Securing E-Voting System using Blockchain

Komal K. Sharma, Prof. Mrunalinee Patole,

M.E. Student, Department of Computer Engineering, RMDSSOE, Pune, Maharashtra, India

Department of Computer Engineering, RMDSSOE, Pune, Maharashtra, India

ABSTRACT: Crypto currency, and its underlying technologies, has been gaining popularity for transaction management beyond financial transactions. Transaction information is preserve in the block chain, which can be used to investigating the purity of the transaction. The target of this paper is the possible availability of block-chain technology of other transactional uses. Block-chain is one of the most steady open register that preserves transaction information, and is difficult to forge. Since the information stored in block-chain is not associated to personally identifiable information, it has the aspect of anonymity. The block-chain allows for transparent transaction verification since all information in the block-chain is accessible to the public. These component are the same as the requirements for a voting system. That is, strong robustness, anonymity, and transparency. Here, we propose an electronic voting system as an application of block chain, and express block-chain based voting at a national level through examples.

KEYWORDS: Blockchain, Multichain, E–voting, Crypto currency.

I. INTRODUCTION

Blockchain technology that shines sort of a star once the doorway and widespread acceptance of Bitcoin [2], the terribly 1st cryptocurrency in peoples' lifestyle, has become a trending topic in today's package world. At the start, Blockchain was solely used for financial transactions and trade, however studies have began to recommend that it will be employed in more areas over time, as a result of there's a high degree of transparency during this system. for instance, in Bitcoin, since the wallets area unit in an exceedingly distributed structure, the whole quantity of coins and instant group action volume within the world will be followed momentarily and clearly. there's no would like for a central authority to approve or complete the operations on this P2P-based system.

As a result of that, not solely the money transfers however additionally all types of structural info will be unbroken during this distributed chain, and with the assistance of some cryptographic ways, the system will be maintained firmly. Like people's assets, wedding certificates, checking account books, medical info, etc., tons of data will be recorded with this method with relevant modifications [3]. Ethereum coin (Ether), another cryptocurrency with utile development environments, that emerged a number of years once Bitcoin, distinguishes the blockchain in an exceedingly real sense, revealing that this technology will manufacture package which will hold info that's structured as delineate higher than.

The package programs enforced by sensible contracts [4] (explained later) area unit written into the blockchain and area unit changeless.they can't be (illegally) removed nor manipulated once written. Hence, they will work properly, autonomously and transparently forever, with none external stimuli [5]. As already mentioned, with its distinctive distributed and secure idea, the blockchain technology could address several problems apart from digital trade. It would be fullly appropriate answer for e-voting comes.

E-voting is beingstudied extensively, and lots of implementations area unit tested and even used for a minute. However, only a few implementations area unit reliable enough and area unit still in use. Of course, there area unit several productive samples of on-line polls and questionnaires, nevertheless we tend to cannot claim an equivalent for on-line elections for governments and businesses. That's principally as a result of official elections area unit essential parts of the democracy and democratic administrations, that area unit the foremost most popular body methodology within the times. More, what's most valued in democratic societies may be a sturdy electoral method that has transparency and privacy. Today, tons of selections area unit being created by individuals (and members in organizations).means that of such choice systems area unit employed in tons of fields starting from the law and act referendums to the TV shows.

II. LITERATURE SURVEY

 [1] Ali KaanKoc, EmreYavuz,Umut Can Cabuk,GokhanDalkoloc, building smart contract of ours, we have succeeded in moving e-voting to the blockchain platform and we addressed some of the fundamental issues that traditional e-voting systems have, by using the potential of the Ethereum network and the blockchain structure. As a result of trials, the concept of blockchain and the security methodology which it uses, namely immovable hash chains, has become adaptable to polls and elections.

[6] E. Maaten supply a secure selection atmosphere and show that a reliable e-voting theme is feasible victimization blockchain. Because, once e-voting is obtainable for everybody UN agency contains a laptop, or a transportable, each single body call may be created by individuals and members; or a minimum of people's opinion are going to be a lot of public and a lot of accessible by politicians and managers. this may eventually lead humanity to actuality direct democracy.

[7] U.C. Çabuk, A. Çavdar, and E. Demirshows that It's necessary for US since elections will simply be corrupted or manipulated particularly in little cities, and even in larger cities placed in corrupt countries. Plus, large-scale ancient elections square measure terribly costly within the long run, particularly if there square measure many geographically distributed vote centers and countless voters. Also, the voters (mainly for members of organizations) can be on vacation, on a business trip or isolated for the other reason, which is able to create not possible for that specific citizen to attend the election and should lower the group action. E-voting are going to be in a position solve these issues, if enforced rigorously

[8]The idea of e-voting is considerably older than blockchain. So that, all celebrated examples to this point used suggests that of centralized computation and storage models. Esthonia may be a excellent example, since the govt of Esthonia is one in every of the primary to implement a totally on-line and comprehensive evoting resolution.

[9]The idea of e-voting was began to be debated within the country in 2001 and formally started by thenational authorities within the summer of 2003.

[10]Their system remains in use, with several enhancements and modifications on the first theme. As reported , it's presently terribly sturdy and reliable. They use sensible digital ID cards and private card readers (distributed by the government) for person-wise authentication.

[11]Switzerland is another one in all the few countries taking part within the electronic option trend. In Switzerland, celebrated for its widespread democracy, each national United Nations agency completes the age of eighteen will take an energetic or passive role within the elections, which can be command in totally different topics for several different choices. they need conjointly begun a politician work on a legal system known as remote option.

III. PROPOSED WORK

In our study, Multichain environment is preferred as the development platform and the blockchain network. That is because, while Bitcoin is only intended to validate coinage transactions, Multichain platform provides a broader range of use cases, with the power of permission based access. All bock of multichain are hashed and stored, so manipulation is not possible on multichain transaction details. Multichain implement user-based networks to conduct as many as 1,000 financial transactions per second. Corporations are now turning to multichain advantage to various tools that were originally organise for use with bitcoin. In your business may have heard the whisper word "multichain" but may not yet understand how it can leading business. Multichain is associated with Blockchain technology. Multichain is a new software development that allows you to arrange your own Blockchain approach. Designed for use on the bitcoin blockchain, Multichain has become necessary software resource for legal contract and web-based assets.
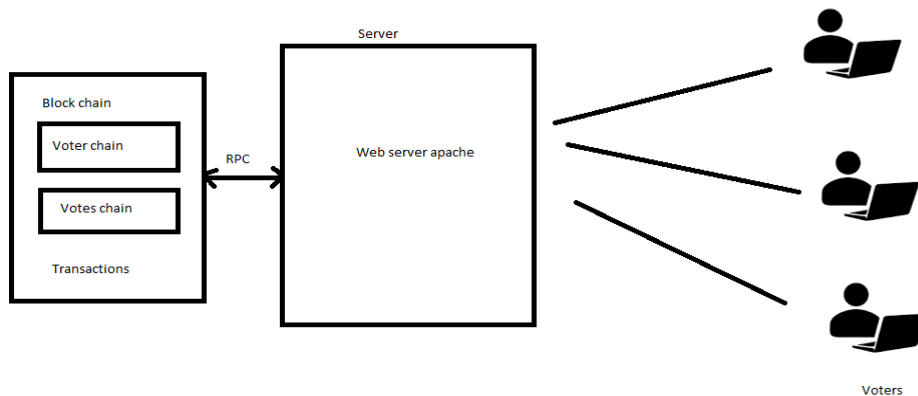
IV. SYSTEM ARCHITECTURE

Fig 1: System Architecture

Fig 1 shows the proposed system architecture. We use multicain stream to store for storing voters information and votes given by the voters.Multichain asset are used for voting i.e for transaction.Webserver is just used for GUI of users and administrators for easy interface or access.Multichain RPC-API are used for communication between webserver and multichain platform.

Working of proposed system is as follows

- Candidates list will displayed on web panel
- Each voter is has an unique ID number
- The voter goes to a valve and receive a token, using the ID number. Each ID number is only grant to earn one token
- The voter can vote online by dispatching the token to the account of the candidate they select. That voter cannot vote again, but the voter can examine the block chain to verify that the vote was correctly recorded, and also see the total votes for each candidate at any time.
- Live result will displayed at admin panel
- Each vote is verified by the server, if valid then it digitally signed by the server for valid transaction
- Invalid truncation where drops after verification

V. MODULE

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. In this paper, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost efficient election while guaranteeing voters privacy. Modules of proposed system is as follows:

- Blockchain creation
- Stream Creation
- Asset Creation
- Candidate Account Setup
- Voting
- Vote Counting
- Display Result

VI. CONCLUSION

By building this proposed permission based multichain platform, we have succeeded in moving e-voting to the blockchain platform and we addressed some of the fundamental issues that legacy e-voting systems have, by using the power of the multichainplatform and the blockchain structure. As a result of our preliminary, the concept of blockchain and the security methodology which it uses, namely immutable hash chains, has become flexible to polls and elections.

REFERENCES

[1] Ali KaanKoc, EmreYavuz,Umut Can Cabuk,GokhanDalkoloc "Towards Secure E-Voting Using EthereumBlockchain", 978-1-5386-3449-3/18/$31.00 ©2018 IEEE.
[2] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[3] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.
[4] C.D. Clack, V.A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape and research directions", Mar 2017, arXiv:1608.00771.
[5] E. Maaten, "Towards remote e-voting: Estonian case", Electronic Voting in Europe-Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004.
[6] U.C. Çabuk, A. Çavdar, and E. Demir, "E-Demokrasi: YeniNesilDo÷rudanDemokrasiveTürkiye'dekiUygulanabilirli÷i", [Online] Available: https://www.researchgate.net/profile/Umut_Cabuk/   publication/308796230_E-Democracy_The_Next_Generation_ Direct_Democracy_and_Applicability_in_Turkey/links/5818a6d408a   ee7cdc685b40b/E-Democracy-The-Next-Generation-DirectDemocracy-and-Applicability-in-Turkey.pdf.
[7] "Final report: study on eGovernment and the reduction of administrative burden (SMART 2012/0061)", 2014, [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/finalreport-study-egovernment-and-reduction-administrative-burdensmart-20120061.
[8] F. Hao and P.Y.A. Ryan, Real-World Electronic Voting: Design, Analysis and Deployment, CRC Press, pp. 143-170, 2017.
[9] N. Braun, S. F. Chancellery, and B. West. "E-Voting: Switzerland's projects and their legal framework–In a European context", Electronic Voting in Europe: Technology, Law, Politics and Society. GesellschaftfürInformatik, Bonn, pp.43-52, 2004.
[10] Estonian National Electoral Committee "E-voting System", 2010. [Online]. Available: https://www.valimised.ee/sites/default/files/ uploads/eng/General_Description_E-Voting_2010.pdf.
[11] P. McCorry, S.F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy", International Conference on Financial Cryptography and Data Security.Springer, Cham, pp. 357-375, 2017.
[12] Y. Takabatake, D. Kotani, and Y. Okabe, "An anonymous distributed electronic voting system using Zerocoin", IEICE Technical Report, pp. 127-131, 2016.
[13] U.C. Çabuk, T. ùenocak, E. Demir, and A. Çavdar, "A Proposal on initial remote user enrollment for IVR-based voice authentication systems", Int. J. of Advanced Research in Computer and Communication Engineering, vol 6, pp.118-123, July 2017.
[14] F. Hao, P.Y.A. Ryan and P. Zielinski, "Anonymous voting by tworound public discussion", IET Information Security, vol. 4, pp. 62-67, June 2010.