e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

SCORE BASED VOTING SYSTEM USING BLOCKCHAIN

Mrs. B. Ranjani[*1], Mr. Rajaguru. S[*2], Mr. Shamsundar. K[*3], Mr. Sriram. A[*4]

[*1]Assistant Professor, EGS Pillay Engineering College, Nagapattinam, India.

[*2,3,4]UG Student, EGS Pillay Engineering College, Nagapattinam, India.

ABSTRACT

The security considerations of the votes are based on blockchain technology using cryptographic hashes to secure end-to-end verification. To this end, a successful vote cast is considered as a transaction within the blockchain of the voting application. Therefore, a vote cast is added as a new block (after successful mining) in the blockchain as well as being recorded in data tables at the backend of the database. The system ensures only one-person, one-vote (democracy) property of voting systems. This is achieved by using the voter's unique face image, which is matched at the beginning of every voting attempt to prevent double voting. The Face Recognition is the study of physical or behavioral characteristics of human being used for the identification of person. So implement real time authentication system using face biometrics for authorized the person for online voting system. This work claims to score voting method and data management challenges in blockchain and provides an improved manifestation of the electronic voting process. Score-based voting methods, also known as range voting or rated voting, are electoral systems where voters are allowed to express their preferences for candidates or options by assigning numerical scores to them. Unlike traditional voting methods where voters choose a single candidate, score-based systems enable voters to provide a more nuanced and detailed assessment of their preferences. It is important here to note that cryptographic hash for a voter is the unique hash of voter by which voter is known in the blockchain. This property facilitates achieving verifiability of the overall voting process. Furthermore, this id is hidden and no one can view it even a system operator cannot view this hash therefore achieving privacy of individual voters.

Keywords: Online Voting System, Biometrics, Score Based Voting System.

I. INTRODUCTION

Blockchain technology utilizes advanced security compared to other platforms or record-keeping systems. Any transaction that is ever recorded needs to be agreed upon according to the consensus method. Also, each transaction is encrypted and has a proper link to the old transaction using a hashing method. Security is also enhanced by the fact that each node holds a copy of the transactions ever performed on the network. So, if any malicious actor ever wanted to make changes in the transaction.

1.1 BLOCKCHAIN TECHNOLOGY

Blockchain builds on the idea of P2P networks and provides a universal data set that every actor can trust, even though they might not know or trust each other. It provides a shared and trusted ledger of transactions, where immutable and encrypted copies of information are stored on every node in the network. Economic incentives in the form of native network tokens are applied to make the network fault tolerant, and attack and collusion resistant.

Blockchain and derived technologies provide a universal and transparent accounting and governance layer for the Internet. All network participants have equal access to the same data in real-time. Transactions running over the network are transparent to all actors and can be traced back to their origin. Blockchain can also be described as a distributed accounting machine or a supranational governance machine that is public and transparent. When the network validates a transaction by majority consensus, the transaction is permanently written to the blockchain. Otherwise, the transaction is rejected and does not go through. Only transactions that have been included in the blockchain are considered as valid and final.

A Blockchain protocol operates on top of the Internet, on a P2P network of computers that all run the protocol and hold an identical copy of the ledger of transactions, enabling P2P value transactions without a middleman though machine consensus. Blockchain itself a file a shared and public ledger of transactions that records all transactions from the genesis block (first block) until today.

Blockchain is a shared, trusted, public ledger of transactions, that everyone can inspect but which no single user

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

controls. It is a distributed database that maintains a continuously growing list of transaction data records, cryptographically secured from tampering and revision. Blockchain has three different types, i.e. public blockchain, private blockchain, and consortium blockchain. Bitcoin and Ethereum are the examples of public blockchain, anyone and from anywhere can join them and can get relieved at the time of his will. This is proofed by the complex mathematical functions. The private blockchain is the internal-public ledger of the company and the joining on that blockchain is granted by the company owning that blockchain. The block construction and mining speed is far better in the private blockchain as compared to public blockchain due to the limited nodes. The consortium blockchain however exists among the companies or group of companies and instead of the consensus the principles of memberships are designated to govern the blockchain transactions more effectively. This research uses consortium blockchain as the blockchain is to be governed by a national authority in the country. Block is the primary component of the blockchain. A block consists of the header and the body, the body of the block contains the transactions being written to the system. The header of the block contains the information about the block that includes previous hash, nonce value and difficulty, and the time stamp of the block and the transactions. The length of the block is variable and deemed to have been among1 to 8 MB of size. The header of the block uniquely identifies the block to be placed.

Fig 1.1: Block Creation

II. LITERATURE SURVEY

A literature survey provides an overview of existing research and scholarly work in user identification and secure voting process.

Kumar, and Chittaranjan Padmanabha Katti et al., (2020) proposed a new identity-based blind signature scheme that ensures the voter's anonymity. Proposed system adopts the Boneh–Lynn–Shacham short signature scheme that ensures the vote privacy with the least ballot size. The system provides a digital witness to a voter that enables him to check whether his vote is recorded as he meant and the public to check if all the recorded ballots are counted correctly.

Wang, Zikai, et al., (2022) proposed WeVoting, which provides weight based flexibility with solid anonymity and enhances usability by designing a voter-independent on-chain counting mechanism. Specifically, we use distributed ElGamal homomorphic encryption and zero-knowledge proof to achieve voting anonymity with weight. Besides, WeVoting develops a counter-based counting mechanism to enhance usability compared with those self-tallying schemes.

Li, Meiqi, et al., (2022) implemented AvecVoting, an anonymous and verifiable blockchain based e-voting scheme, providing both strong security and high performance. Specifically, we utilize threshold encryption and one-time ring signature to protect voters' privacy and ballots' confidentiality. Furthermore, to improve the performance, we introduce the concept "counter" to count the ballots.

Faruk, Md Jobair Hossain et.al., (2022) presented a biometric-enabled and hyperledger fabric-based architectural framework for e-Voting applications to automate identity verification that shall address the existing concern. Leveraging biometrics including facial and fingerprint recognition to automate the identity

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

verification process for election purposes shall enhance security and privacy, improve operational efficiency, and streamline the voter's experience.

Ibitoye, Ayodeji Olusegun, and Esther T. Adekunle., et.el., (2022) implemented a framework by using effective hashing techniques to ensure the security of the data. The concept of block creation and block sealing is introduced in this paper. The introduction of a block sealing concept helps in making the blockchain adjustable to meet the need of the polling process.

Pathak Neeru et.al., (2020) presented a new voting system employing biometrics in order to avoid rigging and to enhance the accuracy and speed of the process. The system uses a biometric method for voter's identification. The major two parts of the system are: enrolling and voting. All the voting machines are connected to a central database network, through which data transfer takes place to the local database. This information will be segregated according to the locality of the voter.

Farooq, Muhammad Shoaib, Misbah Khan, and Adnan Abid et.al., (2020) proposed a blockchain-based charity management platform that aims to provide a transparent, secure, auditable, and efficient system. The proposed platform comprehensively covers charity collection process using crypto wallets, Initial Coin Offering (ICO), economic model, and introduces CharityCoin (CC) as a digital currency.

III. ARCHITECTURE DIAGRAM

System architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes.

System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs).

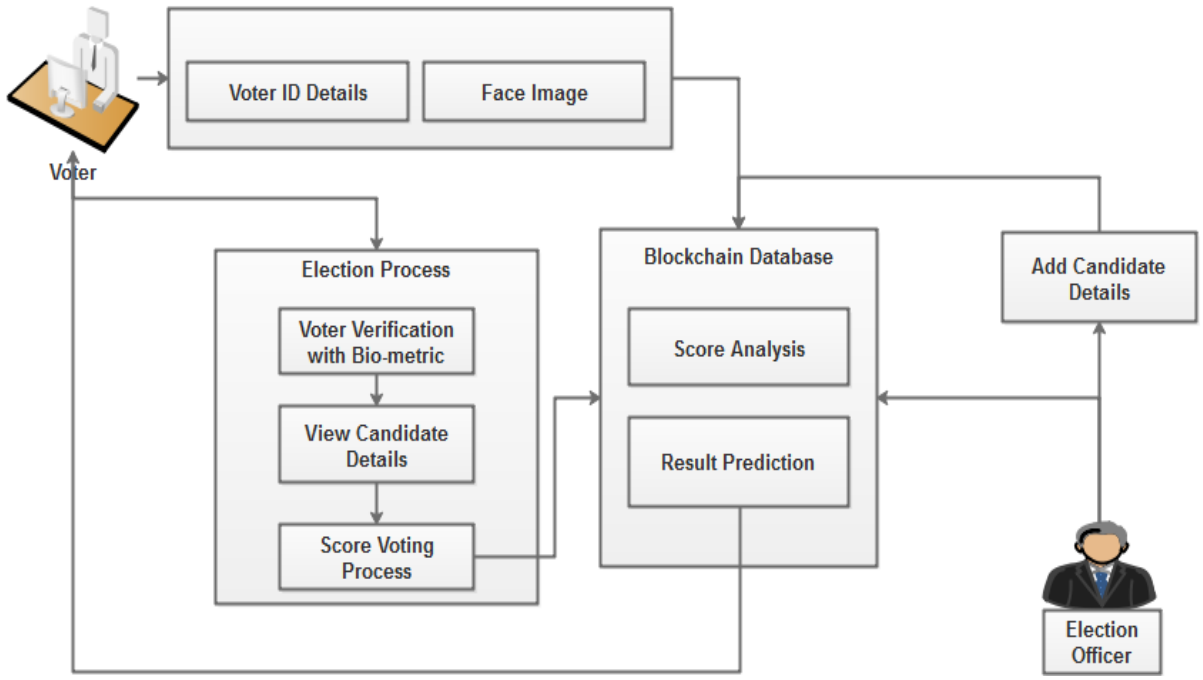

Fig 3.1:

IV. SYSTEM IMPLEMENTATION

MODULE 1: VOTING INTERFACE CREATION

The e-voting process requires the features like privacy, security, anonymity, and verifiability as the core function of this solution, it is important that the choice of the underlying technology is consistent to meet these challenges. It has been identified that the Blockchain technology sufficiently. This module explains about interface creation for secure voting process. Admin can contain unique user name and password to enter into

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

the system. Admin is responsibility to maintain all information in database up to date. In this module, admin can view voter information details are such as voter name, address, mobile number, age, gender and voter Aadhar card number and etc. these details are stored in the database. Admin can check the voter details in the system.

MODULE 2: ADD CANDIDATE DETAILS

This module explains about candidate adding process. The election commission is responsible for making the electoral lists available which are verifiable from the base records. Admin add candidate details like their name, symbol and Party name. These details are verified by candidates and added in voting database. During polling process candidate details will be shown to the voters.

MODULE 3: USER CREDENTIALS

User should enter their details for registration process. Once completion of registration process, users could allowed to access voting application. The details registered by users are Name, mobile number, age, gender, address, Aadhar card number, voter id, password and also capture face image for unique verification process. Admin can view voter registration information details. These details are stored in the system. And then admin can avoid illegal voter details in the system.

MODULE 4: USER VERIFICATION

In this module, voter can login in the system using voter id and password. Once the entered details are verified by server, then face image will be capturing for verification. Facial features are extracted and matched with server. Using these parameters users are verified during login process. From the voting machine the names and respective party symbols of each candidate are displayed and the voter can vote according to his will. Then user could select the candidate to make voting. Once completion of voting, the details are transferred to the server in a secure manner. The voter can vote only once, and once the vote is casted is voting record is marked as ``voted'', which restricts the voters from voting again.

MODULE 5: SCORE VOTING PROCESS

Score voting, also known as range voting or rated preference voting is an electoral system where voters express their preferences for candidates or options by assigning scores rather than choosing a single candidate. This system presents a list of candidates or options to the voters. Voters are provided with a scoring system, typically ranging from a minimum to a maximum value. Voters evaluate each candidate individually and assign a score based on their preferences. Once all voters have submitted their scores, the scores for each candidate are aggregated. The candidate with the highest total score is considered the winner.

MODULE 6: BLOCK CHAIN IMPLEMENTATION

The block creation in the electoral process is a basic entity and the voters can't record their vote if the block is not created. The voters can vote and the transactions are recorded in the blocks, by the time the polling time ends, the blocks are required to be sealed by the hash functions. The data of the block (i.e. the entire result) will be hashed using the SHA-256 algorithm. This is done by concatenating the results inside the block and hashing them in pairs the block is hashed based on the hashed contents of the block. Every proceeding block that confirms the completion of the transactions will have used the hash of previous block, a new random number, and hash of the block to generate the hash value that will be used by the proceeding blocks. The sealing of the block means that the block has now been sealed with a hash function and the contents of the block can't be changed by ensuring the application.

MODULE 7: RESULT ANNOUNCEMENT

The collection of the results is done from the stored data on the blocks through the significant organization of the nodes in the blockchain. Once the polling process is complete and the results have been announced, there will be no further need for continuing the mining or block creation activity.

V. CONCLUSION

This online voting system will manage the voter's information by which voter can login and use his voting rights. The system will incorporate all features of voting system. The transparency of score-based voting lies in the straightforward interpretation of scores. Results can be easily calculated and verified, fostering confidence

in the fairness and accuracy of the electoral process. This online voting system using block chain technology will manage the voter's information by which voter can login and use his voting rights. The system will incorporate all features of voting system. It provides the tools for maintaining voter's vote to every party and it count total no. of votes of every party. There is a database which is maintained by the election commission of India in which all the names of voter with complete information is stored. Voting detail store in database and the result is displayed by calculation. By online voting system percentage of voting is increases. It decreases the cost and time of voting process. In proposed voting system no one can make changes without the knowledge of hash value. This will improve the performance with reduced error rate.

VI. FUTURE ENHANCEMENT

Future work of this project is to include notification system for user's android mobile about result. Admin send all Information about voting to the user mobile. And also implement face recognition algorithm to improve the performance and speed of the face recognition process.

VII. REFERENCES

[1] Kumar, Mahender, Satish Chand, and Chittaranjan Padmanabha Katti. "A secure end-to-end verifiable internet-voting system using identity-based blind signature." IEEE Systems Journal 14, no. 2 (2020): 2032-2041.

[2] Wang, Zikai, Xinyi Luo, Meiqi Li, Wentuo Sun, and Kaiping Xue. "WeVoting: Blockchain-based Weighted E-Voting with Voter Anonymity and Usability." In GLOBECOM 2022-2022 IEEE Global Communications Conference, pp. 2585-2590. IEEE, 2022.

[3] Li, Meiqi, Xinyi Luo, Wentuo Sun, Jian Li, and Kaiping Xue. "AvecVoting: Anonymous and verifiable E-voting with untrustworthy counters on blockchain." In ICC 2022-IEEE International Conference on Communications, pp. 4751-4756. IEEE, 2022.

[4] Faruk, Md Jobair Hossain, Mazharul Islam, Fazlul Alam, Hossain Shahriar, and Akond Rahman. "Bie Vote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework." In 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), pp. 253-258. IEEE, 2022.

[5] Ibitoye, Ayodeji OJ, Halleluyah O. Aworinde, and Esther T. Adekunle. "An enhanced multi-level authentication electronic voting system." (2022).

[6] Pathak Neeru et al. "Biometric Based Secured Remote Electronic Voting System." 2020 7th International Conference on Smart Structures and Systems (ICSSS). IEEE, 2020.

[7] Farooq, Muhammad Shoaib, Misbah Khan, and Adnan Abid. "A framework to make charity collection transparent and auditable using blockchain technology." Computers & Electrical Engineering 83 (2020): 106588.

[8] Ajish, S., and K. S. AnilKumar. "Secure mobile internet voting system using biometric authentication and wavelet based AES." Journal of Information Security and Applications 61 (2021): 102908.

[9] Abayomi-Zannu, T. P., I. A. Odun-Ayo, and T. F. Barka. "A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication." In Journal of Physics: Conference Series, vol. 1378, no. 3, p. 032104. IOP Publishing, 2019.

[10] Ajish, S., and K. S. Anil Kumar. "Secure I-Voting System with Modified Voting and Verification Protocol." In Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT 2019, pp. 189-200. Singapore: Springer Singapore, 2020.