SJIF Impact Factor 2022: 8.197| ISI I.F. Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 5 | May 2022 - Peer Reviewed Journal

BLOCKCHAIN FOR ONLINE VOTING SYSTEM

Rajat Gupta[1], Shallu Bashambu[2]
[1]*Student, Maharaja Agrasen Institute of Technology, Delhi, India*
[2]*Assistant Professor, Maharaja Agrasen Institute of Technology, Delhi, India*

ABSTRACT

Online voting is a trend that is gaining momentum in today's world. It has great potential to truncate operational costs and increase voter turnout. It eliminates the necessity of printing ballot papers or opening polling booths-voters can vote from wherever there is an Internet connection and a smartphone. Despite these benefits, online voting solutions come with a high potential for new threats. A single vulnerability can lead to huge manipulations of votes. Electronic voting systems must be convenient along with safety, accuracy, and legitimacy when used for elections. Nonetheless, acceptance may be restricted by potential risks associated with the online voting system. Blockchain technology came into play to overcome these issues and offers decentralized nodes for electronic voting and is used to produce electronic voting systems mainly because of their end-to-end verification and security advantages. This Blockchain technology is a beautiful alternative for traditional EVM voting, with distributed, non-redundant, and security protection characteristics.

1. INTRODUCTION

In every election, security is of priority concern while conducting it because it ensures voters' right is fulfilled transparently. Security can be achieved using computer applications along with the goal of reducing the cost of having a national election. Conventionally, for electing any candidate, the voting system has been based on pen and paper. Later this system was replaced by an electronic voting machine which is practiced in current times where a voter goes to the polling booth and there are EVMs kept in a room and voter cast his vote by pressing a button corresponding to his favorite leader and after pressing the button, a vote is successfully added to the account of leader.

Electronic voting machines have been viewed as prone to be manipulated, by the security community, based on manual security concerns. Anyone with physical access to EVM can disrupt the EVM, hence affecting the election results.

Now Blockchain Mechanism comes into the scenario. A blockchain is a distributed, incontrovertible, immutable public ledger. Blockchain act as a decentralized database and provides new ways for creating trestles and distributed system. In this system, there is nothing like a central coordinator. Instead, each block that is present in the blockchain holds the data block locally. This technology was introduced for making money transfer applications but with its development researchers tried this technology in various other domains like medical, property reselling, and carbon dating. There are various blockchains developed over time but Ethereum is among the well-known blockchains. It owns a Turing complete programming language and the user can implement the function by the smart contract in the Ethereum network.

The distributed system means the computation is dependent on the decentralized blockchain. The trustless system means the voter is not required to rely on any administrator for elections and the trust is separated among all voters. This whole protocol defines the correctness of the system, additionally, all the votes are cryptographically secured to ensure the privacy of each voter. The final election result is immutable even if the election administrator is malicious because the scheme uses threshold encryption without a trusted third party. An Asymmetric cryptographic technique is used for the purpose. A pair of public/private keys is prepared and a public key is shared with all the parties participating in the election while the complete secret key is kept away till the key reconstruction stage. When at least of n parties upload their secrets, the secret key is reconstructed.

The whole voting scheme is deployed on Ethereum Blockchain by Smart Contract. Smart Contracts on the blockchain act as a trusted computer whose result is publicly trusted. A Smart contract once executed, guarantees to bind parties together to an agreement as written. Ethereum script allows the developer to write a smart contract that will implement the required functionality, in our case, Voting functionality. This functionality will include creating candidates' data and appropriate functions for adding a vote to the respective candidate and various other functioning. All nodes of the Ethereum network will run the smart contract code independently to verify the credibility of the final result. Hence the final result is publicly trusted.

2. LITERATURE SURVEY

Authentication of Voters

There are different techniques for authentication of voters, like private key cryptography that has to be provided to voters before the election process. Voters must be registered by some authority while registering the voter's private key must be generated and shared with the respective voters in

SJIF Impact Factor 2022: 8.197| ISI I.F. Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 5 | May 2022 - Peer Reviewed Journal

hand. The strategy of private key cryptography is suggested by various researchers like Cosmas Krisna Adiputra and Kriti Patidar.

Another approach for the purpose is to use a certain digit PIN code. Each individual will be identified and authenticated by the system through that code which will be generated at the time of registration.

Then comes a unique strategy using the Aadhar database of the citizens. This framework will be using a virtual ID which is provided by the UIDAI which will be unique. Aadhar database will fetch demographic details (Fingerprints) of the voters. The Fingerprint will get converted to a digital signature which can be used for Authentication.

Voters Identification is always a critical challenge in every aspect, various solutions have been tried like facial recognition, fingerprint, and retinal scan but these all can be easily manipulated or gamed. However, this can be improved by using complex algorithms that are not easy to crack. Hashing will be more effective rather than generating binary data from biometric information.

Analysis

The Blockchain system allows us to develop blockchain-based applications. There are many renowned blockchains available like Bitcoin, Ethereum, Solana, and R3 Corda. Hence an appropriate choice is to be made by taking various factors into consideration like Gas Cost, feasibility, etc. Whenever a user will vote a certain amount of fees will be deducted in a form of cryptocurrency against that blockchain for eg. if we add a node into the Ethereum blockchain then we have to pay some fractional ethers to the miners owning the mining rig of that blockchain.

In an analysis of gas cost and time, the researcher Yuxian Zhang chose to deploy and test the contract in the Ethereum private chain. For a 40-person election, calculating the consumption of gas and money, they calculated the real-time price required for the transaction based on the Gas price provided by the Ether gas station and the current Ether price. Gas price=7 gwei, 1ETH=607 USD. The result showed a cost of $20.5 to hold an election for 40 persons. This cost will be low for local elections but for mass scale elections, this can become costly hence election commission can also introduce its own blockchain and can reduce this cost.

3. BLOCKCHAIN AS A SERVICE FOR E-VOTING

In this paper, both conventional system(Non-Blockchain based) and Blockchain-Based system for national elections will be considered in terms of feasibility for implementation. Hence a blockchain-based voting system has been designed. In the following subsection, we will understand the role of smart contracts in voting and several other components along with it.

Election as a Smart Contract: Defining a smart contract includes the identification of the roles that are involved in the agreement and the transactions in the process. First, we will discuss election roles which means the role of different individuals and groups:

- **Election Administrators:** This group will have a crucial role in managing the life cycle of the election because they are responsible for specifying election type and will create the aforementioned election, configuration of ballots, registration of voters, and decision for the election time period.
- **Voters:** Eligible citizens for the voting process are voters hence their role is limited to being present at the time of voting and casting their vote and they are done with their part.
- **District Nodes:** District Nodes will interact with their respective smart contracts. Whenever any vote will be rated then all the district nodes will verify the vote data and if the verification is successful then the vote data will be appended to the blockchain.
- **Boot nodes:** Since district nodes are divided based on the smart contract with which they interact hence a boot node is required to maintain the interaction between all the district nodes. It does not keep any state of the blockchain.

Election Process: The concerned system of Blockchain-based online voting has a well-defined process that is very much required for smoothly conducting elections. In our work, every process is associated with a smart contract which gets instantiated on the blockchain by the administrators. For every voting district, a separate smart contract is prepared for ease.

The following are the main activities in election procedure:

- **Election Creation:** The election administrator will create electoral ballots through the decentralized application. This application will interact with a smart contract for election creation which includes the list of candidates and voting districts. This smart contract will create a set of ballot smart contracts and eventually deploy on the blockchain for further process.
- **Voter registration:** The voter registration phase is handled by election administrators. Whenever an election is initiated the administrators must release a list of eligible voters. Voter Authentication will be done through asymmetric key cryptography. Voters will be given a private key beforehand. At the time of elections, the voter will use that key to log in to the system and cast his vote.
- **Vote Transaction:** When an individual cast his vote at a voting district, the voter interacts with the smart contract of that district. This smart contract will further communicate with the blockchain through the corresponding district nodes and finally appends the vote into the blockchain. Each vote will be represented or stored in the form of a transaction with transaction ID and Contract ID. This transaction will also be shared with the voter as an acknowledgment of a successful vote.
- **Tallying results:** The tallying process is handled by smart contracts on the go. Each smart contract does its tally for the corresponding location in its storage. When the election gets over, the result for each smart contract is published.

SJIF Impact Factor 2022: 8.197| ISI I.F. Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 5 | May 2022 - Peer Reviewed Journal

- **Verifying Vote:** Every voter is to receive a transaction ID for his vote as discussed earlier. The voter can verify his vote by showing that transaction ID and his electronic identification along with the key. The government official will verify the vote by accessing the blockchain and locating that particular transaction.

4. CONCLUSION

In this paper, we discussed EVM based voting system that is practiced currently and a blockchain-based voting system, its implementation, feasibility, and advantages over traditional voting systems. On one hand where traditional voting system process was cumbersome for the government because of the cost and time required for it and voters as well because they have to stand in Queues and if they are not available at their home location then they have to miss the voting. The proposal of adapting the online voting system to make the election process cheaper and faster and more convenient is a compelling one in today's world. It allows the voters to express their wills on proposition thus making a direct form of democracy. Since handling millions of transactions in a small amount of time can be a bit of a challenge but by using Ethereum private blockchain hundreds of transactions can be completed in seconds. Countries with high populations need to take some measures to withhold greater throughput of transactions, for example, the parent and child architecture.

5. REFERENCES

1. *Sos.ca.gov.(2007).Top-to-BottomReview|CaliforniaSecretaryofState.Availableat: 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. *C. K. Adiputra, R. Hjort and H. Sato, "A proposal of Blockchain-Based Electronic Voting System," 2018 Second World Conference on Smart Trends in System, Security and Sustainability(WorldS4), London, 2018, pp. 22-27, dot:10.1109/WorldS4.2018.8611593.*
4. *K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparitive Analysis on E-Voting System Using Blockchain," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/IoT-SIU.2019.8777471.*
5. *K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.*
6. *Nca.tandfonline.com. (2015). Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Par- ties. [Online]. Available at: https://nca.tandfonline.com/doi/abs/10.1080/13183222.2015.1017264#.Wr0zCnVl8YR*
7. *Steve Ellis, Ari Juels and Sergey Nazarov. (2017). ChainLink: A De- centralized Oracle Network Available at: https://link.smartcontract.com/ whitepaper*
8. *Salanfe, "Setup your own private Proof-of-Authority Ethereum network with Geth", Hacker Noon, 2018. Available at: https://tinyurl.com/y7g362kd.*