E-VOTING SYSTEM USING BLOCKCHAIN

Dr. Mohanapriya M[1], Dhulasi T[2], Gunavijayan G V[3], Hema Pradhiksha D[4], Raghul S M[5]

[1]***ASSOCIATE PROFESSOR***, *Department of CSE, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu, India*
[2,3,4,5] *Department of CSE, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu, India*

---***---

Abstract – *The project's main purpose is to establish an effective e-voting mechanism by leveraging blockchain's capabilities, such as cryptographic foundations and transparency. However, there are still barriers to wider adoption of such systems, especially in terms of strengthening their resilience. The old traditional technique, which relies on a centralised infrastructure, has security and transparency issues. Some of the issues with traditional election systems include a lack of complete control over an organization's database and system, as well as the possibility of tampering with the database. Blockchain technology is based on a decentralized system, with multiple users accessing the same database. Blockchain technology creates a network structure data with built-in security features. It is built on the encryption, decentralization, and consensus principles, which ensure transaction confidence. Participants in the network each have their own private keys, which are associated with the transactions they conduct and serve as a personal digital signature. The project's main purpose is to allow voters to vote in the most secure and transparent way possible from anywhere on the planet.*

Key words: Blockchain, cryptography, decentralization.

I. INTRODUCTION

After the advent and widespread acceptance of Bitcoin, blockchain technology shines brightly[2], The first cryptocurrency to enter people's daily lives has become a hot subject in today's software industry. [2]. Blockchain is an open distributed ledger made up of a chain of digital blocks that are linked and interconnected. It was created with the intention of storing only digital currency transactions, but it has subsequently evolved to incorporate additional applications. [13]. There are also various sorts of Blockchains based on their purpose and characteristics:

- Public blockchain
- Private blockchain
- Consortium blockchain

The main motivation for using blockchain is because of its features or properties, such as decentralization, transparency, and immutability.

Blockchain is a distributed ledger to store the digital transactions between two parties efficiently [2]. The transactions are kept in 'blocks', which are a growing list of records. These blocks are impervious to any change and can be verified indefinitely. To make any modifications within blocks, more than half of the network's users must agree.

The 'Genesis block' or 'Block 0' is the first block in a blockchain. The genesis block is frequently hardcoded into software; it is unique in that it contains no references to prior blocks ('Genesis Block') [2]. Once the genesis block has been initialised 'Block 1' is created and when completed, it is attached to the genesis block. Each block comprises a transaction data section, which is followed by hashing copies of each transaction and then the hashes are paired and hashed again, this continues until a single hash remains; also known as a Merkle root. In Blockchain 1.0, a block is a data structure to store transaction records. It consists of two parts:

1) Block Header.
2) Block Body.

The following fields are found in the block header:

- ***Block Version:*** defines the block validity rules.
- ***Merkle Tree Root Hash:*** maintains the hash value of all transactions in the block.
- ***Time Stamp:*** uses universal time to stamp the current time in seconds.
- ***nBits:*** the minimum size of a valid block hash.
- ***Nonce:*** a mathematical value starts with 0 and increases with calculation of every hash.
- ***Parent Block Hash:*** refers to the block before it.

The transactions and transaction counter are stored in the block body. The maximum capacity of block to store the transactions is determined by the block size and size of each transaction contained in it. Fig 1.2 shows the structure of blocks in blockchain[12].

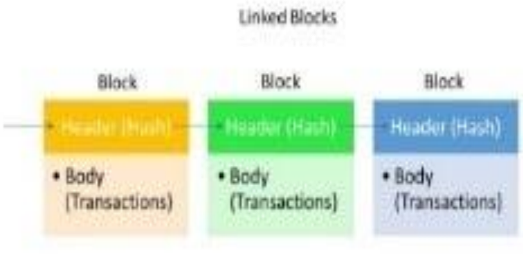


FIG 1.1 BLOCKS IN BLOCKCHAIN

Hash is used to protect the integrity of data. It works by calculating a fixed-sized unique value called 'hash value' for every input. The hast function is one-way, which means original data cannot be calculated back from the unique output. Because of its security strength, it is used to protect the integrity of data. Hashing in Blockchain is shown in Fig 1.2

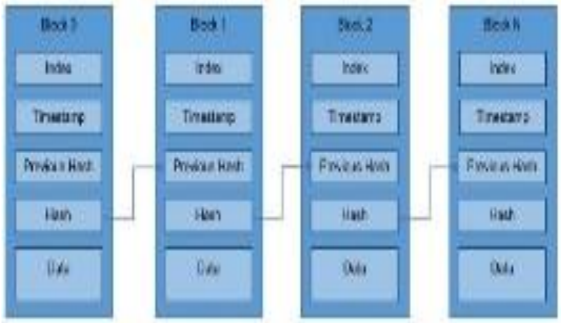


FIG 1.2 HASHING IN BLOCKCHAIN

1.1 BLOCKCHAIN SECURITY:

Blockchain security is a cybersecurity-based risk management technique for a blockchain network. All network participants must agree on data accuracy, and all verified transactions are irreversible. For delivering the data, blockchain is great. Because it provides real-time, shareable, and completely transparent data stored on an immutable ledger accessible only to network users with authorization. The blockchain technology generates a data structure with security measures embedded within. It is based on encryption, decentralisation, and consensus principles, which ensure transaction confidence. Most blockchains or distributed ledger technology (DLT) stores data in blocks, each of which contains one or more transactions. Through the participation of users throughout a distributed network, blockchain technology promotes decentralization. There is no single point of failure, and no single user has the ability to alter the transaction record. The use of blockchain in the distribution of datasets on e-voting systems can decrease one of the main sources of database tampering. The "E-VOTING method using Blockchain" is an online voting system that allows persons over the age of 18 to vote without having to go to a polling location. There is a database that has all of the names of voters along with their complete information.

A voter can exercise his or her voting rights online by using the "E-VOTING Technology using BLOCKCHAIN" system. He / She has to be registered first for him/her to cast the vote. For security concerns, the system administrator is primarily responsible for registration. The System Administrator registers voters on a separate site of the system that he visits by simply filling out a voter registration form. There is one Ethereum account for each voter, and he can only vote once using that account to eliminate the problem of 'double voting'. After enrolling, the voter is issued a private Voter ID, which he or she can use to log into the system and cast their vote. A voter can vote after completing the registration process. The transaction is recorded in the blockchain as soon as the vote is cast. Finally, the results of the vote casted will be verified.

II. PROPOSED SYSTEM

Development of secure e-voting system by leveraging benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for e-voting. A website is used for voter registration, while Aadhaar verification is used for voter authentication. The next stage is vote casting, which requires the user to connect into the page using credentials such as a blockchain account and vote to the respective party he/she chose. Each voter's Ethereum account is created using the Ganache platform. The proposed solution to the problem of duplicate spending is to set a gas limit for each voter, with the limit set so that each voter can only vote once. Fig 2.1 shows the overall system design of E-voting system using Blockchain.

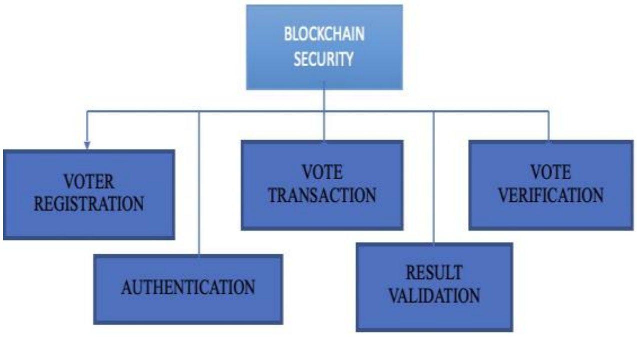


FIG 2.1 OVERALL SYSTEM DESIGN

III. SYSTEM IMPLEMENTATION

OVERVIEW

For the implementation of the system, we used Ganache where we used Ethereum of some accounts to access Smart Contracts. We give one Ethereum account for each user using Ganache. Using that account, user can able to cast his/her vote. If he tries to vote again, he will not be able to vote. The problem of "double spending" is eliminated because each voter can only vote once.

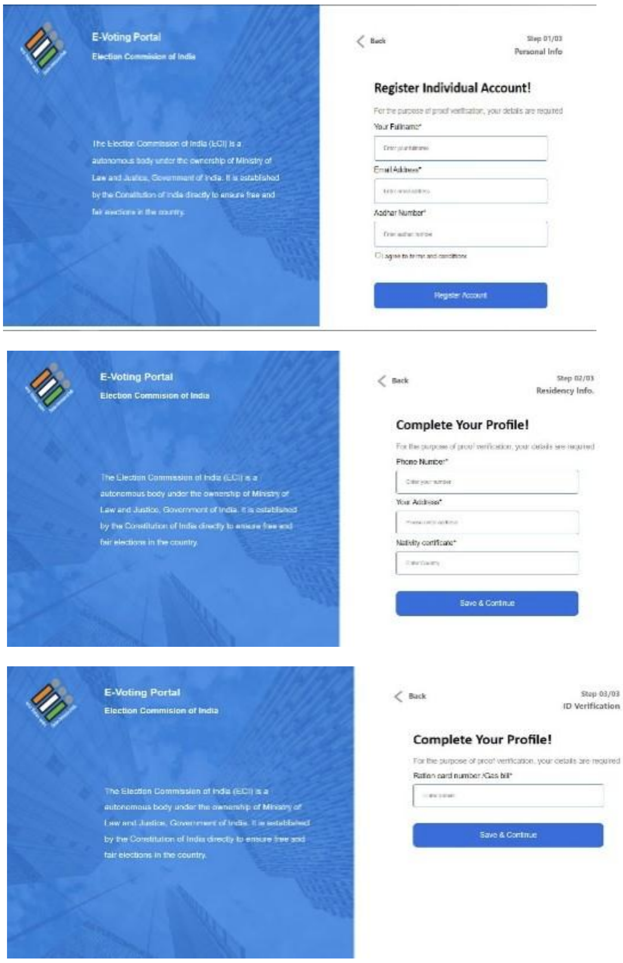
3.1 MODULES

The modules used in the system are:
1. Voter Registration.
2. Authentication.
3. Vote Transaction.
4. Result Validation.
5. Vote Verification.

3.2 METHODOLOGY

3.2.1 VOTER REGISTRATION

The proposed system used registration website as for the users to register themselves. The website collects details like name, e-mail, phone number, Aadhar number of the voter at the time of registration. These details are collected from the user and stored in the database. After successful completion of voter registration, the user is sent a confirmation mail to the e-mail provided at the time of registration. Voter Registration process is shown in Figs. 3.1



E-Voting Portal
Election Commision of India

The Election Commission of India (ECI) is a autonomous body under the ownership of Ministry of Law and Justice, Government of India. It is established by the Constitution of India directly to ensure free and fair elections in the country.

< Back
Step 01/03
Personal Info

Register Individual Account!
For the purpose of proof verification, your details are required
Your Fullname*
Email Address*
Aadhar Number*
□ I agree to terms and conditions
Register Account

E-Voting Portal
Election Commision of India

The Election Commission of India (ECI) is a autonomous body under the ownership of Ministry of Law and Justice, Government of India. It is established by the Constitution of India directly to ensure free and fair elections in the country.

< Back
Step 02/03
Residency Info.

Complete Your Profile!
For the purpose of proof verification, your details are required
Phone Number*
Your Address*
Nativity certificate*
Save & Continue

E-Voting Portal
Election Commision of India

The Election Commission of India (ECI) is a autonomous body under the ownership of Ministry of Law and Justice, Government of India. It is established by the Constitution of India directly to ensure free and fair elections in the country.

< Back
Step 03/03
ID Verification

Complete Your Profile!
For the purpose of proof verification, your details are required
Ration card number /Gas bill*
Save & Continue

FIG 3.1 INDIVIDUAL VOTER REGISTRATION

3.2.2 AUTHENTICATION

Once the details are collected from the user the next step is the authentication process. Aadhar verification is done. Verification is done either by uploading the Aadhar photocopy or the website has a provision for taking the photo at the time of registration. After successful verification the user is provided with the blockchain account address and private key. User has to keep these details intact and protected at all costs. Proof Verification of the voter is shown in Fig. 3.2

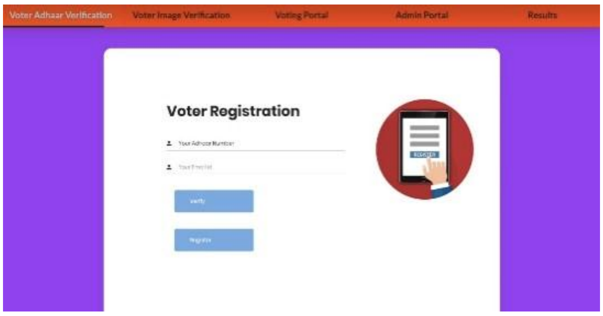


FIG 3.2 PROOF VERIFICATION OF THE VOTER

3.2.3 VOTING PORTAL

The voter logins into the website is shown in Fig 3.3 using their unique Blockchain account. This page will be redirected to the vote casting page where parties are displayed as shown in Fig 3.4, the voter will cast their vote to a specific party.

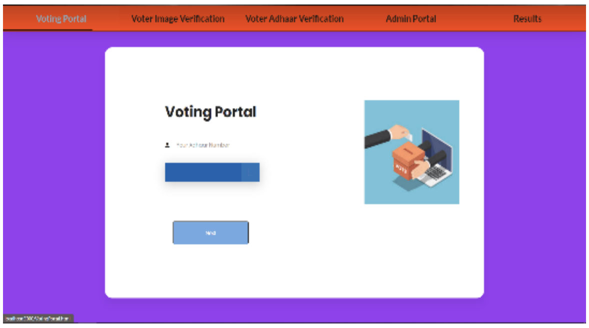


FIG 3.3 VOTING PORTAL FOR THE CANDIDATE

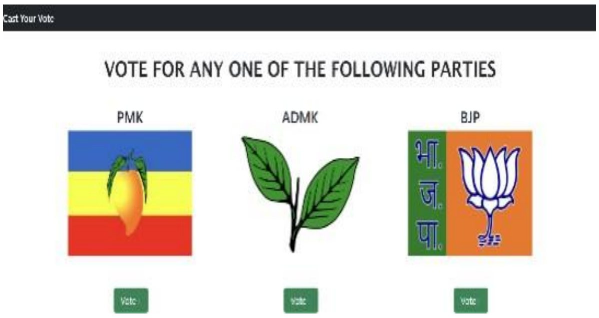
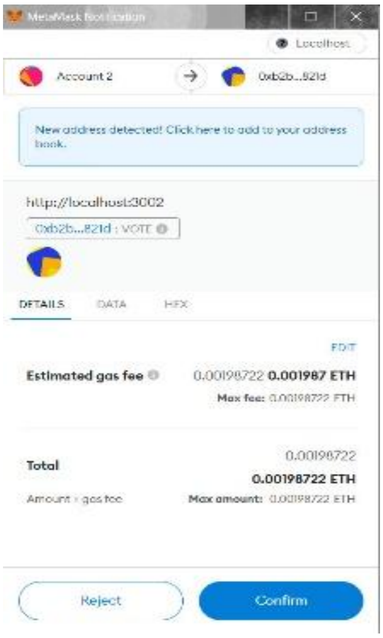


FIG 3.4 VOTE CASTING OF THE CANDIDATE FOR THE SPECIFIC PARTY

3.2.4 VOTE TRANSACTION

The next step is the casting of vote by the user. The voter logins into the e-voting website by entering the login credentials, the blockchain account which was given to the user after the authentication process was complete. The home page displays the candidates and parties of the election. The voters select the party they want to cast their vote for. Once the user casts his vote the page connects to the Metamask, a local blockchain environment where the voter can confirm their vote transaction. Vote transaction of vote casted is shown in Fig 3.5



New address detected! Click here to add to your address book.

http://localhost:3002

0xb2b...821d : VOTE

Estimated gas fee 0.00198722 0.001987 ETH
Max fee: 0.00198722 ETH

Total 0.00198722
0.00198722 ETH
Amount + gas fee Max amount: 0.00198722 ETH

FIG 3.5 VOTE TRANSACTION

3.2.6 RESULT VALIDATION

The next step is the result validation process. The result is computed using JavaScript function. The vote is incrementally added to the data as it is cast.

Once all the voters complete casting their vote the JavaScript function computes the overall result and the result is displayed in the page.

3.2.7 VOTE VERIFICATION

Once the voter is voted, he cannot cast his vote next time because of the blockchain transaction, there is a gas limit set for each transaction once the user finishes the gas limit he can't cast another vote. The gas limit is set as such only one vote can be casted for one cast.

IV. CONCLUSION

This project, "E-voting system using Blockchain" introduces a novel blockchain-based electronic voting system that uses smart contracts to provide secure and cost-effective elections while maintaining voter anonymity. In comparison to previous work, blockchain technology provides a new opportunity for democratic countries to move away from the pen and paper election system and toward a more cost-effective and time-efficient election system, while also increasing the security measures of the current system and demonstrating new transparency possibilities. In both political and scientific circles, e-voting is still a contentious issue. Despite the presence of a few excellent instances, the majority of which are still in use, many more attempts failed to provide the security and privacy aspects of regular elections or had substantial usability and scalability concerns. On the other hand, blockchain-based e-voting solutions, such as those that use smart contracts and the Ethereum network, address practically all of the security concerns, such as voter privacy, integrity, vote verification and non-repudiation, and counting transparency. However, some aspects cannot be addressed purely through the blockchain, such as authentication, which requires the integration of other methods such as biometric factors and digital signatures in the real time usage of the system. Blockchain technology has a lot of potential, but it still needs a lot of research and may not realise its full potential in its current state. A concentrated effort is needed to expand the fundamental blockchain technology's compatibility for increasingly complicated applications.

V. FUTURE WORK

However, there are still some implementation that can be applied to our system. We will continue to work on the additional implementation or improvements to our system in the future, and we will continue to research its future performance.

Basically our focus is on the development of more efficient and sophisticated system for E-voting using blockchain technology and its related variable tools.

VI. REFERENCES

[1] Prof. Mrunal Pathak , Amol Suradkar , Ajinkya Kadam , Akansha Ghodeswar , Prashant Parde's "Blockchain Based E-Voting System"-International Journal of Scientific Research in Science and Technology (2021).

[2] Abishek Yadav, Ashish Uttamrao, Yash Urade "E-Voting using Blockchain Technology" International Journal of Engineering Research & Technology, July-2020.

[3] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson "Blockchain Based E-voting System" International Journal of Scientific Research in Science and Technology(2019).

[4] Ashish Singh and Kakali Chatterjee "Secure Electronic Voting System Using Blockchain" International Conference on Computing, Power and Communication Technologies

(GUCON) Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018.

[5] D. Dwijesh Kumar , D. V. Chandini , B. Dinesh Reddy , Debnath Bhattacharyya and Tai-hoon Kim "Secure Electronic Voting System using Blockchain" International Journal of Advanced Science and Technology Vol.118 (2018).

[6] Cosmas Krisna, Rikard Hjort, Hiroyuki Sato "A Proposal of Blockchain-based Electronic Voting System" 2018 Second World Conference on Smart Trends in System, Security and Sustainability (2018).

[7] Kashif Mehboob, Junaid Arshad, Muhammad Mubashir Khan "Secure Digital Voting System based on Blockchain Technology" International Journal of Electronic Governement Research (2018).

[8] Yash Dalvi, Shivam Jaiswal, Pawan Sharma, "E-voting using Blockchain", International Journal of Engineering Research & Technology (IJERT), 2021.

[9] Bhavani Thuraisingham "Blockchain Technologies and their Applications in Data Science and Cyber Security", 3rd International Conference on Smart BlockChain (SmartBlock) (2020).

[10] LinHao Bai, LuoHui Liu, "Research on Software Defined Network Security Model Based on Blockchain", 2021 IEEE 6th International Conference on Intelligent Computing and Signal Processing (ICSP 2021).

[11] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", [Online]. https://bitcoin.org/bitcoin.pdf.

[12] Pluralsight (Jan. 19, 2019), "Blockchain Architecture", Pluralsight.com. Accessed: Mar. 13, 2019. [Online]. https://www.pluralsight.com/guides/Blockchain-architecture.

[13] M. Swan, Blockchain, "Blueprint for a New Economy", Sebastopol, CA, USA: O'Reilly Media, 2015.

[14] N. Ramkumar, G. Sudhasadaswam, K. G. Saranya, "Survey on different consensus Mechanisms on Blockchain Technology" 2020 International conference on communication and Signal Processing (2020).

[15] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparative Analysis on E-Voting System Using Blockchain", 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (Iot-SIU), Ghaziabad, India, 2019.

[16] T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology", 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020.

[17] Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M., A "Blockchain-based Self-tallying Voting Protocol in Decentralized IoT", IEEE Transactions on Dependable and Secure Computing (2020).

[18] Yang Jun-ho, Jin Min-goo, Lee Kyung-hee, Co-yung-won, "Design of Electronic Voting System based on Block Chain Security Technology", Journal of The Korean Information Science Society, 2018.