IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11629

D App for Voting with Block Chain Security

Mr. Abhinav N D[1], Ms. Rimsha Sultana S[2], Ms. Rakshita A Bhoj[3]

Assistant Professor, Department of Information Science and Engineering, SSIT, TUMKUR, KARNATAKA[1]

Student, Department of Information Science and Engineering, SSIT, TUMKUR, KARNATAKA[2]

Student, Department of Information Science and Engineering, SSIT, TUMKUR, KARNATAKA[3]

Abstract: An electronic voting system using blockchain security offers a robust and innovative solution to many of the challenges associated with traditional and centralized e-voting systems. Blockchain technology provides a decentralized and tamper-resistant framework, ensuring that once votes are cast, they are securely recorded and cannot be altered or deleted. This immutability enhances the integrity of the election process, making it highly resistant to fraud and manipulation. Furthermore, the transparency of blockchain allows for each vote to be independently verified by multiple nodes in the network, increasing trust and confidence among voters. Blockchain's cryptographic techniques ensure voter anonymity, protecting personal data while maintaining the ability to audit and verify the results transparently. This combination of security, transparency, and privacy makes blockchain-based electronic voting systems a compelling choice for modernizing electoral processes.

Keywords: Blockchain, Ethereum, Dapps, RSA.

I. INTRODUCTION

E-voting has become increasingly prevalent in societal affairs, yet ensuring the integrity of outcomes, especially in financially or politically significant decisions, remains a formidable challenge. The paramount attributes of correctness, security, and privacy underscore the necessity for a robust e-voting framework. Secure e-voting essentially embodies a form of secure multi-party computation, where individual choices are confidentially maintained. However, the reliance on a trusted public bulletin board in most e-voting schemes raises questions regarding its veracity, challenging election administrators to establish unequivocal trust in its integrity.

Some proponents have turned to blockchain technology as a potential solution, leveraging its inherently trustworthy nature. Blockchain, serving as a decentralized ledger, introduces novel possibilities for creating trustless and decentralized systems. Unlike traditional setups reliant on a centralized authority, blockchain operates through a network of interconnected nodes, each holding a local copy of the data. Originally conceived for secure monetary transactions, blockchain's versatility has spurred exploration across various domains, including the coordination of the Internet of Things, carbon dating, and healthcare.

The advent of Ethereum marks a pivotal moment in blockchain's evolution, introducing a Turing-complete programming language and the revolutionary concept of smart contracts. These self-executing contracts enable users to automate processes and execute functions within the Ethereum network, effectively eliminating the need for intermediaries.

While blockchain offers promise as a trusted public bulletin board for e-voting systems, a mere substitution may prove inadequate. The sheer volume of transactions and the computational complexity inherent in blockchain present formidable challenges. Thus, a more nuanced approach is necessary.

Enterprises propose a decentralized, trustless e-voting system grounded in blockchain technology. Decentralization distributes computational tasks across the blockchain network, fostering resilience and eliminating single points of failure. Simultaneously, the trustless nature of the system ensures that voters need not rely on a central authority, redistributing trust among all participants.

Critical to the system's integrity is the deployment of threshold encryption without the need for a trusted third party. This encryption scheme, employing a distributed key generation process, safeguards against unauthorized access and manipulation of voting data. Furthermore, even in the event of malicious intervention by election administrators, the integrity of tally results remains inviolate.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11629

The implementation of the voting protocol on Ethereum through smart contracts exemplifies the marriage of cutting-edge technology with democratic principles. Smart contracts empower users to enact transparent and auditable voting processes, with the Ethereum network validating the integrity of the final results.

II. MOTIVATION

Developing a decentralized e-voting application is primarily motivated by the desire for enhanced security, increased trust, and improved privacy. Decentralized systems, often built on blockchain technology, offer tamper-resistant and transparent voting processes. Once a vote is recorded, it becomes immutable, ensuring that the election results cannot be altered or manipulated, thereby preserving the integrity of the voting process. The transparency provided by blockchain allows for all transactions to be audited, which enhances voter confidence in the system. Decentralization removes control from a single entity, thereby reducing the risk of centralized abuse or corruption and fostering a more trustworthy and equitable election environment. Additionally, decentralized systems can better protect voter anonymity and personal data, addressing privacy concerns more effectively than centralized systems.

In contrast Centralized voting applications come with significant disadvantages. These systems are more vulnerable to tampering and manipulation since a single point of control can be exploited by malicious actors, increasing the risk of election fraud. Centralized data storage also poses substantial security risks, as breaches can compromise the entire voting system, exposing sensitive voter information and potentially altering election outcomes. Maintaining trust in centralized systems is challenging, as voters may question the impartiality and security of the voting process, especially if the central authority is perceived as biased or corrupt. Furthermore, centralized systems often struggle to ensure voter anonymity and protect personal data, leading to privacy violations and undermining voter confidence in the election process.

III. LITERATURE SURVEY

[1] Shambhavi Bhardwaj; T. Poongodi; Ashutosh Dixit; Smita Sharma: A Decentralized Digital Voting System Based on Block chain Architecture.

Voting is the cornerstone of democracy and a fundamental right for every citizen. Implementing a blockchain-based election system could revolutionize the way elections are conducted by enabling digital voting. Unlike traditional paper ballots and electronic voting machines (EVMs), blockchain technology offers a safer, smoother, and more convenient election process. Especially in the context of the COVID-19 pandemic, blockchain-enabled elections allow people to vote remotely using a mobile phone or computer, thereby enhancing security and significantly reducing risks such as EVM hacking and overcrowding at polling stations.

In this advanced voting system, each eligible voter would receive a unique personal ID and key, ensuring tamper-proof authentication. The system comprises two main components. The first is the Election Commission, which oversees the process and integrates all candidates into the blockchain. The second component is the user interface for residents, allowing each eligible voter to select their preferred candidate from their respective constituencies. Votes are then securely recorded on the blockchain, ensuring they are tamper-proof and transparently verifiable.

[2] Atharva Jangada; Nimish Dadlani; Sanchit Raina; VS Sooraj; A.R. Buchade: De-Centralized Voting System using Blockchain.

The innovative concept of blockchain, the technology that powers Bitcoin and other cryptocurrencies, has brought about a new era for the Internet and online services. While blockchain is often associated solely with cryptocurrencies, it is increasingly being applied to a wide range of administrative activities and daily services that were traditionally managed offline or privately. One significant and emerging application of blockchain is electronic voting. In our country, traditional voting systems involve using paper ballots at polling stations or electronic voting machines (EVMs). However, the ballot system is vulnerable to tampering, and EVMs, being centralized, are susceptible to hacking. We propose a more secure, transparent, cost-effective, and user-friendly alternative by leveraging blockchain technology.

Smart contracts, which are executable pieces of code within the blockchain, play a crucial role in this system by ensuring that operations are carried out as scheduled at each stage of the blockchain update. Ethereum, known for its stability, versatility, and smart contract functionality, is particularly suitable for this purpose. In this project, we will develop and test a prototype of an e-voting application using the Ethereum Wallet and Solidity programming language to create smart contracts on the Ethereum network.

DOI: 10.17148/IARJSET.2024.11629

[3] Subha P; Padmasree P; Sowndharya Lakshmi R: Voting System based on BlockChain and using Iris Recognition.

The voting system in India often faces issues of corruption and manipulation. To address these problems, we propose the development of an unbiased, secure, fast, and efficient voting system based on blockchain technology. This project aims to create a highly secure voting database that allows for quick processing. An additional feature of this system is iris recognition, which enhances the accuracy and integrity of the process. By utilizing a blockchain-based database, the voting information becomes immutable, reliable, and easily accessible. Authorized result tracking further secures the voting process, making it faster and more efficient through semi-automation. Iris recognition works by identifying unique patterns in the iris using infrared light and generating an encrypted bit pattern. This pattern must match at the time of voting to verify the individual's identity. For visually impaired voters, fingerprint recognition is used as a backup, ensuring their identity is accurately confirmed even if iris recognition is not feasible.

[4] Deni Pramulia; Bayu Anggorojati:Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask:

The deployment of electronic voting (e-voting) systems, which are increasingly replacing traditional voting methods, still faces significant trust issues. E-voting systems are highly susceptible to manipulation, including alterations in election outcomes due to hacking or interference by system administrators. Centralized networks pose a problem because they allow a single party to control and manage data sources. This trust issue inherent in centralized data distribution can be addressed by distributing data across a network. Blockchain technology, being a decentralized ledger where each participant in the network holds an identical copy of the data, offers a solution with its key feature of immutability, making it highly suitable for e-voting applications.

This study proposes an e-voting system based on blockchain using Ethereum and MetaMask. The proposed system adheres to six fundamental election principles: maintaining ballot secrecy, ensuring one-person-one-vote, verifying voter eligibility, providing transparency, accurately recording and counting votes, and ensuring overall reliability. Additionally, performance evaluations of the e-voting system indicate that selecting the slow gas price option results in the lowest gas price per second, offering the best balance between cost and performance.

[5] N Balakrishnan; S Aruna; D Akshaya; P C Karthikeyan; G S Divya Dharshini: Smart Contracts and Blockchain based E-Voting:

Voting is a fundamental right for every citizen, allowing them to express their opinions and choose their representatives to shape society. However, the current voting system is susceptible to security breaches and fraud. To mitigate these issues, e-voting systems leveraging blockchain technology have emerged. This technology enhances the security, transparency, and fraud resistance of the voting process. Each vote generates a separate block that is decentralized to ensure transparency and accuracy. Blockchain technology, operating on a peer-to-peer network, provides secure and transparent record-keeping and verification for each vote. The system's immutability feature safeguards the integrity of the voting process. Votes are stored in encrypted blocks with hash values, and smart contract mechanisms identify fraudulent votes and prevent multiple voting attempts. This research offers a detailed analysis of how the blockchain algorithm records voting results and voter information at each polling location, emphasizing the technology's core structure and features for electronic voting.

IV. PROPOSED SYSTEM

In this today's digitized world, the application or apps at finger tips make humans work very east and fast with maximum efficiency. Normally, in our day to day life we get to see and we are using applications which are centralized applications which are run on a particular server installed by the application developer.

The application is actually built, hosted, run and maintained on a centralized server where the administrator is the only centralized competent authority to make and perform any root level changes to the application. The users of the application only have the authority to use the application and share his/her own user experience with respect to software. On the same lines an application called “voting at tips” which helps the users to carry out or perform their fundamental rights i.e. casting vote staying at home or remote places very easily.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11629

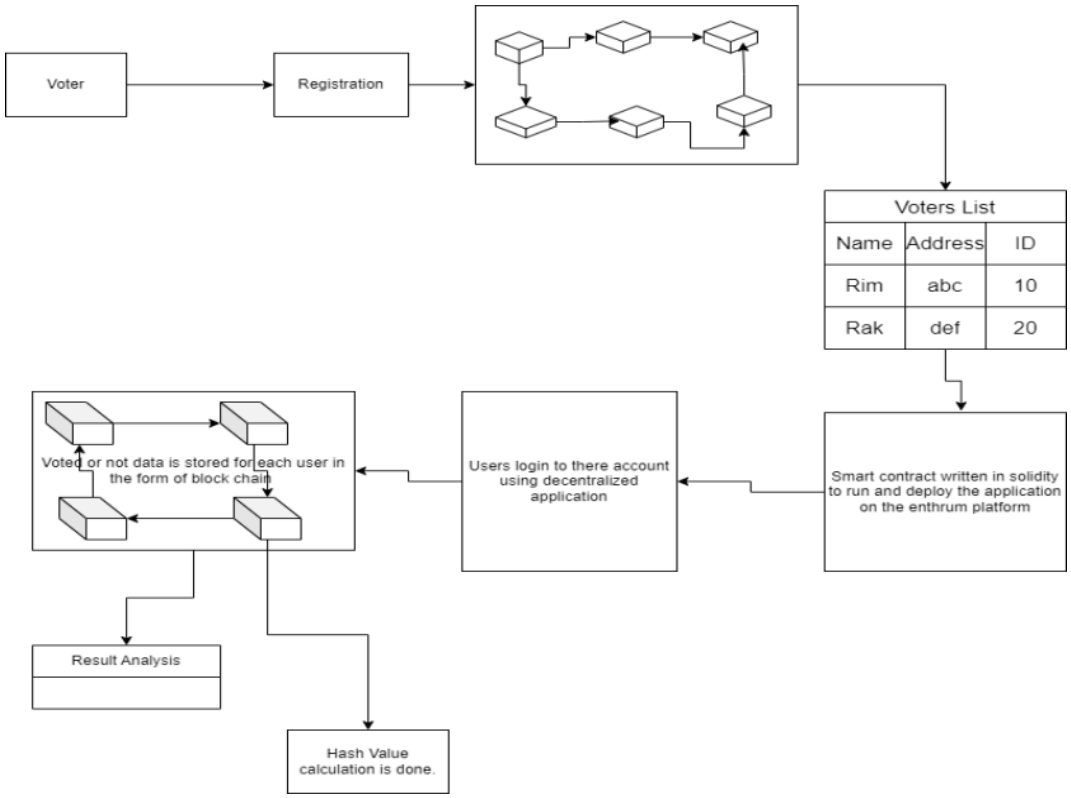

Fig 1: System Architecture

But then the apps that are available for the purpose now a days are actually centralized applications where in the application is been developed, run and maintained by a centralized authority. In this the major advantage is that, the user can cast their valuable votes from remote location and may be his/her response can be transferred to database and be stored in the database in secured manner using any encryption algorithms. But then the major concern is if an third party i.e. hacker tries to access data and get the data, there is all possibility of tampering the data. The only option that would be left with the owner after him/her gets to know that data is tampered is that they can conduct election again or try to retrieve the data but at the initial stage itself they could not ensure security for the voters vote data. To address this concern the concept of block chain makes it a cake wake to provide highest level of security by the various nature of security that it possess and exhibits. The system architecture also shows the same behaviour. Hence for the protecting the data of the voters and by enhancing the security.Here we create a Dapp, i.e. Decentralized application where in the application is developed by a single people or group of people, but the application will be run and controlled by all the people on the network. The network can be formed by providing a platform. The platform that provides the collection of nodes, inter-connection between them and provide unique way of security is “Etherum”. It is a platform which provides a basic infrastructure that is required to collect and group thousands of independent computer network and gives the capability for all the computers to run the Dapp on all of them.

From the architecture it can be seen that the voter registers oneself with the Dapp. Once the user becomes a part of the network and registers himself, all the data corresponding to any specific user is stored in the form of block. Each block has three components. One Data that is stored in the block which can be any data, second one is the hash value which is calculated using the blocks data, and timestamp, third one is the pervious block hash value, where the first block been named “Genesis block” is the first block in the chain. Here the data corresponds to voters registration details stored in each block. After collecting the data, by using the same data of the block we calculate the hash of that block to form a chain . The network were the chain of blocks are present is “Etherum” where each node of the computer in the etherum platform has the entire block chain information. This is possible because of the Dapp’s where the voting application developed is run on each computer in the network. The hash value is been calculated using SHA256. All the voters data is stored in the network database. In order to run the front end part of the application i.e. GUI part of the application, it can be developed using any of the available web technologies like HTML, CSS and JavaScript or any frameworks of JS like react or angular.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11629

As part of the back end when once the user enters the registration data , collecting the data and putting in side the block and the distribution and creation of blocks and the entire chain process on the etherum network is done by the self executable code called as "Smart Contract" which is written using solidity which is a programming language that executes itself when some event triggers in the form of smart contract.

After storing registration details, if one want to add more blocks to the existing block chain network, we can also do it using Consensus rule which states that approval from all the members of the network in majority should be taken and considered to add a new block along with the data. If we change the content of the block's data automatically that particular blocks hash value changes hence affecting and reflecting changes in the next block which shows some one attempted to change the data integrity via which security of user's registration data is secured. When the user votes on any particular day of the election, the log's onto the etherum network via meta mask which gives unique login credentials for all the users on the etherum platform.

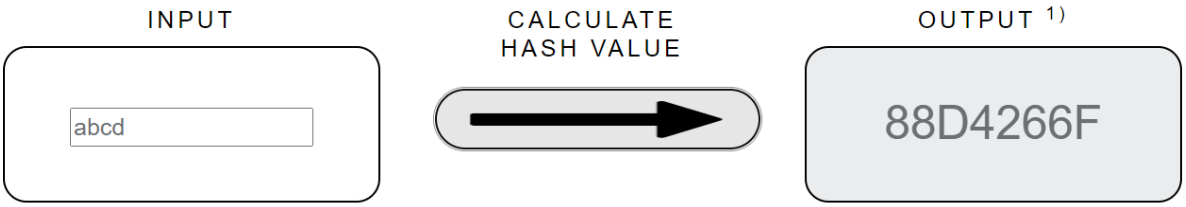

Fig 2: Hash value calculation

User log's in to the etherum platform, access the decentralized voting application and vote for the party of his/her choice.Once the vote is casted, the data i.e. the party to which the person voted is stored in the block and the hash value is been calculated using SHA256 and its hash value is been shared to the subsequent blocks in the network.

Fig 3: Flow chart of block chain creation and hash number

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11629

Based on the region of voting and number of people voted, a block chain network is been created and shared the application to all the members of the network. The data can be encrypted and stored in the block using any cryptographics algorithms. If any one wants to change the data i.e. a person's voted data, the hash changes indicating tampering attempt of the data and the same is been circulated to all the members of the network. After storing all the data, we can access the data in the blocks and analyse the result of the voting and sentiment analysis can also be done. Hence forth voting decentralized application with block chain provides more security compared to other systems.

V. RESULTS

Parameters	Centralized Application	Dapps
Main server	Needed	Not Needed
Failure	Single point	Peer connection
Reliability	80%	95%
Security	50%	90%

VI. CONCLUSION

In conclusion, decentralized e-voting applications leveraging blockchain technology present a transformative approach to modern electoral processes. By providing a decentralized, tamper-resistant framework, blockchain ensures the immutability and security of votes, significantly reducing the risk of fraud and manipulation.

The inherent transparency of blockchain allows for independent verification and auditing, fostering greater trust and confidence among voters. Additionally, advanced cryptographic techniques protect voter anonymity and personal data, addressing privacy concerns more effectively than traditional systems. This combination of enhanced security, transparency, and privacy makes blockchain-based e-voting systems a compelling and robust solution for future elections, promising to enhance democratic participation and integrity in the digital age.

REFERENCES

[1]. Shambhavi Bhardwaj; T. Poongodi; Ashutosh Dixit; Smita Sharma: A Decentralized Digital Voting System Based on Block chain Architecture.,*https://ieeexplore.ieee.org/document/9754194*.
[2]. Atharva Jangada; Nimish Dadlani; Sanchit Raina; VS Sooraj; A.R. Buchade: De-Centralized Voting System using Blockchain.,*https://ieeexplore.ieee.org/document/9936022.*
[3]. Subha P; Padmasree P; Sowndharya Lakshmi R: Voting System based on BlockChain and using Iris Recognition.*https://ieeexplore.ieee.org/document/9711819.*
[4]. Deni Pramulia; Bayu Anggorojati:Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask.,*https://ieeexplore.ieee.org/document/9354310*.
[5]. N Balakrishnan; S Aruna; D Akshaya; P C Karthikeyan; G S Divya Dharshini: Smart Contracts and Blockchain based E-Voting.,*https://ieeexplore.ieee.org/document/10142675*.

BIOGRAPHY

Ms. Rimsha Sultana S, an engineering student at Sri Siddhartha Institute of Technology, currently in my 6th semester under Information Science department. I have developed strong skills in Python, HTML, CSS, JavaScript, C++, and Java. My specialization lies in full stack web development and blockchain, and I am particularly interested in the importance of security in applications, which drives my current research interests.I have worked on several impactful projects, including developing desktop applications, creating user-friendly websites, designing IoT systems, and building web-based solutions. These projects demonstrate my ability to blend design with functionality and create efficient, user-centric systems. I have earned certification of Data Mining from NPTEL platform , the Artificial Intelligence Foundation Certification from Infosys, and completed the IBM SkillsBuild Data Science and Generative AI-CRSBOX Micro-Internship. My research focuses on security concerns in web applications, particularly using blockchain, machine learning, and data analysis. I am passionate about cyber security and am dedicated to exploring new technologies to enhance application security. Outside of tech, I enjoy traveling, self-improvement, food, and photography. I am committed to delivering results and continuously expanding my knowledge and skills.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11629

Ms. Rakshita A Bhoj, 6th semester student in the Information Science and Engineering Department at Sri Siddhartha Institute of Technology, currently pursuing Bachelor of Engineering (B.E) degree, focusing on the intersection of software development, web development, data science, and machine learning. Throughout my academic journey, I have demonstrated a strong commitment to excellence, consistently achieving top grades in my coursework. I have keen interest in artificial intelligence and its applications in solving real-world problems. My research interests include machine learning algorithms, web development, data mining, and cyber security. I have actively participated in various academic projects and workshops. Notably, I contributed to a project on Event Registration System using web development, HTML and CSS, which aimed at providing user friendly interface. This project not only showcased my technical skills but also my ability to work collaboratively in a team environment. My dedication to my studies and research has earned me several accolades. I aim to contribute to the field of Information Science by leveraging my skills to innovate and develop solutions that address contemporary challenges in technology. In my spare time, I enjoy coding, reading about new technological advancements, sketching and painting.