E-Voting With Blockchain Technology

Md Raufur Rahman
Department of Computer Science & Engineering
Galgotias University
Greater Noida, India
shaanunplugged1234@gmail.com

Aanjey Mani Tripathi
Department of Computer Science & Engineering
Galgotias University
Greater Noida, India
Aanjey.tripathi@galgotiasuniversity.edu.in

***Abstract*—Creating an E-Voting system which satisfies every legal requirement of lawmaker or Election Commission has been a challenge for a long time especially in a country like India. The E-Voting were 1st used in 1982 in kerela(India). Since then many questions have been raised against EVM. In every Election, losing party accuses the winning party of hacking the EVM. But the Blockchain Technology offers infinite range of security and assurance that each and every vote given by you is going to right place and to the right person. This paper aims to evaluate every aspect of blockchain based E-Voting and how blockchain based E-voting is different from traditional E-Voting system. Also we elucidate the requirement for the Blockchain based E-Voting system. This paper describes the need of making E- Voting system and identifies the legal and technical limitations of using blockchain. This is a simple and user- friendly web app developed for Indian voting system which is very bigger. Blockchain technology provides scalability and confidentiality and it is more secure than the other traditional voting system. The hash code generated by the user is unique and can be use only one time in one election. User cannot give the vote second time. Blockchain Technology uses peer to peer technology that's why it is highly secure.**

Keywords—E-voting using blockchain, blockchain, blockchain based e-voting system, Decentralized e-voting system,

I. INTRODUCTION

From the past several years, the vote has become the most important way to express the power of citizens by electing their best candidate. In every democratic country, the security of the election is the issue of national security. The Computer Engineers and the Software Engineers studied all the possibilities of the E-Voting system, with the aim of minimum cost of having a national election, highly secure and trustworthy. In the beginning, the vote was cast through the Ballot paper. Replacing the traditional way of voting in 1982 India introduces electronic voting system to the nation. In this you don't need any pen or paper. You just have to press the button beside your candidate and the vote will cast. In this voting system the votes are recorded by government organization like election commission of India. But in this technology there is high chance that it could be hacked or someone trick with its functionality and then you cast the vote to anyone but it goes to only one but no one can see. Apart from this the blockchain technology is that technology which cannot be hacked or edit. Each and every vote cast by voter become a block. And every block connected with previous block which is unbreakable. If someone tried to trick with it, it burn and destroy. The algorithm used in the blockchain based E-Voting is SHA-256. It is a mining algorithm of bitcoin protocol. The hash code is generated using hash algorithm by the user which can be only use once.

II. HOW BLOCKCHAIN TRANSFORM THE E-VOTING SYSTEM

Blockchain is the distributed and decentralized public ledger which is records all the transactions. Save every transaction and generate the proof of the vote. It shows the previous hash from the vote is connected. It is a decentralized technology which means the data are stored in multiple nodes and it is not possible for anyone to hack all the nodes and change or edit the data. In the blockchain based E-voting you have to enter some details for register yourself like your voter card, date of birth. Every data is stored in the database. It is a decentralized scheme and it can record votes from voters across various mobiles and computers. the algorithm which is used in it is Rivest Shamir Adleman (RSA) algorithm which is more secure than the other algorithm exist across the network. Each block is connected to previous block which is impossible to change or tampered. If someone wanted to hack or change the hash block they must have to hack more than fifty percent computer network which is clearly impossible.

Blockchain technology stopped the illegal voting, fraudness, fixed shortcoming. In every Election, losing party accuses the winning party of hacking the EVM. But the Blockchain Technology offers infinite range of security and assurance that each and every vote given by you is going to right place *and to the right person.*

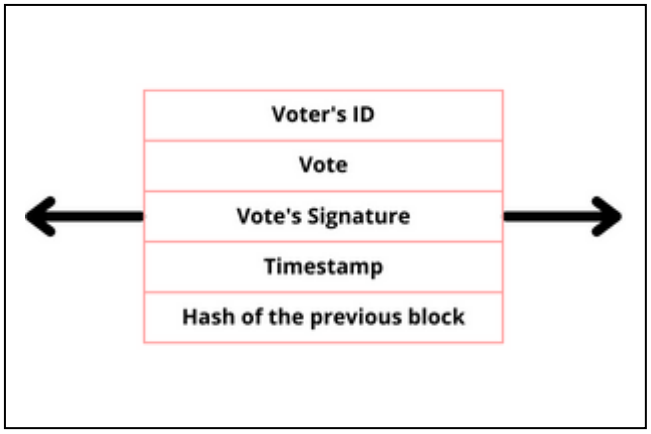

Fig 1. E-voting using blockchain structure

III. Challenges For Blockchain Based Voting System

A. Security
B. Authentication of voter
C. User accessibility
D. Anonymity of the voter

A. Security

A virtual electronic voting may have lots of weak spot. Cyber security risk may come from the system itself. In 2017 researchers found a flow in a cryptography mechanism used to secure the ENID card that may compromised the personal data of more than 7 lacks people. But the blockchain technology is decentralized and fully secure and this is used in voting mainly cause by their end to end verification

B. Authentication Of The Voter

Authentication of the voter is the important part of any type of voting system. A voting system must ensures that the voter is eligible for vote, and hasn't voted already, their information is correct. Without authentication a system cannot prevent multiple voting. In blockchain voting system the authentication process is done by digital identity verification mechanism. Currently it can be authenticate by valid id proof, unique hash code, mobile number and biometrics.

C. User Accessibility

Electronic voting system is the right answer to the problem physical accessibility. Online voting system can increase the participation rate, it is convenient for people to vote from home. But at the same time stable network is required for the online voting system which is not possible for rural area. And the face recognition has the higher error rate among all the authentication process.

D. Anonymity Of The Voter

Voter anonymity is the important aspect of any type of vote either it is small level voting and bigger lever voting. But blockchain technology provides fully anonymity for the voter. And it is end to end encrypted technology.

IV. Background And Related Works

The system implementation is divided into four parts- Client side application, database, server API & authentication API. Client side apps is defined is user interface. It is clearly webbed based through which the user can communicate to the system. It is the simple system which is designed to be user friendly and easy to use to the user. Firstly the user has to create an account. then the user is registered in the system. When the account is successfully created all the data go to the backend by the help of the API. After that the user can login in the blockchain app. When the verification of the user is successfully done after that the unique hash code for the user is generated for the user. User can copy the code. And save the code for future vote. User can only cast one vote with hash code. In every election user get unique and one time use hash code. User can see the privacy policy and user agreement in the next section. When the above work is done then the user interfaced with voting and mining section. After clicking the vote user redirect the page which is hash code id page. User must submit the hash code in the form area, after that the page redirect to the voting page, where the user can see the candidate list and user can cast the vote . and the vote is submitted. After submitting the vote user can see the proof of vote. User can go to the home page and can see the mining button. After clicking on the mining button voter can see the previous block a proof of the work and whom they cast the vote.

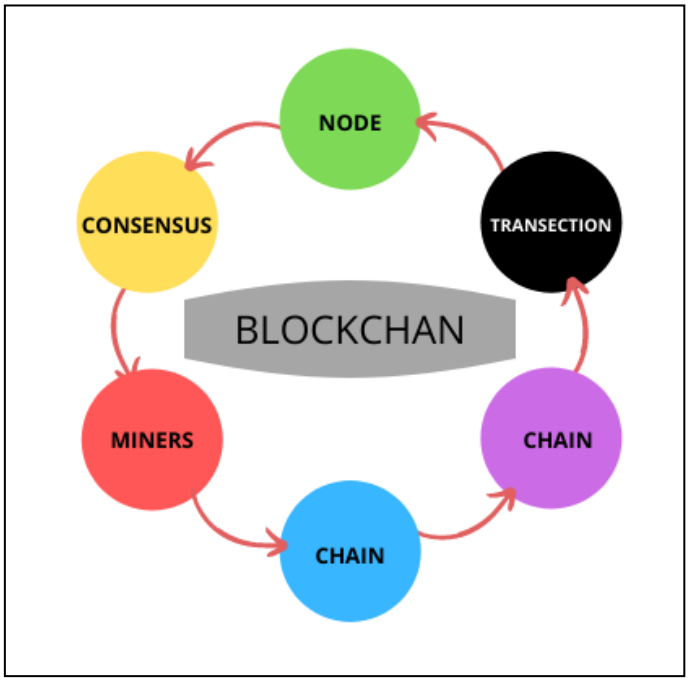

Fig 2. Core components of blockchain

V. CONCLUSION

The aim of this paper is to find error in current research of decentralized voting system. In this research paper we have discussed about traditional voting system and the blockchain based electronic voting system. We have discussed fundamental of the electronic voting system which is blockchain based and the advantaged of fundamental of blockchain based voting system. And later we compared the traditional and blockchain based voting system. This research is all about the discussion of the blockchain voting technology achieve the significant security for the electronic voting system.

VI. FUTURE WORK

Many issues in the traditional electronic voting can be solved by using decentralized technique, so that this technology will become cost effective easy to use, easy to understand, pleasant and safer than other technology We will improve the security of the project. We are working on the user interface through which the system will be more easier to understand. In future we will continue upgrade and improve our service.

ACKNOWLEDGEMENT

This paper and the research behind it would not have been possible without the exceptional support of my Mentor, Aanjey Mani Tripathi. His enthusiasm, knowledge and exacting attention to detail have been an inspiration

REFERENCES

[1] Agora Technologies (2018). Agora bringing our voting systems into the 21st century. https://www.aeora.vote/s/ Agora Whitepaper.pdf. Accessed: 2018-07-25.

[2] coalichain.io (2018). Coalichain - people directdemocracy.https://www,coalichain. io/images/pdf/coalichain ,pdf. Accessed: 2018-07-25.

[3] Dorri, A., Kanhere, S. S,, Jurdak, R., and Gauravaram, P. (2017). Blockchain for iot security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 International Conference on, pages 618 623. OEE.

[4] Kappos, G., Yousaf, H., Maller, M., and Meiklejohn, S.(2018). An empirical analysis of anonymity in zcash. arXiv preprint arXiv:1805.03180.

[5] Khan, K. M., Arshad, J,, and Khan, M.M, (2018). Secure digital voting system

[6] based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1):53 62.

[7] Lenarduzzi, V., Lunesu, I., Marchesi, M., and Tonelli, R. (2018). Blockchain applications for agile methodologies. In 19th International Conference on Agile Processes in Software Engineering and Extreme Programming. XP, volume 2018,

[8] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[9] Neff, C. A. (2001). A verifiable secret shufñ e and its application to e-voting. In Proceedings of the 8th ACM conference on Computer and Communicatio ns Security,pages 125. ACM.

[10] Pinna, A., Tonelli, R., Orru, M., and Marchesi, M. (2018). A petri nets model for blockchain analysis. Computer Journal, pages 1 15.

[11] Rubtcova, M. and Pavenkov, O. (2018). Using of blockchain in electronic election in russia.

[12] Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In 2014 IEEE Symposium on Security and Privacy (SP), pages 459 474. OEE.

[13] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11):612 613.

[14] Spanos, N., Martin, A, R., and Dixon, E, T. (2017). System and method for securely receiving and counting votes in an election, US Patent App. 15/676,