As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 7(12): 173-175, 2021

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0712032
Available online at: http://www.ijmtst.com/vol7issue12.html

Decentralized Voting System

Priyanshu Goel | Anurag Dawar

Department Information Technology, Maharaja Agrasen Institute of Technology, New Delhi, India.

To Cite this Article
Priyanshu Goel and Anurag Dawar. Decentralized Voting System. *International Journal for Modern Trends in Science and Technology* 2021, 7 pp. 173-175. https://doi.org/10.46501/IJMTST0712032

Article Info
Received: 01 October 2021; Accepted: 07 December 2021; Published: 10 December 2021

ABSTRACT

Building an electronic voting system that satisfies thelegal requirements of legislators has been a challenge for a longtime. Distributed ledger technologies is an exciting technological advancement in the information technology world. Blockchaintechnologies offer an infinite range of applications benefiting fromsharing economies. This paper aims to evaluate the applicationof blockchain as service to implement distributed electronicvoting systems. The paper elicitates the requirements of buildingelectronic voting systems and identifies the legal and technologicallimitations of using blockchain as a service for realizing suchsystems. The paper starts by evaluating some of the popularblockchain frameworks that offer blockchain as a service. Wethen propose a novel electronic voting system based on blockchainthat addresses all limitations we discovered. More generally thispaper evaluates the potential of distributed ledger technologiesthrough the description of a case study, namely the process ofan election and implementing a blockchain-based applicationwhich improves the security and decreases the cost of hosting a nationwide election.

KEYWORDS: Blockchain, Framework, Cost, Security, Worldwide

INTRODUCTION

Election security is a concern of national security in any democracy. For a decade, the computer security sector has explored the potential of electronic voting systems. **with the goal of reducing the cost of holding a national election while maintaining and improving election security**.

METHODOLOGY

The voting procedure has been based on pen and paper since the beginning of democratically electing candidates. It is necessary to replace the existing pen and paper voting system with a modern election technology in order to reduce fraud and make the voting process traceable and verifiable.

1. **Smart Contracts** Identifying the tasks involved in the agreement (in our example, the election agreement), as well as the multiple components and transactions involved in the agreement process, is the first step in defining a smart contract. The election procedure is addressed first, followed by the election obligations. **Tokenization** It is the process of separating a piece of words into a token **Units.**
2. **Voters** For elections in which they are eligible voters can authenticate themselves, load election ballots, cast their vote, and validate their vote once the election is over. Voters might be rewarded with tokens if they cast their votes in a future election, which could be linked to a smart city initiative.
3. **Tokens** can be either words, characters or sub-words. Hence tokenization can be broadly

classified into 3 types – word character and sub-word (in gram characters) tokenization. This can help in separating contents that is in the form of sentence to be broken down into small words that is called tokens thus There are various ways for tokenization, the simplest way to tokenize the string is to use the whitespace in the string as a delimiter of words. There are various challenges to tokenize the word simply based on white spaces , so tokenizer implements a variety of rules to tokenize the English words. It separates the phrase terminating with punctuation like (!?.:,) from adjacent tokens besides this it contains rules for English contractions . This can be done by python library NLTK, genism.

4. **District Nodes**Each voting district's ballot smart contract is released onto the blockchain when election administrators organise an election. When the ballot smart contracts are generated, each of the related district nodes is given access to communicate with their corresponding ballot smart contract. When an individual voter uses his or her linked smart contract to vote, the vote data is checked by all of the district nodes in the area, and any votes that they agree on are added to the blockchain once block time has passed.
5. **Booth Nodes**A bootnode is a network server that is hosted by each institution with network permissions. A bootnode is a device that helps district nodes be discovered and communicated with.

   To enable district nodes discover their peers more quickly, the bootnodes don't keep any blockchain state and run on a static IP.
6. **Voting Transactions**When a voter casts a ballot in a voting district, he or she interacts with a ballot smart contract that belongs to the same voting district as all other voters. This smart contract interacts with the blockchain via the appropriate district node, which delivers the vote to the blockchain if the majority of the related district nodes agree.Each vote is recorded as a transaction on the blockchain, and each voter is given the transaction ID for their vote for verification purposes (see section "Verifying vote"). Each blockchain transaction includes information on who was voted for and where the vote was held.Each vote is appended to the blockchain by the accompanying ballot smart contract if and only if all corresponding district nodes agree on the vote data verification. When a voter casts a ballot, the amount of money in their wallet is taken into account. **Compilation** of the findings Smart contracts tally the election results in real time. In its own storage, each ballot smart contract maintains track of its own total for each place. Following the completion of an election, the final result for each smart contract is released..
7. **Votes Verification**: As previously indicated, each voter receives a transaction ID for his vote. Each individual voter can present his transaction ID to his government official after identifying himself with his electronic ID and its associated PIN. The government official uses the blockchain explorer to locate the transaction with the corresponding transaction ID on the blockchain using district node access to the network. As a result, the voter may verify that his vote was counted and counted correctly on the blockchain.
8. **Voters Registration**The voter registration procedure is overseen by election administrators. When creating an election, election administrators must create a deterministic list of eligible voters. As a result, a component for a government identity verification service that can securely identify and approve qualified people must be included. If they employ such verification services, each qualified voter should have an electronic ID and PIN number, as well as information on their voting district. Each qualified voter would receive a wallet similar to this one. The wallet generated for each individual voter should be unique for each election in which the voter is eligible, and an NIZKP could be used to accomplish so so that the system does not know which wallet corresponds to which voter.Oversee the election for the duration of it. A lot of notable institutions and businesses have enrolled in this position. Election administrators design and specify the election type, as well as configure ballots, register voters, set the election's lifetime, and assign permissioned nodes.The election procedure is addressed first.
9. **Permission**We'll use a permissioned blockchain in our proposal, which is a type of consortium-based

chain that uses the proof-of-authority (POA) consensus mechanism. In proof-of-authority networks, transactions and blocks are authenticated by authorised accounts known as validators. We can utilise a permissioned blockchain that employs the POA consensus process to enforce constraints on a group of known entities to authenticate and certify transactions on the blockchain and filter transactions unilaterally, putting their identity and reputation at stake. Otherwise, it would have to be done by miners on a public blockchain using the proof-of-work consensus mechanism. Validators in a permissioned blockchain are compensated for their services by acting as validators in the system, rather than by mining fees, as they are in public blockchains. Furthermore, a private network makes it difficult for an eavesdropper to monitor traffic or read incoming data.

FUTURE SCOPE

All of the components of a secure electronic voting system are included in our electronic voting systems, including four essential parameters:

i) anonymity
ii) authentication
iii) accuracy
iv) verifiability

Only those who are on the list are authorised to vote, and the E-Voting software should provide anonymity both during and after the election. Following that, the vote must be accurate; no votes will be counted if they are duplicated or redundant. The main dependability and flexibility of this system may be validated. When numerous people vote in this Blockchain-based E-voting system at the same time, a problem related to the previously hash may develop. As a result, we devised the Longest Chain Rule as a solution to this problem. Either way, a blockchain-based e-voting system is required.When old EVMs are replaced with a decentralised blockchain application, voting becomes an online event. The bulk of blockchain based e-voting solutions face scalability and voter privacy issues right now. To address these issues and provide solutions, this research employs the Proof of Stake (PoS) based Sharding protocol and zk-SNARKs.

The time between the first use of Blockchain in a general election by a country and today provides a good opportunity to improve the suggested model and create a more reliable system. Blockchain, Smart Contracts, and Decentralization are growing at an exponential rate, and the time between the first use of Blockchain in a general election by a country and today provides a good opportunity to improve the suggested model and create a more reliable system.

APPENDIX

Appendixes, if needed, appear before the acknowledgment.

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments. Avoid expressions such as “One of us (S.B.A.) would like to thank ... .” Instead, write “F. A. Author thanks . .” **Sponsor and financial support acknowledgments are placed in the unnumbered footnote on the first page**.

REFERENCES

[1] David Nikolas Milne “A Knowledge Based Search Engine powered by Wikipedia”
[2] source link to the Learning of Decentralized Voting system: https://blockchain.oodles.io/blog/decentralized-e-voting-with-blockchain/.
[3] S. Nakamoto,"Bitcoin: A Peer-to-Perr Electornic Cash System," 2008.
[4] Snow, David A., and Robert D. Benford. 1988. “Ideology, Frame Resonance, and Participant Mobilization.” *International Social Movement Research* 1, 197–217.
[5] Marx, Karl,and Engels Friedrich. 1971. *Writings on the ParisCommune*. NewYork/London:Monthly Review Press.