Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20250401033
Volume 4, Issue1 (January-April 2025), PP: 209-215.
www.indjcst.com
ISSN No: 2583-5300

Implementation Paper on Voting System Using Ethereum Blockchain and Ganache Tool

Chaitra BV[1], S. Manikantan[2], Purvi Hegde[3], Khushi Rai[4], Teja K M[5]

[1]Assistant Professor, Department of Computer Science and Design Engineering, Dayananda Sagar Academy of Technology & Management, Bengaluru, Karnataka, India.

[2,3,4,5]Undergraduate Students, Department of Computer Science and Design Engineering, Dayananda Sagar Academy of Technology & Management, Bengaluru, Karnataka, India.

To Cite this Article: *Chaitra BV[1], S. Manikantan[2], Purvi Hegde[3], Khushi Rai[4], Teja K M[5]*, *"Implementation Paper on Voting System Using Ethereum Blockchain and Ganache Tool", Indian Journal of Computer Science and Technology, Volume 04, Issue 01 (January-April 2025), PP: 209-215.*

Abstract: *In recent years, the security and integrity of electronic voting systems have become a significant concern for both governments and the public. Traditional voting systems are susceptible to voter fraud, data manipulation, and election tampering. In order to tackle these challenges, we introduce a new voting system that combines blockchain technology and face-based authentication to establish a secure, transparent, and effective voting process. Blockchain provides a decentralized, tamper-proof ledger to cast votes, which guarantees data integrity and does not allow for tampering or unauthorized alterations of voting outcomes. Blockchain uses the decentralized aspect for maximized transparency, with the possibility of tracing and authenticating each vote securely and ensuring that the election outcomes are tamper-proof. Moreover, the system is scalable and user-friendly and can be adopted on large scales such as elections at the national and regional levels. Utilizing blockchain ensures that voting records are stored safely and cannot be tampered with once submitted, and thus voters and election authorities have faith in the results of the elections being accurate. The use of blockchain guarantees that the voting records are securely stored and cannot be altered after submission, providing voters and election authorities with confidence in the accuracy of the election outcomes. This integration of cutting-edge technologies - blockchain for security and transparency, and facial recognition with KNN for authentication- provides a robust solution to modern electoral challenges. The proposed system aims to build a more trustworthy and efficient voting process, ultimately enhancing voter confidence and participation in democratic processes worldwide.*

Keywords: *Blockchain, Electronic voting, Decentralization, Security, Smart contracts, Transparency, Ganache, Ethereum network.*

I.INTRODUCTION

Over the last few years, digital transformation has scaled new heights, and thus there has been renewed emphasis on secure, scalable, and tamper-evident election systems. Traditional voting methods, while longstanding, suffer from systemic issues such as ballot tampering, limited accessibility, and lack of real-time auditability. With democracies around the world expecting more transparency and efficiency, blockchain technology- particularly Ethereum- has come forward as a transformative tool for electronic voting. Ethereum provides a decentralized platform for smart contracts that can be used to automate the logic of elections, validate transactions, and keep records immutable. When combined with tools such as Ganache, which creates a personal Ethereum blockchain for quick development and testing, developers can easily and safely develop and create prototypes of blockchain voting systems. This paper introduces the implementation of a smart contract - driven voting platform using Ethereum and Ganache. The system ensures that voter registration, ballot casting, and vote tallying are all managed on-chain, eliminating single points of failure. The decentralized structure removes the need for third-party oversight, enhancing trust and transparency.

Recent studies support the use of blockchain in voting systems. Parmar and Dewangan suggested a secure voting platform utilizing Ethereum smart contracts, allowing decentralized trust and enhanced accessibility [1]. Nguyen, Singh, and Kumar combined biometric verification with blockchain to prevent impersonation of voters, further enhancing e-voting systems [2]. Mittal and Singh highlighted how smart contracts provide end-to-end traceability of votes without compromising voter anonymity, leading to increased voter confidence.

Furthermore, Liu, Lu, and He analyzed face recognition as a biometric layer for voter verification, which can be integrated into blockchain workflows to restrict voting access to eligible individuals only [4]. Chaudhary and Garg introduced a voting framework under 5G networks, highlighting how Ethereum with tools like Ganache and Remix IDE can handle secure vote recording in distributed environments [5]

These studies collectively demonstrate that Ethereum-based e-voting, supplemented by Ganache for development, offers a compelling path toward modern, secure, and auditable elections.

II.EXISTING SYSTEM

Recent research has extensively explored the domain of privacy-aware electronic voting, with a strong focus on receipt-free and coercion-resistant voting mechanisms. The concept of receipt-free voting ensures that voters cannot produce verifiable evidence of their selections, thereby preventing vote-selling and external coercion. These mechanisms play an important role in preserving the integrity and independence of elections, especially in large-scale or high-stakes environments.

To further enhance privacy, newer systems include coercion resistance, preventing attackers from checking whom a voter voted for, even if the voter is coerced into disclosing his/her private keys. For instance, Park et al. introduced zkVoting, a voting system that relies on zero-knowledge proofs and nullifiable commitments to preserve vote secrecy even in case of coercion [6]. Similarly, Sarier presented a blockchain-powered e-voting scheme that uses biometric credentials and provides non-transferability of the voting rights, greatly enhancing usability and protection for voters [7]. Yet another significant contribution comes from Yin et al., who proposed an efficiently scalable coercion-resistant voting mechanism that is customized for blockchain-enabled decision-making procedures and provides both voter anonymity and verifiability within decentralized systems [8].

In parallel, self-tallying voting has emerged as an important area of development. These systems eliminate the need for centralized authorities in the vote-counting process, allowing any voter or external observer to verify the tally independently. This contributes significantly to the transparency of elections and reduces the risk of centralized manipulation.

Despite these advancements, several limitations remain. Some approaches focus primarily on speed and score evaluation but may sacrifice security in the process. Others adopt technically complex protocols that can be difficult to implement and scale in real-world elections. Additionally, systems that rely on third party verifiers for final results reintroduce trust dependencies, creating potential security vulnerabilities [6][7][8].

III.METHODOLOGY

To build a secure and transparent voting platform based on blockchain technology, utilizing the Ethereum network and the Ganache tool is essential. One of the potential methods is creating smart contracts that enable automated voting, voter registration, and casting of votes, making records decentralized and tamper-proof. Through the use of Ganache as a local blockchain for testing, developers can easily deploy and test smart contracts within a controlled environment. Implementing a token-based voting mechanism allows for unique tokens to be assigned to voters, ensuring anonymity and preventing double voting. Additionally, integrating cryptographic techniques, such as zero-knowledge proofs, enhances voter privacy while maintaining the integrity of the voting process. The user interface can be designed to interact seamlessly with the Ethereum blockchain using Web3.js, ensuring a smooth voting experience. Rigorous testing of smart contracts with frameworks like Mocha and Chai, along with deployment on Ethereum test nets, ensures functionality and security before going live. This architecture not only addresses the challenges of traditional voting systems but also provides a scalable solution for secure electronic voting.

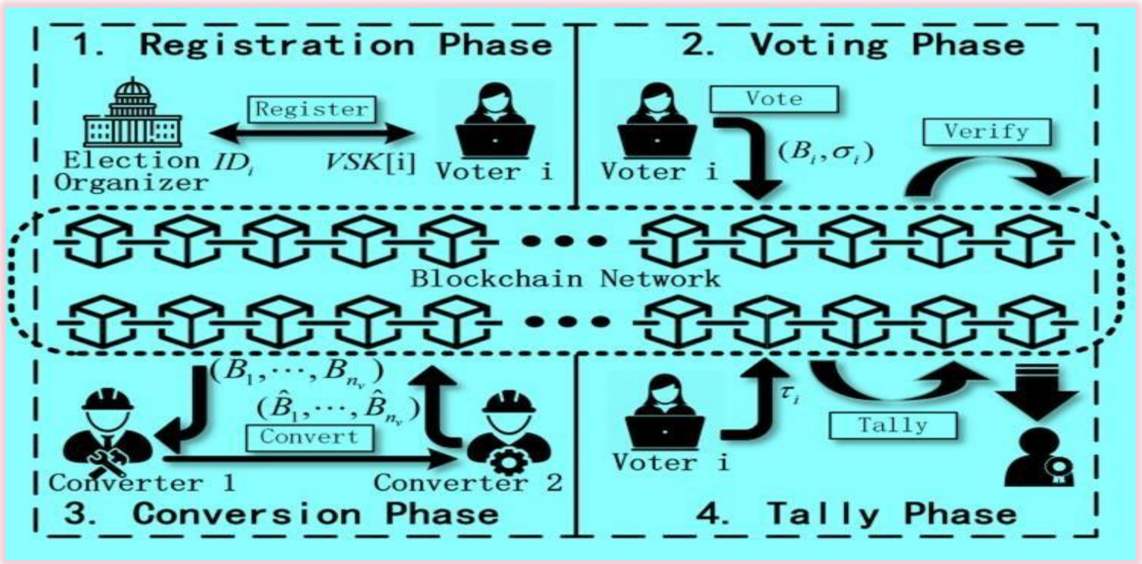


Fig 3.1 System Architecture

- **Election Organizer (EO)** is the entity for organizing and preparing elections, who may be a party, a corporation, a school, and etc. EO determines whether a voter is eligible to vote and issues voter secret keys in the registration phase.

- **Blockchain Network (BN)** refers to peer nodes of blockchain network who store blockchain data, confirm transactions and generate new blocks. In ACB-Vote, BN is responsible to execute smart contracts to store and verify ballots. Note that this work adopts a permission less blockchain, where voters are able to cast ballots or send necessary messages anonymously.

- **Voter (Vi)** is a voter who participates in the voting. In the registration phase, Vi registers to EO to obtain a secret voter key V SKi. Then, he/she computes an anonymous and convertible ballot and a corresponding signature, where the ballot encapsulates his/her voting scores {pi,1, · · · , pi,nc }. The ballot and signature are submit to BN in the voting phase.

- **Converters (CV1, CV2)** are responsible for ballot conversion. To prevent leaking voter privacy to the converter, ACB-Vote distributes the duty of converter to two non-collude entities CV1 and CV2. The role of CV1 and CV2 can be assumed by third-party judicial institutions, such as courts, arbitral tribunals and etc.
  To support a secure and transparent workflow, the system architecture is divided into several functional phases:

Voter and Candidate Registration

In this phase, the Election Organizer (EO) registers eligible voters and authorized candidates. Voter registration includes biometric enrollment using facial recognition, where each voter's facial features are encoded and stored in a secure database. The system assigns each registered voter a unique token or key that ensures both anonymity and authentication during voting.

Biometric Authentication

Prior to casting a vote, each voter must undergo face-based biometric verification. A K-Nearest Neighbors (KNN) classifier is employed to compare real-time captured facial data with preregistered images. This step prevents impersonation and ensures that only legitimate users can access the voting system. The lightweight nature of KNN makes it suitable for rapid classification, while maintaining accuracy across diverse facial structures.

Vote Casting via Smart Contracts

Once authenticated, the voter is presented with the ballot interface. Votes are submitted as transactions on the Ethereum blockchain, invoking smart contract functions that:

- Verify the voter’s eligibility and voting status,
- Record the vote immutably,
- Prevent duplicate or fraudulent voting using cryptographic token checks.

Each transaction includes encrypted vote data to preserve privacy and ensure the vote is not traceable to any individual voter.

Ballot Conversion and Deduplication

To maintain privacy and allow for auditability, submitted ballots undergo a conversion process involving two non-colluding entities (CV1 and CV2). These converters use a privacy preserving interactive protocol to deduplicate and transform ballots into a tally-ready state while ensuring that multiple submissions from the same voter are detected and discarded, all without exposing individual voting choices.

Vote Tallying and Result Publication

After voting concludes, the system enters the tally phase. The blockchain executes smart contract logic to count verified, converted votes. The final results are published on-chain and can be viewed by the public or authorized observers through the frontend interface. Voter anonymity is preserved throughout, while the transparent nature of the blockchain ensures full traceability of the tallying process.

This systematic approach combines cryptographic rigor, biometric authentication, and decentralized infrastructure to provide a secure, transparent, and verifiable voting experience.

IV.IMPLEMENTATION

This section details the practical realization of the blockchain-based secure voting system that integrates face- based authentication using a K-Nearest Neighbors (KNN) classifier. The implementation is modular, addressing various stages of the voting process with clearly defined roles and security mechanisms to ensure data integrity, privacy, and transparency.

Modules Overview

The proposed system comprises five key modules:

1. Initialization Phase 2. Registration Phase 3. Voting Phase 4. Conversion Phase 5. Tally Phase Each module plays a vital role in ensuring the secure and seamless execution of the election process.

Module Descriptions

1. Initialization Phase

The Election Organizer (EO) initiates the setup by generating public parameters and key pairs required for encryption and verification. Keys for the blockchain and converter entities (CV1 and CV2) are created and published on the blockchain to enable secure operations.

2. Registration Phase

Voters submit identity proof (e.g., government-issued ID, passport) to the EO. Upon successful verification, the voter receives a unique secret key that allows them to generate a ballot. The face data is also captured and stored securely for future verification during the voting phase.

3. Voting Phase

Authenticated voters generate a ballot and a corresponding signature using their secret keys. Before a vote is cast:

- The system uses a KNN classifier to perform real-time face recognition against the stored dataset.
- If authentication is successful, the voter is allowed to vote, and their choice is recorded immutably on the blockchain.

The blockchain's smart contracts handle ballot submission, verification, and prevent double voting.

4. Conversion Phase

To handle anonymous vote tallying while preventing duplicate votes, ballots undergo a conversion process. CV1 and CV2, acting as independent non-colluding entities, convert verified ballots using a distributed protocol. This ensures the privacy of voter identities and ballot contents while exposing potential duplicate entries.

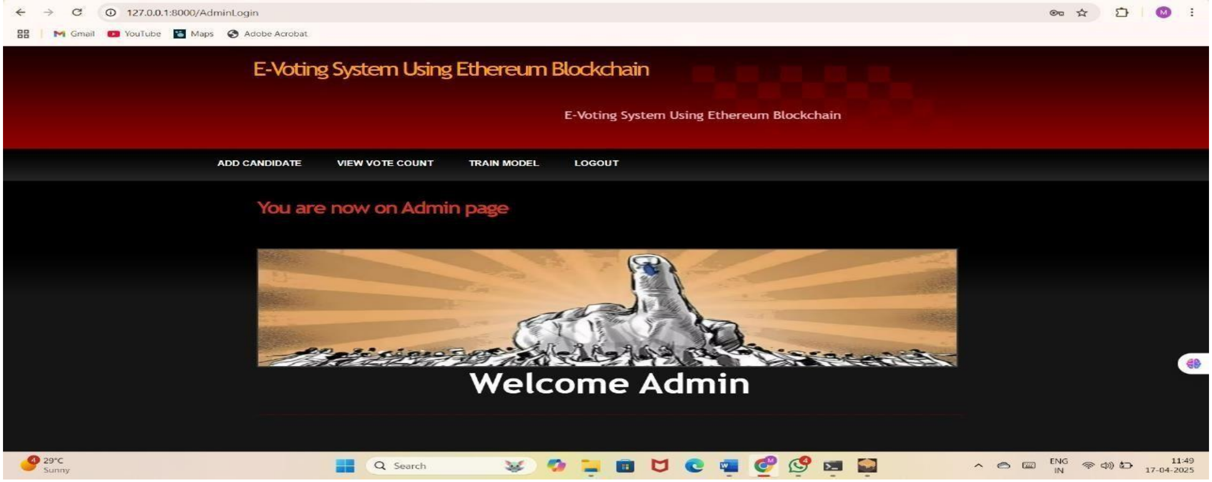
5. Tally Phase

After the election closes, voters anonymously reveal their ballot tags. The system then tallies votes using the verified converted ballots stored on the blockchain. Results are generated while preserving anonymity and are made publicly auditable to ensure transparency.

V.IMPLEMENTATION HIGHLIGHTS

- **Security and Integrity**: All votes are cryptographically signed and stored on the blockchain, preventing tampering and unauthorized changes.
- **Biometric Authentication**: The KNN-based facial recognition ensures only eligible, verified users cast votes.
- **Scalability**: The system architecture supports concurrent users, making it suitable for both small-scale and national- level elections.
- **Auditable Results**: Election results and vote trails are publicly verifiable while maintaining voter anonymity.
- **Duplicate Prevention**: Deduplication and voting status checks ensure voters cannot vote more than once.

VII.RESULTS



E-Voting System Using Ethereum Blockchain

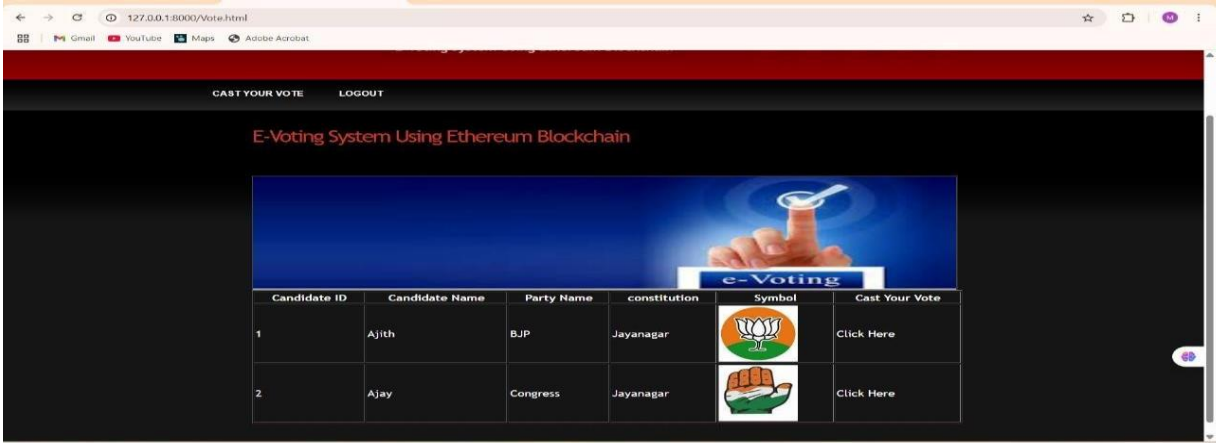
E-Voting System Using Ethereum Blockchain

ADD CANDIDATE VIEW VOTE COUNT TRAIN MODEL LOGOUT

You are now on Admin page

Welcome Admin

Fig 7.1 Admin interface

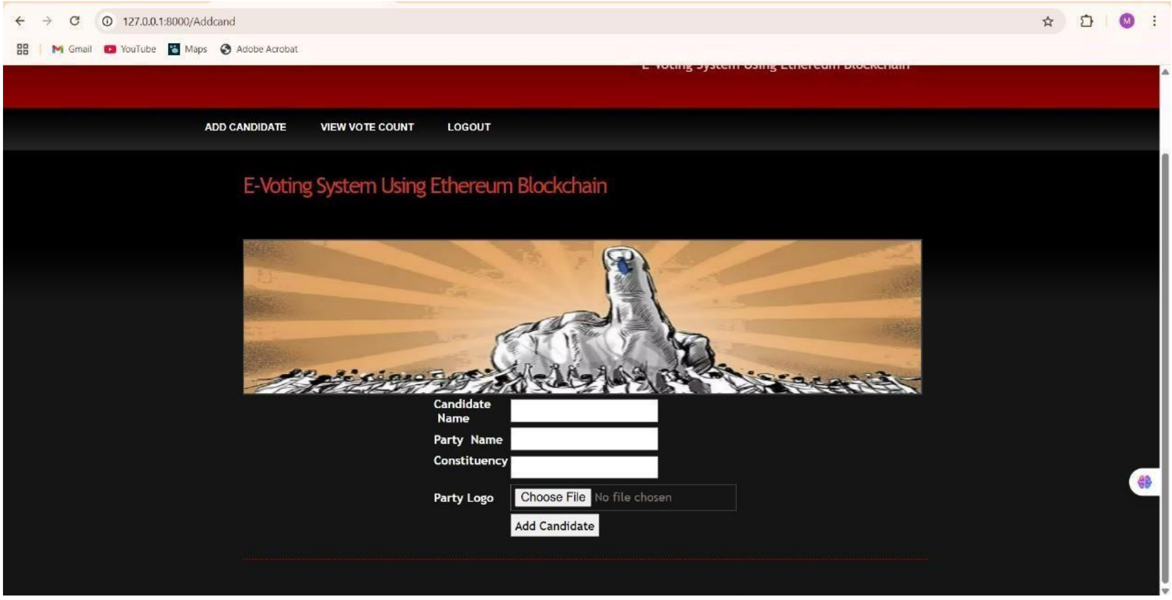


CAST YOUR VOTE LOGOUT

E-Voting System Using Ethereum Blockchain

Candidate ID	Candidate Name	Party Name	constitution	Symbol	Cast Your Vote
1	Ajith	BJP	Jayanagar		Click Here
2	Ajay	Congress	Jayanagar		Click Here

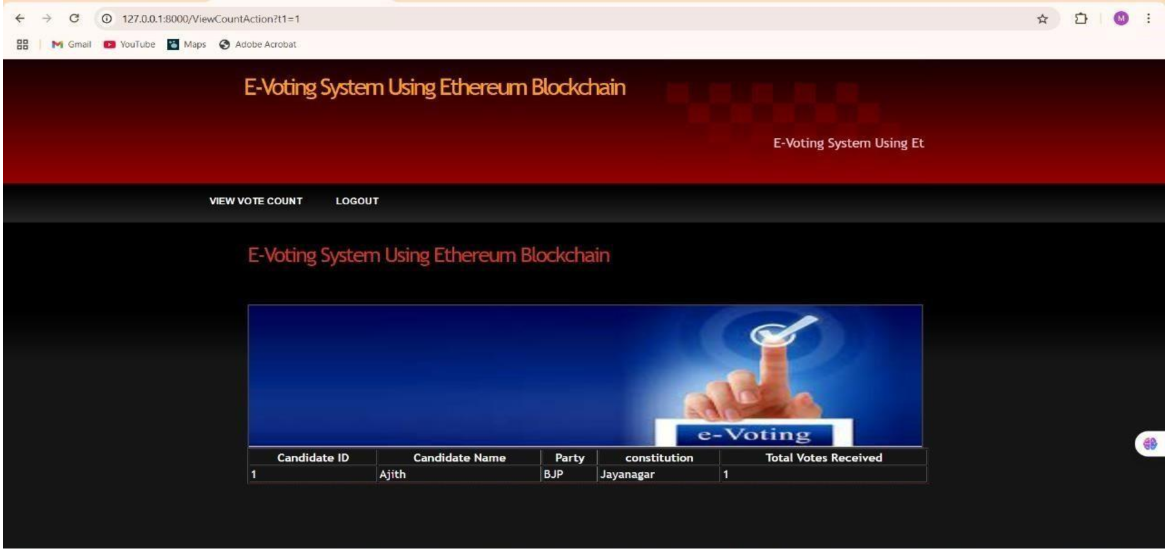
Fig 7.2 Voting for the candidate



E-Voting System Using Ethereum Blockchain

Candidate Name
Party Name
Constituency
Party Logo No file chosen

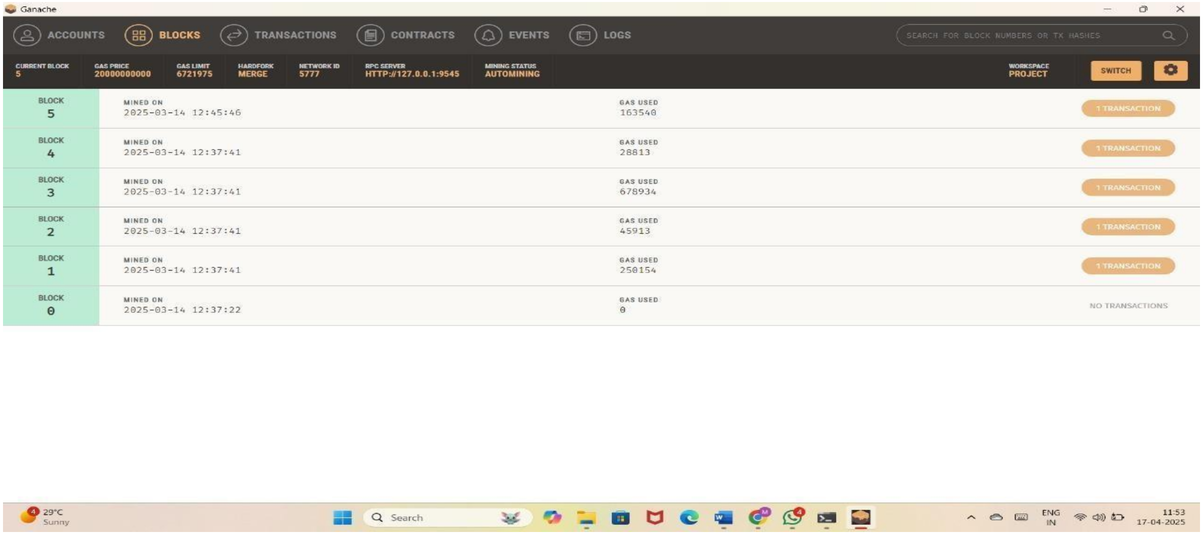
Fig 7.3 Candidate registration



E-Voting System Using Ethereum Blockchain

Candidate ID	Candidate Name	Party	constitution	Total Votes Received
1	Ajith	BJP	Jayanagar	1

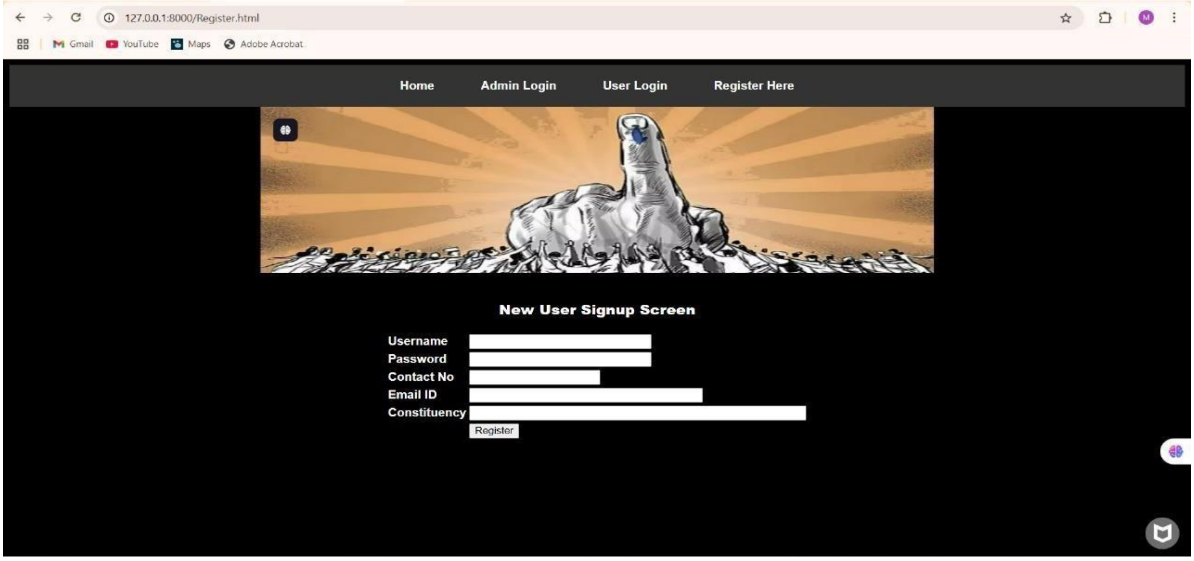
Fig 7.4 Total votes count



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
5	20000000000	6721975	MERGE	5777	HTTP://127.0.0.1:9545	AUTOMINING	PROJECT

BLOCK	MINED ON	GAS USED	
5	2025-03-14 12:45:46	163540	1 TRANSACTION
4	2025-03-14 12:37:41	28813	1 TRANSACTION
3	2025-03-14 12:37:41	678934	1 TRANSACTION
2	2025-03-14 12:37:41	45913	1 TRANSACTION
1	2025-03-14 12:37:41	250154	1 TRANSACTION
0	2025-03-14 12:37:22	0	NO TRANSACTIONS

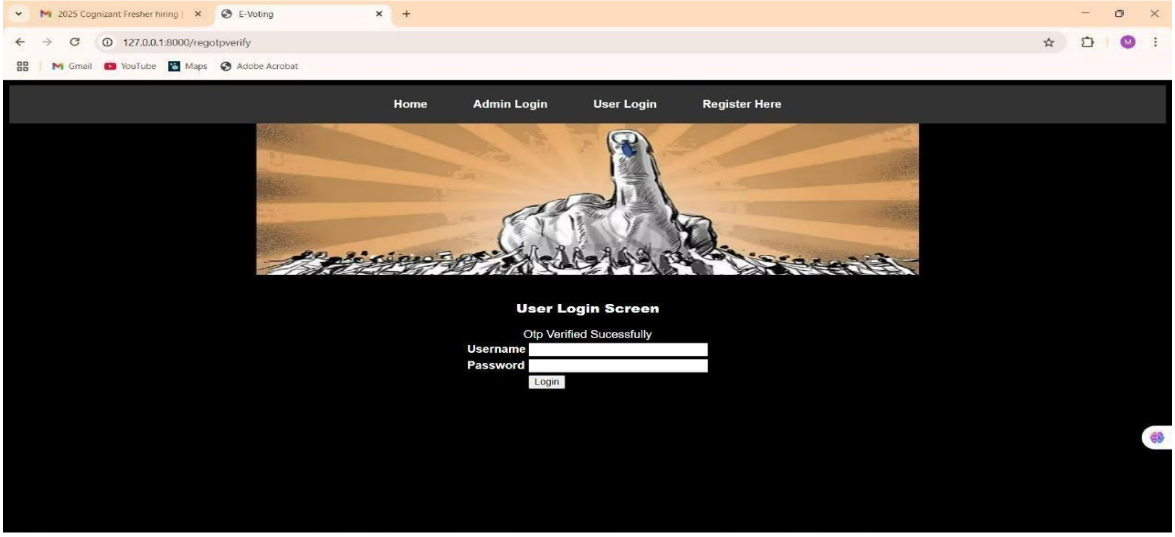
Fig 7.8 Blocks of Transaction



New User Signup Screen

Username
Password
Contact No
Email ID
Constituency

Fig 7.9 Signup page

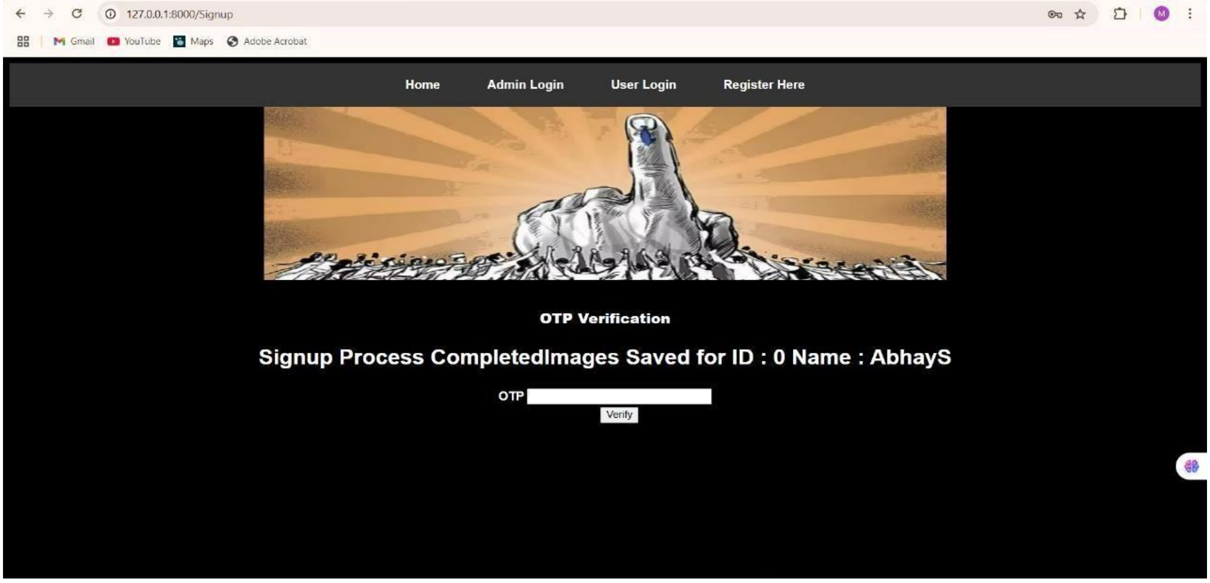


User Login Screen

Otp Verified Sucessfully

Username
Password

Fig 7.10 User Login screen



OTP Verification

Signup Process CompletedImages Saved for ID : 0 Name : AbhayS

OTP

Fig 7.11 OTP authentication for user

VI.CONCLUSION

The implementation of an effective information system, as explored in this study, demonstrates the transformative impact of technology on organizational efficiency, communication, and decision-making. By analyzing the practical aspects of system design, stakeholder involvement, and phased execution, it becomes evident that a structured approach is critical to the success of any technological deployment. The project highlights the importance of aligning system capabilities with user needs, ensuring that the solution not only addresses current challenges but is also scalable for future demands.

Furthermore, the evaluation of system functionalities, performance metrics, and postimplementation feedback reinforces the necessity of continuous monitoring and adaptation.

The involvement of end-users, IT professionals, and management throughout the lifecycle of the implementation fosters a sense of ownership and promotes smoother adoption. Risk management strategies and the incorporation of feedback loops also emerged as vital components in mitigating disruptions and enhancing system robustness.

Ultimately, this implementation serves as a model for future endeavors, providing valuable insights into best practices and common pitfalls. It underscores the significance of strategic planning, cross-functional collaboration, and user-centric design in achieving successful outcomes. By focusing on both technical and human factors, organizations can maximize the return on investment and ensure the long-term sustainability of their information systems.

Reference

[1] Parmar, P., & Dewangan, A. K. Design and Implementation of Blockchain-Based E-Voting System Using Ethereum. IEEE ICBC. https://ieeexplore.ieee.org/document/9461141

[2] Nguyen, K. C., Singh, A. K., & Kumar, R. Blockchain-Based E-Voting System with Biometric Security. IEEE ISCC.https://ieeexplore.ieee.org/document/95519 75

[3] Mittal, P., & Singh, J. Enhancing Voting Transparency Using Blockchain Technology. IEEEBigData. https://ieeexplore.ieee.org/document/9671770

[4] Liu, Y., Lu, K., & He, W. Face Recognition Algorithms for Biometric Authentication in Secure Systems. IEEE Transactions on Information Forensics and Security.https://ieeexplore.ieee.org/document/9336219

[5] Chaudhary, M., & Garg, R. Blockchain-based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach. IEEE Access. https://ieeexplore.ieee.org/document/10036445

[6] Park, S., Choi, J., Kim, J., & Oh, H. zkVoting: Zero-knowledge proof based coercion-resistant and E2E verifiable e-voting system. Cryptology ePrint Archive. https://eprint.iacr.org/2024/1003

[7] Sarier, N. D. Efficient and Usable CoercionResistant E-Voting on the Blockchain. Cryptology ePrint Archive. https://eprint.iacr.org/2023/1509

[8] Yin, Z., Zhang, B., Nastenko, A., Oliynykov, R., & Ren, K. A Scalable Coercion-resistant Voting Scheme for Blockchain Decision-making. Cryptology ePrint Archive.https://eprint.iacr.org/2023/1578

[9] M. Swan, Blockchain: Blueprint for a New Economy, 1st ed. Sebastopol, CA:O'ReillyMedia,2015. https://www.google.co.in/books/edition/Blockchai n/4vFiBgAAQBAJ

[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: Dec. 8, 2024]. bitcoin.pdf

[11] K. Zhang, J. Li, K. Zhang, and W. Yang, "A Blockchain-Based Secure Voting System," in Proceedings of the IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2019, pp. 541-545. https://link.springer.com/chapter/10.1007/9 78-981-97-8537-7_15

[12] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," 2014.[Online].Available: https://arxiv.org/abs/1407.3561. [Accessed: Dec.8,2024]. https://arxiv.org/abs/1407.3561

[13] K. Jain, P. Flynn, and A. Ross, "Handbook of Biometrics," New York, NY: Springer, 2007. Handbook of Biometrics | SpringerLink

[14] D. Chaum, R. Carback, J. Clark, and B. Essex, "Scantegrity: End-to-End Voter Verifiable Optical-Scan Voting," IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 611–627, Dec.2009.Scantegrity- End-to-End-VoterVerifiable-Optical-Scan-Voting.pdf

[15] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," in Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, 2016, pp. 1-4. cachin_dccl.pdf