International Journal of Research in Engineering, Science and Management
Volume-3, Issue-6, June-2020
www.ijresm.com | ISSN (Online): 2581-5792

A Review on Secure Voting System Based on Blockchain Technology

Kapil Aminbhavi[1*], Sanket Kulkarni[2], Preyash Mehta[3], Rishubh Bijlani[4], Rubeena Khan[5]
[1,2,3,4]*Student, Dept. of Computer Engineering, Modern Education Society's College of Engineering, Pune, India*
[5]*Professor, Dept. of Computer Engineering, Modern Education Society's College of Engineering, Pune, India*
*Corresponding author: kaminbhavi1@gmail.com

***Abstract*: Election is a very important event in a modern democracy, it has been rightly called a 'festival of democracy'. In the today's election scheme, no method of transparency can be ordered to participants of the election. When an individual places his ballot in the box at his voting district, there is no guarantee from the scheme that his vote was counted and counted correctly. Any individual vote can be misplaced, counted incorrectly because of human error or simply because the party which the voter voted for could be disliked by the individual which counted the vote. This transparency is non-existent because no ballot has information on who casted aforementioned vote. Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper-based systems such as increased efficiency and reduced errors. With the advent of EVM machines for Electronic voting, stemmed a few more problems, Vote rigging, hacking of the EVM (Electronic voting machine), election manipulation, and polling booth capturing are a major issues and thus a large section of societies around the world do not trust their elections systems and by extension, electoral commission. We can usher in a newer, better world by playing the various ad-vantages Blockchain has to offer and create a trustworthy world working around the social dilemma of trust. Through our project we make an effort to provide a system to deal with the crux of the modern democracy by leveraging the advantages of blockchain such as cryptographic foundations and transparency to successfully pull off an election where the society has no trust issues.**

***Keywords*: Blockchain technology, Firebase authentication, Cryptography, Electronic voting.**

1. Introduction

In today's world, widespread mistrust towards the government and interference in countries processes by external actors have made the democratic process of voting more critical than ever. Democratic countries have been experiencing dictatorial regimes which have introduced widespread terror among their people. People have had their human rights violated and their fundamental freedoms provided by their constitution taken away. In such an atmosphere, having a fair and transparent election is something that is paramount for the freedom most people enjoy today. The pitfalls of the current system of ballot voting are being taken advantage of by people or organizations looking to gain power. In the African countries of Uganda and Kenya there has been widespread controversy over their elections in recent years. The election of 1946 in Romania was heavily rigged. The communists took over Romania and abolished the multi-party system to gain complete control of the country. These instances of controversial elections could all have been avoided if the counting process was fair, transparent and verifiable. The current ballot system does offer anonymity to the voter but the counting process is not transparent. People are supposed to trust the result which is provided by an Election commission or a government body. This makes the process of counting, a major vulnerability in the current process. There are also other major electoral scams such as voter fraud, ballot stuffing and booth capturing. All these make it very difficult for organizers of an election to distinguish between the actual votes and votes added without authorization. The system that is being proposed solves most of the issues such as voter fraud, ballot stuffing, booth capturing and can be implemented in the current world environment. The system of remote blockchain voting will impact society in a very positive way. The system will increase convenience for voters. It will make it very easy for people with disabilities or who have trouble moving around to vote. It is very quick and private way to vote. This will increase the number of voters since the process does not take up too much of their time of the day. It will help increase the trust of the people in the government since it is more transparent than the current ballot system. The system is better for the environment as compared to the paper voting system. It eliminates the need for paper voting and the carbon emitted by the logistics of those ballots. Hence this system has a much smaller carbon footprint.

Table 1
Risk analysis

ID	Risk Description	Probability	Impact		
			Schedule	Quality	Overall
1	51% Attack	Medium	Low	High	Low
2	Manipulation of votes during transit	High	Low	Low	Medium

By storing data across its peer-to-peer network, the blockchain eliminates a number of risks that come with data being held centrally. The decentralized blockchain may use ad hoc message passing and distributed networking. Every node in a decentralized system has a copy of the blockchain. Data quality is maintained by massive database replication and computational trust. No centralized "official" copy exists and no user is "trusted" more than any other. Transactions are broadcast to the network using software. Messages are delivered on a best-effort basis.

With the rise of blockchain technology the core concept of decentralization has gradually drawn attention. In this context, the main objective of this research is to realize more convenient and secure applications through the use of blockchain technology. This research will combine the advantages and properties of blockchain and Decentralized environment along with the consensus algorithm to minimize the attacks to 49% [1]. A consensus algorithm may be defined as the mechanism through which a blockchain network reach consensus. Public (decentralized) blockchains are built as distributed systems and, since they do not rely on a central authority, the distributed nodes need to agree on the validity of transactions. This is where consensus algorithms come into play. They assure that the protocol rules are being followed and guarantee that all transactions occur in a trust-less way, so the coins are only able to be spent once.

The system that is being proposed solves most of the issues such as voter fraud, ballot stuffing, booth capturing and can be implemented in the current world environment. The system of remote blockchain voting will impact society in a very positive way. The system will increase convenience for voters [2]. In the context of cryptocurrencies, the consensus algorithms are a crucial element of every blockchain network as they are responsible for maintaining the integrity and security of these distributed systems. The first cryptocurrency consensus algorithm to be created was the Proof of Work (PoW), which was designed by Satoshi Nakamoto and implemented on Bitcoin as a way to overcome the Byzantine faults.

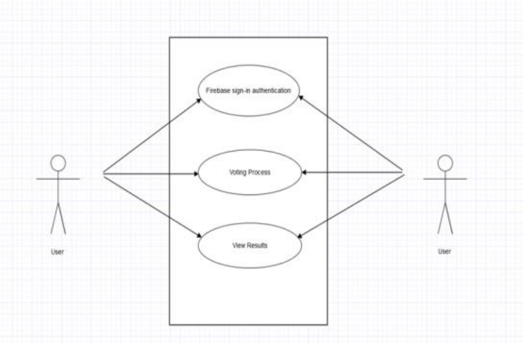


Fig. 1. Use-case diagram of the voting process using Firebase sign-in

2. Motivation

Plato, in Republic has mentioned the order and the character of a just city-state, an ideal democratic system that protects the rights of its citizens. Looking at the current method of election and the seeds of doubt in the minds of man regarding it, our republic has drifted far from Plato's Republic. To protect the basic rights of citizens granted by a democracy we were motivated to undertake this project.

Block chain is a growing list of blocks. Block chain consists of several blocks that are linked to each other and in sequence. The block is related because from the previous hash used in the next block making process, the attempt to change the information will be more difficult as it has to change the next blocks [2]. The main objective of this project is to build an android based application which helps users to register their vote through the block-chain based system where authenticity of the voter is validated by the Firebase-authentication method.

3. Methodology

The block chain is a public ledger, all individuals can synchronize the latest ledger into local, and they have no permission to tamper the content of the public ledger In the proposed paper, we are trying to leverage the block chain technology to ameliorate the security mechanism for an electronic voting system.

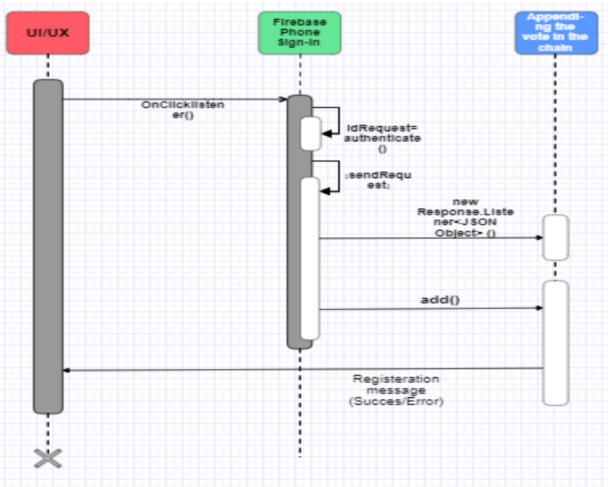

UI/UX
Firebase Phone Sign-in
Appendi-ng the vote in the chain
OnClickListen er()
IdRequest= authenticate ()
sendRequ est
new Response.Liste ner<JSON Object> ()
add()
Registeration message (Succes/Error)

Fig. 2. Methodology of a secure digital voting system based on Blockchain technology using firebase authentication

Parts of the System:

- User: The user should have internet connection to register and vote as well.
- Fire base sign-in authentication: We can use Fire base Authentication to sign in by sending a message to the user's phone. The user signs in using a one-time password contained in the message.
- Voting Process: The vote will be sent as JSON object and it will be annexed to the chain. This chain is visible to all the users thus providing the feature of transparency of thee technology.
- JSON: JSON data format which is the key-value pair, where the key - 'TO' is matched with get method on the backend server after which it appends the value - 'party-name' to the chain along with other facets.
- Fire base authentication: You can use Fire base Authentication to sign in a user by sending an SMS to

the user's phone.

- Block: A Block records some or all of the most recent block chain transactions that have not yet entered any prior blocks.
- Proof of work: A proof of work is a piece of data which is difficult to produce but easy for others to verify and which satisfies certain requirements. Proof of Work is often susceptible to 51 percent attack and a system can be settled if 50 percent or more of the nodes are compromised.
- Nonce: The block numbers cannot be altered, the data inside the block is fixed and so is the previous hash. Changing the value of this block will result in the change of the hash value of the entire block.
- Hash: To get the blocks validated, miners have to be able to identify them with a unique digital password, known as hash. These passwords are like fingerprints. We use SHA-256 algorithm to compute the hash value of the previous block.

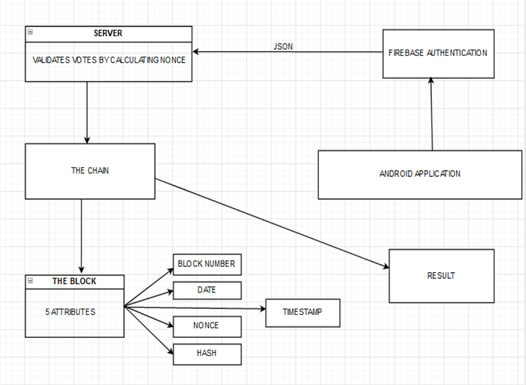


Fig. 3. Blockchain based voting system architecture

Authentication of voters using Firebase Authentication: Firebase Authentication with phone number can sign in a user by sending an SMS message to the user's phone. The user signs in using a one-time code contained in the SMS message. Most of the applications use the email and social login platforms for verification but there are a few which use Phone number authentication feature for validation. In the firebase UI we have a method called "On Verification Completed" through which we need to make an action after the verification (successful or unsuccessful). Based on that check you can either redirect the user or do whatever you'd like if it was successful. Otherwise, you can ask the user to re-enter the code or something similar.

Incentive to run node: The backbone of the distributed Blockchain based system is the individuals running the nodes, for a cryptocurrency backed Blockchain they have a financial motive to spend CPU power by running the node, as our proposed system is a Blockchain without any underline financial system, we intend to run the node on the device on which the app is installed by using a scripting layer.

Verification and validation for acceptance:

For the verification of votes and validation of the user identity along with the privacy of votes will be done using the Firebase authentication method to sign in a user by sending an SMS message to the user's phone. The user signs in using a one-time code contained in the SMS message. The authentication process has 4 steps:

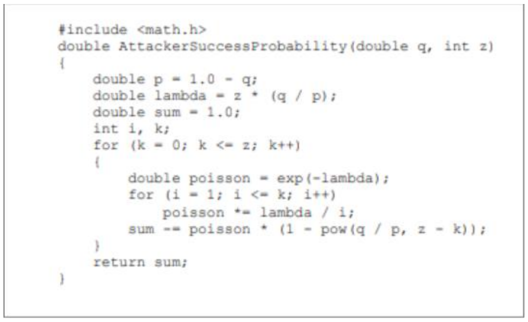
- Enable Phone Number sign-in for your Firebase project.
- Send a verification code to the user's phone.
- Create a PhoneAuthCredential object
- Sign in the user.

All of the above steps are used for the verification. Firebase UI can be used to add a phone number sign in to your app.

System Description:

- Input: JSON data format which is the key-value pair, where the key- 'TO' is matched with get method on the back-end server after which it appends the value - 'party-name' to the chain along with other attributes shown in the output section.
- Output:

"index"- serial number
"nonce"- numeric calculated value
"prev-hash"- random hash value generated
"timestamp"- date along with time in hour:min:sec
"vote":
"to": "Online MCQ"



```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Fig. 4. Mathematical formulation

Blockchains allow different parties that do not trust each other to share information without requiring a central administrator. The value of decentralized control is that it eliminates the risks of centralized control. With a centralized database, anybody with sufficient access to that system can destroy or corrupt the data within. This makes users dependent on the administrators. Some administrators have earned the trust put in them, for the most part. From past examples we have observed many data breaches resulting in data getting compromised. To avoid this unethical breach in database we can use blockchain system. We conducted a mock election in our college to decide the course of action for exams amid the corona virus outbreak. Our application allowed the students to cast their votes through which we could conclude the situation that was lurking around.

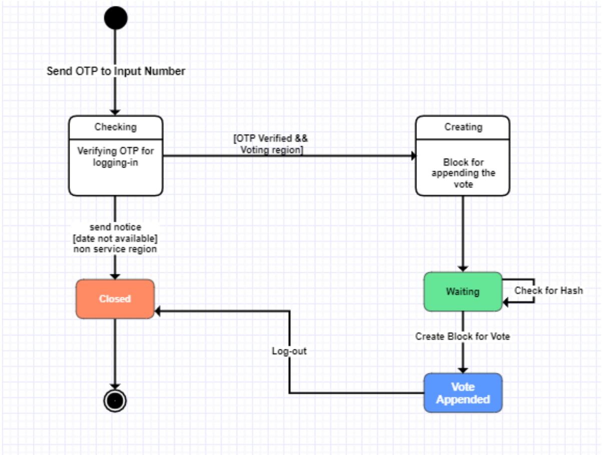

Send OTP to Input Number
Checking
Verifying OTP for logging-in
[OTP Verified && Voting region]
Creating
Block for appending the vote
send notice [date not available] non service region
Closed
Waiting
Check for Hash
Create Block for Vote
Log-out
Vote Appended

Fig. 5. State Diagram of the voting process through a one-time password using fire base authentication

We propose a secure voting application using Block chain, which is an enhancement of the current electronic voting system. The votes in the chain are cryptographically related block by block. There is preferential selection of blocks having the same timestamp in which we elect a block with a higher value of signature. This system increases the convenience for voters. It will make it very easy for people with disabilities or who have trouble moving around to vote. It is very quick and private way to vote. This will increase the number of voters since the process does not take up too much of their time of the day. It will help increase the trust of the people in the government since it is more transparent than the current ballot system.

4. Hashing Function

Every block in the stack contains a hash value on the header. This hash is formed using the Secure Hash Algorithm (SHA-256) to generate a peculiar fixed-size 256 hash. The SHA-256 will take any size plain text as an input, and encrypt it to a 256-byte binary value. The SHA-256 is always a bit binary value, and it is a strictly one-way function.

The header contains the hash of the previous block of the chain and the blocks are connected to the chain with a cryptographic hash of its data. This hash traces back to the origin block of the chain. When the block is created, it is sent to the chain and it gets appended to the block chain.

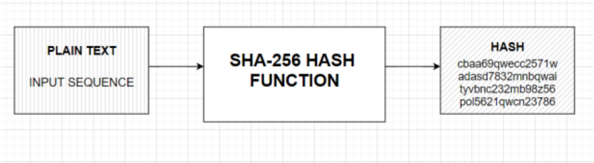


Fig. 6. Working of the SHA-256 hashing function

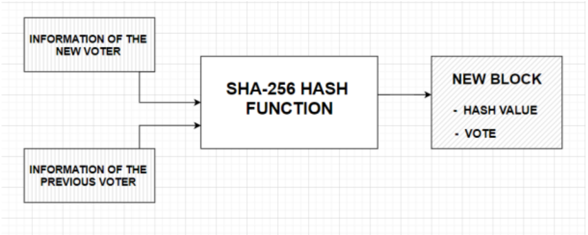

INFORMATION OF THE NEW VOTER
INFORMATION OF THE PREVIOUS VOTER
SHA-256 HASH FUNCTION
NEW BLOCK
- HASH VALUE
- VOTE

Fig. 7. New block formation with hash value and the vote

As soon as a block is created, it is sent over to the block chain.

5. Conclusion

Using blockchain technology, we can make sure that those who are voting are who they say they are and are legally allowed to vote. Plus, by using blockchain technology, anyone who knows how to use a cell phone can understand the technology required for voting. It is vital for a democracy to have a transparent voting system that must have the least number of obstacles for a voter to vote. The proposed system not only handles voter privacy and auditability but also provides a transparent system for verification of the election. The proposed system is shown to be highly cost efficient as compared to other countries and can be implemented with existing infrastructure owned by a nation. Keeping all these factors in mind our proposed system is a comprehensive solution.

References

[1] John Stuartmill, “A Distributed Consensus Algorithm for Cryptocurrency Networks,” October 2016.

[2] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” October 2008.

[3] Fririk Hjalmarsson, Gunnlaugur K. Hreiarsson, Mohammad Ham, Daqa, Gisli Hjalmtysson, “Blockchain Based E-Voting System,” July 2018.

[4] Francesco Fusco, Maria Ilaria Lunesu, Filippo Eros Pani and Andrea Pinna, “Crypto-Voting, a blockchain based e-voting system,” April 2019.

[5] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, “E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy,” July 2018.

[6] Authentication with Firebase on Android using a Phone Number "https://firebase.google.com/docs/auth/android/phone-auth