Volume-09 Issue 03, March-2025 ISSN: 2456-9348
Impact Factor: 8.232

iJETRM

International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

SECUREVOTECHAIN: A DECENTRALIZED BLOCKCHAIN BASED VOTING SYSTEM

Taha Aheras,
Sahil Sapkal,
Shadab Mansuri,
UG Students, Department of Information Technology,
D.Y. Patil College of Engineering, Akurdi, Pune.
Jarvis78ai@gmail.com, sahilsapkal1133@gmail.com, mansurishadab495@gmail.com

ABSTRACT:
The SecureVoteChain is an approach to blockchain technology that helps in the creation of a secure electronic voting solution: highly transparent and user-friendly. Built on the MERN stack, it uses a decentralized ledger to address traditional election challenges by making each vote immutable and verifiable for the elimination of risks like tampering and enhancing trust among the public. Its system includes OTP verification (One-Time Password) to limit voting to eligible users while increasing security.

The application is being developed as a multilingual application to make it more accessible and inclusive for the broad Indian audience. Such feature will enable voters to have a mutually understandable and usable voting experience despite different native languages people may speak, and thereby enables more people to engage in voting confidently. Keeping in view this scenario, SecureVoteChain promises a scalable trustworthy e voting system that is readily available and ensures democratic participation in various regions by implementing user-friendly, multilingual interface, OTP verification, and blockchain's transparency.

I. INTRODUCTION

SecureVoteChain: A Decentralized Blockchain-Based Voting System will introduce a new, secure approach to electronic voting that involves a solution for various difficulties encountered in traditional and electronic voting systems. These include tamper susceptibility, lack of transparency, as well as poor accessibility, which can be offered by each vote through decentralized blockchain distributed ledger to be recorded and verifiable securely by all for the integrity of the electoral process. Built with the MERN stack, consisting of MongoDB, Express.js, React, and Node.js, SecureVoteChain gives users cutting-edge technology combined with user-friendly features to have the most ideal voting system that marshals both security and inclusiveness.

The blockchain is at the core of SecureVoteChain, as it offers a decentralized and distributed ledger for the storage of votes. Recording votes as transactions in the blockchain ensures that after voting, it is not possible to alter or delete them without network consensus. That kind of immutability and transparency will form the core on which public trust will be built because every vote is publicly verifiable while anonymous. Decentralization also negates the need for a single authority to control or manage the election, reducing the risks of fraud or unauthorized interference. Due to its decentralized nature, blockchain technology makes the system hacked-proof, thus further improving the overall security of the system.

The most critical feature of SecureVoteChain is called OTP (One-Time Password) verification, thereby enhancing the authentication of users. An electorate with a registered voter is provided with a one-time OTP through SMS or email to be used for entrance into the voting platform. It checks on someone's identity and gives protection against unauthorized entry into the software. The layer of OTP verification amalgamated with the tamper-resistant ledger of blockchain forges a dual-layered security framework that addressed the voter fraud concerns, such that only verified people could participate in the process.

The SecureVoteChain is going to be a multilingual application; its design is with a high affinity to benefit a vast mix of people from India. Linguistic diversity in India acts as an impediment toward significant accessibility of digital solutions for such civic platforms like the voting process. The SecureVoteChain platform envisions ease in access for the different speakers of languages to participate in the process of voting. This will not only provide wider outreach across regions for the platform but also enable citizens with diverse linguistic backgrounds to be more confident while interacting, thus improving voter turnout and efficiency. It will ensure that the multilingual interface helps guide voters through all voting processes in their preferred language and thereby the platform is accessible and understood to the users across India's diverse regions.

This is a MERN technology stack particularly well-suited towards developing an e-voting platform that's responsive, scalable, and adaptable. This is because the demand for creating an intuitive and interactive interface that offers users an extremely accessible way of voting with smooth functionality on all devices leads to the use of React. MongoDB provides a great database structure as it captures voting data in view ahead of great elections in its efficient handling and storage. All this activity becomes possible using Node.js and Express.js, supporting smooth and secure backend handling of live transactions as well as data requests.

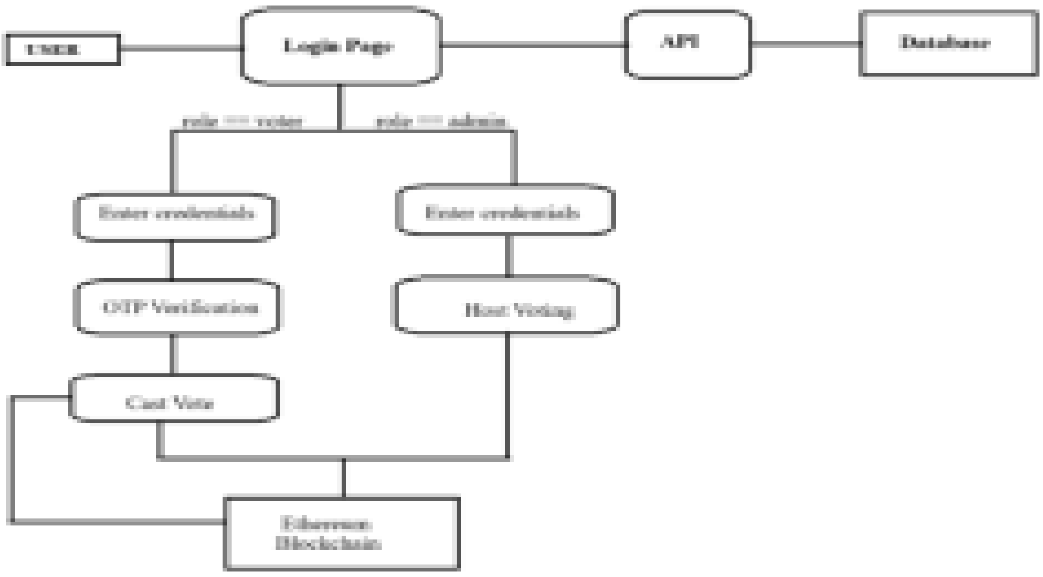
Integrating blockchain technology, OTP verification, and a multilingual interface, SecureVoteChain hopes to redefine the Indian voting process as a secure, transparent, and inclusive process of voting in the future. Its decentralized, tamper-proof blockchain establishes the much-needed foundation for an assured safety feature. Its 'user-centric features' ensure its availability to many more people who might not have voted without any barriers coming their way in conventional voting systems. In other words, this project is looking towards simplifying a

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

scalable solution to on issues of security so that people of different linguistic backgrounds can be confident enough in participating in democratic processes hence the need for more inclusive and transparent voting systems.

II. SYSTEM ARCHITECTURE

Decentralized blockchain-based voting system SecureVoteChain Architecture The system aims to deliver all the security, transparency, and usability that a successful voting experience requires. Blockchain integration with OTP verification using an elaborate role-based access structure provides both security and openness as follows. Taking the system components and workflow as based on the given diagram:



System Architecture

1. Login and authentication of the user

- User Role: The process will start from the user as it can be a voter or an administrator. And all the users require login to the system. So, he inputs his details authenticated through the login page.
- Login Page/Login Interface: Login page is the entry point of users. Inside the page, credentials are entered by the users and checked with the database. This login page communicates with some type of API to access the database and validate the credentials from the database.
- Database Validation: The login page sends a request to the API for the validation of the user's credentials. The API acts as a middle man between the login page and the database. While data is fetched and sent across as and when it's required, when valid user credentials are obtained, it lets access into the procedure ahead of that step, being the OTP verification.

2. OTP Verification

OTP - Security Layer: This is a security layer that ensures only registered users can vote or otherwise go ahead with the access of administrative functions using the One-Time Password verification. The OTP will then be forwarded to the user's registered contact information, which includes SMS or email after successful login.
- Verification Process: Verifies the authenticity by entering an OTP. Therefore, very much verification is there so that access to unintended people cannot be allowed and only authenticated users move further and get confirmed in the system.
- In case of Role-Based Access Control, it authenticates his role after authenticating the OTP. This system has allotted each user with a role as either "voter" or "admin" according to the role one wants to access the data in the system.

3. Role-Based Pages: Voter Page and Admin Page

- Voter Role:
- Voter Page: If the user's role is a voter, he will be taken to the voter page. It will then display the candidate available to vote on which the user can vote and submit it securely.

This means that in blockchain, the transaction is added as soon as a vote is captured and ensures that it's stored without any kind of tampering, and at the same time, its public verifiability without compromising one's privacy in individual voters.
- ADMIN ROLE:

Admin Page: If the user's role has been identified to be an admin, then the user should be taken to the admin page. An administrator is vested with certain privileges. This includes status in the voting process, blockchain transaction, and control over the election process.

— Blockchain Monitoring: The admins are able to monitor and authenticate each transaction added to the blockchain. This ensures that the voting process remains accountable in that the identity of the system's integrity can be seen in real time.

4. Blockchain Integration: Ethereum Blockchain

Decentralized Ledger; each vote is recorded as a transaction on the Ethereum blockchain. Blockchain technology is decentralized and immutable ledgers. Therefore, once the votes are recorded, it is impossible to change or delete any one entry, which significantly enhances a greater level of security and transparency since anyone can verify whether the results have an integrity attribute.

Immortal Transactions: The vote once inculcated in the blockchain, cannot be deleted or modified. Every transaction- in the specific case, a vote- is chained unto the previous one such that the record chain is very secure and tamper-proof. - Transparency and Verifiability: Blockchain technology makes voting transparent, because all the votes are publicly recorded. The voters' identities may remain secret, but the count is verifiable by all parties involved, which gives everyone adequate trust in the outcome of the election.

5. Database and API Layer

Database Storage: The database stores all the very important account information of the users, including login credentials and OTP verification, thus working as the core storage of the application from where the user records are safe.

- API Communication: The API services the entire request communication between all frontend components (login page, OTP verification, voter/admin page) and the database, ensuring smooth data transfer security while in transit. This includes valid responses with checking and validation of credentials for other backend processes as well as digit generation for the OTP.

6. User Workflow in SecureVoteChain

- Step 1: Login

The system verifies the login credentials entered by the user on the login page using the API and the database.

- Step 2: OTP Verification

The system provides the user with an OTP in case he logs in properly. While filling this OTP, his actual identity is verified and extra security is achieved.

- Step 3: Role Assignment

OTP authenticates the user after successful verification. Depending upon this role, the system takes him/her either to the voter page or admin page.

- Step 4: Voting/Monitoring via Admin End

On this page, the voter will vote. Meanwhile, for administrators, their version in the process of voting is the admin page meant for tracking.

- Blockchain Transaction: Step 5

This will make each vote recorded on a safe and transparent blockchain using the Ethereum.

7. Multilingual Support Pursuing Inclusivity

The platform is multilingual; therefore, SecureVoteChain allows the user to navigate through the system in the language in which he or she is comfortable. As a result, people belonging to different linguistic backgrounds would be able to participate better in the voting process. The country of India is also linguistically diversified, and more voters might be comfortable working with technology in their native tongue.

8. Secrecy, Transparency, and Access

- Improved Security: By using OTP verification and blockchain, SecureVoteChain offers a double-layer security that ensures only a verified user can vote-and vote-securely and store -.
- Transparency: Blockchain is transacted in a completely open manner. Here, though the voting person's vote remains anonymous, the count of the total votes is verifiable, thus increasing public confidence in the process. Reach More People: The multilingual interface may reach out to people of other regions and languages which may make them participate in a greater number.

III. Literature Survey

- Decentralized Trust Management for E-Voting: The paper "Blockchain-Enabled Decentralized Trust Management and Secure Voting System" by R. I. Minu and G. Nagarajan has a decentralized voting system. This system relies on blockchain to decentralize trust management. Thus, it builds trust among users through interactions that are recorded open on the blockchain. The voting system is further made completely independent of any central authority due to smart contracts, making voting results tamper-resistant and auditable. The authors argue that this decentralized system increases accountability and allows voters to cast their votes in safety, without intermediaries as practiced traditionally, and thus increases public trust in the electoral process.

- Smart Contract Implementation in Blockchain Voting M. Mahalakshmi, Vedant Bhatnagar, and Kumar Adarsh Pandita introduce an e-voting model based on Ethereum "Decentralizing Voting: Blockchain-based E-Voting System Using Ethereum Smart Contracts." Such a model simply brings the suggestion that smart contracts may create automatic and improve voting while leaving the electronic vote process secure, and every counted vote is a transaction within smart contracts recorded in the blockchain. This model reduces the probability of errors, and it also removes the dependency on third parties. Here, the authors further elaborate on how blockchain can make elections autonomous and secure using smart contracts from Ethereum. Paper Theme: Improving voting systems through smart contracts with full potential to make them reliable, simplified and secured electronic voting systems.

- Federated Learning and Trust in IoT Voting Environments: In their research work, Bi, Muazu, and Samuel focus in the area of trust management in the IoT environment by the paper "Decentralized Federated Learning Trust Management System for IoT." Although targeted mostly towards IoT, the principles of the system are applied in blockchain based voting; hence, their model applies federated learning in the management of trust between the network of devices to ensure that all interactions are secure and transparent. This model, as in the voting system, can be equivalent to a similar decentralized model: IoT devices such as what are used may safely communicate with each other and exchange information. This framework enables the system through distributed; to verify that in a secure environment the votes have accuracy and integrity and thus demonstrates the power of blockchain concerning interaction-requirements high environments.

- Transparency and Accountability in Blockchain Voting: From these articles, it is observed that transparency is the big advantage of this blockchain-based voting system. Minu and Nagarajan in "Blockchain-Enabled Decentralized Trust Management and Secure Voting System" emphasize how the above transparency increases the sense of accountability. By considering every vote as a transaction reflected on the blockchain, voters as well as officials may verify that votes were correctly cast. In like manner, Mahalakshmi et al. demonstrate blockchain's immutable character supports public confidence through independent verification of voting results. The transparency of that helps prevent cases of election fraud and establishes a greater degree of trust in the voting process, which is essential for democratic participation.

- Privacy and security issues Although blockchain may provide openness, each of the documents addresses the issue of keeping voters' secrets. Minu and Nagarajan, "Blockchain-Enabled Decentralized Trust Management and Secure Voting System," explain privacy-type solutions like zero-knowledge proofs to facilitate verification without revealing an identity of a voter. Mahalakshmi et al., whose system uses Ethereum, clearly emphasize safeguarding private information and keeping confidential data on a public chain.

- Such studies indicate that, though blockchain ensures safe records, balancing privacy with transparency is crucial while maintaining the concept of voter anonymity and data protection.

- Scalability Issues in Blockchain Voting: Most of the studies state that one of the major concerns is scalability. Mahalakshmi, Bhatnagar and Pandita point out that Ethereum's PoW will be inefficient for large-scale elections as it reduces the voting speed in "Decentralizing Voting: Blockchain-based E Voting System Using Ethereum Smart Contracts." Further, Minu and Nagarajan mention that the higher the numbers of transactions in the blockchain, the higher the cost and time both in computation. They propose alternative consensus models for scaling up, such as proof of stake. Both come to conclude that addressing all these limitations is important toward realizing large scale, blockchain-based elections.

- Decentralizing Voting Potential: Blockchain-based E-Voting System Using Ethereum Smart Contracts, Mahalakshmi et al. argue that blockchain is helpful for remote access; citizens in far-off or underdeveloped areas can vote. In this regard, the decentralized model of Minu and Nagarajan also supports access by providing a platform that may be safely accessed through online. These include ways whereby blockchain-based voting systems might help in supporting more voters by prospective broader voter participation, especially for people with physical, geographic, or other barriers.

- Cost considerations and implementation challenges: Nevertheless, the implementation of blockchain voting systems is expensive. Minu and Nagarajan elaborate on these concerns in "Blockchain-Enabled Decentralized Trust Management and Secure Voting System," highlighting the point that initial deployment and maintenance costs for blockchain networks may be expensive. Mahalakshmi et al. present even greater challenges in the task of educating public people and government officials. Most ideas consider pilot programs coupled with collaboration with experts in technology would ease these challenges and more would be adopted into using various systems. Educating stakeholders about blockchain's benefits alongside its limitation will help to have a smooth transition into blockchain voting systems.

IV. CONCLUSION

The SecureVoteChain project thus provides new way voting with precedence for security, transparency, and accessibility for a wide Indian audience. By using blockchain, each vote is recorded safely, cannot be altered in any respect, and is verifiable with ease, thereby instilling confidence in the very process of voting. There will be an OTP verification for participation from authorized voters only, thus guarding against intruders and frauds. The multilingual design accommodates people from different backgrounds in terms of language with ease, thus making this voting process more inclusive and easier to access for people around India. SecureVoteChain is a combination of both powerful technology and accessibility in providing a safe and straightforward method of voting through a user friendly interface built on the MERN stack.

SecureVoteChain, through this project, will support the cause of fair and transparent elections wherein every

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

vote counts and democratic participation is strengthened across regions and languages. This platform is a step forward to construct a trustworthy voting platform that can be easily accessed.

V. REFERENCES

1. "Blockchain-Based Secure Electronic Voting System" by Zheng Li, Yun Li, and Jie Wu (2022), published in IEEE Access.
2. "Secure and Transparent Voting System Using Blockchain Technology" by Abhishek Kumar, Priyanka Sharma, and Satish Chand (2022), published in Journal of Blockchain Research and Applications
3. "Blockchain-Based Electronic Voting System for Secure and Transparent Elections" by Sunanda Das, Arpan Kumar Kar, and Partha Pratim Chaudhuri (2022), published in IEEE Transactions on Engineering Management
4. "Secure and Verifiable Blockchain-Based Voting System" by Syed Taha Ali, Vipul Kashyap, and Marthie Grobler (2022), published in IEEE Transactions on Information Forensics and Security
5. "Secure and Reliable Blockchain-Based Electronic Voting System" by Soumya Ranjan Jena, Rajesh Kumar Tiwari, and Ashish Kumar Luhach (2022), published in IEEE Transactions on Engineering Management
6. "Blockchain-Based Secure and Transparent Voting System" by Ananya Bhattacharya, Subhadeep Bhattacharya, and Subhasis Chaudhuri (2022), published in IEEE Transactions on Dependable and Secure Computing.
7. "Secure and Transparent Blockchain-Based Voting System" by Aditya Chaudhary, Neha Gupta, and Sunil Kumar (2022), published in IEEE Transactions on Engineering Management.
8. "Secure and Auditable Blockchain-Based Voting Platform" by Shashank Verma, Ishaan Malhotra, and Nisha Gupta (2023), published in IEEE Transactions on Engineering Management