**Blockballot: Blockchain Based E-Voting System**

Sarveshaa Swar1, Sanika Shinde2, A. Bharat S.K. Reddy3, Parag Nimkar4, Dr. Trupti Lotlikar5

*1(Dept. of Information Technology, Fr. C. Rodrigues Institute of Technology, India) sarveshaaswar@gmail.com*

*2(Dept. of Information Technology, Fr. C. Rodrigues Institute of Technology, India) sanikayshinde@gmail.com*

*3(Dept. of Information Technology, Fr. C. Rodrigues Institute of Technology, India) bharatreddy131002@gmail.com*

*4(Dept. of Information Technology, Fr. C. Rodrigues Institute of Technology, India) nimkarparag5@gmail.com*

*5(Dept. of Information Technology, Fr. C. Rodrigues Institute of Technology, India) trupti.lotlikar@fcrit.ac.in*

|  |
| --- |
| ***Abstract:****Blockballot offers a promising solution to enhance the integrity and security of electoral processes. Leveraging the decentralized and immutable nature of blockchain technology, our system ensures transparency, verifiability, and tamper-resistance. By recording each vote as a transaction on the blockchain, the system provides a transparent audit trail, reducing the risks of fraud and manipulation. Voters can securely cast their votes from anywhere, promoting accessibility and convenience. Cryptographic techniques authenticate voters' identities while maintaining anonymity. As a result, Blockballot: Blockchain based E-Voting System fosters trust in democratic processes, paving the way for a more inclusive, efficient, and trustworthy electoral environment.*  ***Key Word****: Blockchain; E-Voting System; Democracy; Smart Contracts; Voter Anonymity; Elections.* |

1. **Introduction**

The integration of blockchain technology into electronic voting systems presents a significant advancement in the quest for secure and transparent democratic processes. Traditional voting systems often face challenges such as potential fraud, lack of transparency, and limited accessibility. Blockchain-based e-voting systems address these issues by utilizing the core principles of decentralization, immutability, and cryptographic security.

In essence, blockchain e-voting systems revolutionize the way votes are cast, recorded, and verified. Each vote is treated as a tamper-proof transaction, recorded on a distributed ledger accessible to all participants. This ledger, composed of interconnected blocks of data, ensures transparency and provides an immutable record of the entire voting process. By eliminating the need for centralized authorities and intermediaries, trust in the system is bolstered.

Moreover, the cryptographic protocols within blockchain technology guarantee the security and anonymity of voters while maintaining the integrity of the overall process. This introduction of blockchain into e-voting not only enhances the efficiency and accessibility of voting but also instills confidence in citizens, ensuring the democratic principles of fairness and accountability.

1. **Overview**

Blockballot represents a revolutionary approach to modernizing electoral processes, offering a secure, transparent, and accessible method for casting and recording votes. At its core, our system harnesses the power of blockchain technology, a decentralized ledger system, to ensure the integrity and credibility of the voting process. Our system operates through a series of interconnected blocks, each containing a batch of votes. When a voter casts their ballot, it is recorded as a transaction on the blockchain, creating an immutable and transparent record. This decentralized nature eliminates the need for a central authority, reducing the risk of tampering or manipulation.

Transparency is a cornerstone feature of Blockballot. All stakeholders, including voters, election officials and observers, have access to the blockchain ledger. They can verify the authenticity of each vote and track it’s journey through the system. This transparency enhances trust in the electoral process and acts as a deterrent to fraudulent activities. Security is paramount in blockchain e-voting. Advanced cryptographic algorithms ensure that votes are securely encrypted and remain anonymous. This not only protects voter privacy but also maintains the integrity of the election. Furthermore, the decentralized nature of blockchain means that there is no single point of failure, greatly reducing the vulnerability to hacking or cyberattacks.

Accessibility is also greatly enhanced with blockchain e-voting. Citizens can cast their votes remotely from any location with an internet connection, eliminating the need for physical polling stations and enabling greater participation, particularly among remote or disabled voters.

In summary, Blockballot: Blockchain Based E-Voting System offers a comprehensive solution to many challenges faced by traditional voting methods. It ensures transparency, security, and accessibility, thereby fostering trust in democratic processes and paving the way for a more inclusive and efficient electoral environment.

1. **Methodologies Used**

Creating a blockchain-based e-voting system involves careful consideration of various methodologies to ensure security, transparency, and reliability. Here are some key methodologies commonly used in developing our system:

1. Blockchain Consensus Algorithms:
   1. Proof of Work (PoW): Initially popularized by Bitcoin, PoW requires nodes (computers) to solve complex mathematical puzzles to validate transactions. However, it's energy-intensive.
   2. Proof of Stake (PoS): This method selects validators based on the number of coins they hold. Validators are chosen to create and validate new blocks based on their stake in the network.
   3. Delegated Proof of Stake (DPoS): Similar to PoS, but delegates are chosen to validate transactions. This can lead to faster transaction speeds.
   4. Proof of Authority (PoA): A system where validators are identified and approved by a central authority. It's less decentralized but offers faster transactions and less energy consumption.
2. Zero-Knowledge Proofs (ZKPs):

ZKPs allow a prover to prove possession of a piece of information without revealing that information. In e-voting, this can be used to prove a vote was cast without revealing the actual vote.

1. Homomorphic Encryption:

This encryption allows computation on encrypted data without decrypting it first. It can be used to count votes without revealing individual votes.

1. Multi-signature Wallets:

In a multi-signature scheme, multiple private keys are required to authorize a transaction. This adds an extra layer of security, ensuring no single entity can tamper with the system.

1. Decentralized Identity (DID):

DID systems provide a way to manage digital identities that are self-owned, portable, and secure. Each voter could have a DID to ensure their identity is verified.

1. Smart Contracts:

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They can automate various aspects of the voting process, such as tallying votes, ensuring rules are followed, and triggering events based on specific conditions.

1. Immutable Ledger:

The blockchain's immutability ensures that once a vote is cast and recorded, it cannot be altered. This transparency and auditability are crucial for the integrity of the voting process.

1. Multi-level Authentication:

Implementing multi-level authentication for voters ensures that only eligible voters can participate. This could involve traditional methods like email verification combined with blockchain-based identity verification.

1. Off-chain Storage for Sensitive Data:

While blockchain provides security, storing large files (like identity documents) directly on the chain is not efficient. Off-chain storage solutions, with references stored on the blockchain, can be used for sensitive data.

1. Open Source Development:

Developing the e-voting system as open-source allows for community review and scrutiny, which enhances security and transparency.

1. Penetration Testing and Auditing:

Regular penetration testing and independent auditing by security experts are crucial to identify and fix vulnerabilities.

1. User-Friendly Interfaces:

While the backend uses complex blockchain methodologies, the frontend should be user-friendly to encourage voter participation. Clear instructions, intuitive design, and accessibility features are important.

1. **Proposed System**

Blockballot aims to revolutionize the traditional voting process by leveraging the security, transparency, and immutability features of blockchain technology. This system provides a secure platform for voters to cast their votes remotely while ensuring the integrity and transparency of the entire voting process. Below is the proposed workflow for the system:

**Workflow Overview:**

1. **Voter Registration**
   * Voters register on the e-voting platform by providing their personal information, which is verified against government databases or other trusted sources.
   * Each voter is issued a unique digital identity consisting of a public and private key pair. The private key is securely stored by the voter, and the public key is used for identification.
   * Voter information and public keys are stored on the blockchain, ensuring immutability and transparency.
2. **Candidate Registration**
   * Candidates running for office register their candidacy on the platform, providing necessary details such as their name, party affiliation (if any), and position they are running for.
   * Candidate information is verified and recorded on the blockchain.
3. **Voting Phase**
   * **Voter Authentication**:
     + Voters log into the e-voting platform using their unique digital identity (public key).
     + The system verifies the voter's identity through multi-factor authentication, including biometric verification and OTP (One-Time Password) confirmation.
   * **Ballot Creation**:
     + The system generates a digital ballot containing the list of candidates based on the voter's registered constituency.
     + Voters can review the candidates' information and make their selections.
   * **Vote Casting**:
     + Once satisfied with their choices, voters cryptographically sign their ballot using their private key.
     + The signed ballot is then submitted to the blockchain network for validation and inclusion in the ledger.
4. **Vote Recording on Blockchain**
   * The submitted votes are recorded as transactions on the blockchain, ensuring immutability and transparency.
   * Each vote transaction includes details such as the voter's public key, selected candidates, timestamp, and cryptographic signature.
5. **Consensus and Validation**
   * The blockchain network employs a consensus mechanism (e.g., Proof of Authority or Proof of Stake) to validate and confirm the submitted votes.
   * Nodes in the network reach a consensus on the validity of each transaction, ensuring that only legitimate votes are added to the ledger.
6. **Vote Counting**
   * As votes are recorded on the blockchain, the system automatically tallies the votes for each candidate in real-time.
   * Transparency is maintained as the tallying process is visible to all stakeholders, ensuring the integrity of the election results.
7. **Results Publication**
   * Once the voting phase concludes, the final election results are computed and verified by the blockchain network.
   * The election results, including the total votes received by each candidate, are published on the e-voting platform and made publicly accessible.
   * Voters can verify that their votes were correctly recorded and counted using cryptographic proofs without compromising their anonymity.

This proposed system for a blockchain-based e-voting system with a detailed workflow emphasizes security, transparency, voter verification, and accessibility. Each step in the process is designed to ensure the integrity of the voting process while maintaining voter privacy and anonymity.

1. **Results**

**A screenshot of a computer

Description automatically generated**

**BLOCKBALLOT**

Fig. 1. Home Page

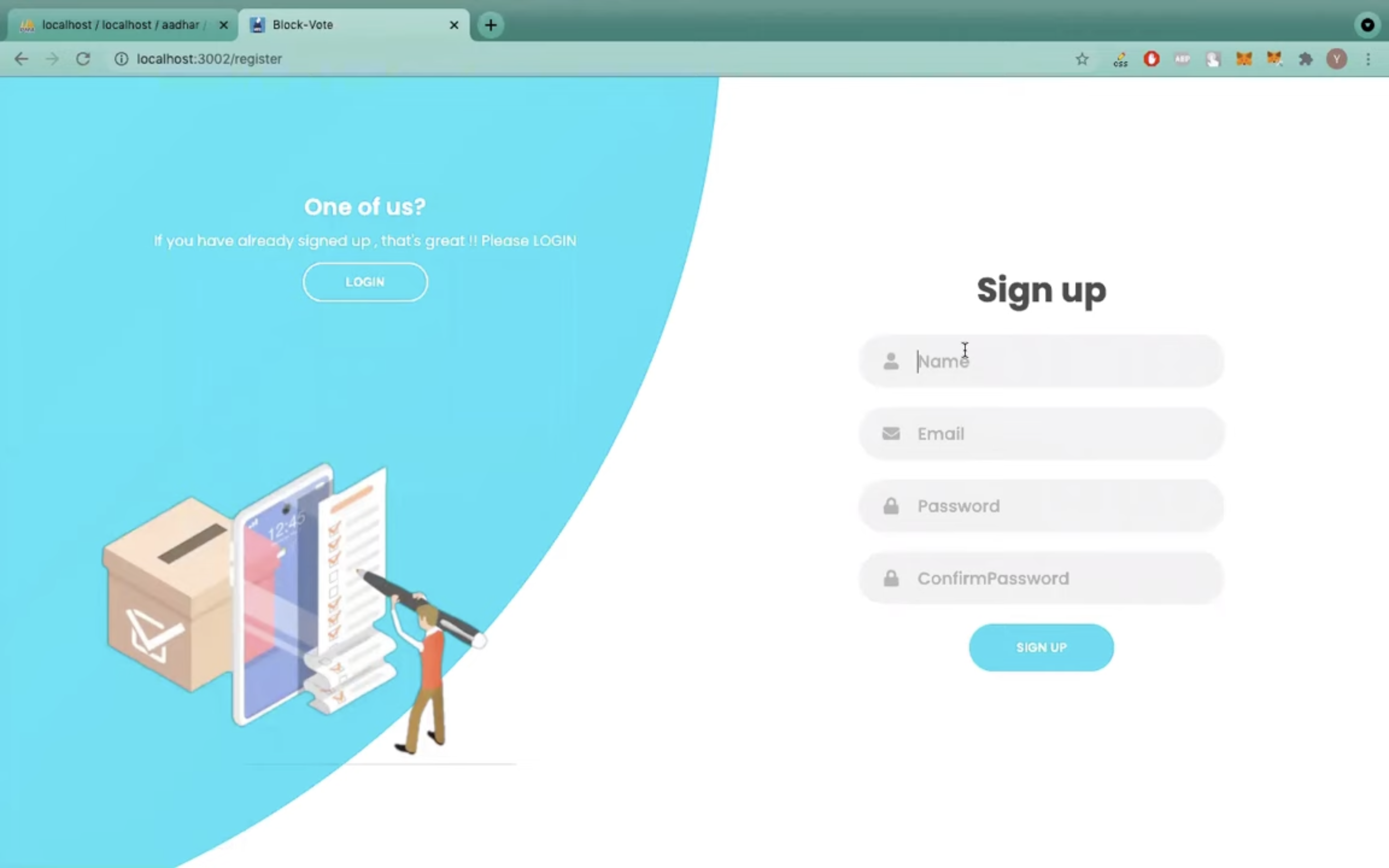
****

Fig. 2. Voter Sign-up Page

A screenshot of a computer

Description automatically generated

Fig. 3. Ganache User-Interface

**A screenshot of a computer

Description automatically generated**

Fig. 4. Voter Interface

**A screenshot of a computer

Description automatically generated**

Fig. 5. Admin Interface

1. **Conclusion**

In conclusion, Blockballot: Blockchain based E-Voting system presents a transformative solution to traditional voting challenges. By harnessing blockchain's immutable ledger and cryptographic security, the system ensures transparent, secure, and verifiable elections. Through a seamless workflow encompassing voter registration, candidate registration, secure ballot creation, and real-time tallying, the system promotes voter trust and engagement. Its benefits include heightened security against fraud, increased accessibility for remote voting, and the preservation of voter anonymity. With the ability for voters to verify their own ballots and the public auditability of results, this system stands as a beacon of integrity, paving the way for modern, inclusive, and democratic elections.

1. **Acknowledgements**

Top of Form

Bottom of Form

Our project ‘Blockballot: Blockchain based E-Voting’ was the result of a collaborative endeavor involving several contributors. Special recognition to our dear guide, Dr. Trupti Lotlikar for her unwavering support and contribution throughout our project. Sincere thanks to Dr. S.M. Khot, the principal of Fr. C. Rodrigues Institute of Technology, Vashi, for providing us with the opportunity to present our talents. Our deep appreciation is also extended to Dr. Shubhangi Vaikole, the Head of the Department of Information Technology, for her constant motivation. Furthermore, we would like to convey our heartfelt thanks to our families and friends.

**References**

1. S. Swar, S. Shinde, A. B. S. K. Reddy, P. Nimkar and T. Lotlikar, "Cryptcast: E-Voting System Utilizing Blockchain," 2023 6th International Conference on Advances in Science and Technology (ICAST), Mumbai, India, 2023.
2. A. M. Al-madani, A. T. Gaikwad, V. Mahale and Z. A. T. Ahmed, "Decentralized E-voting system based on Smart Contract by using Blockchain Technology," 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC).
3. E. Febriyanto, Triyono, N. Rahayu, K. Pangaribuan and P. A. Sunarya, "Using Blockchain Data Security Management for E-Voting Systems," 2020 8th International Conference on Cyber and IT Service Management (CITSM).
4. A. Parmar, S. Gada, T. Loke, Y. Jain, S. Pathak and S. Patil, "Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT).
5. P. Rani, V. Kumar, I. Budhiraja, A. Rathi and S. Kukreja, "Deploying Electronic Voting System Use-case on Ethereum Public Blockchain," 2022 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS).
6. A. Singh and K. Chatterjee, "SecEVS : Secure Electronic Voting System Using Blockchain Technology," 2018 International Conference on Computing, Power and Communication Technologies (GUCON).
7. F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD).
8. A. Balti, A. Prabhu, S. Shahi, S. Dahifale and V. Maheta, "A Decentralized and Immutable E-Voting System using Blockchain," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS).
9. S. Tandon, N. Singh, S. Porwal, Satiram and A. K. Maurya, "E- Matdaan: A Blockchain based Decentralized E-Voting System," 2022 IEEE Students Conference on Engineering and Systems (SCES).
10. R. Kumar, L. Badwal, S. Avasthi and A. Prakash, "A Secure Decentralized E-Voting with Blockchain & Smart Contracts," 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence).
11. Z. Khudoykulov, U. Tojiakbarova, S. Bozorov and D. Ourbonalieva, "Blockchain Based E-Voting System: Open Issues and Challenges," 2021 International Conference on Information Science and Communications Technologies (ICISCT).
12. H. Jayasooriya, D. Bandara, N. Hemachandra, N. Kuruwitaarachchi and S. Kahandawala, "Integrity Assured Digital Voting System by using Blockchain as the Technology," 2022 IEEE International Conference on e-Business Engineering (ICEBE).