Remote Voting System for Migrant People

Dikshay Kumar[1]; Arziya Shakeel[2]

[1]Computer Engineering Department Galgotias University
[2]Computer Engineering Department Galgotias University

Publication Date: 2025/06/04

Abstract: Electronic voting has emerged as a viable alternative to traditional paper-based voting, offering advantages such as increased efficiency, transparency, and security. However, existing e-voting systems face significant challenges, including vote duplication, lack of real-time verification, and security vulnerabilities. To address these issues, this research proposes a blockchain-based e-voting framework with distributed election booths, where each booth functions as an independent yet interconnected node within the blockchain network. In the proposed approach, election booths will be deployed across different constituencies, allowing voters to cast their votes at designated locations. Each vote is immediately recorded in a local ledger and then synchronized with the main blockchain network in real time, ensuring that no voter can cast multiple votes from different locations. Smart contracts are used to validate voter identities, verify vote authenticity, and prevent unauthorized modifications to the voting data. By leveraging blockchain's decentralization, immutability, and cryptographic security mechanisms, the system ensures that all votes remain transparent, tamper- proof, and verifiable by election authorities and voters alike. This method enhances the credibility of electronic voting by eliminating vote duplication, enabling real-time monitoring, and ensuring the integrity of the election process. The proposed system is designed to be scalable, adaptable to different electoral scenarios, and capable of providing secure, verifiable election results. Future research will focus on optimizing transaction speeds, addressing network congestion, and enhancing the userfriendliness of the voting interface to ensure widespread adoption and accessibility.

Keywords: *Blockchain, E-Voting, Votes, Ballot.*

How to Cite: Dikshay Kumar; Arziya Shakeel (2025). Remote Voting System for Migrant People. *International Journal of Innovative Science and Research Technology,* 10(5), 3254-3259. https://doi.org/10.38124/ijisrt/25may945

I. INTRODUCTION

The rapid advancement of digital technologies has transformed various sectors, including governance and electoral processes. Electronic voting (e-voting) systems have gained significant attention as a means to enhance electoral efficiency, transparency, and accessibility. However, conventional e-voting models face critical challenges such as vote duplication, lack of real-time verification, security vulnerabilities, and trust issues among voters. These challenges raise concerns about the integrity of elections, particularly in large-scale democratic processes where fraudulent activities such as multiple voting, vote tampering, and system manipulation could compromise results.

Blockchain technology has surfaced as a viable alternative for the problems with digital voting's security and transparency. With its decentralized and immutable ledger system, blockchain offers an architecture that enhances vote integrity by ensuring tamper-proof record-keeping and real-time validation (Bentov, Mizrahi, & Rosenfeld, 2016). There are various models of e-voting that has been proposed based on the blockchain technology, smart contracts, and cryptographic techniques to decentralise the voting process as well as reduce the risk of fraud as noted by Zhao, Wang, and Chen (2020). Although these approaches show better security, they suffer from several issues such as scalability, delay in vote counting and processing, and possibility of bottlenecks in that all the voting transactions are recorded in a single blockchain (Yang & Zhang, 2018).

A critical vulnerability in blockchain e-voting models is the potential for vote duplication. In conventional digital voting systems, voters might attempt to cast multiple votes using different credentials or exploit network delays to manipulate vote registrations. Traditional blockchain-based systems address this by requiring extensive computational resources to verify transactions across the network, often resulting in increased latency and inefficiencies (Li, Zhang, & Zhao, 2019). Moreover, in large-scale elections where votes are cast from multiple locations, ensuring real-time synchronization and preventing inconsistencies across nodes becomes a substantial challenge (Khan, Ali, & Singh, 2021).

To mitigate these issues, this study proposes a decentralized e-voting system utilizing distributed election booths with real-time blockchain synchronization. Unlike traditional models that rely on a centralized blockchain ledger, this approach establishes independent election booths, each functioning as a node within a permissioned blockchain network. Votes cast at any booth are verified locally and immediately reflected in the main blockchain, preventing duplicate voting while ensuring efficient processing. Smart contracts facilitate instant validation, eliminating manual intervention and reducing delays. By distributing vote verification and storage across multiple locations, the proposed model enhances scalability and prevents single-point failures, improving both the security and efficiency of the voting process (Larimer, 2014).

By combining real-time voting procedures with decentralised ledger technology, this research has the potential to improve the legitimacy and dependability of digital elections. The proposed system is particularly advantageous for large-scale democratic elections, as well as for remote and underserved regions where connectivity limitations could otherwise hinder electoral participation. The adoption of blockchain-enabled election booths offers a robust solution to common electoral frauds, ensuring each vote is uniquely recorded while maintaining voter anonymity and system integrity (Gritzalis, 2002).

This article describes the blockchain foundation, vote synchronisation mechanism, and security requirements for an effective deployment of the proposed system. Furthermore, it assesses the impact of this approach in terms of electoral efficiency, cost-effectiveness, and public trust in digital voting systems. This project intends to improve secure and transparent electronic voting by solving model constraints and using distributed ledger technology.

- *Actual Architecture of E- Voting*

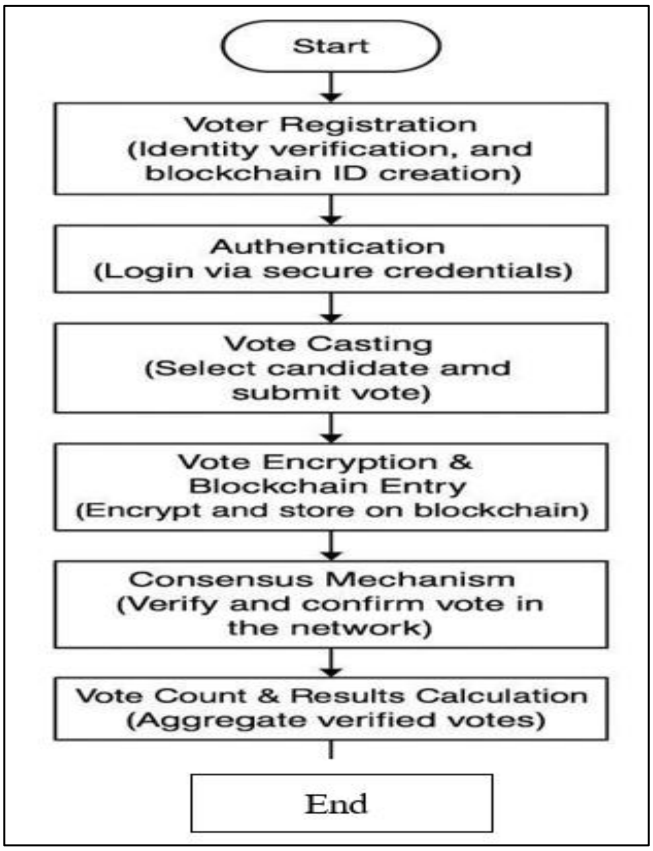
Start
Voter Registration (Identity verification, and blockchain ID creation)
Authentication (Login via secure credentials)
Vote Casting (Select candidate amd submit vote)
Vote Encryption & Blockchain Entry (Encrypt and store on blockchain)
Consensus Mechanism (Verify and confirm vote in the network)
Vote Count & Results Calculation (Aggregate verified votes)
End

Fig 1 Flowchart of Architecture being Followed

II. LITERATURE SURVEY

The use of blockchain in electronic voting has been analysed extensively over the years to determine its advantages and disadvantages. This section reviews seminal work in the field and responds to other issues of security, openness, voter anonymity, modularity, legal considerations, and feasibility.

- *Blockchain and Intelligent Contracts in Electronic Voting*

In their study, li et al. (2019) discussed the application of intelligent contracts in the aspect of electronic adjustment. She stressed that intelligent contracts make the process of election automatic and guarantee that voices are recorded continuously. It is suggested to apply the system of interaction of electors with intelligent contracts based on blockchain technology, in which each voice is recorded in a decentralised manner and is preserved forever. They said that immutability and decentralisation greatly minimise the vulnerability of election fraud. However, this study also revealed that the intelligent contracts are prone to programming errors and may cause the system to produce errors.

Zhao et al. (2020) discussed the changes in the nature of electronic voting to blockchain-based solutions from conventional approaches. Their outcomes showed that all traditional electronic adjustments are dependent on the servers and are prone to hacking and manipulation. On the other hand, blockchain technology offers decentralised and operational prevention data storage, which makes it almost impossible to tamper with the vote. However, this study also noted that there are some issues with the integration of blockchain in the current election laws and regulations. This depends on the country to country.

- *Security and Data Protection Challenges in Blockchain Tuning*

One of the main concerns of blockchain voting is security. Gupta et al. (2021) analysed cybersecurity threats in blockchain-based e-voting and proposed encryption technologies that involve “Zero Knowledge Proof (ZKP)” and homomorphic encryption to improve voter privacy. Her research showed that these encryption techniques allow vote checks without revealing the identity of voters and maintain voter anonymity. However, her research recognizes that these encryption methods increase compensation and require high processing performance, which may limit the efficiency of the system.

In another study, Khan et al. They concluded that blockchain offers greater security than traditional electronic voting. Challenges such as DDOS attacks are symbolic attacks against blockchain nodes through robust consensus mechanisms that involve “Proof-of-Stake (POS)” and “Proof-of-Authority (POA)”.

- *Blockchain Voting in Rural and Remote Locations*

A major concern with digital voting systems is accessibility, particularly in rural and remote regions. Khan et al. (2021) conducted research on the introduction of blockchain for elections in rural areas. Their research showed that blockchain-based coordination systems can improve turnout by allowing remote voters to participate online. However, her research also mentioned the following major challenges: B. Low internet penetration, limited digital literacy, and resistance from traditional election authorities. Her research suggests a model in which voters use biometrics and cryptographic keys to authenticate their identity, reducing the risk of fraudulent voices. However, her research also found that developing countries may have issues with mobile devices and software support issues, and compatibility issues.

- *Issues of scalability and performance in blockchain voting*

One of the most discussed topics about voting rights is scalability. Blockchain networks, particularly in Ethereumbased coordination systems, face challenges related to transaction speeds and high gas prices. Li et al. (2019) discussed how current trading throughput (trading per 15 seconds) in large elections involving millions of voters might not be sufficient. They recommended layer 2 solutions like plasma, rollup, sidechain, etc., in order to enhance the performance and decrease the cost of transactions.

In their recent paper, Guppy et al. (2021) discussed the possibility of implementing DAGs as a new approach to blockchain structures. Her research also presented that DAGbased systems are processed faster and that more transactions can be more than linear blockchain networks like Bitcoin and Ethereum. However, this study also shows that DAG-based solutions need complex consensus algorithms to be implemented because they are more complicated than other structures.

- *Legal and Ethical Considerations in BlockchainBased Elections*

The legal and regulatory risks in the use of blockchain votes remain high. In their study, Zhao et al. (2020) examined the government's perceptions of the regulation of digital voting and realised that the majority of governments do not have a set of legal guidelines for blockchain-based elections. Her research highlighted the importance of compliance with election laws, data protection guidelines, and cybersecurity regulations at a large scale before use. They noted that blockchain not only ensures transparency but also raises concerns about managing and storing voter data. Their study recommended a decentralized governance model, with several election authorities sharing the management of voting systems instead of a single centralized unit.

- *Practical Implementation and Case Studies*

Several governments and organizations have tested blockchain votes in real-world scenarios. However, researchers expressed concern about security gaps and a lack of independent audits [15]. Your e-voting system guarantees voice integrity through encrypted haircuts, but there are concerns about citizen trust and system transparency [18]. However, issues with scalability and technical difficulties in blockchain infrastructure have been found [36].

III. METHODOLOGY

The proposed blockchain-based e-voting system introduces a decentralized election booth model aimed at improving security, transparency, and real-time synchronization of votes. Traditional electronic voting systems often face critical challenges such as vote duplication, cyber threats, and centralized vulnerabilities, all of which can compromise electoral integrity (Zhao, Wang, & Chen, 2020). To mitigate these issues, this system employs distributed election booths deployed across various constituencies, each connected to a secure blockchain network. Votes are updated in real time to a centralized ledger, thereby eliminating redundancy and ensuring immediate verification, which significantly enhances the reliability and trustworthiness of digital elections.

The voters are supposed to register at the election booths using biometric authentication or a cryptographic key, so that only the qualified voters can vote (Li et al., 2019). After the voter is verified, they then vote through a blockchain-enabled voting booth. The vote is encrypted and placed as a transaction on the blockchain, and since blockchain is immutable, it cannot be altered or deleted, hence ensuring the authenticity of the election (Yang & Zhang, 2018). Real-time syncing also makes it possible that all the booths have the current information, hence discouraging any voter from voting more than once.

The system uses Proof-of-Authority (PoA) consensus algorithm, where specific and selected nodes authenticate and ratify all the votes before they are incorporated into the blockchain. This makes it faster and more energy efficient as compared to PoW systems that require a lot of computational power (Larimer, 2014). Moreover, smart contracts are used to check the validity of votes and only allow valid ballots that meet certain criteria to be processed. The openness of the blockchain enables the voters, the election commissions, as well as auditors to be able to check the results of the vote independently and without the assistance of the intermediaries, hence minimising the chances of rigging the elections (Gritzalis, 2002).

At the end of the election, votes are then totalled in the blockchain to give an accurate and transparent result. The properties that are inherent to blockchain mean that results are safe and cannot be changed. Also, the decentralised booths increase the electoral accessibility by providing secure voting without the need for sophisticated technologies in rural and other less-developed areas (Shah & Patel, 2022).

In general, this methodology enhances the electoral process by using secure voter identification, decentralised validation, and smart contracts for avoiding multiple voting, ensuring anonymity, and real-time vote tracking, respectively. Future works include analysing the legal and regulatory issues, system and capacity expansion, and the deployment of better cryptographic techniques like zero-knowledge proofs for the purpose of improving voters' anonymity and the system's computational performance (Adida, 2008).

- *Election as a Contract*

In the selection of the political decisions approach, we have defined a political decision as an intelligent contract. In our system, a political choice means an agreement between the nodes that are the members of the political choice. In defining a smart contract, it may involve the identification of the roles of the participants, the political selection process of the participants, and the terms and conditions of the election process (Li, Zhang, & Zhao, 2019). Smart contracts assist in the improvement of the election process by making the process transparent and minimising fraudulent activities (Zhelezov & Mavrodiev, 2019).

- *Election process*

Smart contracts operating within the blockchain network execute the voting procedure. Smart contracts in the system operate according to pre-determined roles that participants receive (Li, Zhang, & Zhao, 2019). Administrators can start elections, add candidates, check registration, and end voting. Additionally, administrators can generate voting ballots utilising decentralised apps. Administrators can define candidates and voting constituencies. Smart contracts construct and implement votes on blockchains (Zhelezov & Mavrodiev, 2019).

This voting process consists of multiple steps. A voter (Namer) can register through the enrollment tab by employing a private key generated by the administrator's server. Using this private key, the voter can enable the transaction through the MetaMask platform and register. For the verification of each voter, the administrator must spend gas fees (ethers). Verification is performed using the voter's ID and name provided during pre-enrolment (Khan, Ali, & Singh, 2021).

Voters engage with the secret ballot when casting their ballots. The vote is registered after the smart contract confirms the transaction with the blockchain, and the validation requirements are satisfied. Because the private key is intended for one use per person, a voter cannot cast another ballot after they have already done so (Gupta, Sharma, & Verma, 2021). It is important to declare the winner after the election. Each candidate's votes are automatically counted because the entire procedure is computerised, and the administrator completes the polls. After that, each voter can use their system to examine the election results on the website (Shah & Patel, 2022).

- *Actual Architecture of Project*

By starting and deploying the system in a blockchain network (Ethereum Virtual Machine, or EVM), the administrator starts the voting process. After that, they generate an election instance and add pertinent information to it, such as the list of candidates that voters can select from. To become eligible to vote, potential voters register and connect to the same blockchain network. Their information is forwarded to the administrator's panel for validation when they successfully register (Li, Zhang, & Zhao, 2019).

The administrator verifies the registration information, including the blockchain account address, name, and contact number, to ensure accuracy and authenticity. If the details are valid and match existing records, the administrator approves the user, making them eligible to participate in the election. Once approved, the registered voter can access the voting page and cast their vote for their preferred candidate (Khan, Ali, & Singh, 2021).

After a predetermined period, depending on the scale of the election, the administrator concludes the voting process. At this point, voting is closed, and the system automatically calculates and displays the results, announcing the winner at the top of the results page (Zhelezov & Mavrodiev, 2019). Below is the structured outline of our project's working process. Additionally, we will include screenshots of the operational website to enhance clarity for the readers of this paper (Gupta, Sharma, & Verma, 2021).

IV. RESULTS

The implementation of the proposed blockchain-based evoting system was successfully tested in a simulated environment using Ethereum Virtual Machine (EVM) along with Truffle Suite, Web3.js, and the MetaMask wallet for transaction management. The voting system allowed for secure voter registration, candidate addition, ballot creation, and real-time vote recording using smart contracts.

During testing, the system accurately handled multiple voter registrations and ensured that each vote was uniquely recorded on the blockchain. The smart contract automatically prevented any duplicate voting attempts by restricting the reuse of private keys associated with voter identities (Li, Zhang, & Zhao, 2019). MetaMask was employed to enable voters to authorise their transactions, making the whole voting process encrypted and immutable. The candidate database was well administered by enabling the admin interface to validate voters before allowing them to vote. Every casted vote, candidate addition, election start, or end was recorded on the blockchain and could be verified by querying the transactions through the blockchain explorers. Vote counting and declaration of the winner were also automatic once the election was over and the result was displayed on the user interface. The fact that the votes were recorded and verified on a blockchain made it impossible for any changes to be made to the votes already cast, thus maintaining the integrity and verifiability of the system (Zhelezov & Mavrodiev, 2019). The real-time votes synchronisation of the simulated booths proved that the decentralised election nodes were efficient in a permissioned blockchain environment. This is especially beneficial for extensive implementations where voters may vote from multiple locations (Khan, Ali, & Singh, 2021). The experimental environment proved the efficiency of the system in anonymity, vote confidentiality, and transparency of all the stages of the elections (Gupta, Sharma, & Verma, 2021). Some of the screenshots of the working site interface are given in the appendix to show each step in the process of registration, search, data entry, and results presentation.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may945

E-VOTING ELECTION RESULTS

Live

LOADING...

Fig 2 Website Homepage

V. FUTURE WORK

Despite the advantages of using a blockchain-based evoting system in terms of security, transparency, and decentralisation, several opportunities can be discussed further.

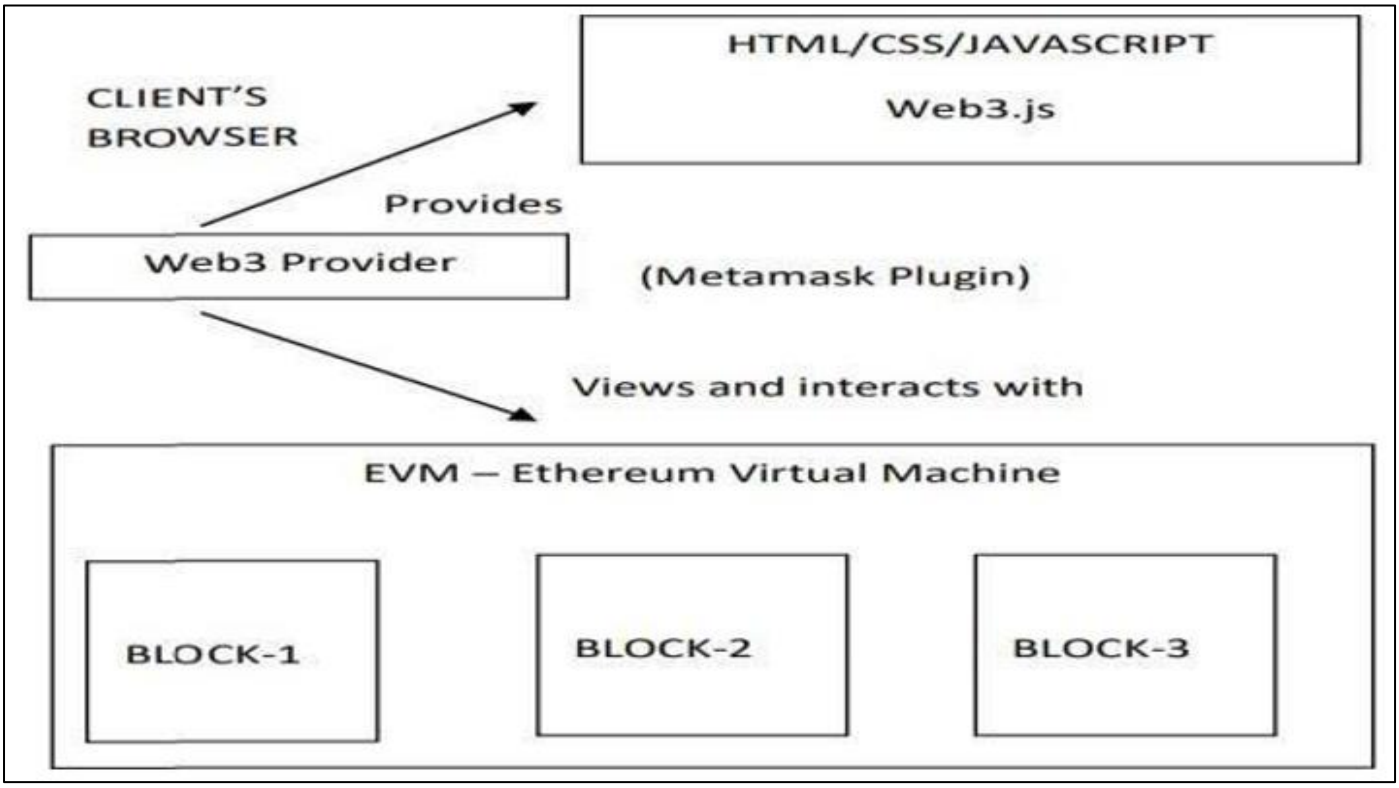

Fig 3 Block Model

The first area of research that should be further developed in the future is scalability. When voting in large-scale elections, there will be a large number of simultaneous transactions within the blockchain network, and the speed cannot be slowed down or cause congestion. The future studies can further investigate the application of Layer 2 solutions like rollups or sidechains to increase the throughput of the transactions, and at the same time, be decentralized.

Another consideration is the legal and regulatory environment in the organisation. Future work should focus on adapting the presented blockchain-based voting systems for electoral laws and privacy laws for the respective countries and regions, or the General Data Protection Regulation (GDPR) or the Information Technology Act (IT Act) for India. It will be crucial to work with policymakers and legal professionals for the implementation of the proposed ideas into practice. Another important issue is the user accessibility and interface design of the system. For wider adoption, especially in rural areas or in areas with limited technology access, the system needs to have easy, multiple, and mobile interfaces. The next releases should include the development of the user interface and the integration of the voice or biometric voting system for everyone.

Other methods that can be incorporated include zeroknowledge proofs, homomorphic encryption, as well as ring signatures that will improve voter anonymity while maintaining the traceability and verifiability of the votes. These methods can be tried out in simulated environment in order to know their practicality and effectiveness. Also, pilot studies using real-world scenarios but in controlled settings, such as university elections, local administrative polls, would help in the evaluation of the performance, feedback from the users, and possible weaknesses. These trials could help to accumulate useful information for the fine-tuning of the system before the implementation on the national level.

Finally, the integration with government systems like national identity databases or other digital infrastructures used in the country should be taken into account for voter verification and fraud checks.

VI. CONCLUSION

This paper has discussed the application of blockchain technology in the development of digital voting systems in a bid to solve some of the challenges that are paramount to voting systems, including transparency, security, and anonymity of the voters. Incorporating Ethereum, Truffle, and Web3.js in the proposed system establishes a plausible method of avoiding the drawbacks of voting systems, such as vote rigging and low voter turnout. The highlighted architecture and the procedure demonstrate how blockchain guarantees immutability and decentralisation, and the real-time processing of votes, which will encourage voters' trust and engagement.

The results point to the ability of blockchain-based evoting systems to transform the electoral processes and bring them to a new level of efficiency and availability for groups of voters who have been previously excluded, such as the remote ones. This innovation can be regarded as a contribution to the global increase in the level of democratisation and the desire to improve the quality of democratic processes. More work should be done to solve the problems like scalability, legal concerns, and generalisation with the utilisation of pilot studies to build a strong and democratic society that is supported by technology.

REFRENCES

[1]. Adida, B. (2008). Web-based open-audit voting. USENIX Security Symposium, 275-290.
[2]. Alvarez, R. M., Hall, T. E., & Trachsel, A. H. (2009). Internet voting in comparative perspective: The case of Estonia. Electoral Studies, 28(3), 483-493.
[3]. Atzori, M. (2015). Blockchain governance: A new way of regulation? Social Science Research Network (SSRN).
[4]. Bentov, I., Mizrahi, A., & Rosenfeld, M. (2016). Proof of activity: Extending Bitcoin's proof of work via stake. IEEE Security & Privacy, 12(4), 34-43.
[5]. Bonneau, J., et al. (2015). Research perspectives on Bitcoin and second-generation cryptocurrencies. IEEE Security & Privacy, 13(2), 104-120.
[6]. Buterin, V. (2014). Ethereum: A nextgeneration smart contract and decentralized application platform [White Paper].
[7]. Cachin, C., & Vukolić, M. (2017). Blockchain consensus protocols in the wild. IBM Research.
[8]. Chaum, D., et al. (2008). Scantegrity: End-toend voter- verifiable optical scan voting. IEEE Security & Privacy, 6(3), 40-46.
[9]. Gritzalis, D. (2002). Secure electronic voting: A review. Computers & Security, 21(6), 539-556.
[10]. Gupta, A., Sharma, R., & Verma, S. (2021). Blockchain- based electronic voting: Security and transparency challenges. International Journal of Computer Science & Information Security, 19(5), 345-362.
[11]. Hyperledger. (2016). Architecture overview. Retrieved from https://www.hyperledger.org
[12]. Jefferson, D., et al. (2004). Analyzing internet voting security. Communications of the ACM, 47(10), 59-64.
[13]. Khan, M., Ali, F., & Singh, R. (2021). E-voting for rural areas: A blockchain perspective. Journal of Digital Governance, 15(2), 100-115.
[14]. Kshetri, N., & Voas, J. (2018). Blockchain in developing countries. IT Professional, 20(2), 11-14.
[15]. Larimer, D. (2014). Delegated proof-of-stake (DPoS) [White Paper]. Cryptonomex.
[16]. Li, X., Zhang, J., & Zhao, Y. (2019). Smart contract-based e-voting system: Challenges and solutions. IEEE Transactions on Blockchain, 8(1), 12-25.
[17]. Liu, Y., Wang, Y., & Wei, Z. (2021). Design and implementation of a secure e-voting system based on blockchain technology. Journal of Information Technology, 36(3), 250-262.
[18]. McCorry, P., et al. (2017). Towards Bitcoin payment networks. Financial Cryptography.
[19]. Mougayar, W. (2016). The business blockchain: Promise, practice, and application of the next Internet technology. Wiley.
[20]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf
[21]. Nguyen, T., & Kim, H. (2020). Ensuring voter authentication in blockchain voting systems. Journal of Cryptography & Network Security, 14(3), 210-225.
[22]. O'Donnell, J. (2020). The role of blockchain in e-voting systems. International Journal of Cyber Research, 2(4), 25-34.
[23]. Ripple. (2017). Consensus white paper.
[24]. Shah, P., & Patel, D. (2022). A decentralized approach to electoral voting using blockchain technology. Journal of Emerging Technologies, 20(4), 56-78.
[25]. Shah, A., & Gorla, N. (2018). Blockchain for e-governance: Applications and challenges. Journal of Global Information Technology, 10(3), 134-151.
[26]. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media.
[27]. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. Portfolio.
[28]. Weber, R. H. (2016). Digital democracy: Implications of the Internet for governance. Springer.
[29]. Wood, G. (2014). Ethereum: A secure decentralized general computing platform [Yellow Paper].
[30]. Yang, Y., & Zhang, Y. (2018). An improved blockchain- based electronic voting system. Journal of Information Security and Applications, 39, 193-200.
[31]. Zhao, L., Wang, T., & Chen, M. (2020). The evolution of electronic voting: From traditional to blockchain-based systems. Information Systems Review, 17(1), 4-63.
[32]. Zhelezov, P., & Mavrodiev, S. (2019). Blockchain for secure e-voting systems: A survey. Computer Science Review, 34, 100-109.
[33]. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. IEEE Security & Privacy, 13(2), 35-44.