ISSN 2395-1621

Secured Electronic Voting Using Blockchain Technology

Pratik Shinde, Vishal Batheja, Shubham Basagare, Aishwarya Chillal,
Prof. Prajwal S Gaikwad

shindepratik488@gmail.com
vishalbatheja97@gmail.com
shubham13mera@gmail.com
aishwaryachillal.12@gmail.com
prajwaltrk@gmail.com

Computer Department, AISSMS IOIT
Kennedy road, near RTO, Pune, India

ABSTRACT

Building a digital voting-system that satisfies the necessities of time from a very long time. This paper mainly focuses for the evaluation on Blockchain as provider to electronic voting-system. Blockchain provides a very long range of application which will definitely benefit the economy. For the fact generation, disbursed ledger is an important technology. We can also propose the electronic voting-system which is totally based on blockchain. More-over this paper, gives you the brief idea for implement of secured electronic voting-system using Blockchain which is secured and cheap. This paper also provides the requirements to build this voting-system. This paper also gives a brief idea about the architecture of the same system. Also, gives the idea about blockchain framework that provides it as a carrier.

Keywords— Blockchain, Electronic Voting

ARTICLE INFO

Article History

Received: 8th March 2020

Received in revised form :

8th March 2020

Accepted: 10th March 2020

Published online :

11th March 2020

I. INTRODUCTION

Now a days, democracy is the backbone of every democratic country. It's been more than 15 years now, the computer enthusiasts have studies all the possible ways to conduct an election digitally, having an aim in mind to control the spends which has been done on general election of any country. Also, to build trust in the people of that democratic country. And, to conduct unbiased and secured elections. From the very start of democratical election process, there are multiple options to cast a vote. Such as pen and paper, ballot and paper, EVM also known as Electronic Voting Machine. By using the EVM's, it is very hard and critical to stop the frauds and keeping the voting process traceable and verifiable.[2]E-Voting machines are always been considered as a weaken key of voting-systems. With the help intrusion in network of such devices, anyone can tamper such devices and we cannot avoid the chances of changes or tampering in the votes. After the entry of Blockchain technology in industry, there is a new hope and way to make solid secure the voting-systems. A blockchain technology is always famous for it's distributive, immutability, incontrovertibility, and being publicly ledger. The Blockchain work on these four primary capabilities:

(i) Not a single point of failure is expected for the maintenance of such a distributed ledger, though the ledger may reside in multiple or in various locations.

(ii) Being a distributed, there is control on the transactions which are happening to the ledger whether it is the new transaction such as append.

(iii) The keeping version tracked is very important. Any of the proposed 'New Blocks' those are the new addition to the ledger has the reference to the previous version of the ledger. Making this chain immutable chain is very important. Such things, helps to get the blocks name, and tampering prevention because of the previous entries.

(iv) While adding a new block as the part of chain there must be an agreement to make it the part of the ledger with the full majority. This can be achieved with the help of highly demanded technological features like advanced

cryptography to provide more security where the data resides. That is nothing but the database.
This review paper evaluates the use of Blockchain as a Service (BaaS) for the implementation of secured and unbiased digital/ electronic voting-systems. That' s the reason the blockchain is considered by most of the people, an ideal and stable tool, which is need to be used in the creation of new and modern way to conduct the democratic voting-systems.

II. PRELIMINARIES OF E-VOTING AND BLOCKCHAIN

In this section, we will have a brief look at liquid democracy and its various aspects. Also, we then can provide broad overview of blockchain and its abilities as mainstream provider to conduct a election with the help of electronic gadgets for the use of voting for the liquid democracy together to give an overview of use and implementation of such technologies in such highly important systems.

A. Liquid Democracy Design Considerations: The basic and simple motive in a liquid democracy is voter is a king. He has the ability and a power to review the way he casted his vote at any given point of time. This helps people to make decisions to cast the votes. Which results the formation of a good and qualified government. Liquid Democracy is the only solution for all the public requests. As we know, there are multiple factors which are the barriers in its way likewise social as well as technical. And to overcome on such technical problems associated with it could be absolutely necessary for the new and strong phase of democracy.
There are some essential prerequisite which needs to be get fulfilled by a electronic voting-systems in order to the conduct successful general elections for the bright future of the nation:
(i) Any voter should not get forced to cast his/her vote.
(ii) System should be secured enough so that, no one can trace a vote which cast by any 'xyz' person.
(iii) As we know, to maintain the secrecy, the identification of a vote is mandatory and should be strict. The counting of votes should give the exact and correct total number of votes casted with compared to total numbers of identified voters.
(iv) The election should be conducted by government only. So that the tampering of vote will be next to impossible.
(v) The calculation of votes should be unbiased and secured.
(vi) As per the country's eligibility criteria to cast a vote, should be followed in electronic voting-systems.

B. Blockchain as a Service: The cryptocurrency named "Bit-Coin" was first introduced by Satoshi Nakamoto in 2008. The mining and generation of Blockchains for the Bitcoins is used with help of decentralized public ledger alongside with concept of 'Proof of Work' which is based on agreement. To document a totally organized and structed collection of those blocks which is nothing but a blockchain. This chain is replicated, cryptographically secured and worldwide-verified for every transaction so that no one can tamper with the data which is written in that block of the blockchain. Whereas the structure of the blockchain is like a append-only in a statistics shape, so that new block of the records can be added to it, and this block or data cannot be altered and deleted. The chaining is implemented in such a fashion that every block has its unique identity which is nothing but a hash value that could be a function of the next or last block. Which gives the assurity of immutability. To complete a chain, Bitcoin powered blockchains publishes each and every factor, so that other types of the chain of that blockchain be public, private, or like a association. Public blockchains make sure that any of the users which is the part of that community can get admission to read, and can create a new transaction. Most of the times such scenario is used for the Cryptocurrencies like Bit-Coin, Ethereum, Dogecoin, Aurorocoin, etc. Consortium type of blockchain is a centralized in manner of blockchain, in which the agreement is done by means of some set on nodes which are already pre-selected.
As public blockchain allows admissions to read, in the same way private blockchains limits to the admission write. But such transaction can be precise internally. Which results the transaction non-public and network cheaper. So that they can be verified by few nodes in the cluster. How well linked and a fault can speedily get fix, results the nodes dependency, to allow the agreement algorithm to charge shorter block instances. In our project, we will use a fully permissioned blockchain. A agreement based system of chains, which allows proof-of-work (POW) agreement types of rules. In such work based clusters, all the blocks of blockchain and transaction of that chain are get validated to check every node of that cluster is part of that agreement. The main moto to pick this protocol make nodes perform computationally fast so that they could present their valuable opinion in the formation or to any of the new block of that chain. The node which first solves the hassle, that node is winner to mine that new block and send messages to other nodes to rectify the values which are present on that block. This happens because all the hashed values are present on that block inside that blockchain on all the last know nodes in the blockchain. If any of the attacker tries to add a single block in between the history that may result as invalid chain. Unless and until future blocks get mined at the point where all the nodes, will be the present on that day so that they could form a long list of blocks.

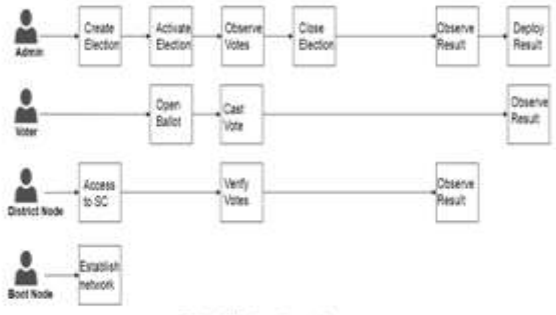


Fig. 1: Election roles and process

1) Smart Contracts: The smart contracts are not able to be undone and mainly tracable packages, which are get processed in a central to local surroundings likewise Blockchain does. Once the cleaver consensus is get done no human being can edit process of encryption while it's get deployed. It ensures both the sides agrees on the same which is mentioned in it. Which helps to builds security and trust and hence does not affect the same. Smart contracts permits the administration to know the reason by which they get processed and verified. Likewise such "cleaver contracts" are attributed to Nick Szabo, who is graduated and diplomate in Computational techniques. He's research helps to find out the best practices for the law and to the law to make such digitized transactions. Ethereum which is a crypto, gives a open supply of blockchain platform which is used by these kind on agreement. Ethereum can be implemented in Solidity, which is same as JavaScript. The same is explained in the third section of this paper. Also, we can actually implement this smart contract in electronic voting-systems.

2) Non interactive Zero-knowledge proof: There is another aim which is not related to the blockchain technology, but which is helpful for the implementation on electronic voting-systems on a device is zero-expertise proof. It is an cryptographical way to implement the verification and of information without authenticate their accounts on their own. Also, they can be able to perform multiple actions on their own such loading of ballots, cast the vote and verification after the results get out. Voters can cast vote from any part of the world, once the identification has been done.

3) District Nodes: On the blockchain, the directors who has knowledge of the values or data.

III. BLOCK CHAIN AS A VOTING

Blockchain as a Service for implementation of electronic-voting systems, we not forgetting the current system which is not works on the principal of Blockchain, which evaluates the general elections country wide. On the basis, we discovered a blockchain-based and totally digitized voting-systems for casting of votes, with all the required study. In the upcoming section, will try to find out the roles and effects of implementation of same systems with cleaver agreement then, we will concluded some outstanding Blockchain frameworks that can be helpful. Hence here the explanation of proposed system design and architecture.

A. Election process with the help of smart contract: Smart agreement is nothing but the involvement of identification of roles which are the part of that agreement and rest of the parts and transactions in that contract. Here we are explaining the process of conducting the same.

1) Election roles: Election process includes the active participation of the people and varies in various roles as shown in Figure1. In which two people or parties can share the exact same role with powers.

(i)Election directors: Directors are the one are responsible to direct and management of the entire end-to-end lifecycle of a election. Multiple factors may depends on this role such as institutions or businesses. The directors mainly provide a brief specification of election's type, process, configuration and security.

(ii) Voters: To cast a vote every country or institution has an eligibility criteria. In this system, eligible voters can authenticate their accounts on their own. Also, they can be able to perform multiple actions on their own such loading of ballots, cast the vote and verification after the results get out. Voters can cast vote from any part of the world, once the identification has been done.

(iii) District Nodes: On the blockchain, the directors who has decided the propaganda of election, each ballot and smart agreements are get deployed on it. When such poll smart contracts get created, each of node who is representing the District is allowed to interact with those respective smart contracts. When the voter casts the vote, the new record has been created with respect to smart contract and the node of that respective district. And hence, the casted vote is get added on the blockchain at real time.

(iv) Boot nodes: Each system, having the administration rights to that network called as a host to a boot node. Boot node has the ability to find and establish the communication with the nearest district node. They have assigned a static IP for the easy discovery/connectivity.

2. Process of Election: In this paper, every system is based on smart contracts, which are hosted by the election directors on the blockchain. Couple of smart contracts are opted in a election so that, it can get defined for the casting of votes for each district of that election. Once the voter himself authenticate himself, they can cast vote with its corresponding district area. Following are some important actions within the process of election:

(i) Creation of election: The directors will create an election with a local to central app. This app will communicate with the smart contracts. Which will have the list of candidates and all the district nodes. A set of smart contracts, ballots are created by this agreement which get to be deployed on Blockchain having the list of candidates. The poll smart contract has been created for the given permission to host the election.

(ii) Registration of Voters: Again, the directors play key role for the registration of voters. A list of eligible voters gets published, which will help it authenticate and identify the voters. Using multiple verifications, each user will get its username and password along with their voting details. Every eligible can cast their vote.

(iii) Transaction of Vote: Once the voter, cast his vote, it communicates with its smart contract, for that assigned district node. With the agreement between general and district nodes, blockchain has the vote on it. After the successful submission of vote, each voter gets a transaction ID for that respective transaction for the verification purpose.

(iv) Counting the votes and verification of votes: The verification and counting of votes, is resides in the smart contract. Smart contracts calculate the votes for its district. Once the election gets over, Final results get posted for each contract. Also, each vote has a transaction id to verify that vote on that blockchain. The voter can actually see his

vote on blockchain unless and until the polling time gets over.

C. Design and Implementation of a system: Our proposed systems is design to apply face-recognition for the authentication purpose. A user will login with user ID, voter ID and lastly with the face authentication.

1) Every eligible voter can cast the vote. A authenticated voter with legitimate voter ID and face authentication can be a eligible voter.

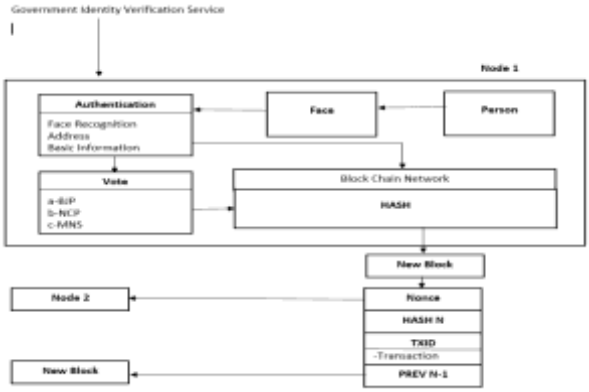
2) If the voter gets authenticate successfully, the new smart contract is gets ready for that election. Which has the list of candidates who are the part of election, and voter can vote.

3) While casting a vote, once he finalized his candidate for vote, he will ensure the final decision with one time password.

4) Once the vote is casted by a voter, the verification has been by a district node, to which a voter is interacting though a smart contract. Once the district accepts the vote, it get added to the database.

5) Once the vote is get accepted by district node, the voter will receive the transaction ID for that respective transaction via email or SMS. Figure 2 will explain it.

6) All the transaction which were received and created ongoing block time are deployed on Blockchain which is hosted on a Docker. Addition of every new block to the blockchain, is result to updation of ledger of that respective district node.



V. SECURITY ANALYSIS AND LEGAL ISSUE

In this section we will do a brief analysis on security and proposed system with the criminal issues.

A. Evaluating the security:

1) DDOS : The attacker might attack every single boot node which is present in the personal network. Byzantine fault tolerance set of regulations are set to accomplish each node to locate the failed nodes.

DDOS is helpful and effective in such cases.

2) Authentication Vulnerability: Using the user ID, valid voter ID, also by authenticating the face voter can be get identified. Any voter can vote without any supervision, which is risky. As a voter may cast multiple votes on the behalf of mutilple person.

3) Sybil: A centralized systems is weak against Sybil Assault. A person may create large number of nodes for hijacking the network. The smart contract protocol is Sybil assaults prone. Blockchain is safe enough for such attacks.

B. Legal Troubles:

1) Remote Balloting: Non supervised may cause remote election no correction resistance. It may not assure the privacy of vote in a incoming voting space. People from family or in a friend circle may be able to see your vote. Which is not legal. A hacking can be a threat for such digitized election-systems. Hacker may cast vote on behalf of other person.

2) Transparency: In the today's election scheme, no technique of transparency may be provided to individuals of the election. When an individual places his poll within the box at his district node, there's no guarantee from the scheme that his vote became counted and counted successfully. Any voter may vote out of place, counted incorrectly due to human mistakes. Which voter voted for will be disliked by using the individual which counted the vote. This transparency is non-existent because no ballot has statistics on who casted aforementioned vote. To introduce transparency within the process of an election might require a brand new law which would allow government officials to offer the offerings which allow such method of transparency

3) Voter privacy: Voter privacy is important in any election system. Voters privacy can be tracked with the proper behavior analysis and may lead to the threat to his privacy.

VI. CONCLUSION

The concept behind to choose the electronic voting-systems, is to make general election less expensive, fast, and more easy, to provide a best system to our society. Making such system may result into the growth in the number of voters. Such system, will give power to people to cast their vote from any corner around the globe. In this paper, we have explained the implementation of secured electronic voting-systems using the Blockchain technology. We also, studied all the aspects like security, architecture, design. We also suggest to add new policies like privacy of voters. The voter decides the new governance and for such voter implement of this system is more important.[10] This system requires safe and smart networks. Our system allows voter to cast a vote from anywhere. Which will doubtlessly grow the voter turnout and may be help to form a awesome and right, 'People's' government.

REFRENCES

[1] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting-systems/ oversight/ top-bottom-review/.

[2] Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/ secure-vote-today.

[3] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: https://techcrunch. com/2018/02/24/liquid-democracy-uses-blockchain/

[4] Nca.tandfonline.com. (2015). Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties. [Online]. Availableat: https://nca.tandfonline.com/doi/abs/10.1080/ 13183222.2015.1017264. Wr0zCnVl8YR

[6] Ronald Cramer, Rosario Gennaro and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme Available at: http://www.win.tue.nl/~berry/papers/euro97.pdf

[7] Ethereum Blog. (2018). On Public and Private Blockchains - Ethereum Blog. Available at: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/

[8] Steve Ellis, Ari Juels and Sergey Nazarov. (2017). ChainLink: A Decentralized Oracle Network Available at: https://link.smartcontract.com/ whitepaper

[9] Vincent Gramoli. (2018). On the Danger of Private Blockchains. [Online] Abailable at: https://www.zurich.ibm.com/dccl/papers/gramoli_ dccl.pdf

[10] Jelurida, "Jelurida", 2017. Available at: https://www.jelurida.com/sites/ default/files/JeluridaWhitepaper.pdf

