IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 4, Issue 2, April 2021
Impact Factor: 4.819

Decentralized Remote Voting System

Prof. Santosh Kale[1], Atulesh Hatmode[2], Milind Deogade[3], Jyoti Ranjan[4] and Vikrant Gudakesh[5]
Professor, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4,5]
NBN Sinhgad School of Engineering, Ambegaon (Bk), Pune

Abstract: *The democratic technique is the instrument for carrying out individuals' view to more readily manage the framework. All through late years, regular votes have satisfied neither individuals nor government specialists. They are not altogether protected since voting forms are easy to strike. It additionally challenges elector wellbeing and straightforwardness. Also, checking the votes takes excessively long adjustment of casting a ballot overall is a charming issue in current casting a ballot framework. To tackle these issues Computerized innovation is utilized in the democratic stage for residents in numerous countries. Digitalization alone can not fix the issues completely. There are additionally numerous methods of controlling or on the other hand adjusting advanced innovation and blocking casting a ballot. There ought to be decency, autonomy and unprejudiced nature in the casting a ballot technique. By breaking down the previously mentioned issues, this research work joins the digitalization with the blockchain innovation to give a democratic system. The primary objectives of our casting a ballot system are to give uprightness, obscurity, protection, furthermore, security of voters. With the utilization of markle tree and finger impression hash, the information trustworthiness and namelessness, protection, security of the citizens has been accomplished in our proposed advanced democratic frameworks.*

Keywords: E-Voting, Blockchain, Fingerprint Hash, SmartContract, Mining, Markle tree, Ethereum

I. INTRODUCTION

This paper considers the Indian Political decision Framework for study furthermore, attempts to propose an answer for the Indian Political decision Framework by restricting the extension. The main rule that characterizes a political decision is that they should address the free articulation of the desire of individuals. This sort of articulation is just conceivable if the races are responsible, straightforward furthermore, comprehensive. These standards are heaped by a few by different appointive interaction related commitments and different key-rights and opportunities and these are gotten from public global law. The principle standards for the respectability of the vote based measure are accuracy, power to illicit conduct, effectiveness, soundness and straightforwardness of the democratic component. Dependability, mystery, honesty and lessen speculation on labor, supplies what's more, innovative gear can be improved by Digital voting system. It basically ensure that the projected votes and the results are right. Digital voting additionally has various restrictions. Counterfeit democratic, cost reserve funds, produce speedier results and so forth are a few vindictive practices all through the democratic cycle. Indeed, an assortment of gatecrashers may harm keen or IoT (Web of Things) frameworks by having an emotional effect on the casting a ballot or computation of casting a ballot to get their own benefit. Certain security measures should be set up which ought to guarantee about a reliable interaction of poling and then some. Various methodologies has been recommended. Notwithstanding, such frameworks can likewise raise the intricacy of organization by expanding the cost of calculation, data transmission, space, and testing. Accordingly, some improved assurance frameworks or instruments are necessitated that ensure a steady democratic or tallying techniques furthermore, forestalling the previously mentioned depicted issues .Blockchain innovation is a decentralized record that keeps up an intelligible comprehension of truth. Blockchain has been utilized in digital forms of money like Bitcoin and Ethereum which is a shared, sealed record and peer - to - peer organizing stage. Here the general population or private key personality ensures client namelessness. There are a few blockchain based model,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 4, Issue 2, April 2021
Impact Factor: 4.819

which gives security and protection. While blockchain give security, protection, responsibility and sturdiness, the fundamental difficulties of executing Block chain technology are identified with speed and versatility.

Our goal is to plan an Digital Voting architecture with the consideration of a smart contract to decrease difficulties created during the appropriation of blockchain with casting a ballot and give verification, straightforwardness, namelessness, precision and self-governance, peculiarity, respectability, versatility. In our framework, from the electors data a hash will be produced and put away in the chain. This will give adaptability and obscurity of electors as the data is put away in the blockchain as a hash. Any progressions will be effectively identified if the hash data is altered. Smart contract running in the chain guarantee security also, privacy. A miner is named by smart contract to improve the speed of the transaction. The nomination relies upon various models like data transmission, energy utilization. counting process of vote is done in each block. Toward the finish of casting a ballot, from the last block total vote can be easily examined. It decrease the time utilization for tallying.

II. LITERATURE SURVEY

Paper titled **"A Secure and Optimally efficient Multi-Authority Election Scheme"** proposed a multi-authority secret-polling form political decision plot that would ensure power, widespread evident, and protection. where electors will partake utilizing a PC, and the primary thought is the citizen's efforts. In this framework electors cast their polling form on a notice board. The notice board works with expanded memory to such an extent that any part can get to its content however will not have the option to adjust the information. The voting form doesn't contain any data about the actual vote yet, it has an affirmation that it is a substantial vote. The last count is done when the cutoff time is finished can be checked by any person against the result of all submitted votes. This guarantees unquestionable due to the encryption technique utilized.[8]

Paper titled **"A Smart Contract For Boardroom Voting with Maximum Voter Privacy"** had proposed the web casting a ballot convention with decentralized highlights what's more, greatest elector security utilizing Open Vote Organization (OVN). The OVN is a shrewd agreement for the Ethereum Blockchain. In the wake of executing this framework the makers presumed that it costs 0.73$ per elector on this framework. They had a furthest cutoff for the quantity of citizens to 50 to diminish the gas utilization. Nonetheless, the scientists before long discovered that OVN is powerless tasks assaults. It could likewise endure gridlocks during the exchange which could defer the democratic interaction for a longer time. Thus this execution is effective for meeting room gatherings with a significant downside that each person who wishes to cast a ballot needs to download the whole duplicate of the organization.[9]

Paper titled **"Blockchain Based Voting System Can Better the Way of Elections in India"** proposed a framework for the Indian Political race Framework dependent on the Hyperledger Organization. The corner specialists at various surveying corners go about as various hubs. These specialists are chosen by the Political race Commission of India. For each stage, the assent of 5 hubs is to be thought of. Participation Specialist organization is additionally present on surveying stalls which assists with validating the electors and create public and private keys. Here they have proposed having three stages. During the readiness stage, a citizen needs to go to the closest approved democratic focus and register with his accreditations so his name is remembered for the Hyperledger organization. [10] During the Democratic Stage, the MSP issues the general population and private keys to the elector. Once the elector makes a choice for an applicant it is considered an exchange. The interaction of the Hyperledger organization starts here. Every exchange is supported by in any event 5 hubs. These exchanges are shipped off the requesting administrations and later to the primary chain. The Post Democratic stage incorporates steps like chronicle casts a ballot in the primary chain after approval, bolting the authority of the elector for the time span, checking of votes thus on.The approval is finished by 5 unique hubs to stay away from any control which is still computationally incomprehensible.[11]

Suporn Pongnumkul, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong in their paper **"Performance Analysis of Private Blockchain Platforms in Varying Workloads"** analyzed the two generally well known Blockchain technology stages vizEthereum and Hyperledger. They built up an application that can move money from account A to account B. comparing execution time, they found that as the no of transactions increases, the execution time increases. However, Hyperledger's execution time is in every case less than that of Ethereum. On comparing

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 4, Issue 2, April 2021
Impact Factor: 4.819

latency it wasfound that on less no of a transaction, Ethereum's latency is 2x times that of Hyperledger. Additionally on differing no of exchanges the difference in normal throughput of Hyperledger is generally bigger than that of Ethereum.[12]

III. Traditional Voting Process

EVM Based System: Electronic Voting System is the one in which we use a machine to handle the process of voting in India. EVM consists of two units namely control unit and ballot unit which are connected by a cable. The polling officer is in charge of the control unit. The ballot unit is for the voters to cast their votes. These units are sealed and directly opened on the vote counting day. Major criticism faced by EVMs is that these systems use microprocessors internally which can be subjected to tampering.

Paper Ballot based System: Here, voters are provided a paper ballot (usually a piece of paper) which consists of names of all candidates. These paper ballots are provided at the polling station. The major disadvantages of such a system are the high duration required to calculate votes, manpower, wastage of paper, ease in manipulation, etc.

3.1 Drawbacks

1. It's hard to tamper with EVMs but not impossible.
2. Software malfunction leading to inaccurate results.
3. Security problems
4. Vulnerability to hacking
5. No means for voters to verify their votes
6. The time gap between the voting and the counting of votes is a risk to possible tampering, as the ballots are physically stored after votes.

IV. Proposed System

In this part we present our proposed voting system that targets settling the current hindrances in Blockchain-based E-voting system. Fig. 1 represents at high level the proposed system architecture and the cooperation between the system's components.

4.1 System Components

Web Application: The web application helps administrators in making and overseeing new voting events. Each voting event is addressed as a different Smart contract in the Blockchain organization.

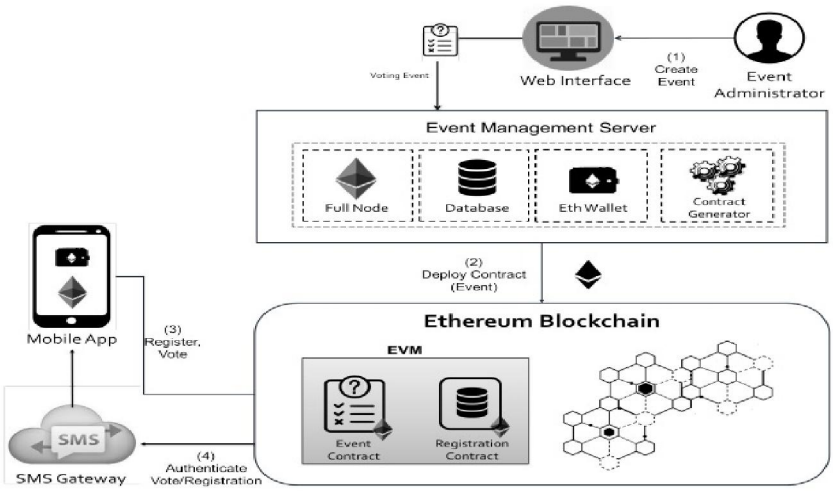

Figure 1: System Architecture

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 4, Issue 2, April 2021
Impact Factor: 4.819

The administrator fills-in the list of questions and their relating answers and afterward start a HTTP request to the Event Management server containing the entered information. The objective of this Internet application is to be accessible as an Application Programming Interface (API) permitting any client to make new voting events.

1. **Event Management Server:** The principle objective of the Event Management Server is to convey the Smart contract to the network with the information (questions and answers) got from the web application. Consequently, it contains an Ethereum Wallet (address) which is needed to send the contract, a full node to interface the Ethereum network, and a database to store the list of contract addresses which will be fetched later by the mobile application.
2. **Smart Contracts:** There are two types of smart contracts exists in our system: 1)Registration contract , 2)Voting contract. The registration contract is sent once for all voting events. It serves at safely enrolling and verifying the electors. The voting contract is written once at development time, furthermore, sent a few times by the Event Management Server with various inquiries and answers determined by the event administrator as clarified beforehand.
3. **Mobile application:** The mobile application is utilized by voters to enlist themselves in the system and afterward vote. It likewise gives the users the ability to fetch occasions, see questions and choices, and envision continuously the outcomes. Besides, the application gives a point by point report appearing the voting event insights identified with the recurrence of votes per time allotment, area, and others. As the voting process happens in the Ethereum network, it is required to have an interface associating the mobile application to the Blockchain network.

4.2 Blockchain Setup

To fulfil the privacy and security prerequisites for e-voting, and to guarantee that the election system should not empower constrained voting, voters should cast a vote in a supervised environment. In our work, we setup a Go-Ethereum permissioned Proof-of-Authority (POA) blockchain to accomplish these objectives. POA utilizes an algorithm that conveys nearly quick transactions through an agreement system dependent on identity as a stake.

4.3 Election as a Smart Contract

1. Election roles: The roles in a smart contract include the parties that need to participate in the agreement. The election process has the following roles:
   i. **Election Administrator:** To deal with the lifecycle of an election. Different believed foundations and organizations may be enrolled in this role. The election administrators make the election, register citizens, choose the lifetime of the election and relegate permissioned nodes.
   ii. **Voter:** A person who is qualified to cast a ballot. Electors can validate themselves, load election ballots, cast their vote and confirm their vote after an election is finished.
2. Election process: In our work, every election process is addressed, by a bunch of smart contracts, which are conveyed on the blockchain by the election administrators.
   i. **Election Creation :** Election administrators make election ballots utilizing a smart contract wherein the administrator characterizes a list of contender for each voting district. The smart contracts are then composed onto the blockchain, where district nodes gain access to interact with theircorresponding smart contract.
   ii. **Voter registration :** The enlistment of citizens stage is led by the election administrators. At the point when a election is made the election administrators should characterize a deterministic list of qualified electors. This may require a segment for an a government identity verification service to safely validate and approve qualified people. Utilizing such an assistance is important to fulfil the prerequisite of secure validation as this is not ensured, naturally, when utilizing a blockchain framework. In our work, for each qualified elector, acorresponding identity wallet would be created. A unique wallet is created for every elector for every election that the elector is qualified to partake in.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 4, Issue 2, April 2021
Impact Factor: 4.819

iii. **Tallying results:** The counting of the election is done on the fly in the smart contracts. Each ballot smart contract does their own count for their relating area in its own storage.

iv. **Verifying votes:** In the voting transaction, every elector gets the transaction ID of his vote. In our e-voting system, electors can utilize this transaction ID and go to an official election site (or authority) utilizing a blockchain explorer and (subsequent to validating themselves utilizing their electronic ID) find the transaction with the corresponding transaction ID on the blockchain. Voters can, in this manner, see their votes on the blockchain, and confirm that the votes were recorded and tallied effectively. This kind of verification fulfils the transparency prerequisites while preventing traceability of votes.

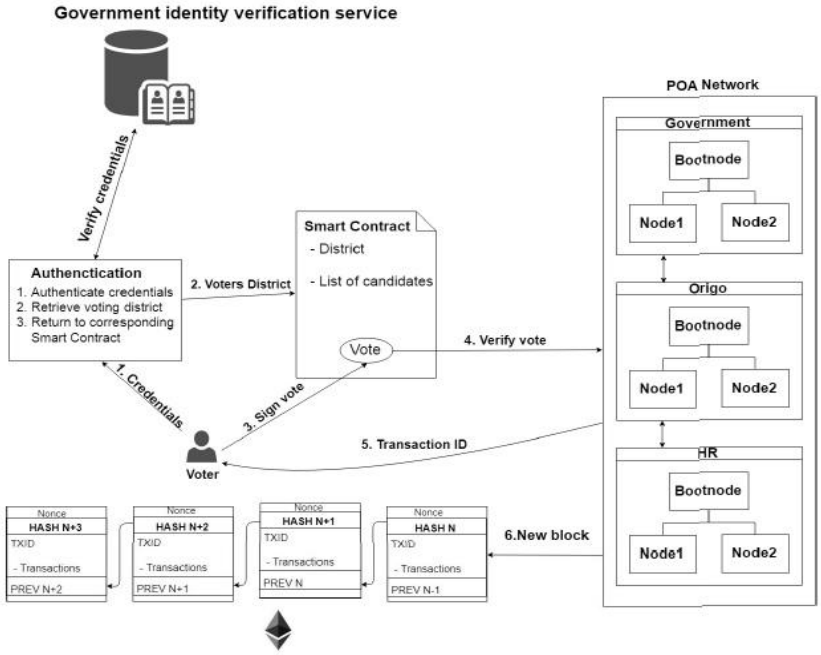

Figure 2: The Voting process

3. **Voting Transaction:** Every elector connects with a ballot smart contract for her corresponding voting district. This smart contract connects with the blockchain through the corresponding district node, which adds the vote to the blockchain. Every individual elector gets the transaction ID for their vote in favour of confirmation purposes. Each vote that is settled upon, by the larger part of the corresponding district nodes, is recorded as a transaction and afterward affixed on the blockchain. Figure 2 is a visual portrayal of this cycle.

V. Conclusion and Future Work

In this paper, we presented a blockchain-based electronic voting system that uses smart contracts to empower secure and cost-proficient election while ensuring voters privacy. We have shown that the blockchain technology offers a new possibility to defeat the restrictions and appropriation barriers of electronic voting systems which guarantees the election security and integrity and lays the ground for transparency. Utilizing an Ethereum private blockchain, it is feasible to send hundreds of transactions each second onto the blockchain, using each part of the smart contract to facilitate the heap on the blockchain. For nations of more prominent size, some extra measures would be expected to help more noteworthy throughput of transaction per second.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 4, Issue 2, April 2021
Impact Factor: 4.819

REFERENCES

[1] "Supporting free and fair elections," https://www.usaid.gov/what-wedo/democracy-human-rights-and-governance/supporting-free-and-fairelections,accessed: 2020-01-24.
[2] "Can blockchain change the election scenario in india?" Available at https://link.medium.com/kgJJ2No5F3, accessed: 2019-12-22.
[3] "Features of blockchain technology," Available at https://guide.freecodecamp.org/blockchain/features/, accessed: 2020-01-26.
[4] "An introduction to hyperledger," Available at https://guide.freecodecamp.org/blockchain/features/, accessed: 2020-01-26.
[5] S. Haber and W. S. Stornetta, "How to time stamp a digital document," in Advances in Cryptology-CRYPTO' 90, A. J. Menezes and S. A.Vanstone, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991,pp. 99–111.
[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.
[7] G. Albeanu, "Blockchain technology and education," in The 12th International Conference on Virtual Learning ICVL, 2017, pp. 271–275.
[8] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," European transactions on Telecommunications, vol. 8, no. 5, pp. 481–490, 1997.
[9] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp.357–375.
[10] N. Pandey and N. Singh, "Blockchain based voting system can better the way of elections in india."
[11] M. B. Verwer, I. Dionysiou, and H. Gjermundrød, "Trustedevoting (tev) a secure, anonymous and verifiable blockchain-based e-voting framework," in International Conference on e-Democracy. Springer,2019, pp. 129–143.
[12] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in2017 26th International Conference on Computer Communication andNetworks (ICCCN). IEEE, 2017, pp. 1–6.
[13] D. Kirillov, V. Korkhov, V. Petrunin, M. Makarov, I. M. Khamitov, andV. Dostov, "Implementation of an e-voting scheme using hyperledger fabric permissioned blockchain," in International Conference on Computational Science and Its Applications. Springer, 2019, pp. 509–521.
[14] V. Buterin et al., "A next-generation smart contract and decentralized application platform," white paper, vol. 3, no. 37, 2014.
[15] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y," ACM SIGMETRICS Performance Evaluation Review, vol. 42, no. 3,pp. 34–37, 2014.
[16] C. Cachin et al., "Architecture of the hyper ledger blockchain fabric," in Workshop on distributed cryptocurrencies and consensus ledgers, vol.310, 2016, p. 4.
[17] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in2017 26th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2017, pp. 1–6.