Blockchain Enabled Online-Voting System

Akhil Shah
Ramrao Adik Institute of Technology
Mumbai University
Navi Mumbai, India
akhilhshah04@gmail.com

Nishita Sodhia
Ramrao Adik Institute of Technology
Mumbai University
Navi Mumbai, India
sodhiablue@gmail.com

Shruti Saha
Ramrao Adik Institute of Technology
Mumbai University
Navi Mumbai, India
shrutisaha96@gmail.com

Soumi Banerjee
Ramrao Adik Institute of Technology
Mumbai University
Navi Mumbai, India
soumi.banerjee@rait.ac.in

Madhuri Chavan
Ramrao Adik Institute of Technology
Mumbai University
Navi Mumbai, India
madhuri.chavan@rait.ac.in

***Abstract*—A blockchain-enabled online-voting system is being proposed in this following paper. Blockchain technologies deliver an endless variety of applications that benefit from distributed economies. The proposed model is an android application that has enhanced security features which includes both authentication and authorization. Authentication is incorporated by using a unique identification key and authorization is done by using fingerprint. Voters are also being verified by One-time password. The security in this project is implemented by using a 128 bit AES encryption algorithm and SHA-256 along with blockchain. The vote is casted in the form of transaction, where a blockchain is created, which keeps track of tallies of votes. Through this atomicity and integrity are maintained. [4]**

***Index Terms*—Voting System , Blockchain , SHA-256, Security, AES-128, Ballot**

I. Introduction

Election has a very major role in democracy because it is the deciding factor of the future of a country but the major concern is that society doesn't trust the election system. Flawed electoral system is the issue faced by even the world's largest democracies like India, United States, and Japan. Overtime, the voting systems have evolved and the breach of security has evolved. The major issues that need to be addressed in the current voting system are vote rigging, EVM hacking, polling booth capture and election manipulation.

The problems were investigated in the voting systems in this project and attempting to propose the online-voting model that can solve these problems. Using an efficient hashing algorithm technique, block formation and sealing, data collection and result declaration by versatile blockchain method is needed to solve the issue a high-end to end system that ensures security and privacy. This project proposes an online-voting system that uses the Blockchain Ethereum to create a wallet with the credentials of the user. The elector will obtain an authenticated and tamper-proof personal ID. The voter will be getting the chance to vote in the form of token which would be transferred anonymously from voter's wallet to candidate's wallet. The vote can be casted from any geographical area for voter's allotted constituency. Blockchain also helps to preserve voters's anonymity while still being open to public inspection.

The proposed voting system uses more stable, tamperproof blockchain (unchanged from voting modifications either by the voter or by any other third party) and cost-effective. We would also extend the constraints of structure, engineering, design and implementation in our society of the voting mechanism.

II. Literature Survey

A. Online Voting System For India Based on AADHAR ID - Himanshu Agarwal, G. N. Pandey in the year 2013 [5]

A high security password is checked in the main database before voting is allowed. The voter will be able to confirm if the vote is transferred to the correct candidate or party. A person from his or her allocated constituency may also vote. The tallying of the votes can be done manually, thus saving the data.

B. Biometric voting system using aadhar card in india - S Chakraborty, S Mukherjee in the year 2016 [6]

The main goal of this venture is to build a safe electronic voting machine using Finger printing technique that distinguishes evidence, so that we can use the Aadhar card database for specific marks. The online-voting confirmation process should be possible during the race voting season using finger vein detection, which enables the electronic poll reset to allow voters to cast their votes.

C. Trustworthy Electronic Voting Using Adjusted Blockchain Technology - Basit Shahzad Raju, Jon Crowcroft in the year 2019 [7]

This paper suggests a system that makes use of appropriate hashing methods to ensure data security. This paper introduces the concept of block-creation and block sealing. The implementation of a block sealing principle helps to make the blockchain flexible to meet polling process requirements.

D. Security Analysis of India's Voting Machine - Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri in the year 2010 [8]

A Real Indian EVM Security Review is taken from anonymous source. The paper states that EVM is vulnerable to extreme attacks that may alter the outcome and breach the ballot's confidentiality. Use custom hardware, two attacks have been demonstrated.

III. Proposed System

We are proposing a system which has greater accessibility as it is an android application and possess greater security as authentication, authorisation 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.

IV. Proposed Methodology

A. BLOCKCHAIN

Blockchain is a decentralized, distributed, public leadger. [4]Blockchain is of three different types, i.e. public, private, and consortium blockchain. Ethereum and Bitcoin are examples of a public blockchain. This is proofed by the complex mathematical functions. This research uses public blockchain (Ethereum). Blockchain basically consists of a chain of blocks where a block is the primary component of the blockchain. A block is the header and the body, the block body contains the transactions that are being written to the network. The block header contains the block information which includes previous hash, nonce value and difficulty, block timestamp and transactions. [7] Each block also stores information about the person participating in the transaction. The block length is variable, and is estimated to be about 1 and 8 MB in size. The block header uniquely defines the block which should be put.

1) Working of Blockchain: Blockchain is a system that is built around peer to peer system that can be shared openly among the users to generate record of transaction that is immutable. In order to generate a block, a transaction needs to occur, after that the legitimacy of transaction needs to be verified. The transaction will then be stored in the block and a hash value must be given to the block for sealing. Thus a block is created and sealed.

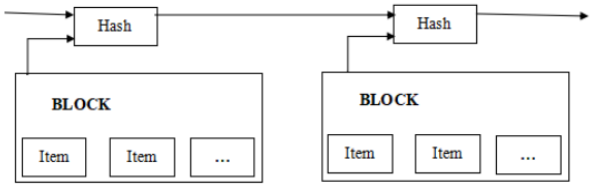

Fig. 1. Blockchain

B. ETHEREUM

Complex legal and financial applications such as Smart contract can be built and deployed using Ethereum as an open platform. Ethereum can be imagined as a programmable Bitcoin in which the underlying blockchain can be used by developers to build markets, mutual ledgers, digital associations and other endless possibilities involving unchanging data and agreements, all without the need for a middleman.Released in 2015, Ethereum is the brainchild of prodigious Vitalik Buterin who saw the possible applications of Bitcoins by Blockchain technologies as the next move in furthering the growth of the Blockchain culture. Ethereum is now the cryptocurrency with the second-highest coin market cap and is projected to overtake Bitcoin as both a valued investment and as the most common cryptocurrency in the world. [1]

C. HASHING

Hashing is the method of adjusting the arbitrary and variable input size to a fixed output size. There are various functions which perform different levels of hashing. We have implemented security by using SHA-256. SHA-256 is one of the SHA-1 (collectively referred to as SHA-2) successor hash functions and is one of the strongest hash functions available. SHA-256 is not much more difficult to code than SHA-1 and is in no way corrupted yet. [3] The 256-bit key makes AES a good partner feature which is a symmetrical key encryption cipher, meaning that the same key is used for encryption and decryption. Unlike its other predecessors, the algorithm's versatility is that it embraces any input length and produces an arbitrary output length, whilst all other algorithms generate a set output length.

D. Registration Module

The client or an individual will fill out the registration form in the registration module of the process after which their entry

will be registered in the database and they are now eligible to vote for their preferred candidate. Registration form filling is mandatory without which the person is not allowed or is not eligible to vote. The registration form includes the voter information and also some documents have to be uploaded once it is done the form is submitted and the entry is reflected in the database. After the registration form is submitted the phone number and the email id given by the user is verified and the registration process is completed.

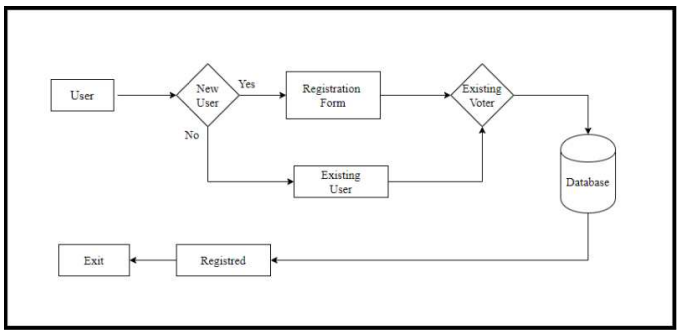

Fig. 2. Registration Module

E. Login Module

Once the registration form is submitted, the person is now eligible to vote. The user will sign in to the credentials in the authentication module and after which credentials will be checked and the user will only be able to access the dashboard after the verification has been completed. The first process in the dashboard is the OTP Verification. Once the user is verified then the user is authenticated with their fingerprint only after which the voter wallet is generated and a token is provided to the voter which will be used to cast their vote. The votes are casted by transferring the token from the voter's wallet to the respective candidate's wallet.

V. RESULT

In Fig 3, the login screen is being displayed wherein if a person is a new user the person can register itself with the application and if the user is an existing one they can login with valid user-id and password and thus login for the further process. The user will sign in to the credentials in the authentication module and after which credentials will be checked and the user will only be able to access the dashboard after the verification has been completed. The first process in the dashboard is the OTP Verification. Once the user is verified then the user is authenticated with their fingerprint only after which the voter wallet is generated and a token is provided to the voter which will be used to cast their vote. The votes are casted by transferring the token from the voter's wallet to the respective candidate's wallet

The above figure 4, displays the registration module wherein a new user can register oneself for the process and make a favourable vote. The users are allowed to register only once and cannot re-register thus avoiding repetitions.

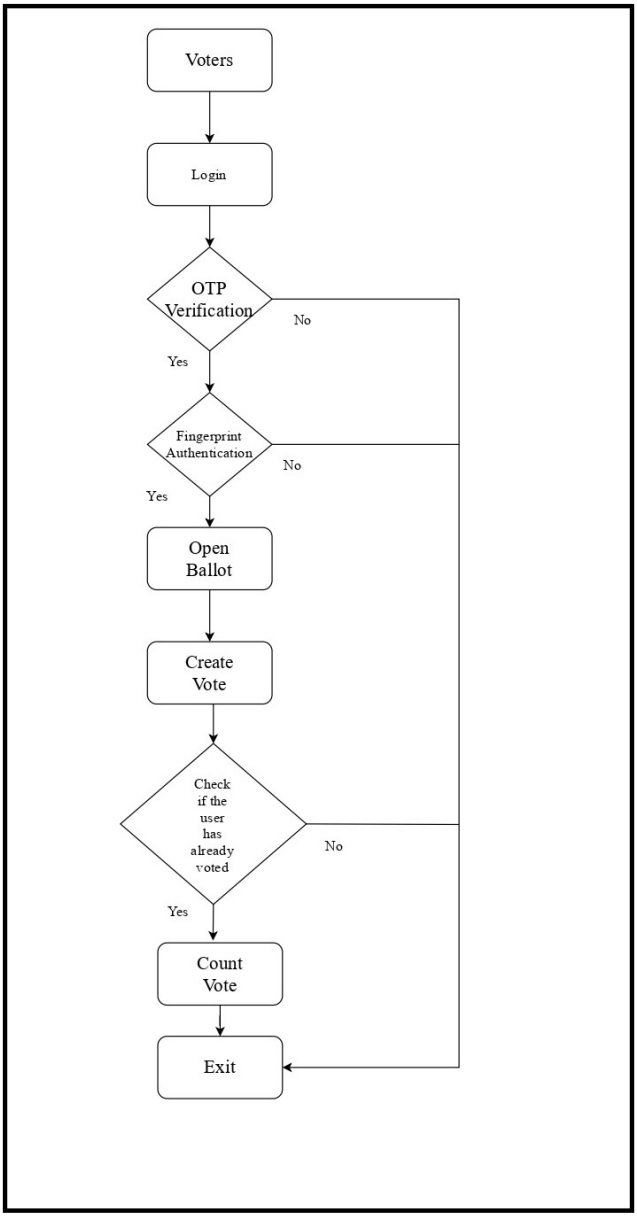

Fig. 3. Flowchart

The registration form contains various details which are to be filled by the user such as name, phone number, email-id, password, Aadhar card number etc.

In Fig 5 the verification module is being displayed in which as soon as the person logs in, the user receives a One-time password on the registered phone number. The person is logged into its respective dashboard only after the OTP is verified.

The above figure 6 displays the fingerprint authorisation

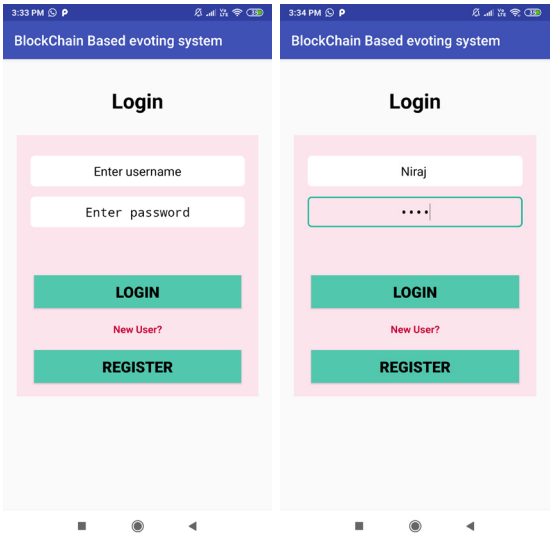

Fig. 4. Login Module

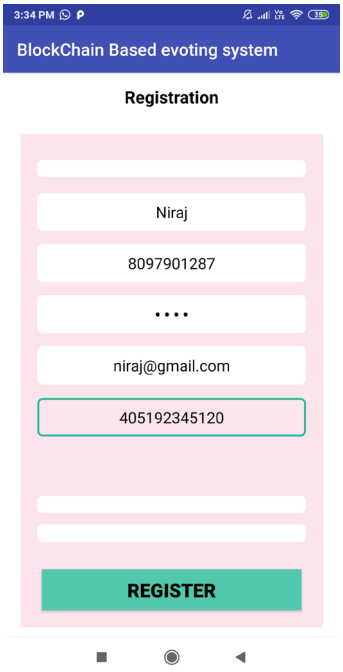

Fig. 5. Registration Module

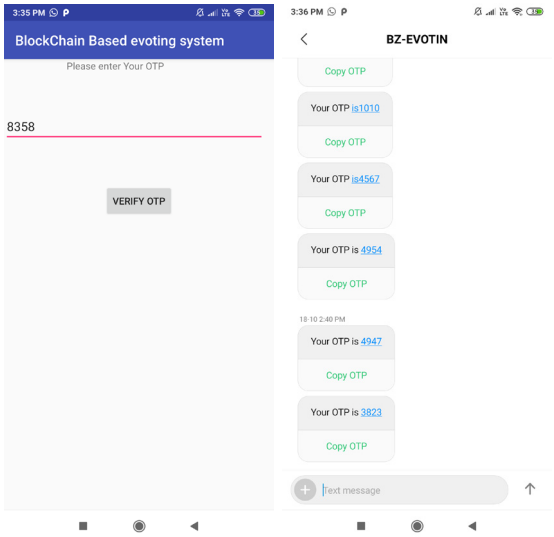

Fig. 6. Verification Module

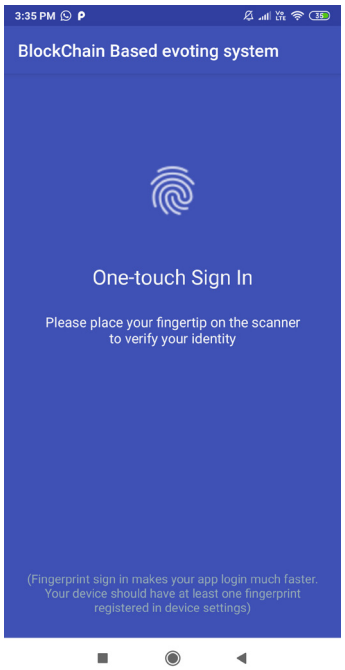

Fig. 7. Authorisation Module

module which enables only authorised users to login and be a part of the voting process.

Figure 7 depicts the dashboard screen where the electoral symbol of participating parties are displayed, which on click casts a vote to the respective party and once a vote is being casted the voter is not allowed to cast a vote again and after some time the user is automatically logged out to avoid multiple casting of vote from an individual.

Figure 8 depicts the admin module where the process of vote counting takes place.

Figure 9 depicts creation of new blocks. New blocks are added and sealed, the blocks are sealed using SHA-256 along with AES-128 algorithm.

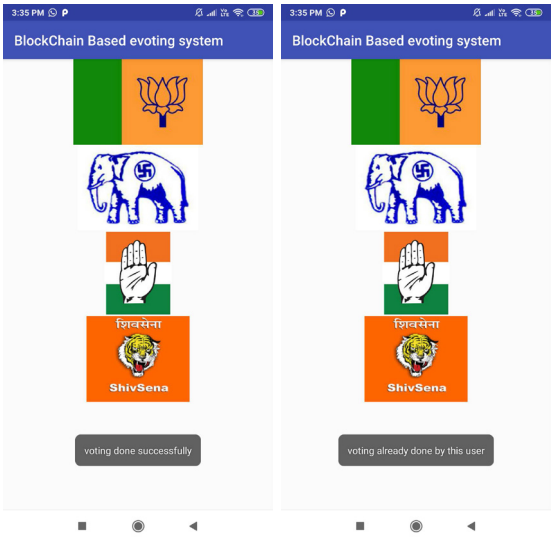

Fig. 8. Dashboard

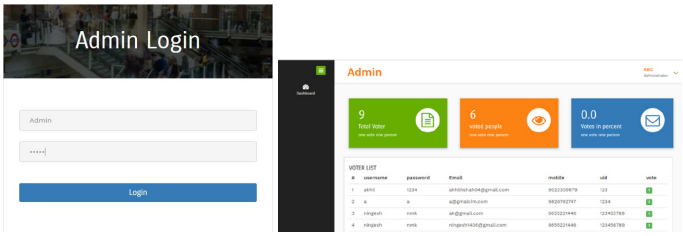

Fig. 9. Admin

VI. Conclusion

The concept of incorporating online voting systems to make the public election process cheaper, quicker and easier is a compelling one in modern society.Having the electoral process cheap and fast, normalizing it in the electorate's eyes, removing a certain control barrier between the elector and the elected official and putting some pressure on the elected official. It also opens the door to a more transparent type of democracy that requires electors to speak their will on specific bills and initiatives.

We have deployed online-based blockchain voting framework in this project where smart contracts are used to allow secure and cost-effective election while preserving the secrecy of the voters. Compared with previous research, we have shown that the blockchain technology provides a new opportunity for democratic countries to move from the pen and paper election scheme and paperless direct-recording electronic voting machine (DRE) to a more cost-effective and time-efficient election scheme, thus mounting the security measures of the current scheme and offering new accessibility.

VII. Comparative Study

A. Online Voting System For India Based on AADHAR ID - 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 in many ways such as, tampering with software before CPU manufacture, tampering with machine state, substituting a look a-like CPU and/or a unit and thus secrecy of the ballot can be violated. The proposed voting system does not have any major hardware requirements, thus elimination all the above disadvantages of EVM. Also the proposed model uses blockchain which ensures that the vote transfer to candidate's ballot is easy and secure.

VIII. Future Scope

The current system uses ethereum which is public blockchain. It is permissionless in nature as nothing is standing in the way of participation and anyone is able to engage with consensus mechanism, scaling obstacles have been encountered and throughput is relatively weak. [2] To avoid such issues consortium blockchain can be used which combines elements from both public as well as private blockchain.

The current project is built for small organization, but in future we would build it as a national voting system. In addition to the present fingerprint module which is used

for authorization a facial recognition module would be incorporated for better security.

REFERENCES

[1] The ethos blog. https://www.ethos.io/cryptocurrency-news-ethos-blog. Accessed: 2020-01-27.
[2] Private, public, and consortium blockchains - what's the difference? https://www.binance.vision/blockchain/private-public-and-consortium-blockchains-whats-the-difference. Accessed: 2020-01-24.
[3] Sha-256 hashing algorithm. https://www.movable-type.co.uk/scripts/sha256.html. Accessed: 2020-01-27.
[4] What is blockchain. https://www.investopedia.com/terms/b/blockchain.asp. Accessed: 2020-01-24.
[5] Himanshu Agarwal and GN Pandey. Online voting system for india based on aadhaar id. In *2013 Eleventh International Conference on ICT and Knowledge Engineering*, pages 1–4. IEEE, 2013.
[6] Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan, and Kazi Tanvi Yasmin. Biometric voting system using aadhar card in india. *International journal of Innovative research in Computer and Communication Engineering*, 4(4), 2016.
[7] Basit Shahzad and Jon Crowcroft. Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, 7:24477–24488, 2019.
[8] Scott Wolchok, Eric Wustrow, J Alex Halderman, Hari K Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. Security analysis of india's electronic voting machines. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 1–14, 2010.