SECURE ONLINE VOTING BASED ON BLOCKCHAIN TECHNOLOGY

Dr. M. Saraswathi[1], Arikatla Rajesh[2], Bommmisetti Hima Sagar Koteeswar[3]

[1]Assistant Professor, Dept. Of CSE, SCSVMV (Deemed to be University)

[2]Student, Dept. Of CSE, SCSVMV (Deemed to be University)

[3]Student, Dept. Of CSE, SCSVMV (Deemed to be University)

---***---

Abstract - This paper is based on electronic voting machines, which are often used in elections and offer the ability to execute the process safely using blockchain technology. The prime aim of this system is to ensure security, integrity as well as transparency. One of the main considerations in the electronic voting site that offers a blockchain-based voting system to address a number of shortcomings of the current voting methods is voter privacy. The portal also offers a simple, dependable, rapid, and economical e-voting solution.

Key Words: Blockchain technology, EVM's, authentication, validation, security, decentralized voting.

1.INTRODUCTION

Voting is understood to be a type of choice. This form of expression can be accomplished through the ballot box or any other electoral scheme. Electronic voting is a method of retrieving, tallying, and storing votes cast by voters using a specific electronic medium. The project will focus on the current voting method used by the student union and identify a way to model it with the internet voting system that will be implemented. The system will implement various election mechanisms for voting.

The system will be designed with strict security features. These security features will apply from the time a voter logs into the voting system until they cast their vote for their preferred candidate and exit the system. The system will include safeguards that prevent voters from voting for the same candidates more than once.

The system that will be implemented must address the issues concerning the security requirements of a vote cast over the internet. Authentication and validation of users, access rights, information encryption, and vote security must all be thoroughly investigated to create a secure means of voting online.

2. LITERATURE SURVEY:

V. Meenakshi, V. Vijeya Kaveri, etc. [1]. The development of a decentralized voting system that can readily support an open, logical, and easily verifiable democratic plan is the main goal of this research study.

Reza Tourani, Michele Scarlato, etc. [2] The author of this research suggests Sancus, an electronic voting system based on blockchain. Sancus provides characteristics like voter authentication and anonymity, which satisfy the fundamental requirements of fair voting.

JON C. ROWCROFT and BASTSHAHZAD. [3] The author of this paper discusses the use of the blockchain for reliable electronic voting, and it is noted that the current blockchain may require some modifications .

Gunnlaugur K. Hreioarsson, Friorik P., Hjalmarsson, etc .[4] The study offers a novel blockchain-based electronic voting system that tackles some of the drawbacks of current systems and assesses some of the blockchain-based electronic voting systems using well-known blockchain technologies.

2.1 PROBLEM STATEMENT:

In the current system, EVMs and traditional methodologies are used, which run the risk of tampering with and manipulating voting results, resulting in the wrong or unfit person governing the country. So, to address this issue, we are incorporating blockchain and smart contract technology into the online voting system.

Blockchain has the advantage of running on a network that is not maintained by any third party or humans. Blockchain is also considered transparent and secure against attacks that target a system's central point. This also eliminates the need to rely on a single authority to ensure the accuracy of the transactions. More democratic processes can be added to electronic voting due to the characteristics of a decentralized network.

3 PROPOSED SYSTEM:

In this paper, we will introduce and implement Blockchain technology to replace traditional voting systems. Blockchain is a peer-to-peer (P2P) network that is completely decentralized. It is a tamper-proof digital ledger that operates autonomously. This allows the User's Community to keep track of transactions in a Shared ledger, but the normal operation cannot be modified for transactions exposed as part of blockchain networks.

ADVANTAGES:

- It is transparent and protects against attacks on a system's core point.
- Because of the properties of a decentralized network, electronic voting can be enhanced with more democratic processes.
- Cost-effective while also being quick and effective.
- There is no requirement for the authorization of a third party.

3.1 SYSTEM ARCHITECTURE:

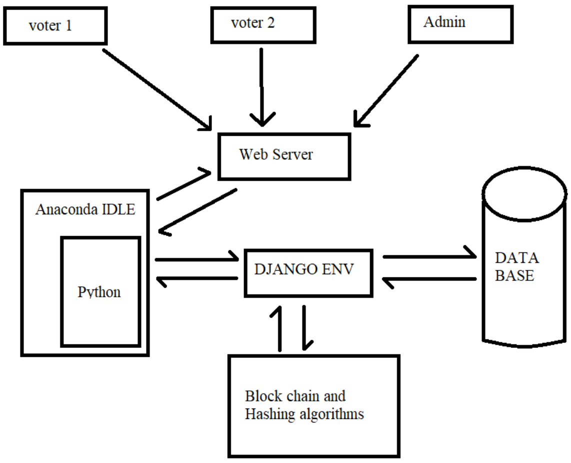


Fig1: Architecture diagram

3. CONCLUSIONS

The online version of the volume will be available in LNCS Online. Members of institutes subscribing to the Lecture Notes in Computer Science series have access to all the pdfs of all the online publications. Non-subscribers can only read as far as the abstracts. If they try to go beyond this point, they are automatically asked, whether they would like to order the pdf, and are given instructions as to how to do so.

4 MODULE DESCRIPTION:

BLOCK: In a blockchain, blocks are the basic information containers. They contain transaction data. A block that has been added to the blockchain cannot be modified. Cryptographic procedures are used to protect blocks.

USER: The user presents his relevant evidence and puts his ID into the user ID port. After submitting his legal id evidence, he selects his election candidate by clicking on the id listed in the ballot region. This completes the voting procedure on the user side.

Ballot sealing and verification:

A block is created and initialized with the voter ID, vote, timestamp, and hash. The ballot will be sealed, i.e. mined, after a careful examination of the block with the previous hash, transaction hash (vote), block hash, nonce, and timestamp.

CHAIN:

Transaction: Once the ballot is sealed in the blockchain-based e-voting system, the list of confirmed votes is displayed as transactions, with each transaction containing the Voter Id, vote, Timestamp, Hash, and Block.

Chained Blocks: Once the transactions are completed, the blocks are added to the ledger and chained to one another using the previous hash and block hash. Once inserted, blocks cannot be changed.

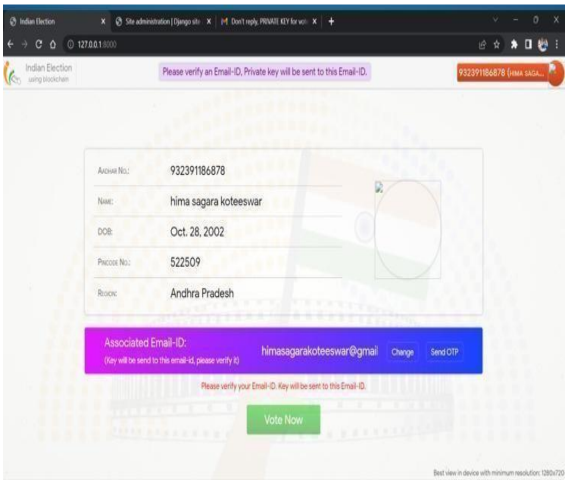
4.1 ALGORITHM USED:

Rivest-Shamir-Adleman (RSA) Algorithm- It is one of the most well-known cryptosystems for key transfer and block encryption. The bit length is 1024 or 2048.

Merkle root Algorithm- It is generally referred to as the hash of all the hashes of all the transactions in a blockchain block.

SHA 512 HASH ALGORITHM — The Homomorphic Algorithm is a block cipher that operates on data blocks of fixed size.

5 RESULTS:


Indian Election
Site administration | Django site
Don't reply, PRIVATE KEY for vot
127.0.0.1:8000
Indian Election
using blockchain
932391186878 (HIMA SAGA...
Change
Send OTP
Vote Now

Please verify an Email-ID, Private key will be sent to this Email-ID.

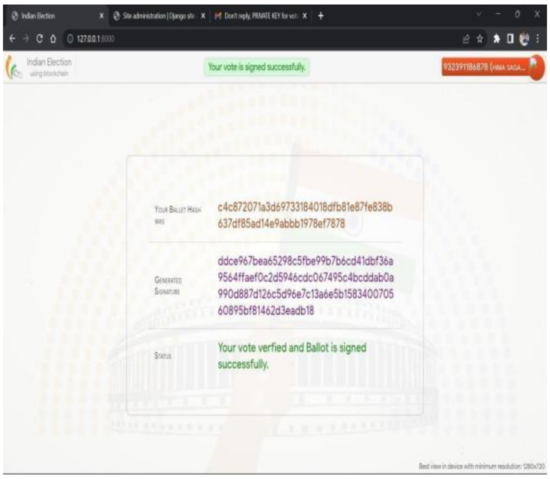
AADHAR NO.:	932391186878
NAME:	hima sagara koteeswar
DOB:	Oct. 28, 2002
PINCODE NO.:	522509
REGION:	Andhra Pradesh

Associated Email-ID: himasagarakoteeswar@gmail
(Key will be send to this email-id, please verify it)

Please verify your Email-ID. Key will be sent to this Email-ID.

Best view in device with minimum resolution: 1280x720

Fig 2 : Verification of voter


Indian Election
Site administration | Django site
Don't reply, PRIVATE KEY for vot
127.0.0.1:8000
Indian Election
using blockchain
932391186878 (HIMA SAGA...
Best view in device with minimum resolution: 1280x720

Your vote is signed successfully.

YOUR BALLET HASH WAS c4c872071a3d69733184018dfb81e87fe838b637df85ad14e9abbb1978ef7878

GENERATED SIGNATURE ddce967bea65298c5fbe99b7b6cd41dbf36a9564ffaef0c2d5946cdc067495c4bcddab0a990d887d126c5d96e7c13a6e5b158340070560895bf81462d3eadb18

STATUS Your vote verfied and Ballot is signed successfully.

Fig 3: Hashing of vote ballet

6 CONCLUSION:

This paper will provide insight into the general techniques used to implement the online voting system. It will also describe the initial proposal's aims and objectives, as well as the objectives that could not be met. It will discuss the project's flaws as well as the necessary work that can be done to improve the system in the future. The project helps us to switch from paper-based voting to electronic voting, This project will allow citizens to vote remotely from any location via the internet. The testing phase of the project was utilized to carefully test the system to identify any defects and flaws that the system may have had. The test findings indicated whether or not the system was ready to be supplied to its ultimate customer. The constructed system met its aims by being simple to use and secure, which was vital because it would be utilized for the student union electoral process.

REFERENCES:

[1]. Sancus: An Anonymous and Trustworthy Blockchain-based Electronic Voting Architecture by Michele Scarlato, Reza Tourani, Moongu Jeon. (IEEE-2022)

[2]. V. Vijeya Kaveri, V. Meenakshi, Ananth S, Akshayavarshini P, KavyaShree B, "Blockchain based Reliable Electronic Voting Technology", 2022.

[3]. Atharva Jangada, Nimish Dadlani, Sanchit Raina, VS Sooraj, A.R. Buchade, "De- Centralized Voting System using Blockchain", 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), pp.1-5, 2022.

[4]. Michele Scarlato, Reza Tourani, Moongu Jeon, "Sancus: an Anonymous and Trustworthy Blockchain-based Electronic Voting Architecture", 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), pp.93-98, 2022.

[5]. G. Pranitha, T. Rukmini, T. N. Shankar, Basant Sah, Naween Kumar, Sasmita Padhy, "Utilization of Blockchain in E-Voting System", 2022 2nd International Conference on Intelligent Technologies (CONIT), pp.1-5, 2022.

[6]. Mohit Kumar, "Securing the E-voting system through blockchain using the concept of proof of work", 2021 International Conference on Technological Advancements and Innovations (ICTAI), pp.423-427, 2021.

[7]. Asmae El Fezzazi, Amina Adadi, Mohammed Berrada, "Towards a Blockchain based Intelligent and Secure Voting", 2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS), pp.1-8, 2021.

[8]. T Vairam, S Sarathambekai, R Balaji, "Blockchain based Voting system in Local Network", 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), vol.1, pp.363-366, 2021.

[9]. Uryaa Pranav Meduri, Saketh Kamatham, Sneha Subramanian, Anupama Meduri,

Neha Diwan, "A Secure Network Monitored Balloting System", 2021 6th International Conference on Inventive Computation Technologies (ICICT), pp.31-35, 2021.

[10]. Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application. September 2018,Authors:Meiliana Sumagita,Imam Riadi.

[13]. Analysis of Secure Hash Algorithm (SHA-512) For Encryption Process on C College Web Based Application,2020, Iconic Research and Engineering Journals,SUJITHA KAMEPALLI, A SUDHARSAN REDDY.

[14]. Research on Big Data Security and Privacy Risk Governance,XinRui Wang;Wei Luo;XiaoLi Bai;Yi Wang,2021 International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR),Year: 2021 | Conference Paper |Publisher:IEEE .