Building E-Voting Solution using Blockchain

A BTP Report

by

Ashutosh Chauhan: S20180010017
Vitthal Inani: S20180010193
Rajeev: S20180010072
Valluri Deepak: S20170010171

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRICITY

12 May 2020

1st Semester Report

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRICITY

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the BTP entitled "**Building E-Voting Solution using Blockchain**" in the partial fulfillment of the requirements for the award of the degree of B. Tech and submitted in the Indian Institute of Information Technology SriCity, is an authentic record of my own work carried out during the time period from January 2021 to May 2021 under the supervision of Prof. Rajendra Prasath, Indian Institute of Information Technology SriCity, India.
The matter presented in this report has not been submitted by me for the award of any other degree of this or any other institute.

Vitthal Inani

_ _

Ashutosh Chauhan

_ _

Valluri Deepak

_ _

Rajeev

_ _

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

BTP Supervisor
(Prof. Rajendra Prasath)

Abstract

People in every democratic country have the freedom to elect their own leader and eventually, The Government. And to do so, every citizen above the age 18 have the right to vote. It is our civic duty. There have been many alternatives for security while voting but vulnerable processes are still use throughout the world. The main reason is that we still have not come up with a better alternative for the voting system we are using at present. E-voting is one of the reliable solutions but it has to be refined to its finest version in order to be of some practical use.

Below is a requirement list for making a voting system applicable to the real-world, based on .

- Availability: An e-voting system must remain available during the whole election and must serve voters connecting from their devices
- Eligibility: Only eligible voters must be allowed to cast a ballot, and only one vote per voter count
- Integrity: A voting system must guarantee the integrity of the vote
- Anonymity: The connection between the vote of a user and the user herself must not be reconstructable without her help (and preferably not even with her help)
- Fairness: The (partial) results must be secret until the tallying has ended
- Correctness: The election results must be appropriately counted and correctly published
- Robustness: The system should be able to tolerate (some) faulty votes
- Universal verifiability: After the tallying process, the results are published and must be verifiable by everybody
- Voter verifiability: The voter must be able to verify that her ballot arrived in the ballot box
- Coercion freeness: The system must provide security mechanisms to prevent a coercer from forcing a voter to place a vote for a specific party or candidate; or even to see that she voted

To solve the problems, in this paper we propose a blockchain based electronic voting system. A blockchain is a distributed database, where the complete data is shared among all participants in the network. A blockchain system by its nature has several advantages that suit an electronic voting system. Its distributed architecture provides high availability to the system because it does not rely on a centralized server. As all participants have complete data, the protocol allows them to verify each block that is appended to the chain. We try to combine the double envelope encryption technique and blockchain technology for our proposed electronic voting system.

Table of Contents

Introduction

Democracy and public election are pillars of present-day culture, yet the customary paper voting forms are inclined to misrepresentation and disappointment; polling forms can be miscalculated, or Electronic Voting Machines (EVMs) might be reprogrammed on the way. The customary democratic framework likewise conveys the expenses of Human Resources, Voting ballot Printing, and safety efforts. An enormous measure of cash is normally spent each political race in each country. Declining rate of votes casted in certain nations have additionally showed up lately. One of the reasons is by all accounts that adolescents find going to casting a ballot places to cast a ballot unfeasible. Therefore, the requirement for a more useful democratic framework is expanding. As the web might be a promising stage for youth commitment in legislative issues, web casting a ballot appears to be a characteristic method to build interest. Some unique unfavorable conditions likewise should be thought of. In India there are many cases of riots either overpowering the voting booths or preventing the casting of the votes. This is one illustration of the risky idea of holding a popularity-based vote during a flimsy situation. For electronic democratic frameworks to be practical, we think of it as important that they are simpler to utilize and at any rate as secure as secure as customary races and should have the option to take out human mistake. This is hard to accomplish because electronic democratic frameworks need solid encryption to ensure security, respectability, and secrecy of the vote, while as yet being auditable. This should be guaranteed and still outcome in an easy-to-use application, which is frequently difficult to accomplish.

The following is a prerequisite for making a democratic framework appropriate to this present reality,

1. **Accessibility**: An e-casting a ballot framework should stay accessible during the entire political race and should serve electors interfacing from their gadgets.
2. **Eligibility**: Only qualified electors should be permitted to project a polling form, and just one vote for every citizen check.
3. **Trust**: A democratic framework should ensure the uprightness of the vote.

4. **Privacy**: The association between the vote of a client and the client herself should not be reconstruct able without her assistance (and ideally not even with her assistance).
5. **Reasonableness**: The (fractional) results should be secret until the counting has finished. rightness: The political race results should be suitably tallied and effectively distributed.
6. **Available**: After the counting interaction, the outcomes are distributed and should be undeniable by everyone. citizen
7. **Verifiable**: The elector should have the option to check that her polling form showed up in the voting station.
8. **Openness and Safety from interference**: The framework should give security systems to forestall a coercer from driving a citizen to put a decision in favor of a particular gathering or competitor.

At the point when Bitcoin was presented in 2008, it empowered exchanges of assets without a confided in go between. Nonetheless, the basic innovation, called "**blockchain**", has discovered many further uses, both through expanding on top of Bitcoin and by making new blockchain conventions. A blockchain is an unchanging record of occasions, and those occasions can be any sort of information. **Ethereum** utilizes the record to perform self-assertive (Turing complete) registering assignments and information stockpiling. Purported shaded coins utilize the Bitcoin blockchain for making a structure of advanced monetary standards with additional capacities. A blockchain is pseudonymous, which means all action is noticeable to anybody, yet every entertainer may take cover behind a "**name**" with no association with their genuine identity, similar as on an online message board. A productive use case for blockchain innovation is majority rule casting a ballot. This could consider majority rule casts a ballot that can be effectively checked by outside onlookers, making miscalculating close to unthinkable. We intend to plan and assemble a blockchain-based democratic framework that can deal with the most unfriendly conditions imaginable. By using the qualities of blockchain that appropriates trust to member in its organization, we can improve the accessibility of a democratic framework without depending on friendly trust. Additionally, the transparency of blockchain can improve the widespread certainty of a democratic framework. In this paper, we are implementing our first blockchain-based electronic voting framework that settles accessibility and verifiability.

Reference Paper/Literature Survey

We refer to many working existing solutions being use for parliamentary elections. The systems included Estonian e-voting system, The DC Digital Vote by Mail System (DVBM) and Civitas. The Reference paper used the Electronic system in Estonia as there their base reference for their model which we will implement.

The Reference Paper defined the voting solution in multiple steps. The blockchain based voting system provided privacy and verifiability and required trust on the election authority.

The Protocol Used Public Key Cryptography to encrypt and decrypt vote messages to prevent anyone from decoding and sign and verify to prevent unauthorized voting and verification.

They Used blockchain to store the votes with a Proof of Work (PoW) consensus algorithm which requires more than half of the entire networks compute power to modify a blockchain, over that the attacker(s) will also need to re-encrypt the vote messages and sign with voters' private key, making it even more computationally expensive to modify.

The verification of the votes is done by decrypting the vote message and checking the candidate address.

Why Blockchain for E-Voting System?

A blockchain has several advantages, which make it a robust and secure alternative to other databases:

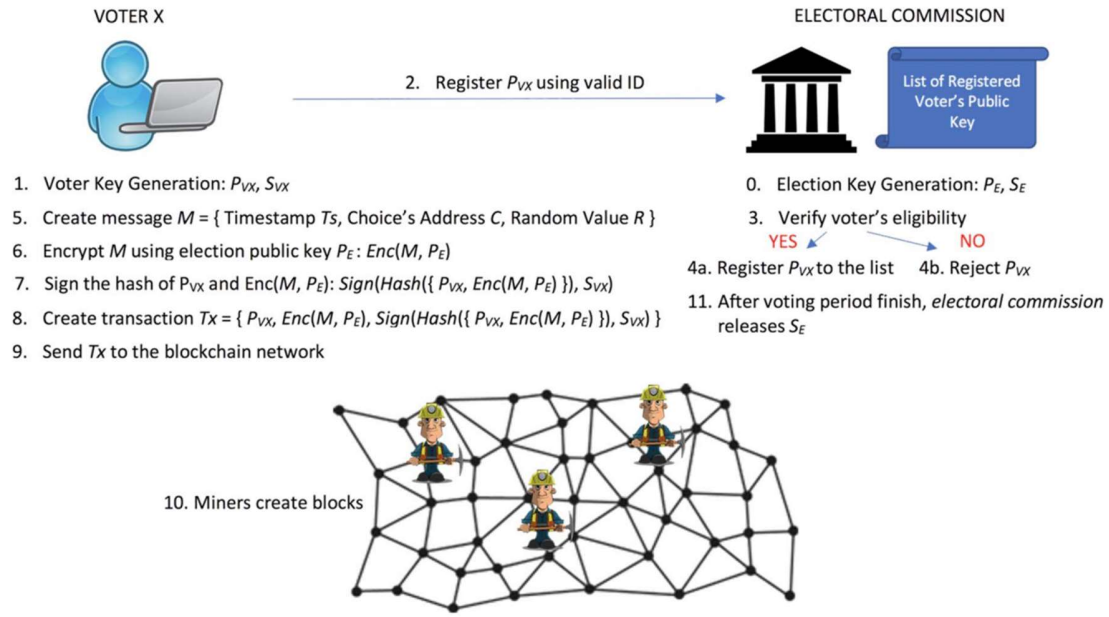
High availability: Completely distributed with many nodes storing the complete database.

Verifiability: Each block contains the hash of its previous block and is appended to the blockchain. Everyone can calculate the hash and verify them.

Integrity: It is hard to alter an older value in the chain, since all following blocks must be recalculated, which needs much computational power due to the proof-of-work.

Application Design

The main idea of our proposal is described in Figure. We combine the idea of double envelope encryption and blockchain technology to implement our system. The figure consists of 3 sides: **voter's side**, **electoral commission's side**, and the **blockchain network**.



To begin with, we need to assume a few things for our system to work properly.

- The election is correctly set up.
- The voter's computer or device can be trusted.
- There is a third party, electoral commission, that can be trusted to organize an election. Not all trustees of the election are compromised. A proof-of-work blockchain can only work properly if less than 50% of the computational resources in the network are trying to cheat by changing the blockchain in a malicious way.

In Steps 0-4 it shows preparations needed for the election. At the beginning, the electoral commission (or another election manager) generates a key-pair for the

election (P_E; S_E) which later is used for encrypting and decrypting messages of voters. Then, each voter needs to generate their own key-pair. In Fig, (P_{V_x}; S_{V_x}) denote the key pair of voter X. This key pair is later used for signing the message created by the voter herself. Voters need to register their public key PV X to the electoral commission for their voting eligibility using a designated valid ID.
The electoral commission then verifies each voter's ID and registers the corresponding public key P_{V_x} to a public list; or rejects it if the voter is not eligible. It is crucial that each voter keeps their public key secret in this scheme and only sends it to the governing body. After the registration finishes, a voter can start making a transaction T x that is described in Fig. from steps. 5 to 9. Firstly, a voter creates a message as follows

$$M = Ts;\ C;\ Rg;$$

which consists of a timestamp T s, the voter's choice address C, and a random value R. Timestamp Ts shows the time when a voter vote. The timestamp Ts also prevent multiple votes, so only the one vote is counted. The voter's choice address C contains any value that points to the voting candidates, e.g., their public keys. A random value R is needed to prevent an attacker to guess the voter's key pair from encrypted messages created by the voter herself. Secondly, the voter encrypts the created message M using election public key P_{V_x} denoted as $Enc(M; P_E)$. Thirdly, the voter signs the hash of her public key P_{V_x} followed by the encrypted message $Enc(M;\ PE)$:

$$Sign\left(Hash\left(\mathrm{P_{V_x}}; Enc(M; P_E)g\right); S_{V_x}\right)$$

denotes the said signature. At this point, a voter can create her transaction Tx.
A transaction:

$$Tx = P_{V_x};\ Enc(M;\ P\_E);\ Signg;$$

contains the voter's public key P_{V_x}, the encrypted message $Enc(M; P_E)$, and the signature of hash, Sign, combining both previous data.

Lastly, the voter can send the transaction Tx to the blockchain network. Miners in the blockchain network collect transactions and create blocks. After a block containing a specific number of transactions is created and appended to the chain, any voter can verify that the vote is collected. The voter can wait for a few more

blocks to be added on top to make sure that the block containing her transaction is inside the longest chain.
This process continues until the voting period finishes. After the voting period finishes, the electoral commission destroys all the public keys they have on record and releases the election private key S_E, so everyone can start counting votes and verifying the result.

Our Application Implementation

We will be using **Ethereum Blockchain** and making our voting smart contract.
For development and testing, we would use **Ubuntu** (**Linux**) and **Windows** machine.
We will use **Ganache** and/or **Hardhat** for simulating our network.
We will use **Solidity** Programming Language for developing our smart contracts.

Results

An attacker cannot easily tamper votes. First, the voting message, M is encrypted with double envelop scheme. The attacker needs to figure out how to decrypt the encrypted message, $Enc(M; P_E)$ to tamper it.
Then, although the attacker can decrypt it, only changing the vote and re-encrypt it will not make the vote valid. The signature described in (2) will tell that the vote has been tampered with. Everyone can verify the signature by using public key P_{V_x} and calculate the hash of the public key P_{V_x} and its corresponding encrypted message $Enc(M; P_E)$ that can be seen from the transaction.

Therefore, the attacker also needs to figure out how to make the signature valid. Second, changing or removing a collected transaction inside a block changes the hash of the block itself. So, an attacker needs to re-calculate all hashes of next blocks which needs huge computational work.

References

- A Proposal of Blockchain-Based Electronic Voting System | IEEE Conference Publication | IEEE Xplore
- Home | ethereum.org
- Truffle | Truffle Suite
- Ganache | Truffle Suite