OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

E-VOTING USING BLOCK CHAIN

Lahane Amol Vishvnath

PG Student, Computer Science & Engineering Department, EESGOI, Aurangabad

---

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.

----------∴∴∴----------

I INTRODUCTION

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 statewide 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 voters ballot from being tampered with. Many electronic voting systems rely on Tor 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. In every democracy, the security of an election is a matter of national security.

The computer security eld has for a decade studied the possibilities of electronic voting systems [1], with the goal of minimizing the cost of having a national election, while fullling and increasing the security conditions of an election. From the dawn of democratically electing candidates, the voting system has been based on pen and paper. Replacing the traditional pen and paper scheme with a new election system is critical to limit fraud and having the voting process traceable and veriable [2]. Electronic voting machines have been viewed as awed, by the security community, primarily based on physical security concerns. Anyone with physical access to such machine can sabotage the machine, thereby affecting all votes cast on the aforementioned machine. Enter blockchain technology. A blockchain is a distributed, immutable, incontrovertible, public ledger. This new technology works through four main features:

(i) The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.

(ii) There is distributed control over who can append new transactions to the ledger.

(iii) Any proposed new block to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.

(iv) A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger. These technological features operate through advanced cryptography, providing a security level equal and/or greater than any previously known database. The blockchain technology is therefore considered by many [3], including us, to be the ideal tool, to be used to create the new modern democratic voting process.

II LITERATURE SURVEY

1. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System A purely peer-to-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 doublespending. We propose a solution to the double-spending problem using a peertopeer 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, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages 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 agreement 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 supportSmart 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 fundamentally 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 environmentto 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 IoT-based machine-to-machine network without consuming high system resources and breaching the privacy of participants.

III SYSTEM DESIGN

The block-chain technology used mostly works the same as the blockchain technology contained in the E-voting system and focuses on database recording. The nodes involved in Blockchain that have been used by Bitcoin are independently random and not counted. However, in this e-voting system a blockchain permission is used, for nodes to be made the opposite of the Bitcoin system and the Node in question is a place of general election because the place of elections must be registered before the commencement of implementation, it must be clear the amount and the identity.

This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process. This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes.

When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once valid, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node

gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in block-chain creation to avoid collision and ensure that all nodes into blockchain. The submitted block contains the id node, the next id node as used as the token, time stamp, voting result, hash of the previous node, and the digital signature of the node.

III SYSTEM ARCHITECTURE

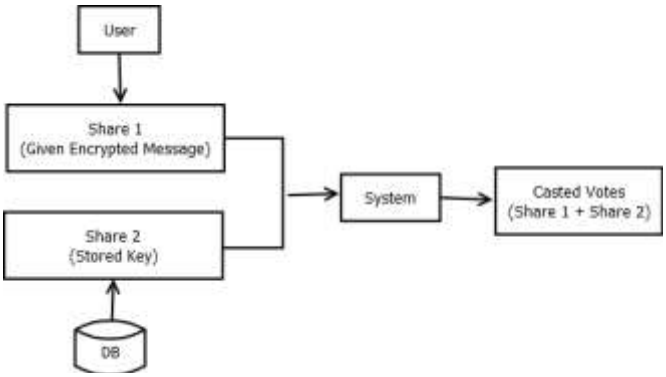

Figure 1: Architecture diagram

IV RESULTS

Figure 2: Home Page

Figure 3: Result Page

CONCLUSION

A nation with less voting percentage will struggle to develop as choosing a right leader for the nation is very essential. Our proposed system designed to provide a secure data and a trustworthy E-voting amongst the people of the democracy. 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.

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.
2. RifaHanifatunnisa, Budi Rahardjo, Blockchain Based E-Voting Recording System Design,IEEE 2017.
3. Kejiao Li, HuiLi,HanxuHou, KedanLi,Yongle Chen, Proof of Vote: A High- Performance 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.
4. Ali KaanKo, EmreYavuz, Umut Can abuk, GkhanDalkilic, Towards Secure E-Voting Using Ethereum Blockchain,2018 IEEE.
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.
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.
7. KashifMehboob Khan, Junaid Arshad, Muhammad Mubashir Khan, Secure Digital Voting System based on BlockchainTechnology,IEEE 2017.
8. Huaiqing Wang, Kun Chen and DongmingXu. 2016. A maturity model for blockchain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186 / s40854-016-0031-z
9. Buterin, Vitalik. 2015, On Public and Private Blockchains. [Online]https:// blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/
10. Zyskindet. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Securityand Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online].Available: http: //dx.doi.org /10.1109/ SPW.

2015 Jian liang Meng, JunweiZhang, Haoquan Zhao, Overview of the SpeechRecognition Technology, 2012 Fourth International Conference on Computational and Information Sciences.

11. Gallup, ”Trust in Government,” Gallup, 30 September 2015. [Online]. Available: http: //www.gallup.com /poll /5392/trust-government.aspx. [Accessed 28 Septmeber 2016.

12. Wikipedia, ”List of controversial elections,” 20 September 2016. [Online]. Available: https: //en.wikipedia.org /wiki /List-of-controversial-elections. [Accessed 27 September 2016].

13. R. Skudnov, ”Bitcoin Clients,” Turku University of Applied Sciences, Turku, 2012.

14. Affectiva, ”Affective Product Overview,” 15 January 2016. [Online]. Available: http: //www.affectiva.com / wp-content / uploads/2014/11/Affectiva ProductOverview. pdf. [Accessed 28 September 2016.

15. P. Noizat, ”Blockchain Electronic Vote,” in handbook of digital Currency, Paris, Elsevier Inc., 2015, pp. 453-461.

16. The electoral knowledge network, ”Cost of Registration and Elections,” ACE Project, 15 Jan 2016.

17. N. Uribe, ”10 Benefits of Electronic Voting,” 01 August 2016. [Online]. Available: http:// www.fobsoftware.com/ blog/ 10-benefits-of-electronic- votingfor- home- owner associations. [Accessed 28 September 2016].

18. G. Schryen, ”Security Aspects of Internet Voting,” in IEEE, Hawaii, 2004.

19. Wikipedia, ”List of countries by number of Internet users,” 23 September 2016. [Online]. Available: https:// en.wikipedia.org /wiki/. [Accessed 29 September 2016.