International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

Secure Voting System using Blockchain

Dipali Pawar, Pooja Sarode,
Shilpa Santpure, Poonam Thore
Department of Computer Engineering
JSPM's Imperial College of Engineering and Research
Pune, India

Prof. Pravin Nimbalkar
Department of Computer Engineering
JSPM's Imperial College of Engineering and Research
Pune, India

***Abstract*— Technology has positive impacts on various aspects of our social life. Designing a globally connected architecture enables ease of access to a variety of resources and services. Furthermore, technology like the Internet has been a fertile ground for innovation and creativity. One such innovation is blockchain – a keystone of cryptocurrencies. The blockchain technology is presented as a game-changer for many existing and emerging technologies. With its immutability property and decentralized architecture, it is taking centre stage in many services as an equalization factor to the current parity between consumers and large corporations/governments. One future application of the blockchain is in e-voting. The objective of such a scheme would be to provide a decentralized architecture to run and support a voting scheme that is open, fair, and independently verifiable. In this paper, we propose a potential new e-voting protocol that utilises the blockchain as a transparent ballot box. The protocol has been designed to achieve fundamental e-voting properties as well as offer a degree of decentralization and allow for the voter to change/update their vote (within the permissible voting period). This paper highlights the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts.**

Keywords*— Blockchain; Cryptocurrency; SHA-3; E-Voting; Decentralized.

1. INTRODUCTION

1.1 What is Blockchain?

Blockchain is a chain of blocks. In this context, "block" means digital information and "chain" means public database. So "Blockchain is secure, decentralize, a distributed database managed by a cluster of computers." It is a shared and immutable ledger.The information in blockchain is open for anyone and everyone to see. Blockchain is a technology that does not use third parties in data exchange. Third-party cannot temper blockchain data as it is stored on thousands of machines. Blockchain is public and private type, A public blockchain is readable and writable for everyone where private blockchain sets restrictions on who can read or interact with it.

Blockchain is the backbone technology of Digital Cryptocurrency Bitcoin. Blockchain technology was first used in Bitcoin.It is a public ledger of all transactions. A blockchain stores these transactions in a block, when more transactions are carried out the block eventually becomes completed. For example, in Bitcoin, since the wallets are in a distributed structure, the total amount of coins and transactions followed clearly. There is no need for a central authority to approve or complete the operations on this P2P system[3].

Fig 1: Blockchain

1.2 Key features of Blockchain :

- High Availability
- Verifiability
- Transparency
- Immutability
- Distributed Ledgers
- Decentralized
- Enhanced Security

1.3 Current Voting System :

Electronic Voting Machines ("EVM") are being used in Indian General and state elections to implement electronic voting in part from 1999 elections and recently in 2019 Vidhan Sabha Elections. Before EVM, vote counting was done by paper ballot but with the advancement in technology, electronic voting machines came into the picture. EVMs have replaced paper ballots in local, state and general elections in India.

Fig 2: EVM Machine

There are two units in EVM : the control unit and the balloting unit. These units are joined together with the help of cable. The control unit of the EVM is kept with the presiding officer or the polling officer. The balloting unit is kept within the voting compartment for electors to cast

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

their votes. This helps polling officer to verify your identity. With the EVM, instead of issuing a ballot paper, the polling officer will press the Ballot Button which enables the voter to cast their vote. A list of candidate's names and/or symbols will be available on the machine with a blue button next to it. The voter can press the button next to the candidate's name they wish to vote for.

No part of the EVM is "networked" is the most important thing .EVM machines are extremely simple machines, like pocket calculators, with no connection to the internet, no operating system and no way of being altered without physical access to the machines.

There were earlier claims regarding EVMs' temper ability and security which have not been proved.

Disadvantages of EVM or Current Voting System

- Vulnerability to hacking.
- Susceptibility to fraud.
- Malicious programming.
- The time gap between the voting and counting of votes is large which leads to tampering.
- Due to the physical accessibility to the EVM, the third party can interrupt and change the count of votes.

1.4 Proposed System :

Propose system is internet voting system . We provide an online platform for voting i.e a website. Propose system three parts as Voter, Election Administrator and Election Process.

A) **Voter :** Voter is the main part of system which participate in election process. He register himself in system by giving his personal information.
B) **Election Administrator :** To manage all the data coming from voter during registration
C) and election process, election administrator has worked. Also it generate public and private keys for voters. It is nothing but python packages.
D) **Election Process :** In this process voter select the candidate to vote and give his vote for selected candidate.

Working Of Propose System :

In propose system as told earlier voter register himself. During registration system takes voter's unique identity number. Unique identity is for generating unique public and private key for every voter. So here problem of double voting is solved.

After taking all required information from voter, if voter is eligible for voting process then only system accept registration of voter. Then system i.e election administrator generate public and private keys for voter

Public Key and Private Key :

Private key and public key are the hash value data which is unreadable. During election process for login purpose and giving vote to candidate public key and private key is required. It act like login id and password in this voting process. But voter cannot always remember it as it is large value. After successful registration this keys send to the registered email or mobile number.

Also during voting process for data encryption and decryption purpose it is used.

E) After successful authentication and generating public and private key pair, voter login himself in system using keys. When voter enter in system he gets list of all candidates.Voter chooses candidate for voting and give him vote. That vote is a block which is added in blockchain and broadcast to every system in network. Every voter follow this process and every block is added in blockchain and hash value of each block is calculated. Every block contains previous block's hash value. So every block is connected with each other by hash value of previous block. As blockchain is decentralized then blockchain is created on every computer systems in network. So hacking of blockchain and tempered with data is not possible.When whole election process is over, all votes calculated and result get declared.

Process of Blockchain creation :

Every block has data, hash of the block and hash of previous block. When new block is created then hash of previous block is store in this block and then hash of new block is calculate and store in it. In this way blockchain is created.

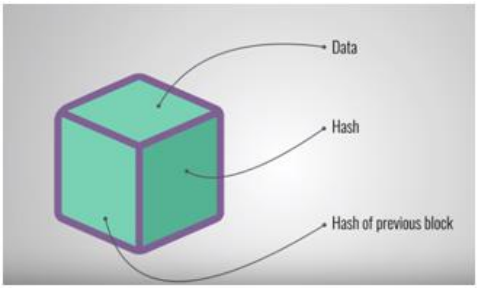


Fig 3: Block Representation

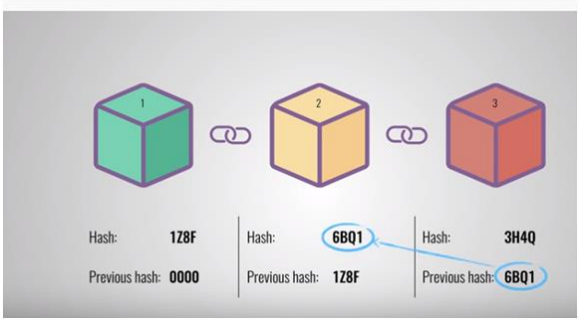
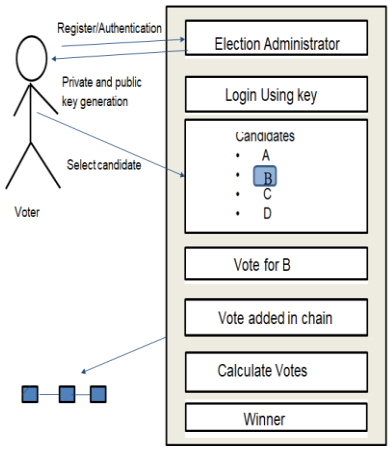


Fig 4 : Blockchain creation

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

Architecture Of Proposed System :



Advantages of propose system :

- ❖ Blockchain offers an updated system which is secure and fair.
- ❖ Transparency allow votes to be followed, counted, and correlated by many different sources.
- ❖ Anonymous transactions of blockchain maintain privacy of the voters.
- ❖ As it is distributed system, data is stored on multiple machines in networks. So problem of data loss is avoided.

Blockchain voting is just one of the many use cases of blockchain technology. As the world develops, the evolution of voting is imperative.

With the current voting system being so flawed and scrutinised, blockchain aims to introduce a new way for people to vote and communicate in their local and global elections.

Transparency :

Without transparency, people can become discouraged about the legitimacy of their votes and can lead to questions about tampering and falsified results. Transparency makes for a trustworthy election which then leads to more positive outcomes from the votes.

Security :

Everything that occurs on the blockchain is encrypted and it's possible to prove that data has not been altered. Also, it is decentralized. So it is too secure.

Anonymity :

People want privacy while voting and also don't want to disclose their votes. This anonymity is achieved using private key. This may encourage more people to take part in voting process and use the voting system.

Processing time :

Current voting systems often take time to collect and calculate votes. When voting stations are in different areas and offices are not all together, it can be difficult to gather all the information quickly and efficiently which leads to time and cost issues. Instead of having to wait for a large number of people to communicate manually, all organisers will be able to see the outcome instantly on the blockchain. Results can be gathered and processed quickly after the voting has finished.

Algorithm Used :

F) Python's Django Framework is used for front end.

G) In this system data structure used is single linked list as structure of Blockchain is like single linked list.

H) Another practical use is a data structure called a hash table where data is stored associatively.

I) A hash function is used to map data of arbitrary size to fixed-size values.

J) In this system, Algorithm used is SHA-3. SHA-3 (Secure Hash Algorithm Version 3), also called Keccak, is a unidirectional function for generating digital prints of the selected length (the standard accepts 224, 256, 384 or 512 bits) from input data of any size.The algorithm works by means of the mixing function with compression to the selected size "cryptographic sponge".

2. CONCLUSION

Blockchain Technology is gaining popularity day by day. Using blockchain in voting system will help to achieve secure and cost-efficient election while guaranteeing voter's privacy. Also, due to the encryption mechanism, it is impossible for any person to gain access to all the votes without first taking control of the entire service network.

REFERENCES

[1] Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato, " A Proposal of Blockchain-based Electronic Voting System ", Dept. of Electrical Engineering and Information Systems.Artis Mednis, Girts Strazdins, Reinholds Zviedris, Georgijs Kanonirs, Leo Selavo, "Real Time Pothole Detection using Android Smartphones with Accelerometers."

[2] Fridrik P. Hjálmarsson, Gunnlaugur K. Hreidarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson,"Blockchain-Based E-Voting System ".Available at: https://ieeexplore.ieee.org/document/8457919.

[3] Ali Kaan Koc,Umut Can abuk,Emre Yavuz ,Gokhan Dalkoloc,"Towards Secure E-Voting Using Ethereum Blockchain".Available at: ieeexplore.ieee.org/document/8355340/.

[4] Henry Rossi Andrian, Novianto Budi Kurniawan, Suhardi,"Blockchain Technology and Implementation : A Systematic Literature Review".2018 International Conference on Information Technology Systems and Innovation (ICITSI) October 22-25,2018.

[5] Ashish Singh,Kakali Chatterjee," Secure Electronic Voting System Using Blockchain Technology",2018 International Conference on Computing, Power and Communication Technologies (GUCON) Sep 28-29, 2018.

[6] Nir Kshetri and Jeffrey Voas,"Blockchain-Enabled E-Voting",https://Blockchain%20Papers/kshetri2018.pdf.

[7]]Basit Shahzad and Jon Crowcraft,"Trustworthy Electronic Voting Using Adjusted Blockchain Technology."

[8] Tareq Ahram,Aman Sargotzaei,Saman Sargotzaei,Jeff Daniels,Ben Amaba,"Blockchain technology Innovations".Availabe at:https://ieeexplore.ieee.org/document/7998367/authors.

[9] Rishav Chatterjee,Rajdeep Chatterjee,"An Overview of the Emerging Technology:Blockchain".Available at:https://ieeexplore.ieee.org/document/8307344

[10] Christopher G.Harris,"The Risks and Challenges of Implementing Ethereum Smart Contracts".Available at:https://ieeexplore.ieee.org/document/8751493.

[11] H Halpin,M Piekarska,"Introduction to Security and Privacy on the Blockchain", 2017 IEEE European Symposium on 2017 - ieeexplore.ieee.org.