E-Voting using Blockchain Technology

ABSTRACT:

From the past decades, traditional means of voting has been put to use; many countries are still using the same ballot paper and EVM machines till today. The main disadvantages of these systems are; unfairness in the conduction of voting pattern, as it is based on centralized system the main authority can manipulate the vote count; in booth system people from various places has to come to the booth to vote, this puts the system at the main disadvantage, the voting rate also decreases due to this. To overcome all of these issues e-voting system has come into existence; with blockchain technology the voters vote can be can be more secure than the traditional systems; the use of smart contracts enables only the authorized users to vote only once in the network; the use of Ethereum blockchain is suggested, which ensures only authorized people to vote, and doesn't allow unauthorized users in the network. This framework proposed in this paper discusses the use of Ethereum blockchain which provides more security to the system. This increases the security, integrity and transparency of the e-voting system.

Keywords: hashing; Ethereum blockchain; EVM; Smart contracts.

1. INTRODUTION:

A vote represents the opinion of the people based on the options provided to decide the formation of electoral bodies. Voting can be implemented in college elections, associations, political elections, organizations events and in companies. To make the best decisions through voting, some critical factors should be taken into consideration, among such factors one finds: decentralization, as the name itself defines there will no fixed central organisation to monitor the votes or to provide the results of the poll; accessibility/user-friendly the whole voting process should be easily accessible to the voters, and should not be burden to people to cast their vote; unchangeability, this ensures that the cast vote cannot be manipulated or altered; variability, this is to verify whether the cast vote has been altered or not; intractability, the cast vote has to be untraceable to any user, and the vote should be confidential and secure. If any of these factors are altered, then the whole voting system will be compromised.

As India is the largest democratic country in the world, the election process must be fully secure and confidential, currently all over the world voting is done through ballot paper and through EVM Machines, these methods of voting has many disadvantages like, tampering of votes, low-voter turnout, security issues, delayed results, transparency and forging of voter-ID's. To cease all these drawbacks of the traditional voting mechanisms.

The escalation of blockchain has been since the cryptocurrencies and bitcoin came into existence. Blockchain ensures that the whole system can be decentralized and secure to make any transactions according to user's choice. As blockchain implements peer-to-peer connections among its blocks, therefore data tampering or forging is almost impossible, if one has to alter data, then the whole system(every peer) data should be altered, thus making impossible to alter data in blockchain, blockchain improves system's integrity, anonymity and non-repudiation.

Many countries have taken e-voting system into serious consideration in implementing e-voting and are working on it to get accurate voting rate and easy, secure voting system; Government of Estonia is the first country to implement e-voting system. Currently they are using e-voting system and are working on the more secure ways to vote easily; now their system is robust, reliable and cost-efficient that the traditional voting systems in other countries. Switzerland is another such example, that is covering its voting system to e-voting system, although Switzerland is known for its widespread democracy, and every citizen above 18 years can participate in elections. So by taking these countries as example India can implement e-voting system to provide secure and fair elections to the people. This makes voting easier, cost-efficient, and with the advantage that people can vote from wherever they are, can make the voting percentage vote to upswing.

This article mainly focus on implementing voting system through blockchain technology. This paper describes implementing e-voting through smart contracts, Ethereum blockchain technologies, and upgrading existing e-voting systems with facial authentication for more secure process, and maintaining core values: trust, transparency and immutability of e-voting system.

1.1 Block chain

Blockchains are incredibly popular nowadays; like the name indicates, a blockchain is a chain of blocks that contain information. This technique was originally described in 1991 by a group of researchers and was originally intended to timestamp digital documents so that it’s not possible to backdate them or to tamper with them. Later it was adapted by Satoshi Nakamoto in 2009 to create the digital cryptocurrency bitcoin. A blockchain is a distributed ledger that is completely open to anyone. Properties of blockchain are: once some data has been recorded inside a blockchain, it becomes very difficult to change it.

Each block in a blockchain contains some data, the hash of the block and the hash of the previous block. The data that is stored inside a block depends on the type of blockchain. A block also has a hash, it works same as finger print; it identifies a block and all of its contents and its always unique, just as fingerprint. Once a block is created, its hash is being calculated. Changing something inside the block changes the hash value. It helps to detect the changes in the block hence it is easier to detect changes with the hash value therefore the voters vote cannot be tampered.

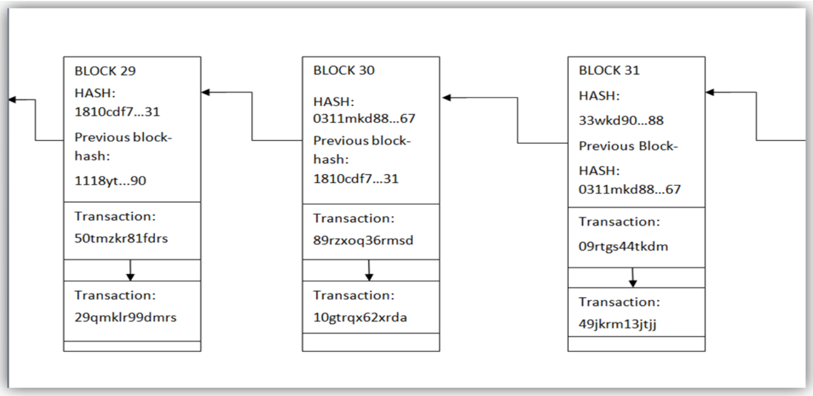


Figure-1 Simplified Block-chain

This technique helps the system with added security and resolves tampering and transparency issues which were part of traditional voting system; and provides best way to the user to cast their vote in a easier and secure way

1.2 Smart contracts

smart contracts are trackable and immutable application that runs on a decentralized environment. Once smart contract is deployed, then it cannot be changed or edited in its execution behavior. Smart contract allows the block to bind together, and execute or run a transaction in an agreement manner.. We implemented e-voting system based on smart contracts in a permissions blockchain. Smart contract is a collection of code and data, that runs on a Ethereum blockchain.

2. LITERATURE SURVEY:

Although there are many alternatives for implementing voting in online platforms, there are certain challenges in all these proposed architectures, among many challenges, blockchain can resolve the security issues using a decentralized system

As Traditional voting systems like ballot paper voting and EVM voting failed to provide the required security, Anonymity and Integrity to the voter's vote, due to this e-voting system became prominent and effective.

Many people have worked on different ways to promote voting on the internet platform, for an easier and more secure voting system. Out of those a journal paper[1] The author uses, the smart contracts and the PKIs for the verification and digital signatures for the first step of e-voting which is well grounded and effective, also explains the e-voting using decentralized e-voting system with the voter privacy rights.

Limitations: Implementing the changing or updating the vote, may lead to a less productive system, which increases the complexity of the algorithm, the affects the ongoing process of e-voting statistics.

In another paper[2], the Author put forwards the idea of using the Ethereum blockchain technique in the e-voting systems, this paper uses smart contracts for the verification and digital signatures of the blocks, which is secure, cost inexpensive, unmistakable and convenient to use e-voting systems. The idea of using Ethereum blockchain and smart contracts for e-voting is itself a high-minded, if an implementation is successful, then e-voting will be secure enough to process all the voting through e-voting systems.

Limitations: Using smart contracts and Ethereum alone takes up more storage.

Paper[3], the author institutes about various authentication types like using biometric fingerprint using Aadhar card authentication, which enables the user to access the e-voting system using biometric fingerprint and verifies the Aadhar number for further processing of the voting system.

In paper[4] author has used neural networks after extracting the facial features of the voter and with that a reference to voting during an election. If the details match the existing details the user is allowed to vote.

In Paper [5]" Author insinuates, the whole blockchain process and how it works in the process of e-voting and explains how the hashing and Elliptic curve digital signature algorithm, provides the same amount of security as DSA but with smaller key length, allowing for faster calculations. This algorithm is a development of a generalized digital signature algorithm using the ECC algorithm in the digital signature generation process and its verification

3. SYSTEM PROPOSAL:

Phases of Proposed system:

The paper is divided into three modules based on the functionalities in each phase.

3.1 Pre-voting phase:

1. The user has to register to the network and get permission to vote in the described chain of networks.

The user has to create an id according to his official voter id information and log in to the network, here the previous blocks verify the new block(user) information, whether it is according to the data stored in the database or not. If the new block is validated correctly, the network allows the block to process to the next stage in the voting process.

2. The user has to verify his identification using facial authentication and then process further steps in the voting process

3.2 Voting phase:

After successful face authentication, the user is allowed to vote, the user's vote will be encrypted by the public key encryption and once the user has voted, then he cannot re-login and vote in the network, this re-voting using the same id is restricted using smart contracts.

The vote cannot be manipulated, if one has to change his/her vote after voting, then it is almost impossible because to change one vote, the entire system of blocks should be changed, and every node in the network should authenticate, as every block contains every block information and transaction.

3.3 Post-voting phase:

Once the user has cast his vote,

1. If the voting poll has not ended: then he can only view the percentage of voting, that is how many people have cast their vote

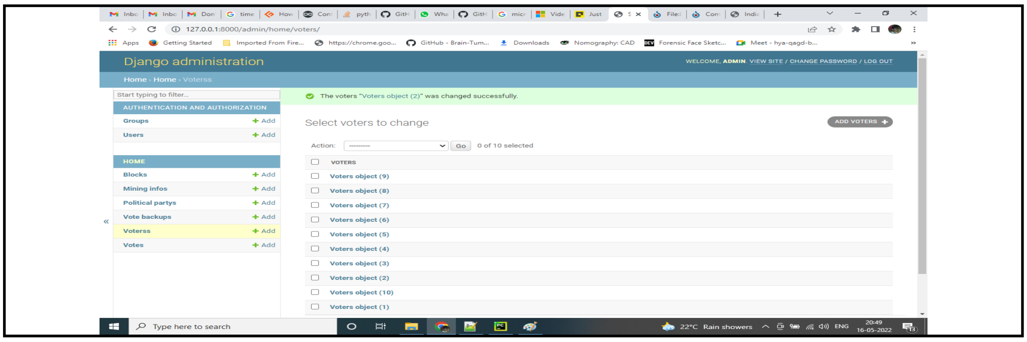
2. If the voting poll has ended: then he can see the complete result of the election with the percentage and rate of the vote.

4. IMPLEMENTATION:

In this module, we demonstrate each phase in the voting web applications; where the user can cast his vote with privacy and transparency in a web application platform.

1. Enrollment phase: the voter has to enroll his details before voting, like by providing the unique-id, name and other attributes. All this recorded data will be registered in the database.
2. Login phase: once the user registers, he can directly login with the unique-id provided. In this phase the user has to authenticate themselves using face-id; this provides enhanced security to the system.
3. Ethereum Blockchain: blockchain is mainly used to enhance the security of the system by providing integrity and privacy to the user to cat his/her vote; with the convection of smart contracts enables the user to cast his/her vote only once in the provided network.
4. Database(storage): the user/voters particular attributes like name, gender, age, date of birth and address are recorded into the database. We have implemented dijango databases for accelerated operations in the network.
5. Result phase: all the voters votes are taken into considerations to provide the end-result to the voters on the same website. With the show vote count option in the website the users can know the percentage of voting and live result.

Admin controls the user and candidate profile in the website designed; admin is responsible for adding the candidate details and maintaining the user details in the database.



Django administration

WELCOME, **ADMIN**. VIEW SITE / CHANGE PASSWORD / LOG OUT

Home › Home › Voterss

Start typing to filter...

AUTHENTICATION AND AUTHORIZATION

Groups + Add

Users + Add

HOME

Blocks + Add

Mining infos + Add

Political partys + Add

Vote backups + Add

Voterss + Add

Votes + Add

The voters "Voters object (2)" was changed successfully.

Select voters to change

ADD VOTERS +

Action: --------- Go 0 of 10 selected

□ VOTERS

□ Voters object (9)

□ Voters object (8)

□ Voters object (7)

□ Voters object (6)

□ Voters object (5)

□ Voters object (4)

□ Voters object (3)

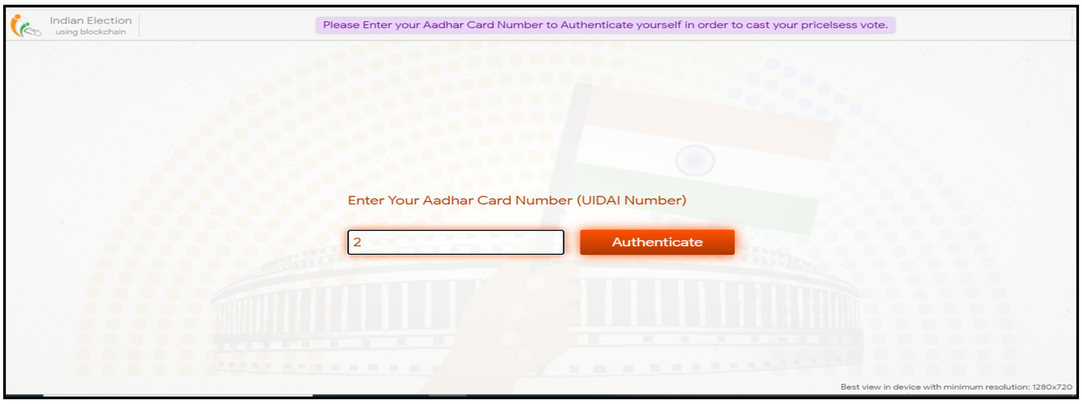
□ Voters object (2)

□ Voters object (10)

□ Voters object (1)

Figure-3 Admin Administration

With the designed application webpage, the user has to register with his unique Aadhar number, to proceed further in voting phase



Indian Election using blockchain

Please Enter your Aadhar Card Number to Authenticate yourself in order to cast your pricelsess vote.

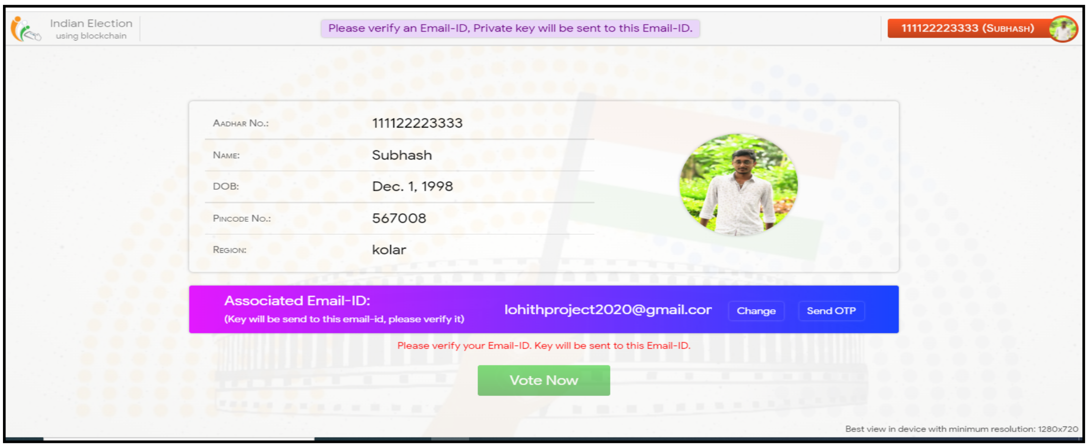
Enter Your Aadhar Card Number (UIDAI Number)

2

Best view in device with minimum resolution: 1280x720

Figure-4 Aadhar authentication

verifying the details of the voter, to send the private key to the voter e-mail id



Indian Election using blockchain

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

111122223333 (Subhash)

Aadhar No.:	111122223333
Name:	Subhash
DOB:	Dec. 1, 1998
Pincode No.:	567008
Region:	kolar

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

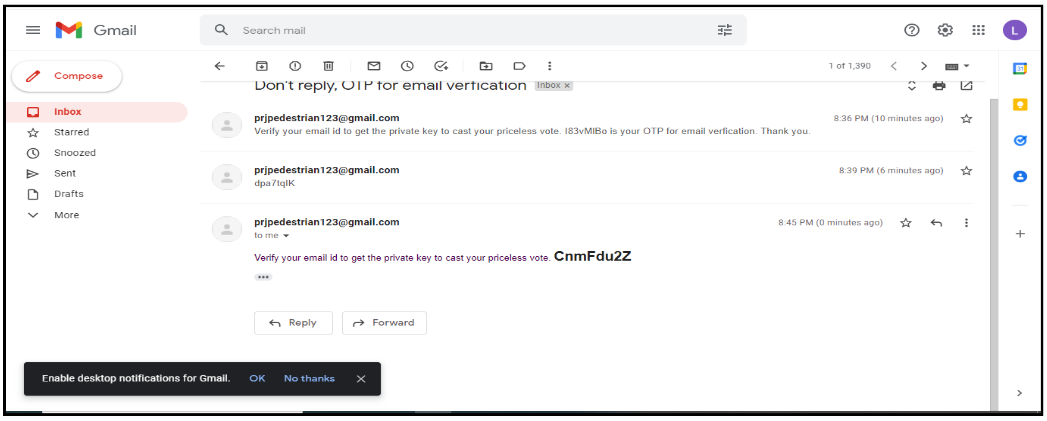
lohithproject2020@gmail.cor

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

Best view in device with minimum resolution: 1280x720

Figure-5 voter details

Once the Aadhar number is verified, the user details will be display as stored in the database, and unique private key(block-no) will be sent to the recorded e-mail id, by which the user will be authorized to vote.



Don't reply, OTP for email verfication Inbox ×

prjpedestrian123@gmail.com 8:36 PM (10 minutes ago)
Verify your email id to get the private key to cast your priceless vote. I83vMIBo is your OTP for email verfication. Thank you.

prjpedestrian123@gmail.com 8:39 PM (6 minutes ago)
dpa7tqlK

prjpedestrian123@gmail.com 8:45 PM (0 minutes ago)
to me

Verify your email id to get the private key to cast your priceless vote. CnmFdu2Z

Enable desktop notifications for Gmail. OK No thanks

Figure-6 Block and private key creation

Private key will be directed to the recorded email-id, with the key, the voter can vote to the respective party and choice. With the confirmation of the block number and private key, the user is authorized to vote; Once the poll ends, the users can view the result on the same web application

6. CONCLUSION:

The proposed framework provides complete security to the e-voting system, with the usage of Ethereum blockchain and smart contracts to provide added security to the system. Blockchain implementation prevents vote manipulation and provides privacy, integrity for voters to cast their vote. Smart contracts ensures that the voter can vote only once using his/her unique id (Aadhar number); with the convention of different security algorithms like SHA-256, Merkel hash and SMTP prototyping, enhances the security of the system. As a result, the voter is authorized to cast his/her vote from where ever they are; provides high security standards to the system and convenient and easier ways to vote.

References

[1] AMNA Qureshi ‘‘SEVEP: Verifiable, secure and privacy preserving remote pollingwith untrusted computing devices,” in Future Network Systems and Security Feb 22(2019) IEEE.
[2] S. Ganesh Prabhu, Rachel, Agnes Shiny, and A. R. Roshinee. "Tracking Real Time Vehicle and Locking System Using Lab View Applications." In 2020 6th International Conference onAdvanced Computing and Communication Systems (ICACCS), pp. 55-57.IEEE, 2020.
[3] Annoshmitha Das “VOT-EL: Three Tier Secured State Of-The-Art EVM DesignUsing Pragmatic Fingerprint Detection Annexed with NFC Enabled Voter -ID Card” (2016) IEEE.

[4] Shekhar Mishra and Y. Roja Peter - “Electronic Voting Machine using Biometric Finger Print with Aadhar Card Authentication”, International Journal of Engg. Scienceand Computing, March 2018.

[5] Maaten, “Towards remote e-voting: Estonian case”, Electronic Voting in Europe-Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004.

[6] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[7] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, [Online]. Available: https://bitcoin.org/bitcoin.pdf .

[8] F. Hao and P.Y.A. Ryan, Real-World Electronic Voting: Design, Analysis and Deployment, CRC Press, pp. 143-170, 2017.

[9] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[10] Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* 2014, *151*, 1–32.

[11] Çabuk, U.C.; Adiguzel, E.; Karaarslan, E. A survey on feasibility and suitability of blockchain techniques for the e-voting systems. *arXiv* 2020, arXiv:2002.07175.

[12] Khan, K.M.; Arshad, J.; Khan, M.M. Secure digital voting system based on blockchain technology. Int. J. Electron. Gov. Res. 2018, 14, 53–62.

[13] Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. Future Gener. Comput. Syst. 2020, 105, 13–26.

[14] Baran´ski, S.; Szyman´ski, J.; Sobecki, A.; Gil, D.; Mora, H. Practical I-voting on stellar blockchain. Appl. Sci. 2020, 10, 7606.

[15] Gorenflo, C.; Lee, S.; Golab, L.; Keshav, S. FastFabric: Scaling hyperledger fabric to 20 000 transactions per second. Int. J. Netw. Manag. 2020, 30.