STM JOURNALS

Journal of
Electronic Design Technology

ISSN: 2229-6980 (Online)
ISSN: 2321-4228 (Print)
Volume 16, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoEDT

https://journals.stmjournals.com/joedt

Research JoEDT

Blockchain-Assisted Electronic Voting: A System Design Perspective

Nagendra Pathak[1,*], Shagil Suhail[1], Shivam Yadav[1], Chitrangada Chaubey[2]

Abstract

Voting plays a vital role in upholding democratic principles by allowing individuals to express their preferences and take part in shaping the decisions that affect their lives. Despite its importance, traditional voting systems—whether manual or digital—continue to encounter major obstacles. These include a lack of transparency, declining voter turnout, vulnerability to fraud, and concerns around manipulation. While digital voting platforms offer a modern alternative, they often face skepticism due to risks related to centralized control, cybersecurity threats, and the integrity of stored data. In this context, blockchain technology offers a new path forward. Its decentralized and tamper-resistant architecture presents an opportunity to reimagine the voting process with greater trust, security, and transparency. This paper presents the design and development of a blockchain-based electronic voting system that leverages the Ethereum network. The proposed system is implemented as a web-based application, where voting operations are governed by smart contracts written in Solidity. These contracts ensure that each vote is recorded immutably, preventing duplication or unauthorized activity. Users participate through digital wallets that authenticate their identities and facilitate secure, gas-limited transactions. This approach enhances vote integrity while protecting the privacy and autonomy of individual voters. In addition to the system's technical architecture, the paper explores the broader benefits of blockchain in electoral applications, including improved auditability, greater voter confidence, and real-time verifiability. The study also reflects on the practical limitations of the approach, such as transaction fees, user accessibility challenges, and the scalability constraints of current blockchain infrastructures. By addressing both the strengths and limitations, this research aims to demonstrate how blockchain can serve as a reliable and innovative alternative to traditional voting methods, encouraging further exploration and refinement in real-world democratic systems.

Keywords: E-voting, smart contracts, blockchain, Ethereum

INTRODUCTION

Blockchain technology, initially introduced as the foundation for cryptocurrencies like Bitcoin, has rapidly evolved into a powerful framework with applications far beyond digital finance. At its core, blockchain is a distributed ledger that records transactions in a secure, verifiable, and tamper-proof manner across a decentralized network. Its fundamental properties—such as immutability, decentralization, and transparency—position it as a promising solution for improving the integrity and reliability of voting systems. Conventional voting methods, such as paper ballots and electronic voting machines, often suffer from various limitations. These include challenges in maintaining transparency, ensuring data security, and preventing fraudulent activities. Furthermore, public confidence in these systems is frequently undermined due to concerns about tampering,

***Author for Correspondence**
Nagendra Pathak
E-mail: nagendrapathak9838@gmail.com

[1]Student, Department of Computer Science & Engineering, Galgotias College of Engineering Technology, Greater Noida, Uttar Pradesh, India
[2]Assistant Professor, Department of Computer Science & Engineering, Galgotias College of Engineering Technology, Greater Noida, Uttar Pradesh, India

Received Date: May 01, 2025
Accepted Date: May 06, 2025
Published Date: May 22, 2025

Citation: Nagendra Pathak, Shagil Suhail, Shivam Yadav, Chitrangada Chaubey. Blockchain-Assisted Electronic Voting: A System Design Perspective. Journal of Electronic Design Technology. 2025; 16(2): 9–16p.

manipulation, and lack of verifiable audit trails. Although digital voting platforms have attempted to address some of these issues, they still rely heavily on centralized infrastructures that may expose them to cybersecurity risks and data breaches [1].

Blockchain, when integrated with smart contracts, offers an innovative alternative by allowing election data to be stored in a distributed and immutable manner. Smart contracts are self-executing programs deployed on the blockchain that automate key functions such as vote validation and counting, ensuring that the process remains transparent, fair, and resistant to manipulation. This paper explores the development and implementation of a secure e-voting system built on the Ethereum blockchain, leveraging its smart contract capabilities to maintain election integrity.

A fundamental concept in blockchain architecture is the "genesis block" or "Block 0." This initial block is embedded within the blockchain software and serves as the starting point for the entire chain, lacking any reference to a previous block. Subsequent blocks, beginning with "Block 1," are linked to their predecessors, creating a chain of verified data entries. Each block's transaction data is processed through a cryptographic structure known as a Merkle tree, where individual transaction hashes are recursively combined until a single hash, called the Merkle root, represents the entire block's contents [2–4].

In a blockchain network, each block contains a header that stores critical metadata, including the Merkle root—a cryptographic summary representing all transactions within that block (Figure 1). This structure ensures data integrity, as any attempt to alter a single transaction would require modifying the corresponding Merkle root and, consequently, the block header. Furthermore, each block also retains a reference to the header of the previous block, forming an interlinked chain. This chaining mechanism makes it extremely difficult to tamper with historical data, as doing so would require re-computing and altering all subsequent blocks across the chain [5].

Blockchain networks (Figure 2) operate over peer-to-peer (P2P) infrastructures, where each node (or peer) connects with others to share and validate transaction data. Once a node joins the network, it begins exchanging information about other peers, creating a decentralized method of peer discovery that eliminates the need for a central authority. The primary responsibility of these nodes is to validate newly mined blocks and pending transactions, ensuring the network's consistency and trustworthiness.

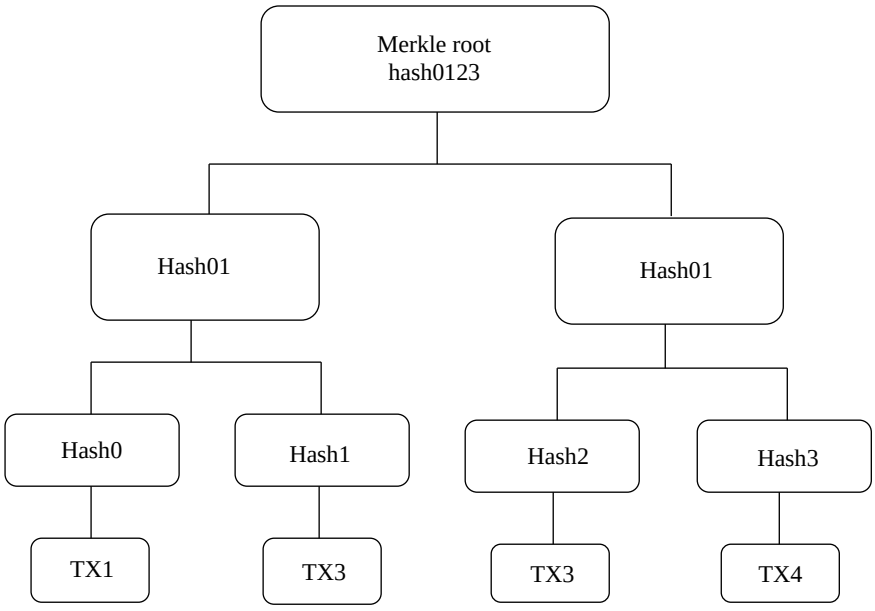

Figure 1. Hash table.

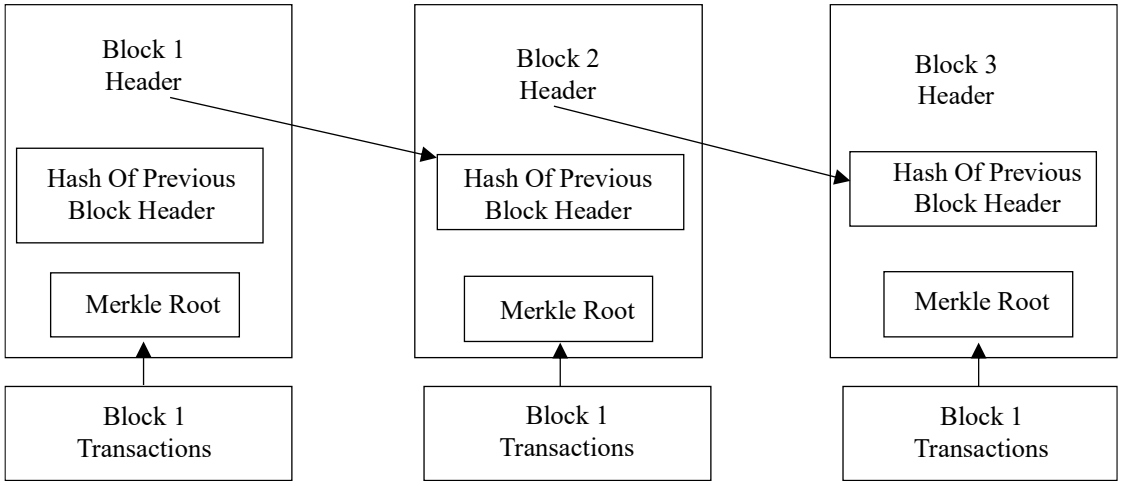

Figure 2. Simplified Bitcoin blockchain.
Source: bitcoin.org

Before a newly added node can contribute to block validation, it must first undergo a process known as the initial block download (IBD). During IBD, the node systematically downloads and verifies all blocks starting from the first block after the genesis block up to the most recent one. This comprehensive download ensures the node's complete synchronization with the network, allowing it to actively participate in consensus and transaction verification. Only after this synchronization process is complete can the node fully function as part of the distributed validation system.

Blockchain presents a promising solution for electronic voting (e-voting), a field that has seen extensive research and several experimental implementations. However, only a few systems have proven reliable enough for continued use. While online polls and surveys are common, secure digital elections—especially for governments and large organizations—remain rare.

This is largely because official elections are fundamental to democratic systems, where transparency and privacy are essential. In such contexts, even minor flaws in the voting process can undermine public trust. As decision-making increasingly shifts to digital platforms, the need for secure, verifiable, and private voting solutions becomes more urgent. Blockchain's core features—immutability, decentralization, and traceability—make it a strong candidate for meeting these needs, though widespread adoption still faces several hurdles.

MOTIVATION AND RELATED WORKS

The core motivation behind this project is to create a secure, transparent, and reliable e-voting system utilizing blockchain technology. With the rise of digital tools, voting can now become more accessible, reaching people with computers or smartphones. This can potentially shift power back into the hands of citizens, making administrative decisions more democratic.

This vision could bring us closer to a true form of direct democracy. Our focus lies in addressing the corruption and manipulation that can plague traditional elections, particularly in smaller towns or corrupt regions. Moreover, large-scale elections come with high costs, particularly when multiple voting centers are involved across vast geographical areas [4].

One of the major benefits of e-voting is that it can overcome barriers like low voter turnout, which often happens when people are unable to vote due to logistical reasons, such as being away from their registered address. If implemented properly, e-voting can overcome these issues and make voting more inclusive.

Historically, e-voting systems have relied on centralized models for computation and storage. A notable example is Estonia, which implemented one of the first comprehensive online e-voting solutions. Since its introduction in 2003, Estonia's system has evolved into a robust platform that allows citizens to vote remotely using a smart digital ID card and personal readers. Estonia's system has seen widespread use, with nearly 30% voter participation in recent elections. Citizens can also digitally sign petitions and participate in legislative processes, showcasing how technology can enhance democracy [6].

However, despite its successes, the Estonian system faces challenges. Its centralized nature makes it vulnerable to attacks like distributed denial of service (DDoS), and the reliance on physical ID cards adds an extra layer of cost and complexity. The system's scalability is also a concern, especially in large populations, which raises questions about whether the model could be effective in larger nations like China.

Switzerland is another country exploring e-voting, specifically remote voting, to allow citizens to participate in elections across various topics. A notable instance is Sierra Leone's 2018 general election, where Agora, a Swiss startup, used blockchain to verify votes in two districts, ensuring transparency in the tallying process. Similarly, the Russian city of Moscow utilized blockchain in the "Active Citizen" program, where community votes were securely recorded on a blockchain, allowing the results to be publicly audited [7].

While platforms like Strawpoll.me allow users to create and participate in online polls, they highlight the importance of secure and authenticated voting. The platform is convenient, but it lacks the necessary security measures to be used in official elections. Figure 3 further illustrates the need for secure, blockchain-powered e-voting systems that can ensure trust, prevent fraud, and guarantee the integrity of the electoral process.

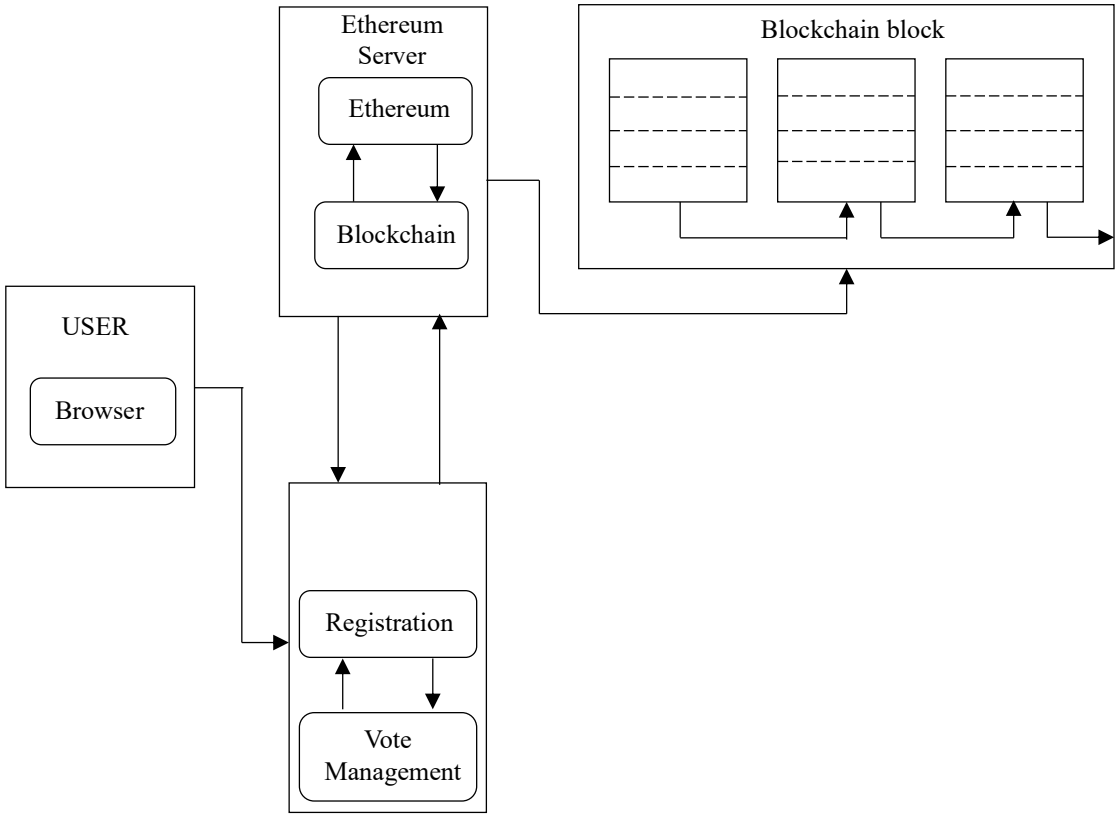

Figure 3. System overview.

In this paper, we integrate blockchain technology into e-voting, proposing a feasible protocol that eliminates the need for a trusted third party (TTP) and offers a flexible, secure voting mechanism. Our solution meets the core requirements for a robust e-voting system, reinforcing the strength and transparency of the election process is recorded on a decentralized ledger, which can be publicly audited and verified [8].

IMPLEMENTATION AND DISCUSSION

The proposed e-voting system is built on the Model–View–Controller (MVC) architecture (Figure 4), which divides the application into three core components for better organization and scalability:

- *Model:* The Model component is responsible for managing the system's data, which is stored securely in a MySQL database. It holds voter details, election data, and other essential information required for the voting process. This data is encrypted and handled with strict security measures to ensure the integrity of sensitive information.
- *View:* The View component acts as the user interface, enabling voters to interact with the system in a user-friendly manner. Through this interface, users can register, authenticate, and cast their votes. The View component ensures an intuitive design, with clear instructions and responsive features, making it accessible to voters of all technological backgrounds.
- *Controller:* The Controller component contains the core business logic of the system. It handles user authentication, ensures that only eligible voters can participate, and validates votes before they are submitted. It also manages interactions with the blockchain network, ensuring that each vote is securely recorded and immutable [9]. The Controller acts as the mediator between the Model and View, ensuring smooth data flow and execution of the voting process.

By organizing the system in this way, the architecture ensures modularity and scalability, making it easier to maintain and upgrade as the e-voting system evolves. The blockchain network plays a critical role in ensuring transparency and security.

- *Registration:* Voters begin by creating an account and providing their personal identification details (Figure 5). These details are securely stored in a database to ensure only eligible individuals can participate. The registration process forms the foundation for verifying voter eligibility and protecting against unauthorized participation.
- *Login and authentication:* After registration, voters log into the system using their username and password. To further enhance security, voters authenticate their identity by receiving and entering a one-time password (OTP) sent to their registered mobile number. This ensures that the person voting is indeed the one registered, preventing fraudulent activity.
- *Voting process:* When casting their vote, voters select their preferred candidate or option. The system encrypts their vote and records it on the Ethereum blockchain using smart contracts. This process involves a small fee, known as gas, ensuring the secure processing of the vote. The blockchain’s decentralized nature guarantees that the vote is tamper-proof and remains immutable once cast [10].
- *Result compilation:* After voting concludes, the results are compiled and made available on the web interface for voters to review. Voters can verify their individual vote using their public key, providing a transparent method for confirming their participation in the election. This step reinforces trust in the system by allowing independent verification, ensuring the process is both accurate and transparent.

In our application, users must have an account with a wallet address and a small balance of Ether, Ethereum's native cryptocurrency, in order to participate in voting. Once connected to the blockchain network, users can cast their vote by paying a minimal transaction fee, known as "gas," which is required to record the vote on the blockchain. This "gas" fee compensates the miner-node that processes the transaction.

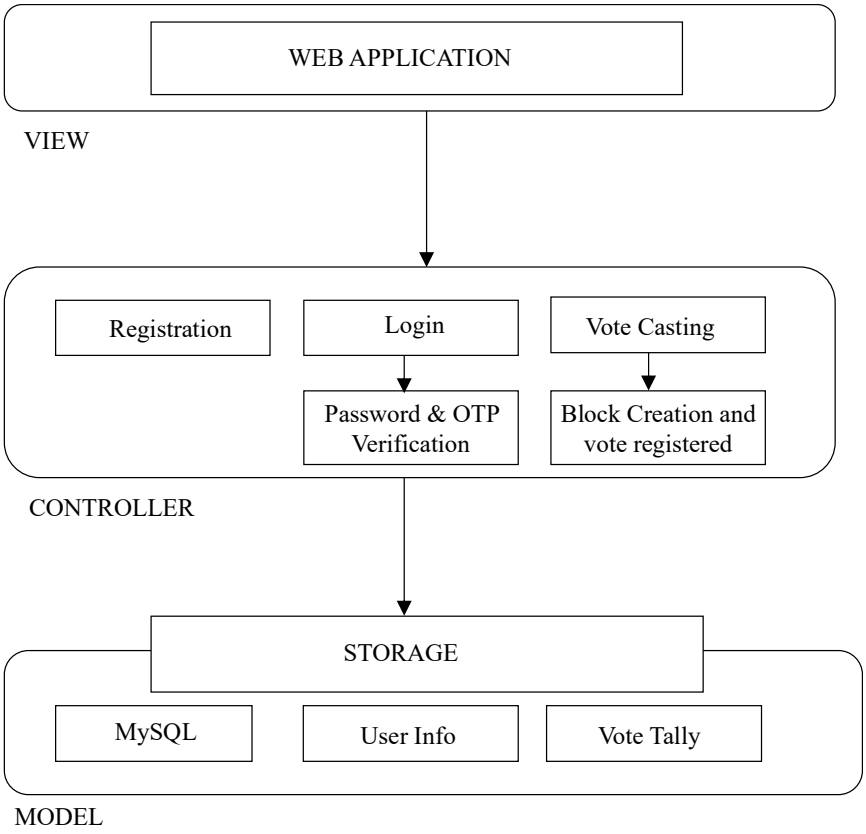

Figure 4. Model–View–Controller (MVC) architecture.

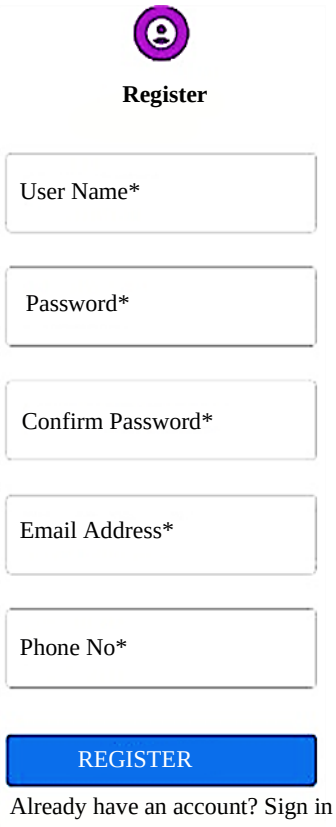

Figure 5. Screenshot of application during registration process.

While submitting a vote incurs this cost due to writing data onto the blockchain, viewing the list of candidates does not require a fee, as reading data from the blockchain is free of charge.

Our system utilizes the Ethereum blockchain, which allows code execution through the Ethereum Virtual Machine (EVM) via smart contracts. These smart contracts, written in Solidity, serve as automated agreements and manage the logic of voting. Specifically, the smart contract ensures that each vote is counted once, prevents double voting, and determines the candidate with the highest number of votes as the winner [11].

To implement the application, the first step is to set up the required dependencies, write the smart contract, and deploy it to the blockchain. The smart contract is initiated using the keyword "contract," followed by a name for the contract. State variables are then declared to store the candidate names, and these variables allow data to be written to the blockchain. The constructor of the contract is executed when the contract is deployed.

Once the smart contract is deployed and the webpage is developed, users need to log in to the blockchain. This is accomplished by importing one of the accounts from Ganache (a tool providing 10 accounts with addresses and test Ether) into MetaMask, a browser extension that enables interaction with the Ethereum blockchain. After connecting, users can interact with the deployed smart contract, view the contract details, and access their account information, enabling secure and transparent voting. When a user casts their vote, they pay a small "gas" fee, which is rewarded to the miner-node that processes and records the vote on the blockchain. After the vote is successfully cast and recorded, the results are compiled and displayed. The candidate with the highest number of votes is determined as the winner, ensuring a transparent and secure election process.

The election results are displayed after votes have been successfully cast. The details of each vote entry are recorded on the blockchain, including transaction hashes, block creation information, contract addresses, timestamps, account data, block numbers, gas usage, and the overall transaction cost for casting the vote.

This project primarily focuses on small-scale polls and elections, such as those held within educational institutions. Large-scale elections involving millions of voters present challenges that require further research. The scalability of the Ethereum network is still uncertain, which makes it unsuitable for nationwide elections at this point. Since the contracts are deployed on the Ethereum blockchain, the voting application can be accessed from any device or platform capable of running a web browser.

A key challenge with blockchain-based e-voting systems is maintaining voter anonymity while ensuring transparency. On the blockchain, transactions, including votes, are stored in plain text. This means that a vote from one wallet address to another is visible to anyone with access to the blockchain, which creates a significant privacy issue. Therefore, such systems are not yet viable for official or sensitive elections. Ensuring voter privacy while maintaining transparency remains a major challenge in current blockchain-based e- voting research. A solution using the Diffie–Hellman process, which employs public/private key pairs and random numbers to enable a “two-round” referendum while keeping the ballot private [12].

CONCLUSION

This study highlights the transformative potential of blockchain technology in modernizing the voting process by providing a secure, transparent, and decentralized platform. Although the current system is effective for small-scale elections, there is a need for further development in blockchain scalability and privacy features to facilitate wider implementation. Future research should prioritize improving voter anonymity and optimizing transaction costs to enable the use of blockchain-based e-voting systems on a larger, national scale.

REFERENCES

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. [Online]. Bitcoin.org. n.d. Available at https://bitcoin.org/bitcoin.pdf
2. Wood G. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151. April 2014. pp. 1–32.
3. Clack CD, Bakshi VA, Braine L. Smart contract templates: foundations, design landscape and research directions. arXiv preprint. arXiv:1608.00771. August 2, 2016.
4. Maaten E. Towards remote e-voting: Estonian case. In: Electronic voting in Europe – Technology, Law, Politics and Society, Workshop of the ESF TED Programme Together with GI and OCG, Schloß Hofen/Bregenz, Lake of Constance, July 7–9, 2004. Bonn, Germany: Gesellschaft für Informatik eV; 2004. pp. 83–90.
5. Çabuk UC, Çavdar A, Demir E. E-Demokrasi: Yeni Nesil Doğrudan Demokrasi ve Türkiye'deki Uygulanabilirliği [E-Democracy: The Next Generation Direct Democracy and Applicability in Turkey]. In: International Conference of Turkey, Ankara, Turkey, November 2016. Vol. 21.Available at https://www.researchgate.net/profile/Umut-Cabuk/publication/308796230_E-Democracy_The_Next_Generation_Direct_Democracy_and_Applicability_in_Turkey/links/5818a6d408aee7cdc685b40b/E-Democracy-The-Next-Generation-Direct-Democracy-and-Applicability-in-Turkey.pdf
6. Gaikwad MP, Jadhav VD, Palange LA. Electronic voting system security based on multichain platform. Int J Innov Eng Res Technol. 2019; 1–3: 150–152.
7. Hao F, Ryan PY, editors. Real-World Electronic Voting: Design, Analysis and Deployment. Boca Raton, FL, USA: CRC Press; 2016.
8. Braun N. E-voting: Switzerland's projects and their legal framework – in a European context. In: Electronic Voting in Europe – Technology, Law, Politics and Society, Workshop of the ESF TED Programme Together with GI and OCG, Schloß Hofen/Bregenz, Lake of Constance, July 7–9, 2004. Bonn, Germany: Gesellschaft für Informatik eV; 2004. pp. 43–52.
9. Kshetri N, Voas J. Blockchain-enabled e-voting. IEEE Softw. 2018; 35 (4): 95–99.
10. McCorry P, Shahandashti SF, Hao F. A smart contract for boardroom voting with maximum voter privacy. In: Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta, April 3–7, 2017, Revised Selected Papers 21 2017. Cham, Switzerland: Springer International Publishing; 2017. pp. 357–375.
11. Çabuk UC, Şenocak T, Demir E, Çavdar A. A Proposal on initial remote user enrollment for IVR-based voice authentication systems. Int J Adv Res Computer Commun Eng. 2017; 6: 118–123.
12. Takabatake Y, Okabe Y. An anonymous distributed electronic voting system using Zerocoin. In: 2021 International Conference on Information Networking (ICOIN), Jeju Island, South Korea, January 13–16, 2021. pp. 163–168.

