IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

Digitalized Voting System using Blockchain Technology

Mrs. K. Divya Kalyani[1], Sayeeda Fathima[2], S. Maha Lakshmi[3], K Hemanth[4], P Manikanta[5]
Dadi Institute of Engineering & Technology, Anakapalle , India[1,2,3,4,5]
sayeedafathima698@gmail.com

Abstract: *This paper introduces a novel Digitalized Voting System designed to address the shortcomings of current voting methods employed in India. With a focus on enhancing transparency and trust in the electoral process, the system aims to overcome challenges present in both traditional and digital voting systems, including instances of mishaps and injustice. Leveraging blockchain technology, the proposed system seeks to ensure fair elections and minimise occurrences of injustice. While electronic voting has been introduced as a solution to paper-based voting, it has encountered obstacles primarily related to security and privacy concerns. To address these issues, our framework emphasises the effectiveness of various components such as the polling process, hashing algorithms, contract and block creation, data accumulation, and result declaration.Utilising an adjustable blockchain method, the system aims to provide a robust solution to the security and data management challenges inherent in blockchain technology. By incorporating elements such as blockchain, hashing algorithms, block creation, OTP verification, and Ethereum, our approach endeavours to digitalize the voting process comprehensively. This paper contributes to the advancement of electoral integrity by presenting an improved manifestation of electronic voting, paving the way for more transparent and secure elections*

Keywords: Blockchain, Hashing algorithms, E-Voting System, Ethereum, Digitalizing

I. INTRODUCTION

The rise of blockchain technology has sparked interest in transforming traditional systems into more secure, transparent, and efficient processes. One promising application is the digitalized voting system using blockchain technology, designed to modernise and enhance the integrity of electoral processes.A digitalized voting system based on blockchain operates on the principles of decentralisation, cryptographic security, and immutability. Each vote is recorded as a transaction on a distributed ledger, creating a secure and tamper-resistant environment. This approach addresses significant issues in traditional voting, such as voter fraud, ballot tampering, and lack of transparency.The system leverages smart contracts to automate various voting processes, including voter registration, vote casting, and result tallying. This automation reduces the risk of human error and manipulation, ensuring that voting rules are strictly enforced.Blockchain's transparency allows for real-time auditing and verification, fostering public trust in the electoral process. However, privacy is maintained through cryptographic techniques that ensure voter anonymity while preserving accountability.The digitalized voting system using blockchain technology represents a step forward in electoral security and accessibility. It offers a scalable solution adaptable to different voting scenarios, from national elections to local referendums, with the potential to revolutionise how we vote in the digital age.

II. LITERATURE REVIEW

A. Digital Voting System

A digital voting system, also known as electronic voting or e-voting, encompasses various technologies that allow voters to cast their votes electronically. This literature review explores key themes and developments in digital voting, focusing on technology, security, reliability, accessibility, and legal frameworks.

Technological Developments:

The evolution of digital voting systems has paralleled advancements in information technology. Early systems relied on electronic voting machines (EVMs) in controlled environments like polling stations, using proprietary software and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

hardware. As technology evolved, Internet-based voting emerged, allowing remote voting through web platforms and mobile applications.

Security and Integrity:
Security is a primary concern in digital voting. Literature indicates that vulnerabilities can arise from software flaws, unauthorised access, and manipulation of results. Researchers emphasise the need for robust encryption, secure authentication, and transparent audit mechanisms. Notable cases of successful e-voting, such as Estonia's national elections, demonstrate that with rigorous security protocols, e-voting can be reliable.

Reliability and Accuracy:
Digital voting systems must ensure that votes are accurately recorded and counted. Issues such as system crashes, software bugs, or hardware malfunctions can undermine reliability. Studies suggest that rigorous testing, redundancy, and fail-safe mechanisms are crucial to ensure accurate vote capture and counting.

Accessibility and Inclusivity:
Digital voting systems offer the potential to increase voter accessibility, allowing people with disabilities, those living abroad, and residents in remote areas to participate in elections. Research indicates that well-designed digital voting platforms can reduce barriers and promote inclusivity. However, the digital divide and varying levels of technology literacy remain challenges.

Blockchain and Emerging Technologies:
Recent literature explores blockchain technology's role in enhancing digital voting security and transparency. Blockchain's decentralised, tamper-resistant nature can address some traditional e-voting security concerns. However, challenges like scalability, consensus mechanisms, and energy consumption persist.

B. Blockchain:
Blockchain is a decentralised, distributed ledger technology where transactions are recorded in blocks andlinked in a chain. Each block contains transaction data, a timestamp, and a cryptographic hash of the previous block, ensuring data integrity and immutability. Blockchains use consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate transactions without a central authority. This architecture provides transparency and security, making it suitable for applications like cryptocurrencies, supply chain tracking, and smart contracts. Blockchain's decentralised nature reduces the risk of fraud and tampering, fostering trust amongparticipants.

C. Blockchain Using Python
Python, a versatile programming language, is widely used for building blockchain applications due to its simplicity and extensive library support. To create a basic blockchain in Python, developers typically focus on key elements like block structure, hashing, and consensus.
A basic block structure includes a list of transactions, a timestamp, a nonce (for Proof of Work), and a cryptographic hash of the previous block, ensuring a linked chain. The most common hashing algorithm used is SHA-256, which provides a unique, irreversible hash value for each block.
Python's rich ecosystem offers libraries such as `hashlib` for hashing, `datetime` for timestamps, and `Flask` for creating RESTful APIs, allowing developers to build and test blockchain networks. Developers can also implement smart contracts with frameworks like Ethereum's `web3.py`.
Consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) are implemented to ensure the integrity and security of the blockchain network, preventing tampering and enabling decentralised control.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

D. Blockchain Based E-Voting

Blockchain-based e-voting is an advanced method for conducting electronic voting, capitalising on blockchain's inherent security, transparency, and decentralised features. In this system, votes are securely recorded on a distributed ledger, ensuring the integrity and immutability of election results.

The primary components of a blockchain-based e-voting system include:

Blockchain Network: This decentralised infrastructure consists of nodes that maintain a shared ledger. Each vote is encrypted and added to the blockchain, ensuring it cannot be altered or deleted.

Smart Contracts: These are code-based protocols that automatically execute predefined actions based on specific conditions, like vote validation and tallying. They help enforce voting rules without human interference.

Voter Authentication: Security mechanisms ensure only eligible voters participate. Methods like digital identity verification, cryptographic keys, or biometric authentication enhance security and prevent fraud.

Anonymity and Privacy: Although the blockchain is transparent, ensuring voter anonymity is crucial. Techniques such as zero-knowledge proofs and ring signatures can anonymize votes while allowing auditability. Transparency and Auditability: The blockchain's immutable nature allows auditors to track the entire voting process, fostering public trust in the election's fairness and accuracy.

Consensus Mechanisms: These protocols maintain the integrity of the blockchain, ensuring that votes are validated and added to the ledger by agreement among network nodes.

By integrating these components, blockchain-based e-voting systems can offer a secure, transparent, and trustworthy alternative to traditional voting methods. This approach can help combat electoral fraud, improve accessibility, and increase public confidence in democratic processes.

III. METHODOLOGY

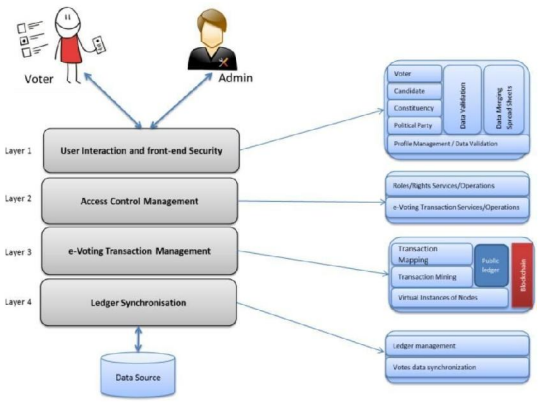
A. Blockchain Architecture

Designing blockchain architecture using Python involves several key methodologies that focus on structure, security, and functionality. Here's an overview:

1. Block Structure: Define the core components of a block, typically including a list of transactions, a timestamp, a nonce (for Proof of Work), and the previous block's hash. This structure forms the backbone of the blockchain.
2. Hashing and Cryptography: Utilise cryptographic algorithms like SHA-256 for hashing. This ensures data integrity and creates a unique identifier for each block, allowing blocks to be securely linked in a chain.
3. Consensus Mechanisms: Implement a consensus algorithm to validate new blocks and ensure network agreement. Common approaches include Proof of Work (PoW) and Proof of Stake (PoS), each with different security and scalability implications.
4. Blockchain Network: Design a decentralised network where nodes (participants) maintain the blockchain. Using Python libraries like `Flask` for RESTful APIs or `socket` for peer-to-peer communication helps build network connectivity.
5. Smart Contracts: Integrate smart contracts to automate processes on the blockchain. Frameworks like Ethereum's `web3.py` enable interaction with smart contracts.
6. Security and Privacy: Incorporate robust security measures to protect against attacks and ensure user privacy. Techniques like digital signatures, encryption, and permissioned blockchains enhance security.

By following these methodologies, developers can design a reliable, secure, and scalable blockchain architecture in Python.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024



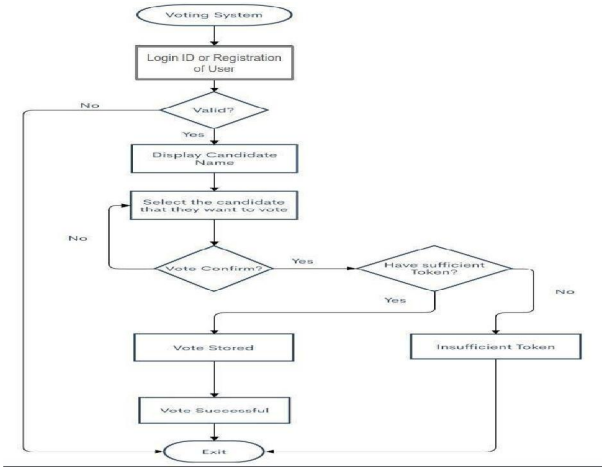


Fig. 1. Architecture of the Proposed System Fig. 2. Flowchart of the Proposed System

B. Developing UI Using Django:

Developing a User Interface (UI) using Django involves a structured approach to create dynamic, interactive web applications. Here's a concise methodology:

1. Project Setup: Start by creating a Django project with `django-admin startproject Digitalized Voting System Using Blockchain Technology. This sets up the basic structure, including settings, URLs, and WSGI configuration.
2. App Creation: Create Django apps for modularity with `python manage.py startapp VOtnation. Apps encapsulate specific functionalities, making code management easier.
3. Database Modelling: Define models in `models.py` to represent database tables. Use Django's ORM for creating and managing these models, ensuring a seamless data-to-view integration.
4. Templates and Static Files: Develop the UI using Django templates in the `templates/` directory. This allows dynamic rendering of HTML with Django template tags. Organise static files (CSS, JS, images) in the `static/` directory.
5. Views and URLs: Define views in `views.py` to handle HTTP requests and generate responses. Use URL patterns in `urls.py` to map URLs to specific views, enabling user navigation.
6. Forms and Validation: Utilise Django forms for user input, providing validation and error handling. This ensures a smooth and secure user experience.

Testing and Deployment: Test the UI with Django's built-in test framework to ensure functionality. Deploy using popular platforms like Heroku, AWS, or DigitalOcean, following Django's deployment best practices. Following this methodology helps create a robust, scalable, and user-friendly UI with Django.

IV. RESULTS

The results of our study indicate that the proposed Digitalized Voting System provides a more secure and transparent approach to voting. The implementation of blockchain technology and Ethereum smart contracts ensures a tamper-resistant environment, while the OTP verification system adds an additional layer of authentication, reducing the risk of voter fraud. Testing revealed that the system effectively prevents unauthorised access and maintains voter privacy through the use of advanced hashing algorithms and secure block creation. The adjustable blockchain method proved efficient in data management and processing. Overall, the results demonstrate that our system significantly reduces security risks and enhances the integrity of the electoral process, offering a reliable solution for conducting fair and trustworthy elections.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

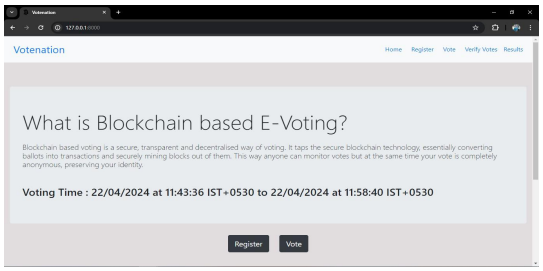


Fig. 3. UI of the Proposed System

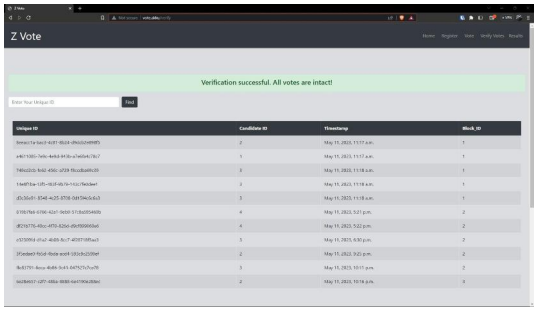


Fig.4. Blocks of each vote

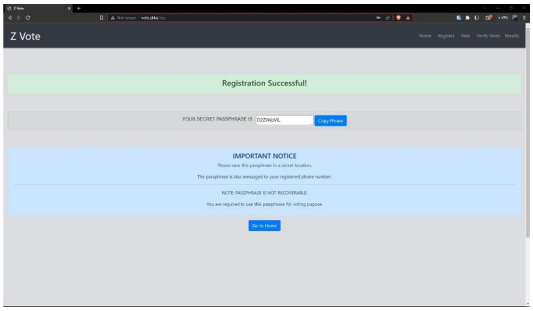


Fig.5. Secrete Token for Vote after Registration

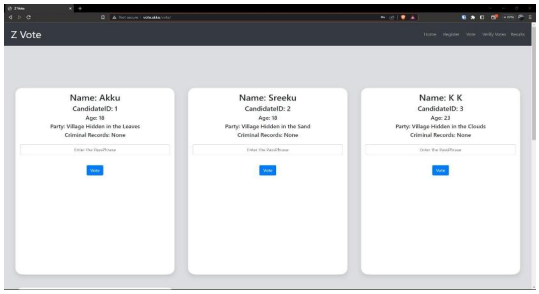


Fig.6. Candidates for ballet

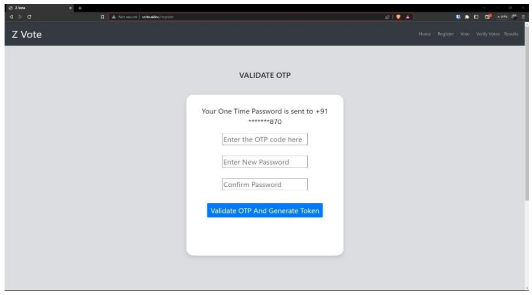


Fig.7. Registration of Voters

V. CONCLUSION

A reliable and transparent voting system is the cornerstone of any democratic society. Trusted elections are essential for strong democracies, yet traditional paper-based methods often fall short of providing the necessary trustworthiness. The shift toward digital voting systems offers a promising solution, making the electoral process cheaper, faster, and more accessible.

Digital voting helps normalise the election process for voters, reducing barriers and creating a more direct connection between the electorate and elected officials. This approach can also pave the way for more direct forms of democracy, allowing voters to voice their opinions on individual bills and propositions.

Our project presents a blockchain-based electronic voting system that uses smart contracts to ensure secure and cost-effective elections while protecting voters' privacy. The system architecture integrates advanced security features to prevent tampering and unauthorised access, offering a comprehensive design and security analysis.

In the upcoming build, we plan to create tailored client interfaces for different roles, including the election commission and registered candidates from specific parties, in addition to the existing voting client design. Current versions lack robust authentication due to limited access to government-issued identity services, like Aadhar or Voter SDK. Future improvements will include a notification system that reminds voters to cast their votes on election day, encouraging higher voter turnout.

Overall, this blockchain-based voting system aims to revolutionise the electoral process by providing a secure, efficient, and inclusive platform for democratic participation.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

REFERENCES

[1] Wolchok, Scott, et al. "Security analysis of India's electronic voting machines." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.
[2] Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law." Tex. L. Rev. 95 (2016): 1579.
[3] Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2017): 01-09.
[4] Hanifa Tunisia, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." 2017 11th International Conference on Telecommunication Systems Services and Applications. IEEE, 2017.
[5] Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." International Conference on Information Security. Springer, Cham, 2018.
[6] Madise, Ü. Madise and T. Martens, "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world.",Electronic voting, 2nd International Workshop, Bregenz, Austria,(2006) August 2-4.
[7] I. S. G. Stenerud and C. Bull, "When reality comes knocking Norwegian experiences with verifiable electronic voting", Electronic Voting. Vol. 205. (2012), pp. 21-33.
[8] C. Meter and A. Schneider and M. Mauve, "Tor is not enough: Coercion in Remote Electronic Voting Systems. arXiv preprint. (2017).
[9] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communication of the ACM. Vol. 24(2). (1981), pp. 84-90.
[10] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Info. Theory. Vol. 31. (1985), pp. 469-472.
[11] S. Ibrahim and M. Kamat and M. Salleh and S. R. A. Aziz, "Secure E-Voting with Blind Signature", Proceedings of the 4th National Conference of Communication Technology, Johor, Malaysia, (2003) January 14-15.
[12] J. Jan and Y. Chen and Y. Lin, "The Design of Protocol for e-Voting on the Internet", Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology, London, England, (2001) October 16-19.
[13] Trueb Baltic, "Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application."
[14] Ministry of Local Government and Modernisation. "Internet Voting Pilot to be Discontinued."
[15] J. A. Halderman, and V. Teague, "The New South Wales iVote System: Security Failures and Verifications Flaws in a Live Online Election." International Conference on E-Voting and Identity. (2015), pp. 35-53.