ISSN 2395-1621

E-voting system using Blockchain Technology and Fingerprint Authentication

Sonali Malhari Tambe, Piyusha Vijaykumar Vhanakde,
Pratiksha Ashok Wagh, Shraddha Umesh Adhav, Prof. Pranita Ingale

DEPARTMENT OF INFORMATION TECHNOLOGY
JSPM'S
BHIVARABAI SAWANT INSTITUTE OF TECHNOLOGY & RESEARCH, NAGAR ROAD, WAGHOLI, PUNE-412207

ABSTRACT

Increasing digital technology has revolutionalized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, where in one organization manages it. Some of the problems that can occur in traditional electoral systems is with the organization that has full control over the database and system. It is possible to tamper with the database of considerable opportunities. Block chain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this will be a method based on a predetermined turn on the system for each node in the built of block chain.

ARTICLE INFO

Article History

Received: 10th April 2023

Received in revised form :

11th April 2023

Accepted:14th April 2023

Published online :

14th April 2023

KEYWORDS: Blockchain, Voting System, Fingerprint, Authentication

I. INTRODUCTION

From the dawn of democratically electing candidates, the voting system has been based on pen and paper scheme. Replacing the traditional pen and paper scheme with a new election system is a new idea for researchers.

An E-voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with.

Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its state- wide elections [2], and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e- Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes.

MOTIVATION

The proposed system can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election.

II. PROBLEM DEFINITION

Proposed a E-voting using block chain Technology and fingerprint authentication for providing a facility to cast vote for critical and confidential. The flexibility to allow casting vote from any remote place.

III. LITERATURE SURVEY

[1] Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System A purely peerto-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double- spending. We propose a solution to the

double-spending problem using a peer- to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, theyll generate the longest chain and outpace attackers. The network itself requires minimal structure. Mes- sages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

[2] Christopher D. Clack, Smart Contract Templates: foundations, design landscape and research directions. In this position paper, we consider some foundational topics regarding smart contracts (such as terminology, automation, enforceability, and semantics) and define a smart contract as an agree- ment whose execution is both automatable and enforceable. We explore a simple semantic framework for smart contracts, covering both operational and non- operational aspects. We describe templates and agreements for legally- enforceable smart contracts, based on legal documents. Building upon the Ricardian Contract triple, we identify operational parameters in the legal documents and use these to connect legal agreements to standardised code. We also explore the design landscape, including increasing sophistication of parameters, increasing use of common standardised code, and long-term academic research. We conclude by identifying further work and sketching an initial set of requirements for a common language to support Smart Contract Templates.

[3] EppMaaten, Towards remote e-voting: Estonian case This paper gives an overview about the Estonian e-voting system. Paper discusses how the concept of e-voting system is designed to resist some of the main challenges of remote e-voting: secure voters authentication, assurance of privacy of voters, giving the possibility of re-vote, and how an e-voting system can be made comprehensible to build the public trust.

[4] Paul Gibson, A review of E-voting: the past, present and future Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability , dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is different different when complex communications technology is involved in the process. Electronic voting has been deployed in many different types of election throughout the world for several decades.

[5] Muhammad Ajmal Azad, M2M-REP: Reputation of Machines in the Internet of Things 2017. The Internet of Things (IoT) is the integration of a large number of autonomous heterogeneous devices that report information from the physical environment to the monitoring system for analytics and meaningful decisions. The compromised machines in the IoT network may not only be used for spreading unwanted content such as spam, malware, viruses etc, but can also report incorrect information about the physical world that might have a disastrous consequence. The challenge is to design a collaborative reputation system that calculates trustworthiness of machines in the IoTbased machine-to-machine network without consuming high system resources and breaching the privacy of participants. To address the challenge of privacy preserving reputation system for the decentralized IoT environment, this paper presents a novel M2M-REP (Machine to Machine Reputation) system that computes global reputation of the machine by aggregating the encrypted local feedback provided by machines in a fully decentralized and secure way.

[6] Kashif Mehboob Khan Secure Digital Voting System based on Blockchain Technology. 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. However, there remain challenges to achieve wide spread adoption of such systems especially with respect to improving their resilience against potential faults. Blockchain is a disruptive technology of current era and promises to improve the overall resilience of evoting systems. This paper presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for evoting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verifiability. The paper presents details of the proposed e-voting scheme along with its implementation using Multichain platform.

IV. PROPOSED SYSTEM

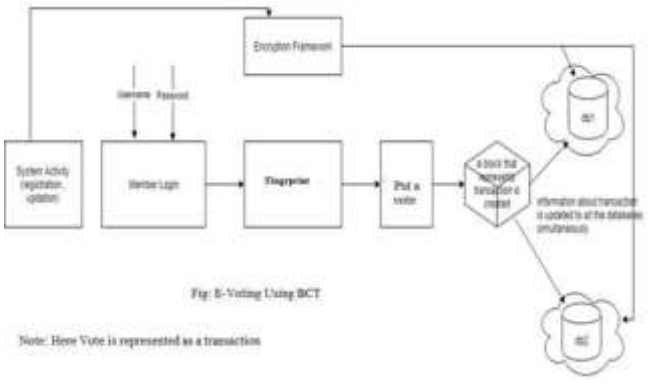

Fig 1. Proposed System

Whenever any transaction will occur in the system, the record of that transaction is maintained in the form of hash value in a block. Each next block will get attached to the previous block and in this way a virtual block chain will occur. The hash value of a current block is generated using the data of a current block and the hash of the previous block. In this way if any of the block is tempered the subsequent all the block's hash must be changed. Such multiple copies are maintained at different servers, which will assure the data security and confidentiality. As everything is through application interface, it will maintain the transparency in the voting system.

• Admin: admin can add candidate, voter, ward and election. He/she can perform update delete operation and declared result also.

• FingerPrint: Administrator (Election officer) sends share 1 to voter e-mail id before election and share 2 will be available in the voting system for his login during election.Voter will get the secret password to cast his vote by combining share 1 and share 2 using FingerPrint.

• User: Voter can vote only if he/she logs into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images)using Fingerprint scheme.

• Block Chain: Block chain is a distributed database that stores data records that continue to grow, controlled by multiple entities. Block-chain (distributed ledger) is a trustworthy service system to a group of nodes or non-trusting parties, generally block chain acts as a reliable third party to keep things together, mediate exchanges, and provide secure computing machines.

V. CONCLUSION

The proposed system will be designed to provide a secure data and a trustworthy Evoting amongst the people of the democracy. Block chain itself has been used in the Bit-coin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election.

VI. REFERENCES

[1] Ahmed Ben Ayed,A Conceptual Secure Block Chain-Based Electronic Voting System,2017 IEEE International Journal of network & Its Applications(IJNSA),03 May 2017[1].

[2] RifaHanifatunnisa, Budi Rahardjo, Blockchain Based E-Voting Recording System Design,IEEE 2017[2]

[3] Kejiao Li, HuiLi,HanxuHou, KedanLi,Yongle Chen, Proof of Vote: A HighPerformance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain, 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems[3]

[4] Ali KaanKo, EmreYavuz, Umut Can abuk, GkhanDalkilic, Towards Secure E-Voting Using Ethereum Blockchain,2018 IEEE[4]

[5] Supriya Thakur Aras, Vrushali Kulkarni, Blockchain and Its Applications A Detailed Survey, International Journal of Computer Applications (0975 8887) Volume 180 No.3, December 2017[5].

[6] Freya Sheer Hardwick, ApostolosGioulis, Raja Naeem Akram,Konstantinos Markantonakis, E-Voting with Blockchain: An E-Voting Protocolwith Decentralisation and Voter Privacy,IEEE 2018,03 July 2018[6]

