IJCRT2405804 | International Journal of Creative Research Thoughts (IJCRT)www.ijcrt.org | h385

DECENTRALIZED VOTING SYSTEM

Prachit Kanwar, Parv Jain, Mukund Khandelwal, Naman Acharya

Department Of Computer Science and Engineering, Acropolis Institute of Technology and Research, Indore, Madhya Pradesh, India.

I. ABSTRACT

This project explains about decentralized voting system for conducting elections is a revolutionary approach designed to ensure accessibility, transparency, and impartiality in the electoral process. By leveraging blockchain technology and secure cryptographic techniques, this system allows voters to cast their ballots remotely, eliminating the need for physical polling locations. Each vote is securely recorded on an immutable and transparent ledger, preventing tampering or fraud. Furthermore, the decentralized nature of the system means that it is not controlled by any single entity, reducing the potential for bias or manipulation. This innovative voting system holds the promise of greater inclusivity, integrity, and trust in the democratic process, making it a vital tool for modernizing elections and ensuring fair representation.

II. INTRODUCTION

A decentralized voting system, implemented as a decentralized application (Dapp) using web technologies, represents a pioneering solution for conducting fair and secure elections online. Unlike traditional voting systems, which often rely on centralized authorities and paper ballots, a decentralized voting Dapp leverages the power of blockchain technology to create a transparent, tamper-resistant, and trustless voting process. Key features that set it apart from its conventional counterpart include cryptographic security to protect voter privacy, immutable ledger for transparent and auditable results, elimination of intermediaries, and accessibility from anywhere with an internet connection. This innovative approach not only enhances the integrity of the electoral process but also increases inclusivity and convenience for voters, potentially revolutionizing the way we participate in democratic decision-making.

Key features:
1. Trust and Transparency
2. Accessibility
3. Anonymity
4. Immutable records
5. Real-time results
6. Decentralization

III. METHODOLOGY

This application is implemented via visual studio code platform or remix IDE (open-source IDE) to write smart contracts and deploy. With NodeJS (NPM packet manager) for server-side development and using solidity (smart contract language) for storing records on blockchain, for frontend we will use HTML and CSS for designing the layer of interaction for the voter and we will use react framework to make it more interactive and the other dependencies are Web3.js, hardhat and meta mask wallet.

1. Node.js: - Node.js is an open-source runtime environment that allows developers to execute JavaScript code outside of a web browser. It is built on the V8 JavaScript engine and provides a server-side platform for building scalable and high-performance applications. Node.js is known for its non-blocking, event-driven architecture, which makes it particularly well-suited for building real-time, data-intensive applications like web servers, APIs, and microservices. Its extensive package ecosystem, powered by npm (Node Package Manager), offers a wide range of libraries and modules, making it a popular choice for web development and other server-side applications. Node.js has gained widespread adoption and popularity for its ability to streamline the development process by enabling both server-side and client-side code to be written in the same programming language, JavaScript.

2. Hardhat: - Hardhat is a popular development framework and toolset for Ethereum developers. It is designed to simplify the process of building and deploying smart contracts on the Ethereum blockchain. Hardhat offers a range of features and capabilities, including a built-in Ethereum development network, automated testing, and a comprehensive set of development tasks. It also supports integration with other Ethereum development tools and libraries, making it a versatile choice for building decentralized applications (Dapps) and interacting with the Ethereum blockchain. With its robust functionality and developer-friendly environment, Hardhat has become a valuable tool for those looking to streamline the Ethereum development process and ensure the reliability and security of their smart contracts.

3. Remix IDE: - Remix IDE is a popular integrated development environment (IDE) for Ethereum blockchain development. It provides a user-friendly and web-based platform for creating, testing, and deploying smart contracts and decentralized applications (Dapps) on the Ethereum network. Remix offers a range of features, including a code editor, a Solidity compiler, a debugger, and a web3 provider, making it a comprehensive tool for Ethereum developers. It simplifies the development process by offering a real-time development environment with built-in testing capabilities and easy deployment options, ultimately streamlining the creation of Ethereum-based projects.

4. MetaMask: - To use blockchain we must connect to it. We'll have to install a special browser extension to use Ethereum blockchain. we'll be able to connect our local Ethereum blockchain with our personal account and interact with smart contract.
IV. SURVEY OF EXISTING SYSTEMS

1. Nir Kshetri Proposed System:

Introduction:

The Concept of Treating Voters as Wallets and Candidates as Receivers: Kshetri's e-voting approach introduces the concept of treating each voter as a wallet and candidates as receivers. In this system, voters hold digital tokens, akin to cryptocurrencies, which they can allocate to their preferred candidates. This innovative approach aims to bring the benefits of blockchain technology into the voting process.

Limitations:

Despite its innovative features, Kshetri's e-voting approach has several limitations. These include:

1. Limited Decentralization: The system's lack of decentralization limits its potential for secure and transparent voting on a larger scale.

2. Lack of Consensus Mechanism: The absence of a clear consensus mechanism raises concerns about the reliability and integrity of the voting process.

3. Applicability to a Single Location: The approach's applicability is confined to a single location or organization, which restricts its utility for broader electoral contexts.


2. Fridrik Proposed System:

Introduction:

Fridrik delved into the possibilities of blockchain technology, with a specific focus on utilizing Go-Ethereum Proof-of-Authority (POA) for bolstering the security and cost-effectiveness of national elections. The study explored a novel approach that employs identity-based stake and district nodes to validate and record votes on a blockchain, offering several advantages, such as a developer-friendly framework and centralized consensus. This innovative approach aimed to address critical issues in traditional election systems, such as transparency, security, and accessibility.

Limitations:

1. Scalability Concerns:

One of the primary limitations of using Go-Ethereum Proof-of-Authority for national elections is its inherent scalability constraint. The system can handle a limited number of transactions per second, which in this case, translates to a restriction on the number of votes that can be processed in each timeframe. The study revealed that the system's capacity was limited to around 5000 votes per second, which may be insufficient for large-scale national elections. To accommodate a significantly higher number of voters, a more scalable blockchain framework would be necessary.
2. Centralized Consensus:

While the use of Proof-of-Authority brings benefits like faster transaction validation and lower energy consumption, it also comes with the drawback of centralization. In this approach, a limited number of authorities are responsible for validating transactions and maintaining the blockchain, potentially raising concerns about single points of failure and the concentration of power. Critics might argue that a centralized consensus mechanism can undermine the democratic ideals of elections, where decentralization and security are paramount.

3. Identity Verification Challenges:

The approach discussed in the case study relies on identity-based stake and district nodes for vote validation. While this can enhance the integrity of the election process by ensuring that each voter is a legitimate participant, it also introduces challenges related to identity verification. The accuracy and security of the identity verification process must be rigorously maintained to prevent identity theft and fraud, which can be complex and costly to manage.

4. Adoption and Infrastructure:

Implementing blockchain technology for national elections requires a significant overhaul of existing infrastructure and processes. This includes ensuring that voters have access to the necessary technology and are comfortable using it, addressing potential cybersecurity threats, and dealing with legal and regulatory challenges. The study did not delve into these aspects, which can be substantial barriers to adoption.

3. Zhang's Proposed System

Introduction:

Zhang's proposed blockchain-based local voting mechanism represents a promising advancement in the realm of decentralized decision-making processes. By harnessing blockchain technology, it aims to not only enhance the integrity and transparency of local voting but also protect privacy and detect cheating. This innovative approach leverages distributed consensus algorithms, seamlessly integrates with smart contracts and peer-to-peer networks, and incorporates a two-phase validation process, which holds the potential to revolutionize how communities and organizations make decisions. However, while the concept shows great promise, it is essential to recognize its limitations and areas where further research and development are needed.

Limitations:

1. Lack of Efficacy Proof: One of the primary limitations of Zhang's proposed mechanism is the absence of empirical evidence or real-world implementations to demonstrate its efficacy. While the concept is sound in theory, its performance and reliability need to be rigorously tested in practical scenarios.

2. Compatibility with Blockchain Frameworks: The proposal, as described, has not been tested with a wide range of blockchain frameworks. Different blockchain platforms have distinct characteristics and scalability, and the mechanism's compatibility and performance may vary across these platforms. Evaluating its
effectiveness across different blockchain frameworks is crucial to ensuring its broad applicability.

3. Transaction Throughput: Blockchain networks, especially those built on public blockchains like Bitcoin and Ethereum, often suffer from limited transaction throughput. While the proposed mechanism may offer enhanced privacy and cheating detection, it may not be suitable for applications requiring high transaction processing speed. Faster blockchain frameworks or layer 2 scaling solutions might be necessary to address this limitation.

V. Conclusion

In this project, we introduced a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient elections while guaranteeing voters privacy. It offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain. To this end, we believe an effective model to establish trustworthy provenance for e-voting systems will be crucial to achieve an end-to-end verifiable e-voting scheme.

VI. References