008). Additionally, the integration of smart contracts automates various processes, reducing the potential for human error and further improving efficiency. Overall, the proposed blockchain-based voting system addresses critical security vulnerabilities and performance bottlenecks present in existing systems, making it a robust and reliable solution for modern electoral processes.

The proposed Blockchain technology based electoral solution, while offers enhanced security and transparency for electronic voting systems, can have a significant environmental impact due to its energy consumption. Traditional blockchain networks, especially those utilising PoW consensus mechanisms like Bitcoin, require substantial computational power, leading to high electricity usage and consequently large carbon

footprints (https://digiconomist.net/bitcoin-energy-consumption). For instance, the Bitcoin network consumes approximately 120 terawatt-hours (TWh) annually, which is comparable to the energy consumption of a small country like Argentina. This results in roughly 57 million tonnes of CO_2 emissions per year. Applying this to a blockchain-based voting system, even on a smaller scale, could result in considerable energy usage. If a voting process required similar computational intensity, conducting nationwide elections could lead to substantial CO_2 emissions, raising environmental concerns. As the electorate size increases, the number of transactions (votes) processed by the blockchain also increases, potentially leading to higher energy consumption. In a country like India, with over 900 million eligible voters (https://digiconomist.net/bitcoin-energy-consumption), implementing a PoW-based blockchain voting system could be environmentally and economically unsustainable due to the massive energy requirements. To mitigate these issues, alternative consensus mechanisms such as PoS or Proof of Authority (PoA) can be employed (Fahim et al., 2023). These methods are significantly more energy-efficient, reducing the environmental footprint drastically. Additionally, utilising renewable energy sources to power the network infrastructure can further decrease CO_2 emissions. Governments can conduct cost-benefit analyses to assess the feasibility and invest in energy-efficient infrastructure to support such systems at scale.

Blockchain-powered e-voting is a promising tool for enhancing transparency and security in governance, but its integration into existing legal frameworks requires careful consideration. Existing legal structures may not fully address the new technological dimensions introduced by blockchain, such as its immutable ledger, which may conflict with laws ensuring voter anonymity. Data protection and privacy concerns arise as blockchain handles sensitive personal data, necessitating adaptation to legal frameworks like the General Data Protection Regulation (GDPR) (Finck, 2019). Blockchain operates across borders, potentially creating conflicts with national and regional legal requirements. Trust and legitimacy are also crucial, necessitating new regulations for blockchain security, auditing processes, and dispute resolution protocols. While existing e-voting regulations could serve as a foundation for blockchain integration, they require significant updates to ensure technology-specific provisions, interoperability with traditional systems, pilot programs, and gradual implementation. To sum up, blockchain-powered electronic voting would probably need major changes to the law before it could be fully implemented. These changes would have to deal with specific technological, legal, and trust issues in order for it to work well with open and safe government systems.

Implementing blockchain-powered e-voting for transparent governance necessitates a robust digital infrastructure and specific prerequisites. This includes deciding between a centralised national blockchain infrastructure or a decentralised public blockchain, both requiring significant investment in technology, security, and governance frameworks. A national blockchain would ensure control and integration with existing systems, but demands secure data centers and interoperable nodes. High network bandwidth and reliable internet connectivity are essential to managing the large data transmissions involved in blockchain transactions (Wang and Zhao, 2023). Ensuring scalability and nationwide access, especially in remote areas, is crucial to prevent disenfranchisement. Digital literacy among the electorate is another key requirement. Voters need to understand and use the technology securely, necessitating comprehensive education programs. Beyond literacy, public acceptance of blockchain is vital, requiring trust in the system's transparency and security. User-friendly interfaces are also critical to accommodate varying literacy levels.

Overall, successful implementation of blockchain e-voting requires substantial investments in national infrastructure, network capabilities, and public education to ensure both the system's functionality and the electorate's confidence in its use.

6 Conclusion

Our project presents an innovative electronic voting system using blockchain technology, utilising smart contracts to ensure secure and affordable elections, all while protecting the confidentiality of voters. Additionally, we have introduced an important security measure: the use of QR verification for voters, enhancing the strength of the system. Proposed system effectively handles large transaction volumes by utilising optimised smart contract functionality on an Ethereum private blockchain. Recognising the scalability requirements in heavily populated countries, we support the implementation of additional measures. Blockchain technology's natural transparency greatly improves the ability to audit and understand elections, which is essential for efficient voting processes. We aim to increase the use of blockchain technology in order to improve the transparency and auditability of e-voting, transforming the electoral process for greater security, accessibility, and transparency.

7 Future scope

In envisioning the future of blockchain-based e-voting systems, particularly in a country as vast and diverse as India, several key strategies emerge to propel its widespread adoption. One promising avenue involves allocating blockchain accounts to eligible voters, seamlessly linked to their Voter cards. This integration not only ensures the verifiability and security of each vote but also lays the foundation for a more inclusive and accessible electoral process. Additionally, the Election Commission head plays a crucial role in addressing challenges related to voter accessibility and digital inclusion. Recognising the importance of universal access to the voting platform, the Commission may work to bridge the digital divide by implementing initiatives to provide smartphones or other internet-enabled devices to citizens who lack access.

Furthermore, the decentralised architecture of blockchain eliminates the need for intermediaries, streamlining administrative procedures and cutting down on overhead expenses associated with traditional voting methods. Additionally, the efficiency gains enabled by blockchain technology promise faster and more accurate tabulation and reporting of election results. This not only expedites the electoral process but also enhances its reliability, ensuring fair and credible outcomes.

References

Abayomi-Zannu, T.P., Odun-Ayo, I.A. and Barka, T.F. (2019) 'A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication', *J. Phys Conf Ser.*, Vol. 1378, No. 3, December, p.32104, doi: 10.1088/1742-6596/1378/3/032104.

Alsunaidi, S.J. and Alhaidari, F.A. (2019) 'A survey of consensus algorithms for blockchain technology', *2019 International Conference on Computer and Information Sciences (ICCIS)*, IEEE, Sakaka, Saudi Arabia, pp.1–6.

Bandhu, K.C., Litoriya, R., Bagwala, M., Barwaniwala, A. and Garg, M. (2023a) 'Blockchain and smart contract enabled smart and secure electronic voting system', *International Journal of Electronic Governance*, Vol. 15, No. 1, p.56, doi: 10.1504/IJEG.2023.130173.

Bandhu, K.C., Litoriya, R., Lowanshi, P., Jindal, M., Chouhan, L. and Jain, S. (2023b) 'Making drug supply chain secure traceable and efficient: a blockchain and smart contract based implementation', *Multimed Tools Appl*, Vol. 82, No. 15, June, pp.23541–23568, doi: 10.1007/s11042-022-14238-4.

Benítez-Martínez, F.L., Hurtado-Torres, M.V. and Romero-Frías, E. (2021) 'A neural blockchain for a tokenizable e-participation model', *Neurocomputing*, Vol. 423, pp.703–712, https://doi.org/10.1016/j.neucom.2020.03.116

Chondros, N., Zhang, B., Zacharias, T., Diamantopoulos, P., Maneas, S., Patsonakis, C., Delis, A., Kiayias, A., Roussopoulos, M. (2019) 'Distributed, end-to-end verifiable, and privacy-preserving internet voting systems', *Comput Secur.*, Vol. 83, pp.268–299, doi: https://doi.org/10.1016/j.cose.2019.03.001

Cohen, J.D. and Fischer, M.J. (1985) *A Robust and Verifiable Cryptographically Secure Election Scheme*, Department of Computer Science, Yale University.

Davor, D.D. and Sajter (2019) 'Blockchain applications in supply chain', in Kawa Arkadiusz, A. and Maryniak, A. (Eds.): *SMART Supply Network*, Springer International Publishing, Cham, pp.21–46, doi: 10.1007/978-3-319-91668-2_2.

Díaz-Santiso, J. and Fraga-Lamas, P. (2021) 'E-voting system using hyperledger fabric blockchain and smart contracts', *Engineering Proceedings*, Vol. 7, No. 1,. pp.1–3, doi: 10.3390/engproc2021007011.

Elisa, N., Yang, L., Li, H., Chao, N.F. and Naik, N. (2019) 'Consortium blockchain for security and privacy-preserving in E-government systems', *ICEB 2019 Proceedings*, Newcastle Upon Tyne, UK, p.17, https://aisel.aisnet.org/iceb2019/17

Everett, S.P., Greene, K.K., Byrne, M., Wallach, D., Derr, K., Sandler, D. and Torous, T. (2008) 'Electronic voting machines vs. traditional methods', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, April, ACM, New York, NY, USA, pp.883–892, doi: 10.1145/1357054.1357195.

Fahim, S., Katibur Rahman, S. and Mahmood, S. (2023) 'Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV', *International Journal of Mathematical Sciences and Computing*, Vol. 9, No. 3, August, pp.46–57, doi: 10.5815/ijmsc.2023.03.04.

Finck, M. (2019) *Blockchain and the General Data Protection Regulation*, [Online], Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Fusco, F., Lunesu, M.I., Pani, F.E. and Pinna, A. (2018) 'Crypto-voting, a blockchain based e-voting system', *KMIS*, Seville, Spain, pp.221–225.

Hanifatunnisa, R. and Rahardjo, B. (2017) 'Blockchain based e-voting recording system design', *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, Lombok, Indonesia, pp.1–6, doi: 10.1109/Tssa.2017.8272896.

Jafar, U., Aziz, M.J.A. and Shukur, Z. (2021) 'Blockchain for electronic voting system–review and open research challenges', *Sensors*, Vol. 21, No. 17, pp.1–22, doi: 10.3390/s21175874.

Khan, K.M., Arshad, J. and Khan, M.M. (2020) 'Investigating performance constraints for blockchain based secure e-voting system', *Future Generation Computer Systems*, Vol. 105, pp.13–26, doi: https://doi.org/10.1016/j.future.2019.11.005

Khoury, D., Kfoury, E.F., Kassem, A. and Harb, H. (2018) 'Decentralized voting platform based on ethereum blockchain', *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, Beirut, Lebanon, pp.1–6, doi: 10.1109/Imcet.2018.8603050.

Kumari, S. and Farheen, S. (2020) 'Blockchain based data security for financial transaction system', *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, pp.829–833, doi: 10.1109/ICICCS48265.2020.9121108.

Nakamoto, S. (2009) *Bitcoin: A Peer-to-Peer Electronic Cash System Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin.org. Disponible en https://bitcoin.org/en/bitcoin-paper

Pierro, G.A. and Tonelli, R. (2022) 'Can solana be the solution to the blockchain scalability problem?', *2022 IEEE International Conference on Software Analysis*, *Evolution and Reengineering* (*SANER*), IEEE, Honolulu, HI, USA, pp.1219–1226.

Poniszewska-Maraundefinedda, A., Pawlak, M. and Guziur, J. (2020) 'Auditable blockchain voting system – the blockchain technology toward the electronic voting process', *Int. J. Web Grid Serv.*, Vol. 16, No. 1, January, pp.1–21, doi: 10.1504/ijwgs.2020.106102.

Rexha, B., Neziri, V. and Dervishi, R. (2012) 'Improving authentication and transparency of e-voting system–Kosovo case', *International Journal of Computers and Communications*, Vol. 6, No. 1, pp.84–91.

Selvarani, X.I., Shruthi, M., Geethanjali, R., Syamala, R. and Pavithra, S. (2017) 'Secure voting system through SMS and using smart phone application', *2017 International Conference on Algorithms*, *Methodology*, *Models and Applications in Emerging Technologies* (*ICAMMAET*), Chennai, India, pp.1–3, doi: 10.1109/ICAMMAET.2017.8186724.

Sridharan, S. (2013) 'Implementation of authenticated and secure online voting system', *2013 Fourth International Conference on Computing*, *Communications and Networking Technologies* (*ICCCNT*), Tiruchengode, India, pp.1–7, doi: 10.1109/Icccnt.2013.6726801.

Sun, X., Wang, Q., Kulicki, P. and Sopek, M. (2019) 'A simple voting protocol on quantum blockchain', *International Journal of Theoretical Physics*, Vol. 58, pp.275–281.

Taş, R. and Tanrıöver, Ö.Ö. (2020) 'A systematic review of challenges and opportunities of blockchain for E-voting', *Symmetry* (*Basel*), Vol. 12, No. 8, pp.1–24, doi: 10.3390/sym12081328.

Vaigandla, K.K., Karne, R., Siluveru, M. and Kesoju, M. (2023) 'Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications', *Mesopotamian Journal of CyberSecurity*, Vol. 2023, March, pp.73–84, doi: 10.58496/MJCS/2023/012.

Wang, C. and Zhao, J. (2023) 'Network approaches in blockchain-based systems: applications, challenges, and future directions', *Comput Commun*, Vol. 212, December, pp.141–150, doi: 10.1016/j.comcom.2023.09.018.

Yi, H. (2019) 'Securing e-voting based on blockchain in P2P network', *EURASIP J. Wirel Commun Netw.*, Vol. 2019, No. 1, p.137, doi: 10.1186/s13638-019-1473-6.

Zachariadis, M., Hileman, G. and Scott, S.V. (2019) 'Governance and control in distributed ledgers: understanding the challenges facing blockchain technology in financial services', *Information and Organization*, Vol. 29, No. 2, pp.105–117, https://doi.org/10.1016/j.infoandorg.2019.03.001

Zhang, W., Yuan, Y., Hu, Y., Huang, S., Cao, S., Chopra, A. and Huang, S. (2018) 'A privacy-preserving voting protocol on blockchain', *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, pp.401–408, doi: 10.1109/CLOUD.2018.00057.

Websites

"Bitcoin Energy Consumption Index", Digiconomist, [Online] Available: https://digiconomist.net/bitcoin-energy-consumption (Accessed 20 February, 2024).

"Largest electorate for General Elections – over 96.88 crore electors registered across the country", [Online], Available: https://pib.gov.in/PressReleasePage.aspx?PRID = 2005189