International Journal of Computational and Electronic Aspects in Engineering
Volume 2, Issue 3, July 2021, pp 71 - 75
https://doi.org/10.26706/ijceae.2.3.20210606

Next-Generation Digital Voting System

Irshad Shah
Irshadshah9916@gmail.com

Wrushabh Dange
wwrushabh@gmail.com

Nilesh Nirgule
nileshnirgule08@gmail.com

Dinesh Ilme
dinesh.ilme@rediffmail.com

Department of Computer Engineering, Smt. Radhikatai Pandav college of Engineering, Nagpur, India

***Abstract*—Building an electronic voting system that meets legislators' legal criteria has been a long-standing challenge. Distributed ledger technologies are a revolutionary innovation in the field of information technology. Blockchain technologies can be used in an unlimited number of ways to profit from sharing economies. All current electronic voting methods have a fundamental design problem. They're designed to be tightly controlled, which means there seems to be one source in charge of the code base, database, and system outputs, as well as the monitoring tools to ensure the results are accurate. Due to the lack of an independently verified output, these centralized systems struggle to gain the trustworthiness necessary by voters, either restricting voter participation or casting doubt on the election's declared results. The study seeks to use the cryptographic ledger as a safe transaction database to establish an immutable, verifiable, and secure online voting system. Voters will be able to independently audit the inclusion of their vote, as well in the election's overall outcome, using this public ledger, while knowing that the results cannot be altered due to the immutability of the Blockchain.**

***Keywords*—** blockchain, smart contract, E-voting, hash, security, Ethereum, decentralized, digitalizing

I. Introduction

Electronic voting (E-voting) has progressively become a prominent study field as cryptography and Internet technology have advanced. Electronic voting was first proposed in 1981. Security and privacy have always been at the forefront of electronic voting research over its nearly four decades of existence. Many academics suggest a wide variety of safe electronic voting systems employing diverse technologies such as informatics and cryptography in order to improve the security of electronic voting. Fujioka and colleagues presented a new form of the electronic voting protocol in 1992 that employs blind signature technology to increase the voting system's security.[1]. In 2001, Magkos and others proposed a largescale voting scheme, which is based on an anonymous channel to improve the anonymity of voting users [2]. Blockchain technology has recently been utilized in electronic voting. If the voter can verify that their vote was accurately tallied and any party can validate the election results, an electronic voting system provides end-to-end verifiability. Several suggestions have been made detailing prospective systems, however, they have all been constructed on top of protocols that are primarily meant as a transaction ledger. This article presents a voting system based on the Ethereum protocol that uses the characteristics of smart contracts to impose tight constraints on electoral votes. The outcomes of these ballots are globally verifiable and retain all of the blockchain's beneficial features (such as immutability). All of this is accomplished without jeopardizing the privacy of voters or the integrity of the voting process.

II. Blockchain

Bitcoin's core technology, blockchain, first appeared in 2008 [3] A blockchain is a public ledger that is distributed, unchangeable, and irrefutable. The four key aspects of this innovative technology are as follows:

Research Article
First Online on – 10 July 2021

Cite this article – Irshad Shah, Wrushabh Dange, Nilesh Nirgule, Dinesh Ilme, "Next-Generation Digital Voting System", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 2, issue 3, pp. 71-75, 2021.
https://doi.org/10.26706/ijceae.2.3.20210606

(i) The ledger can be found in a variety of places: There is no single point of failure in the distributed ledger's upkeep.
(ii) The ability to append new transactions to the ledger is dispersed.
(iii) Any proposed "new block" to the ledger must relate to the previous version of the ledger, forming an immutable chain that gives the blockchain its name and precludes tampering with preceding entries.
(iv) Before a proposed new block of records becomes a permanent part of the ledger, a majority of the nodes in the network must reach a consensus.

A. *Smart Contracts*

Smart contracts are traceable and irreversible apps that run on a decentralized platform (such as blockchain). Nobody can amend the code or change the execution behavior of a smart contract once it has been launched. Smart contract execution ensures that parties are bound by the terms of the agreement as written. This establishes a new, more powerful sort of trust connection that is not dependent on a single party. Because smart contracts are self-verifying and self-executing, they allow for improved management of the realization and administration of digital agreements [4].

III. Design

The designed schema for this protocol is the following:

A. *Ballot Creation*

1. The ballots that will be used in the election are designed and chosen.
2. For each ballot, a smart contract comprising all of the voting possibilities is constructed and sent to the blockchain.

B. *Pre-election voter verification*

1. After submitting a valid ID, the voter registers with an external voter registrar (this might be done using pre-existing government electoral registration procedures).
2. The voter can log in to the system using the user id and nonce generated by the external registrar.
3. The voter's user id is then linked to any ballots for which the individual is eligible.

C. *Voter registration*

1. The voter logs into the system with the received user id and nonce, after which they must change their login credentials promptly.
2. The voter can then use the online method to register to vote for each of the ballots for which they are authorized.
3. A unique Ethereum address, the voter address, is produced and validated (while not being linked to the user id).
4. The user address is added to the ballot's smart contract, granting that address the right to vote on that ballot.
5. The address is funded with enough Ether for the voter to cast their vote.

D. *Voting*

1. When a voter chooses to vote, they are provided with an interface that mirrors the ballot smart contract's possibilities.
2. The contract is funded with the options chosen by the voters.
3. At this point, the voters' choices are immutably recorded in the blockchain, and the results are open to all to verify.

E. *Election Result*

1. Due to the nature of the smart contract architecture, no more votes for any candidate can be cast after the election has ended.
2. All of the financed transactions casting votes, as well as the tally for each candidate, are publicly verifiable by anybody.

IV. System Architecture

When creating the high-level strategy for this voting system, there were numerous factors to consider. The most essential of them is the need that a voter's account (connected to a human) and the address used to vote in the ballot contract be kept separate. This had a direct impact on how I designed the system, prompting me to divide it into distinct sections to fulfill specific roles: the Application

server (voter interaction), the Online Account Verifier (verify the legitimacy of an account to vote), and the Online Ballot Regulator (manage ballot contracts).

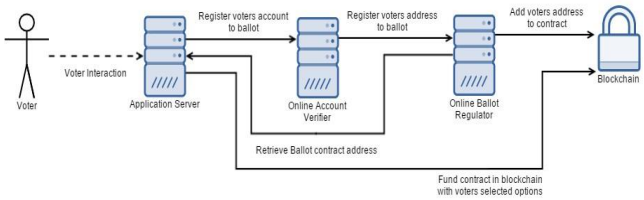

Figure 1. Outline of the system showing the basic interactions between nodes.

The registration procedure is the first stage in the design; confirming a voter is critical to the system's security. It's critical to ensure that someone's identity isn't being exploited for fraudulent reasons, especially when voting is involved because every vote counts. To allow users to register to vote, our suggested service uses recognition devices and legitimate identification card numbers to cross-check whether the person is in the database and allowed to vote.

After that, voters are given a unique hash address to use to cast their votes. Each hash is given Ethers, which he can use to vote once. During voting, the user will go through a verification procedure before casting a vote using the address provided. Once the vote is cast, the user will be instantly logged out of the system.

A. External Voter Registration

The “External Voter Registration” node is intended to represent an external registrar who is not a direct part of the established voting system but plays a critical function in verifying the legitimacy of a voter (e.g. government-issued cards like SSN, Addhar Card, etc). During the "pre-election registration" stage, when the voting public declares their intention to vote in the next election, their involvement should be limited.

B. Application Server

The “Application Server” node is where voters engage with the system the most. The user interface is centered around a dashboard page that shows key system information to the user (eligible ballots, whether they have voted, and so on). From here, the user may access all voting options, including registering for a ballot and voting.

C. Online Account Verifier

The role of the "Online Account Verifier" is to verify that a user is qualified for a ballot while maintaining the anonymity of the final Ethereum address with which the user votes. This is achieved through the use of blind token signing, which is the act of signing a message without viewing its contents. This implies that we may authenticate a voter and send them a signed token in the future, along with an Ethereum address to verify that the address is valid.

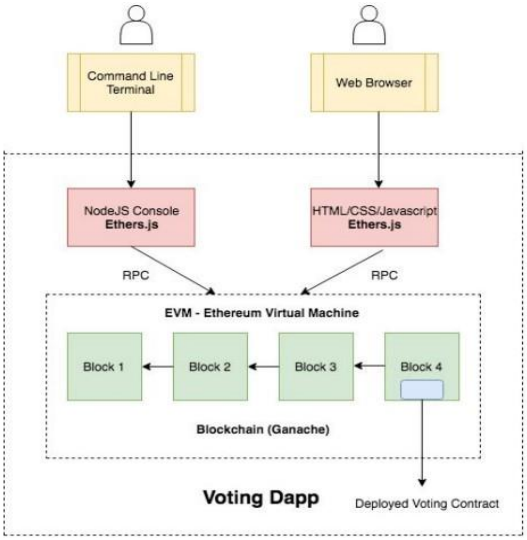

Figure 2. System Architecture

V. OVERVIEW

Next-generation voting systems can be thought of as a replacement for existing voting systems. CSS, HTML, Bootstrap, NodeJS, web3, solidity, JavaScript, Ethereum, and Firebase have been used in the proposed system. In the smart contract, the candidate's name is stated together with the candidate's symbol.

A smart contract is the most important component of the voting mechanism. A Transaction is a name given to every change performed in a blockchain. The transaction is the mechanism through which the Ethereum network communicates with the outside world. The transaction is in charge of changing or updating the state of the Ethereum network. A transaction fee or service charge is required for

each transaction. A native currency, ether, flows within the Ethereum network.

Ether is primarily used as a transaction or service fee, often known as a gas cost. Ganache-CLI is being used in this project. The process of setting up a private network is sped significantly, and transactions are mined nearly instantly.

VI. Security Analysis And Helpful Hints

A. Basic framework of the blockchain voting system

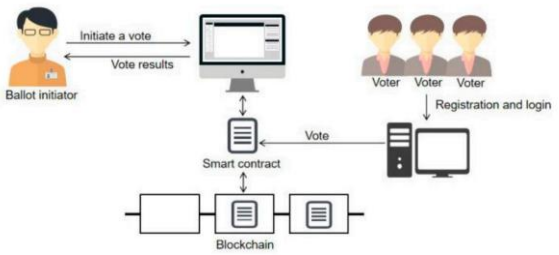

Figure 3. The basic framework of the blockchain voting system

B. The Mechanisms of a block.

When a participant wants to add a block to the chain, it is up to the peer nodes to validate it. After the majority decides to add the block to the blockchain, the block is added to the blockchain [5]. If the majority denies, the block is thrown out.

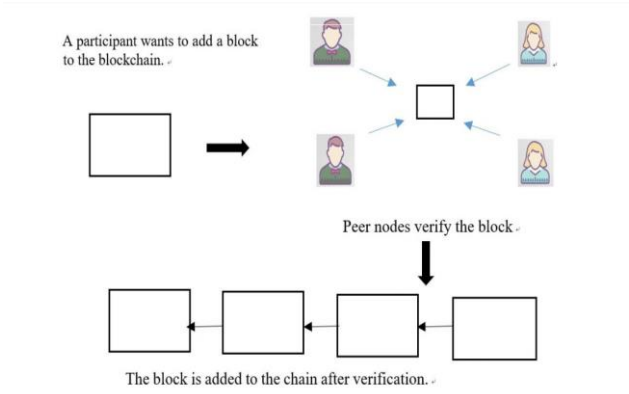

Figure 4. The mechanisms of adding a block in the blockchain.

C. Blind Signatures

A "blind signature" is a signing technique in which the signer is unaware of the content of the message he or she is signing, but the resultant blind signature may be validated against the original unblinded message in the same way as a conventional digital signature [6]. This is comparable to a person, Alice, inserting a letter inside a carbon paper-lined envelope.

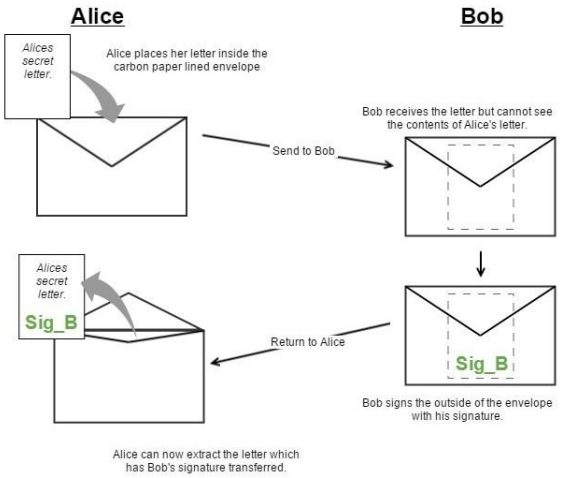

Figure 5. Blind signature analogy showing how Bob never sees the contents of Alice's message despite being able to sign it.

This is then entrusted to Bob, a trustworthy third party, who signs the exterior of the letter and returns it to Alice without examining it. Bob's signature is transferred to the letter within the envelope due to the carbon paper within. Alice may then remove the letter, which now has Bob's signature even though he has never read the contents of the letter.

D. Privacy

The most crucial feature of a voting system is voter privacy (the inability to link a voter to a vote), since once it is broken, coercion and collusion cannot be avoided, and no other criterion can be guaranteed. Except for each voter's securely kept private key, the system's architecture assures that no information is retained that might link a user account (and the person behind it) to an Ethereum address.

Unfortunately, there is still a level of faith that must be placed in the central authority that they are operating the system as specified and preserving the secret that many users are hesitant to do.

While open sourcing the codebase might help with some of this, there will always be elements of the system that aren't available to the public; nevertheless, how to establish

public trust in such a system is outside the focus of this paper.

VII. CONCLUSIONS

In today's culture, the notion of adopting digital voting technologies to make the public political process cheaper, faster, and easier is appealing. Making the election process inexpensive and quick normalizes it in the eyes of voters, reduces a power barrier between the voter and the elected official, and puts pressure on the elected official. It also allows for a more direct form of democracy, letting people voice their preferences on specific laws and initiatives.

We presented a novel blockchain-based electronic voting system that uses smart contracts to provide safe and cost-effective elections while maintaining voter privacy in this article. The system's architecture, design, and security analysis have all been documented. By comparing our findings to previous research, we have demonstrated that blockchain technology provides a new opportunity for democratic countries to move away from the pen and paper election system and toward a more cost- and time-effective election system, while also improving security and transparency. It is feasible to transmit hundreds of transactions per second into an Ethereum private blockchain, leveraging every feature of the smart contract to reduce the load on the blockchain.

For larger nations, various steps must be made to limit transaction throughput per second, such as the parent & child architecture [7], which lowers the number of transactions recorded on the blockchain to a 1:100 ratio without jeopardizing the security of the network. Our election plan effectively allows voters to vote in their preferred voting district while ensuring that each voter's vote is counted from the right district, potentially increasing voter turnout.

REFERENCES

[1] Fujioka A., Okamoto T., Ohta K., “A practical secret voting scheme for large scale elections”, *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol 718, 1993,. https://doi.org/10.1007/3-540-57220-1_66.

[2] Magkos, E.; Burmester, M.; Chrissikopoulos, V., “Receipt-Freeness in Large-Scale Elections without Untappable Channels”, *Springer*: Boston, MA, USA, 2001.

[3] Nakamoto, S., “Bitcoin: A Peer-To-Peer Electronic Cash System [EB/OL]”, 12 February 2019. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 22 October 2020).

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

[5] R. Bohme, N. Christin, B. Edelman, and T. Moore: “Bitcoin: Economics, Technology, and Governance”, *Journal Of Economic Perspectives*, Vol-29, No.2, Spring 2015, Pages 213-238.

[6] Chaum, David, "Blind signatures for untraceable payments", *Advances in Cryptology Proceedings of Crypto*, Volume 82 (3): 199–203, 1983.

[7] Jelurida, IGNIS Crowdsale, 5 August 2017. www.jelurida.com/sites/default/files/JeluridaWhitepaper.pdf