www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Leveraging Blockchain for Transparent and Secure E-Voting

Mr.Valle Shyam Kumar[1]., B.Rajeshwari[2]
1 Assistant Professor, Department of CSE, Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India
2, B.Tech CSE (20RG1A0508),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

ABSTRACT

Some forms of voting have been here ever since. Mostly used form all over the world are paper ballots. Electronic voting schemes are being popular only in the last decade and they are still unsolved. E-voting schemes bring problems mainly regarding security, credibility, transparency, reliability, and functionality. Estonia is the pioneer in this field and may be considered the state of the art. But there are only a few solutions using blockchain. Blockchain can deliver an answer to all of the mentioned problems and furthermore bring some advantages such as immutability and decentralization. The main problems of technologies utilizing blockchain for e-voting are their focus on only one field or lack of testing and comparison. In this paper, we present a blockchain-based e-voting platform, which can be used for any kind of voting. It is fully utilized by blockchain and all processes can be handled within it. After the start of the voting, the platform behaves as fully independent and decentralized without possibilities to affect the voting process. The data are fully transparent, but the identity of voters is secured by homomorphic encryption. We have tested and compared our solution in three different blockchains. The results show, that both public and private blockchains can be used with only a little difference in the speed. The key novelty of our solution is a fully decentralized management of e-voting platform through blockchain, transparency of the whole process and at the same time security and privacy of the voters thanks to homomorphic encryption.

I. INTRODUCTION

The topic of e-voting systems is still at an early stage of development. We have chosen this domain not only for its recency but also because there are not many solutions that address problems of e-voting. Nowadays, popularity grows also in the development of e-

Government. However, such a system is not feasible if basic services for citizens such as elections do not become electronic. "E-voting is one of the key public sectors that can be transformed by blockchain technology" [1]. Hand by hand with e-voting come also new challenges, which need to be addressed. One of them is e.g. securing the elections, which needs to be at least as safe as the classic voting systems with ballots. That is why we have decided to create safe elections in which voters do not have to worry about someone abusing the electoral system. In recent years blockchain is often mentioned as an example of secure technology used in an online environment. Our evoting system uses blockchain to manage all election processes. Its main advantage is that there is no need for confidence in the centralized authority that created the elections. This authority cannot affect the election results in our system. Another challenge in e-voting is the lack of transparency in the functioning of the system, leading to a lack of confidence in voters [2]. This problem is solved by blockchain in a way of total transparency that allows everyone to see the stored data and processes such as how are these data handled. In the field of security, this technology is more suitable in every way than the classic e-voting platform without blockchain.

II. LITERATURE SURVEY

1.Blockchain-enabled e-voting,N. Kshetri and J. Voas,Blockchain-enabled e-voting (BEV) could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV uses an encrypted key and tamper-proof personal IDs. This article highlights some BEV implementations and the approach's potential benefits and challenges.

2.Voting Processwith Blockchain Technology: Auditable Blockchain Voting System,M. Pawlak, J. Guziur, and A. Poniszewska-Mara nda,There are various methods and approaches to electronic voting all around the world. Each is connected with different benefits and issues. One of the most important and prevalent problems is lack of auditing capabilities and system verification methods. Blockchain technology, which recently gained a lot of attention, can provide a solution to this issue. This paper presents Auditable Blockchain Voting System (ABVS), which describes e-voting processes and components of a supervised internet voting system that is audit and

verification capable. ABVS achieves this through utilization of blockchain technology and voter-verified paper audit trail.

3. A Smart Contract forBoardroom Voting with Maximum Voter Privacy,P. McCorry, S. F. Shahandashti, and F. Hao,,We present the first implementation of a decentralised and self-tallying internet voting protocol with maximum voter privacy using the Blockchain. The Open Vote Network is suitable for boardroom elections and is written as a smart contract for Ethereum. Unlike previously proposed Blockchain e-voting protocols, this is the first implementation that does not rely on any trusted authority to compute the tally or to protect the voter's privacy. Instead, the Open Vote Network is a selftallying protocol, and each voter is in control of the privacy of their own vote such that it can only be breached by a full collusion involving all other voters. The execution of the protocol is enforced using the consensus mechanism that also secures the Ethereum blockchain. We tested the implementation on Ethereum's official test network to demonstrate its feasibility. Also, we provide a financial and computational breakdown of its execution cost.

4. Definitions and properties of zeroknowledgeproof systems, O. Goldreich and Y. Oren,In this paper we investigate some properties of zero-knowledge proofs, a notion introduced by Goldwasser, Micali, and Rackoff. We introduce and classify two definitions of zero-knowledge: auxiliary-input zero-knowledge and blackbox-simulation zero-knowledge. We explain why auxiliary-input zero-knowledge is a definition more suitable for cryptographic applications than the original [GMR1] definition. In particular, we show that any protocol solely composed of subprotocols which are auxiliary-input zero-knowledge is itself auxiliary-input zero-knowledge. We show that blackbox-simulation zero-knowledge implies auxiliary-input zero-knowledge (which in turn implies the [GMR1] definition). We argue that all known zero-knowledge proofs are in fact blackbox-simulation zero-knowledge (i.e., we proved zero-knowledge using blackbox-simulation of the verifier). As a result, all known zero-knowledge proof systems are shown to be auxiliary-input zero-knowledge and can be used for cryptographic applications such as those in [GMW2]. We demonstrate the triviality of certain classes of zero-knowledge proof systems,

in the sense that only languages in BPP have zero-knowledge proofs of these classes. In particular, we show that any language having a Las Vegas zero-knowledge proof system necessarily belongs to RP. We show that randomness of both the verifier and the prover, and nontriviality of the interaction are essential properties of (nontrivial) auxiliary-input zero-knowledge proofs.

III. EXISTING SYSTEM:

In recent years blockchain is often mentioned as an example of secure technology used in an online environment. Our e-voting system uses blockchain to manage all election processes. Its main advantage is that there is no need for confidence in the centralized authority that created the elections. This authority cannot affect the election results in our system. Another challenge in e-voting is the lack of transparency in the functioning of the system, leading to a lack of confidence in voters.

Disadvantages of existing system:

1.It is a manual procees.

IV.PROPOSED SYSTEM:

The proposed blockchain voting system considers all requirements for voting and is designed generally for any elections e.g. president, student parliament, etc. The system allows more round elections and preferably uses a public blockchain. The public blockchain can be replaced by other types of blockchain but the stored data (votes) have to be easily verified by any user. The user represents any observer who is interested in the blockchain voting. In our proposed system we identify three main roles: vote publisher; key authority; and voter. These three roles can represent an organization, a company, or a user. The roles vote publisher and key authority can be grouped to one role due to that they can be the same organization or person. The voter attends the elections depending on vote configuration. The configuration of the votes is performed by the vote publisher and is included in the smart contract. The vote publisher has to know all cipher keys before publishing the smart contract. The close collaboration between the vote publisher and the key authority is required. The key authority creates and distributes all cipher keys to a voter and vote publisher. The distributing channel has to be secured and should not be vulnerable to any 3rd party.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Advantages of proposed system:

1. We can vote through automatic process.it is easy to vote.

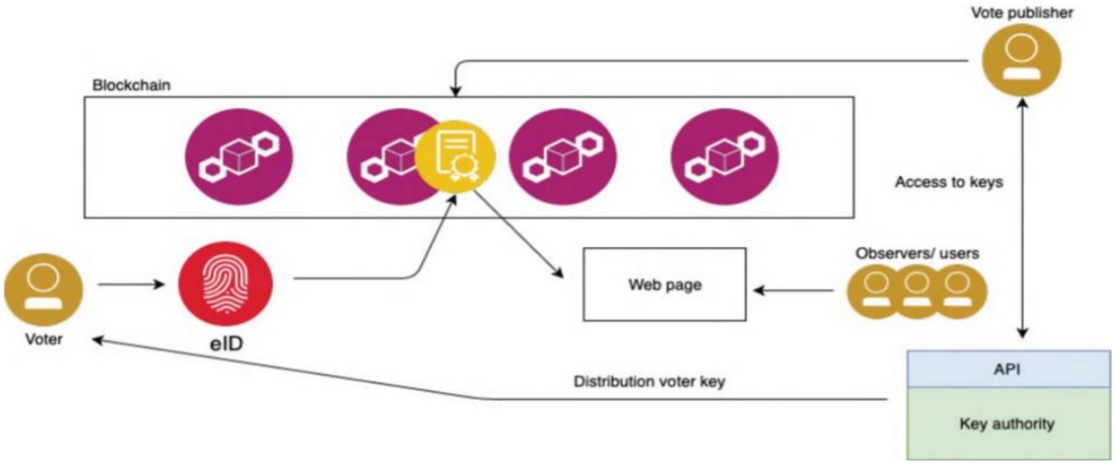


Fig. 1. High-Level architecture

V.IMPLEMENTATION

MODULES:

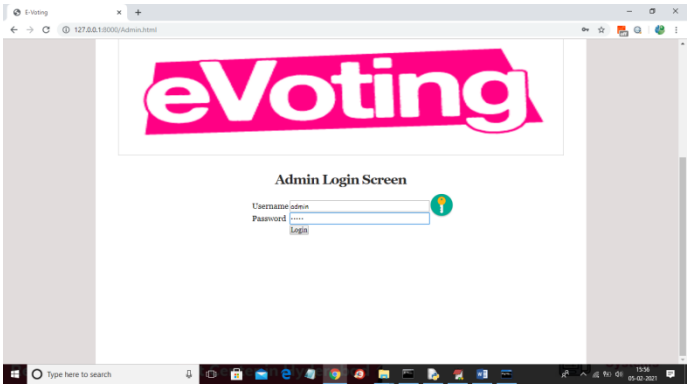
1. Admin
2. User

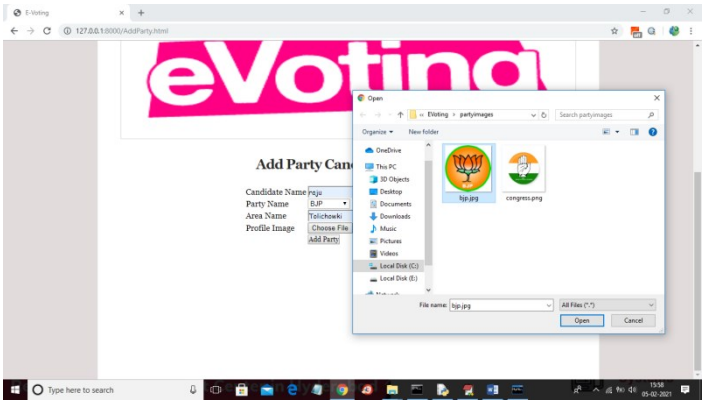
MODULES DESCRIPTION:

In this project we are using public python Blockchain API's to store and manage voting data as Blockchain provides secure and tamper proof of data storage and to implement this project we have designed following modules.

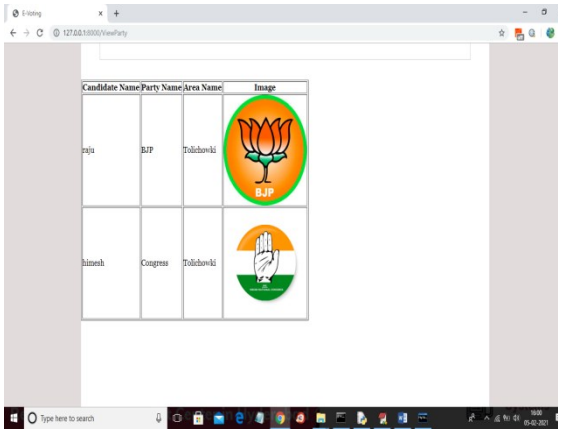
Admin module: this user responsible to add new party and candidate details and can view party details and vote count. Admin login to system by using username as 'admin' and password as 'admin'.

User Module: this user has to signup with the application by using username as his ID and then upload his face photo which capture from webcam. After registering user can go for login which validate user id and after successful login user can go for cast vote module which execute following functionality

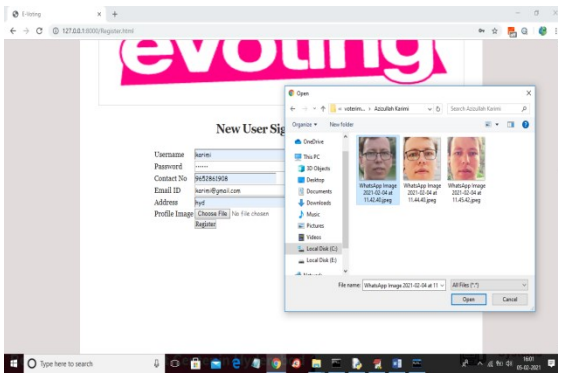




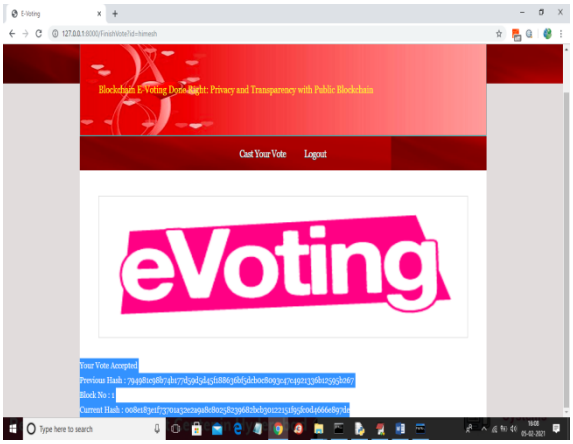
www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86



displaying add added party details and now click on 'Logout' link to logout as admin and then add new user



In above screen adding new user and then selecting his face photo taken from webcam and then click on 'Register' button to complete signup process. Here you have given images taken from phone but we need to capture from webcam for dataset as quality of webcam image and phone image vary and then problem comes in prediction.



the first vote so block will be added to Blockchain with block No as 1 and we can see Blockchain created a chain of blocks with previous and current hash code validation. Now try again with same user to cast vote

VI. CONCLUSION:

Although we can see slight differences in network times, they are so negligible that public blockchain has more advantages in such an electoral system due to its openness of data and that anyone can watch them in the real time. A private blockchain is a bit faster, but it reduces the credibility of the whole system by being partially centralized because it only runs where the authority wants it. The table shows that the average times to add one person's voice are: Ganache 6.32 s (median 6.34 s), Hyperledger Composer 6.05 s (median 6.04 s), and Ethereum Ropsten 17.75 s (median 17.93 s). These times are influenced by the used consensus algorithm and also by the block time.

VII. BIBLIOGRAPHY

[1] N. Kshetri and J. Voas, “Blockchain-Enabled E-Voting,”IEEE Software,vol. 35, pp. 95-99, jul 2018.

[2] M. Pawlak, J. Guziur, and A. Poniszewska-Mara nda, “Voting Processwith Blockchain Technology: Auditable Blockchain Voting System,” inLecture Notes on Data Engineering and Communications Technologies,pp. 233-244, Springer, Cham, 2019.

[3] B. Singhal, G. Dhameja, and P. S. Panda, “How Blockchain Works,” inBeginning Blockchain, pp. 31-148, Berkeley, CA: Apress, 2018.

[4] Agora, “Agora Whitepaper,” 2018.

[5] R. Perper, “ Sierra Leone is the first country to use blockchain duringan election - Business Insider,” 2018.

[6] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” tech.rep., 2008.

[7] G. Wood et al., “Ethereum: A secure decentralised generalised transaction ledger,”Ethereum project yellow paper, vol. 151, pp. 1-32, 2014.

[8] S. Landers, “Netvote: A Decentralized Voting Platform - Netvote ProjectMedium,” 2018.

[9] P. McCorry, S. F. Shahandashti, and F. Hao, “A Smart Contract forBoardroom Voting with Maximum Voter Privacy,” inLecture Notes inComputer Science, ch. FCDS, pp. 357-375, Springer, Cham, 2017.

[10] Z. Brakerski and V. Vaikuntanathan, “Efficient Fully Homomorphic Encryption from (Standard) LWE,” SIAM Journal on Computing, vol. 43,pp. 831-871, jan 2014.