**Secure Vote - A Decentralized Voting System using React and Web3**

**PROJECT SYNOPSIS**

OF MAJOR PROJECT

**BACHELOR OF TECHNOLOGY**

## CSE

SUBMITTED BY

Name: Md Armaan Ansari

University Roll no.: 2100290100096

Class Roll no.: 30

Batch: 2021-25

Team members: Sion Chowdhary (CSE)

Ashish Gupta (CS)

August 2022



## **KIET Group of Institutions, Delhi-NCR,**

## **Ghaziabad (UP)**

## **Department of Computer Science and Engineering**

**Table of Contents**

|  |  |
| --- | --- |
| **Content** | **Page no.** |
| Introduction | 3 |
| Rationale | 4 |
| Objectives | 5 |
| Literature Review | 6-8 |
| Feasibility Study | 9 |
| Methodology/Planning of Work | 10 |
| Facilities required for proposed work | 11 |
| Expected Outcomes | 11 |
| References | 11 |

**Introduction**

In today's technologically driven world, ensuring the integrity and security of voting systems is of paramount importance. Traditional voting methods have their limitations and are susceptible to various issues such as fraud, tampering, and lack of transparency. To address these challenges, this project proposes the development of a decentralized voting system called "Secure Vote" using modern technologies like React and Web3.

The Secure Vote system aims to leverage blockchain technology and smart contracts to provide a secure, transparent, and tamper-proof platform for conducting elections. By implementing end-to-end encryption, identity verification, and decentralized storage, the system aims to enhance the trustworthiness of the voting process and encourage greater participation from the electorate.

**Rationale**

Traditional voting and polling methods are often plagued by issues related to security, transparency, and trust. Paper-based systems are vulnerable to fraud, and electronic voting systems are susceptible to hacking. Project SecureVote aims to address these challenges by harnessing the security features of blockchain technology. Blockchain ensures that every vote is secure, immutable, and tamper-proof, offering a new level of trust in the electoral process.

Ethereum, one of the most established and widely adopted blockchain platforms, serves as the foundation for SecureVote. Its smart contract capabilities enable the creation of a decentralized, transparent, and efficient voting system. Ethereum's security model, consensus algorithms, and robust developer ecosystem make it an ideal choice for our project.

One of the core principles of blockchain technology is immutability. Once a vote is recorded on the Ethereum blockchain, it cannot be altered or deleted. This immutability ensures that the results of elections and polls remain tamper-proof and transparent, reinforcing trust in the electoral process.

The SecureVote platform is designed to be user-friendly and accessible to a wide range of users, regardless of their technical expertise. We aim to make the voting process as simple and intuitive as possible, ensuring that every eligible voter can participate in elections and polls without barriers.

**Objectives**

With the help of this project, we wish to achieve the following major objectives:

1. Security: To provides a secure network through anonymity and privacy preservation as it encrypts digital identity using a hash algorithm and public-key cryptography.
2. Establish a Secure and Immutable Voting System: Our first and foremost objective is to create a voting system that is inherently secure and immutable. By leveraging the Ethereum blockchain, we will ensure that every vote cast on SecureVote is tamper-proof and resistant to fraud. This foundational security is essential to building trust in our platform.
3. Enable Transparent and Trustworthy Elections: Transparency is a cornerstone of SecureVote's objectives. We aim to provide a platform where the entire voting and polling process is transparent, from voter registration to result declaration. This transparency will reinforce trust in the electoral process and encourage participation.
4. Foster Decentralization and Trust lessness: We are committed to fostering decentralization and trust lessness in the voting process. Our objective is to create a platform that eliminates the need for centralized authorities, ensuring that voters have direct control over their votes and minimizing the potential for manipulation or bias.

**Literature Review**

**1)** **Secure Digital Voting System based on Blockchain Technology**

Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan

Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Blockchain CORE Metadata, citation and similar papers at core.ac.uk Provided by UWL Repository allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks (Rosenfeld, 2017; Kadam et al, 2015; Nakamoto, 2009). Each block is assigned a cryptographic hash (which may also be treated as a finger print of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains (Nakamoto, 2009; Kraft, 2015; Narayanan et al, 2015). Bitcoin remains the most distinguished application of blockchain however researchers are keen to explore the use of blockchain technology to facilitate applications across different domains leveraging benefits such as non-repudiation, integrity and anonymity. In this paper, we explore the use of blockchain to facilitate e-voting applications with the ability to assure voter anonymity, vote integrity and end-to verification. We believe e-voting can leverage from fundamental blockchain features such as self-cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records. The blockchain technology can play key role in the domain of electronic voting due to inherent nature of preserving anonymity, maintaining decentralized and publicly distributed ledger of transactions across all the nodes. This makes blockchain technology very efficient to deal with the threat of utilizing a voting token more than once and the attempt to influence the transparency of the result.

Electronic voting has been an area of research focus for many years by using computing machines and equipment for casting votes and producing high quality and precise results in accordance with the sentiments of the participating voters. Various attempts have been adopted in practice to support election process. Initially computer counting system allowed the voter to cast vote on papers. Later on, those cards went through the process of scanning and tallying at every polling cell on a central server (Kadam et al, 2015; Rockwell, 2017; Hao et al, 2010). Direct Recording Electronic (DRE) voting systems were put in place later on which were admired and acknowledged greatly by the voters in-spite of the resistance from computer scientists. If the voting system is well understood by the voters, the system’s usability can be increased remarkably. DRE systems in particular have gathered a lot of successes in bringing the voters to use this technology

**2****) Blockchain based E-voting System**

Albin Benny, Aparna Ashok Kumar, Abdul Basit, Betina Cherian and Amol Kharat

Voting System: The voting system can be considered as a replacement for EVM.It is a decentralized app with a front-end in Bootstrap or Html and a Blockchain in back-end. The smart contract is written in solidity language. The candidate’s name with symbol of candidate is mentioned in smart-contract. A smart contract is the actual logic piece of entire voting system. Each and every change made in a blockchain is called a Transaction. Transaction is the way, by which the external world interacts with the Ethereum network. Transaction is used when we wish to modify or update the state stored in the Ethereum network. Each Transaction requires a transaction fee or service charge. Within an Ethereum network circulates a native currency: ether.

Registration System: A voting registration System is developed using Html/Css front-end and SQL back-end which contains the user's personal details already stored for eg: One can consider this as an Aadhar database. A biometric device would be used for validation purpose. If the user is a valid user then he/her is handed a hash code /address which is used as a credential for login into the voting machine.

**3)** **Blockchain technology-based e-voting system.**

Prof. Anita A. Lahane, Junaid Patel, Talif Pathan1, and Prathmesh Potdar.

Limitations of Existing system or Research gap

Recent major technical challenges relating to e-voting systems embody, however not restricted to secure digital identity management. Any potential citizen ought to are registered to the electoral system before the elections. Their data ought to be during a digitally processable format. Besides, their identity data ought to be unbroken non-public in any involving info. ancient E-voting system might face following problems:

• **Anonymous vote-casting**: Each vote may or may not contain any choice per candidate, should be anonymous to everyone including the system administrators, after the vote is submitted through the system.

• **Individualized ballot processes:** How a vote are depicted within the involving net applications or databases continues to be AN open discussion. whereas a transparent text message is that the worst plan, a hashed token is wont to offer obscurity and integrity. Meanwhile, the vote ought to be non-reputable, that can’t be bonded by the token resolution.

• **Ballot casting verifiability by (and only by) the voter:** The elector ought to be ready to see and verify his/her own vote, when he/she submitted the vote. this is often vital to realize so as to forestall, or a minimum of to note, any potential malicious activity. This counter live, except for providing suggests that of non-repudiation, can sure boost the sensation of trust of the voters

• **High initial setup costs**: Though sustaining and maintaining on-line selection systems is way cheaper than ancient elections, initial deployments could be pricy, particularly for businesses.

• **Increasing security problems**: Cyber-attacks cause an excellent threat to the general public polls. nobody would settle for the responsibility if associate degree hacking try succeeds throughout an election. The DDoS attacks documented and largely not the case within the elections

Here are some of the features of blockchain technology that will help in overcoming the above challenges. These include decentralization, immutability, non-repudiation, transparency, pseudonymity and traceability. Smart contract is an entity that plays the major role in implementation of blockchain in IoT.

**Working**:

• The SHA-256 algorithm takes an input of any random length and produces an output of a fixed length (256 bits).

• In the case of SHA-256 algorithm no matter how big or small is the input, the output is of fixed length (256 bits). A cryptographic hash function has the following properties: 3 ITM Web of Conferences 32, 03001 (2020) [https://doi.org/10.1051/itmconf/20203203001 ICACC-2020](https://doi.org/10.1051/itmconf/20203203001%20ICACC-2020)

1. Deterministic: This means that no matter how many times we enter the same input we will get same result.

2. Quick Computation: This means that the result is generated quickly and this leads to an increase in the system efficiency.

3. Pre-Image resistance: Suppose we are rolling a dot(1-6) and instead of getting a specific number we get the hash value. Now we calculate the hash value of each number and then compare it with the result.And for a larger data sets it is possible to break pre-Image resistance by brute force method and this takes too long that it does not matter.

4. Small changes in Input change the whole Output: A minor change in the input significantly changes the whole output.

5. Collision Resistant: Every input will have a unique hash value.

6. Puzzle friendly: The combination of two values gives the hash value of new variable.

**4)** **Blockchain Enabled Online-Voting System**

Akhil Shah , Nishita Sodhia , Shruti Saha , Soumi Banerjee , Madhuri Chavan

We are proposing a system which has greater accessibility as it is an android application and possess greater security as authentication, authorization and verification. In this system the voter/user has to first register themselves using a registration form available within the android application and once the registration form is being submitted, an entry is being made in the centralized database. After the registration the user can log into the application and be a part of the polling process. The user with its valid credentials can log into the system and verify them by entering the one-time-password which is valid for a limited period of time. Once the user is logged into their respective account the dashboard contains all the information which is retrieved from the centralized database. After the user logs into the account the user is being authenticated using fingerprint. Each account is provided with a single token which he will use to cast a vote, casting of vote will take place by transferring the token from the respective user account to the candidate’s wallet. A web application is being developed to measure the majority of votes which has the details about the total number of voters, the number of votes cast and the percentage of votes cast. Only one vote can be casted from one account and once a vote is being casted from an account the account is disabled from current voting process.

Himanshu Agarwal, G. N. Pandey in the year 2013 [5] A high security password is confirmed before the vote is accepted in the main database and authentication is done by incorporating fingerprint module. The voter will be able to confirm if the vote is transferred to the correct candidate or party .The tallying of the votes can be done manually, whereas in this system the vote count is done directly ensuring that each vote is counted and no vote is misinterpreted.

B. Biometric voting system using Aadhar card in India - S Chakraborty, S Mukherjee in the year 2016 [6] An electronic voting machine utilizing Finger print is developed to build a safe voting machine with distinguishing proof technique to get unique mark as Aadhar card database is utilized. But it consists of same threat faced by any other EVM such as physical security of machines, secure storage of vote, and software could be tampered.

C. Trustworthy Electronic Voting Using Adjusted Blockchain Technology - Basit Shahzad Raju, Jon Crowcroft in the year 2019 [7] A framework is suggested that uses effective hashing techniques that ensure the security of the data. In this paper the concept of block creation and block sealing is introduced. The block sealing concept helps blockchain to be adjustable meeting the need of polling process.

D. Security Analysis of India’s Voting Machine - Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri in the year 2010 [8] Security Analysis was performed on real Indian EVM system. This paper states that EVM can be tampered

**Feasibility Study**

**Feasibility of Project SecureVote:**

1. **Technological Feasibility:** Blockchain technology, especially Ethereum, has matured significantly, making it technically feasible to implement SecureVote. Smart contracts, cryptographic techniques, and the Ethereum Virtual Machine (EVM) are readily available for building secure voting systems.
2. **Scalability**: Evaluating the scalability of the platform is crucial. Ethereum's scalability solutions, like Ethereum 2.0 and Layer 2 solutions, address potential bottlenecks, ensuring SecureVote can handle a large number of transactions efficiently.
3. **Development Resources:** Assessing the availability of skilled developers and resources for building and maintaining SecureVote is essential. The project will require a dedicated team with expertise in blockchain, smart contract development, and cybersecurity.
4. **Cost and Funding**: Estimating the project's cost and identifying potential sources of funding are critical feasibility considerations. SecureVote may require significant initial investment, but it could attract interest from public or private sectors concerned with secure elections

**Need for Project SecureVote:**

1. **Election Integrity:** Traditional voting systems often face issues of fraud and manipulation. SecureVote addresses the need for a more secure and transparent way of conducting elections, ensuring the integrity of the democratic process.
2. **Accessibility:** Many eligible voters face barriers to participating in elections, including geographical constraints or disabilities. SecureVote can provide a more accessible platform for these individuals, increasing overall voter turnout.
3. **Trust in Elections:** Recent concerns about the security of electronic voting systems and doubts about election results highlight the need for a trustworthy and tamper-proof voting platform like SecureVote.
4. **Global Applications:** The need for secure and transparent elections is not limited to one country. SecureVote can have global applications, supporting democratic processes in various regions.

**Significance of Project SecureVote:**

1. **Enhanced Democracy:** SecureVote has the potential to enhance democratic processes by providing a secure, transparent, and tamper-proof platform for elections and polls. This contributes to the foundational principles of democracy.
2. **Trust in Technology:** As the world becomes more digital, trust in technology is essential. SecureVote sets a precedent for the secure implementation of blockchain technology in critical societal functions, demonstrating its potential beyond cryptocurrencies.
3. **Reducing Fraud:** By utilizing blockchain and NFTs, SecureVote significantly reduces the risk of voter fraud, making elections more reliable and results more trustworthy.
4. **Global Impact:** SecureVote's impact extends beyond a single election cycle. It has the potential to influence the way elections are conducted worldwide, contributing to the improvement of democratic processes on a global scale.

**Methodology/Planning of work**

The development of the project is to be divided among the following major phases or steps:

1. Research and Requirements Gathering
2. Design Phase
3. Development
4. Security and Compliance
5. Full-Scale Deployment

Achieving the objectives of Project SecureVote entails a well-structured project development process. Initiation begins with defining project goals, assembling a skilled team, and setting up communication channels. Research and requirements gathering follow, involving an in-depth analysis of existing voting systems, stakeholder feedback, and technical specifications. The design phase focuses on architecting the platform, including smart contracts, security features, and user interfaces. Development entails coding the platform, emphasizing smart contract logic and NFT-based identity verification while conducting rigorous testing and security audits. Deployment on the chosen blockchain network and comprehensive documentation precedes pilot testing, ensuring real-world functionality and user feedback incorporation. Full-scale deployment follows, with continuous security monitoring and compliance checks. Regular evaluation, community engagement, scalability planning, and ongoing maintenance and support round out the project development process, ensuring the SecureVote platform's effectiveness, security, and responsiveness to evolving needs.

We prioritize community engagement, maintaining transparency, and fostering collaboration to refine the platform further. Scalability remains a focal point to accommodate a growing user base and evolving technological demands, ensuring that SecureVote remains a dependable solution for secure and transparent elections. Continuous monitoring and maintenance are integral, guaranteeing the platform's stability and responsiveness to potential security threats or emerging requirements. In this way, Project SecureVote remains committed to its mission of enhancing democracy, promoting trust in technology, and contributing to a more secure and inclusive electoral process.

**Facilities required for proposed work**

The proposed work can be carried out with standard computing facilities. A computer with sufficient processing power and memory to support development environments for React and Ethereum (for Web3 integration) would be required. Access to the internet and development platforms like GitHub would also be essential for collaboration and version control.

**Expected Outcomes**

The expected outcome of the Secure Vote project is a functional decentralized voting system prototype. This prototype will demonstrate the end-to-end process of user registration, candidate selection, secure voting, vote tallying, and result verification through blockchain technology. The system's user interface will be developed using React, providing a seamless and user-friendly experience. The successful implementation of this project will showcase the potential of blockchain in revolutionizing voting systems.

**References**

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
2. Buterin, V. (2013). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
3. Swan, M. (2015). Blockchain: Blueprint for a New Economy.
4. Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology.
5. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. doi:10.1016/j.future.2017.11.022