INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 2 - V7I2-1171)
Available online at: https://www.ijariit.com

Secured and robust E-voting system using blockchain technology

Arati Chaudhari
aratihp04@gmail.com
Pune Institute of Computer Technology, Pune, Maharashtra

Siddhi Uttarwar
siddhiuttarwar1310@gmail.com
Pune Institute of Computer Technology, Pune, Maharashtra

Saurabh Zanwar
saurabhzanwar88@gmail.com
Pune Institute of Computer Technology, Pune, Maharashtra

Prabhav Jakhete
jakheteprabhav@gmail.com
Pune Institute of Computer Technology, Pune, Maharashtra

ABSTRACT

Voting is the process of representation of democracy in a country. Voting systems have been around of hundreds of years and but they were evolving very slowly. Many solutions were proposed in the history, but most of them were rejected because of some security issues and limitations. Finally at the 21st century, e- voting systems started to bloom with the development of the web technologies with the development of the blockchain 2.0, the researchers started to go towards a new destination by applying blockchain to software engineering applications. E-voting systems were developed based on Ethereum as well as Z-cash and bitcoin. But they were not full e-voting frameworks. Due to the limitations of proposed solution, those were unable to exist with the modern world. To maintain user privacy, zk-SNARK which is a concept used in Z-cash for maintaining private transactions, can be used. To write Immutable codes, a conceptcalled smart contract can be used. Thus by using ethereum and z-cash blockchain technologies we can implement a full e- voting framework with voter registration, voter verification, voting, tallying and end to end verification.

Keywords: *E-Voting, Blockchain, Ethereum, Smart Contracts, Z-Cash, Zk-Snark*

1. INTRODUCTION

Election, the formal process of selecting a person for public office or of accepting or rejecting a political proposition by voting. Voting systems have been around of hundreds of years and but they were evolving very slowly. India still uses paper ballots based voting methodology for government elections. But current existing paper ballot based voting methodologies have lot of drawbacks. Some of them are Voter have to wait in a queue, Results are not trustworthy because of voting process is not visible to the public, Cost is very high because, have to pay for all the officers who work at polling locations as well as counting locations, Voter participation is less, Takes some time to release the results, results depend on the physical security, have to trust the officers in the polling locations as well as tallying locations, people who live in abroad are not able to cast their vote etc.

Blockchain is a distributed decentralized public ledger which can be used to store e-voting transactions securely. So it can be used as a substitution to a database approach. Transactions that are stored in a blockchain is publicly visible. But in e-voting scenarios all the voting transactions should be anonymous. That means “To whom the voter voted should be publicly visible” but the details of the person who voted should not be publicly visible.

There are some blockchains that support for anonymous transactions. But there are other disadvantages as well in those blockchains. In this paper the solution is based on Ethereum blockchain which is not supported for anonymous transactions. The reason for using that kind of blockchain was based on literature review. The concept called zero knowledge proof (ZKSnarks) was used to allow for the authentication of transactions without giving any personal information to the contract.

2. LITERATURE SURVEY

Ali Kaan Koç, Emre Yavuz,[1] focuses on the use of etherium blockchain technology due to its own advantages. It is implementation and test a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language.

Asraful Alam1, S. M. Zia Ur Rashid2 and Md. Abdus Salam3, Ariful Islam4,[2] proposes about Electric voting (E-voting) model that ensures security, privacy and transparency. An internet of things (IOT) based system is designed to exchange data from e-voting devices to the nodes.

Malik Hamza Murtaza , Zahoor Ahmed Alizai, Zubair Iqbal,[3] focuses on a relatively new type of zero knowledgeproof known as zkSNARKs has been used to provide vote unlinkability. The scheme uses digital signatures to provide message authentication, cryptographic hashes to create hash chains and zero knowledge proofs (zkSNARKs) to attain unlink ability.

Harsh Jain, Rajvardhan Oak, Jay Bansal,[4] proposes a novel model in which the blockchain is exploited to developa secure, transparent and fully digital voting system. It uses a permissioned blockchain where the nodes of the blockchain are the voting centers. We have allocated a unique key pair to every individual, and votes are recorded in the blockchain.

Vijayalakshmi V, Vimal S,[5] proposes Blockchain technology and addresses most of the issues faced in the balloting scheme and is used to avoid proxy casting and recasting. They modified balloting system in which one can verify that no votes were changed or removed and no illegitimate votes were added. The proposed system is cost- efficient when compared to the traditional electronic voting machines. The system can be further enhanced by replacing OTP verification by fingerprint verification or face recognition in real time implementation.

S. Gao,[6] proposes about using a framework consisting of security model and system model of the process. The framework also discusses the code-based cryptographic algorithm. The concrete scheme of the protocol specifies about the phases of e-voting. In the private blockchain only the eligible nodes can see the details of the votes and transaction and the voting process does not remain visible tothe voters. This makes the voting process less transparent as compared to paper based voting.

Mrs. Harsha V. Patil, Mrs. Kanchan G. Rathi, Mrs. Malati V.Tribhuwan,[7] proposed about use of blockchain technology for the working of E-Voting system. It proposesa structure for the working of e-voting system consisting of 4 steps for an individual. Those 4 steps are requesting to vote, casting a vote encrypting votes and adding the votes to the blockchain. It addresses voter tampering, blockchains generate cryptographically secure voting records. Votes are recorded accurately, permanently, securely, and transparently.

Manoj Shrinivas1, Chandan S2, Mohammed Shamail Farhan3, Ramyashree,[8] proposed about use of blockchain technology like ethereum, smart contracts, adding candidates, etc. It proposes a structure for the implementation of the solution using decentralized methods. It enforces voting data immutability and data integrity ensuring robustness and reliability of the voting.

Emanuele Bellini1, Paolo Ceravolo2, Ernesto Damiani,[9] proposes the process of e-voting using a cloud based approach. The services are deployed on demand to optimize costs and service performance. The cloud providers such as IBM and Oracle are offering ready-to-use blockchain installation on cloud.

Rumeysa Bulut, Alperen Kantarcı, Safa Keskin, ŞerifBahtiyar, [10] proposes a solution using block chain to eliminate all disadvantages of conventional elections. It proposes the voting procedures according to the different protocols used in this procedure. The synchronization and algorithms can be discussed and improved for better performance and security.

Taban Habibu1, Konde Sharif, Sebwato Nicholas,[11]proposed use of blockchain technology to develop an E- Voting system in order to achieve an enhanced, speedy and accurate performance. It proposes a computer software developed using PHP programming language and MYSQL(a relational database management system). This application is design to satisfy the important properties such as receipt-freeness, verifiability, authentication, and integrity, efficient and easy-to-use graphical interface, saves money, time requirement.

Rifa Hanifatunnisa, Budi Rahardjo, [12] proposed blockchain technology as one of solutions, because it embraces a decentralized system and the entire database are owned by many users. Unlike Bitcoin with its Proof of Work, this survey proposes a method based on a predetermined turn on the system for each node in the built of blockchain. The hash values and digital signatures used in this paper makes the system more secure and reliable.

3. PROPOSE METHODOLOGY

Blockchain technology provided the base for the peer-to- peer digital currency and led to the bitcoin platform. But the applications of blockchain technology are far more than crypto-currencies, and it can provide an excellent solution for E-Voting System. So, let's understand the working of the blockchain network and how it can be used to implement a secure and robust E-Voting system.

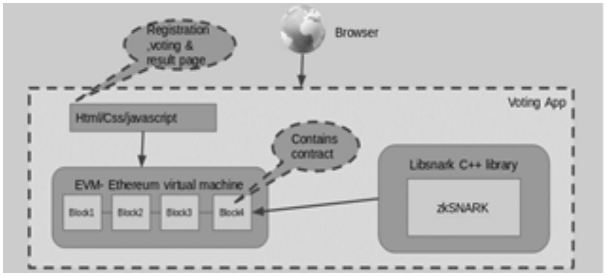

Fig. 1: High level architecture

Here, the connection to the blockchain from user interfaces are handled via web3.js (Ethereum JavaScript API). It's a collection of libraries which allows to interact with a local or remote ethereum node using HTTP or IPC connection. The solution consists of six contracts and those are running in ethereum virtual machine.

To communicate with the blockchain, it should contain with pre specified interfaces called as ABI definitions Libsnark c++ library is an implementation of zkSNARK. It is used to protect voter privacy in smart contracts. The proof is generated using an ethereum tool kit called as Zokrates. Html, css react js files are running as off-chain components.

The e voting system can be divided into 6 phases:

3.1 Registration phase

Users who hope to participate the election need to download the metamask browser extension. By downloading and creating account there, citizens will get an ethereum address (id). To register their id in e-voting voter.sol contract, the citizens sign-in to the e voting portal by creating temporary account with their ethereum address. The e voting web portal is requesting to register for the election with their ethereum address. The address which is used to sign the election registration transaction and address which is used to logged-in to portal should be same.

3.2 Registration verification phase

User Registration verification can be done using biometric verification technique such as aadhar no.(UID).

3.3 Election Preparation phase

In this phase an arithmetic circuit will be created using collected hash values of the verified voters with the help of Zokrates ethereum tool kit. Then system will generate the verification and proving key which is used to prove and verify zero knowledge proof.

3.4 Voting phase

After login to the web portal via valid ethereum address exist in the metamask, registered voters can cast their vote. The design of voting phase facilitates to protect the privacy of voters by hiding the voter details and identity. The zero knowledge proof helps to do that.

3.5 Tallying phase

The Tallying will be done automatically. When voters cast their votes, results will not be displayed to them until the election ends. After the election ended up, the calculated votes for each candidate will be displayed.

3.6 Verification phase

In this phase users will be able to check whether the casted votes are casted as intended by verifying. To verify their votes they need to have transaction hash which they got at the voting phase. The verification process will check whether user's transaction is included in a block or not.

4. CONCLUSION

There exists no proper e-voting system. Thus, we are proposing a blockchain based E-Voting system that can create a decentralized app to effectively verify, secure and manage various elections. There were solutions based on zcash blockchain and ethereum blockchain. The main strength of ethereum was the smart contracts. But the problem in ethereum is, it doesn't provide private transactions. Then, moved towards zcash like coins which provide private transactions and enables to hide transaction details from the public but the problem in zcash is it doesn't provide smart contract like concepts to write custom logic. Thus our solution was integrate zk-SNARK and smart contract together and apply that in to e-voting problem.

5. REFERENCES

[1] Trustworthy Electronic Voting Using Adjusted Blockchain Technology BASIT SHAHZAD 1 AND JON CROWCROFT 2 1Department of Engineering, National University of Modern Languages, Islamabad 44000, Pakistan 2Computer Laboratory, University of Cambridge, Cambridge CB30FD, U.K

[2] An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function SHIYAO GAO , DONG ZHENG , RUI GUO , CHUNMING JING , AND CHENCHENG HU National Engineering Laboratory for Wireless Security, School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

[3] Towards secure e-voting using ethereum blockchain," *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya.

[4] "Towards Developing a Secure and Robust Solution for E-Voting using Blockchain," *2019 International Conference on Nascent Technologies in Engineering (ICNTE)*, Navi Mumbai, India.

[5] A Study on Decentralized E-Voting System Using Blockchain Technology Mrs. Harsha V. Patil1, Mrs. Kanchan G. Rathi2, Mrs. Malati V.Tribhuwan3 1,2,3 Assistant Professor, Dept. of Computer Science, Dr. D Y. Patil ACS College, Pimpri , Pune-18, Maharashtra, India.

[6] 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

