JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Ethereum Voting System using Blockchain

Abhishek Choudhry, Deshdeep, Smrati Singh, Ms. Minakshi Chauhan
Department of INFORMATION TECHNOLOGY, KIET Group of Institution, Ghaziabad, India

ABSTRACT

Election is the essential tool to elect genuine leaders in democratic countries. To elect leaders with free will of the voters and great interests of voters in democratic countries, election must be transparent, authenticated, secure, and fair. Traditional paper-based voting system faces many challenges like highly expensive, time consuming, wastage of natural resources and various management issues. Therefore, it is not economical in terms of nature and finance. Along with mentioned major downsides of the traditional paper based voting system, voting system is required to possess certain properties: anonymity, authentication, verifiability and robustness. In this paper we proposed an ethereum voting system using blockchain which is easy to use, easily adaptable and less expensive.

Keywords:*Electronic voting, bitcoin, Ethereum, blockchain*

INTRODUCTION

Blockchain is a new type of data technology that combines cryptography with a distributed ledger. Pre-requisites of blockchain (such as Transaction verification and validity checking, Consistency maintenance, Security and Integrity of data, Hashing algorithm, Decentralized network, No double spending) makes blockchain technology more secure and applicable for the application such as electronic voting [1]. The blockchain pre-requisite, architecture, features, working, and different types of blockchains described in [2] In democratic countries, elections are the most important mechanism for electing leaders. In democratic countries, elections must be transparent, verified, secure, and fair in order to elect leaders who represent the voters' free will and major interests. Extensive research shows that installing electronic voting systems can improve security. When considering whether or not to use an electronic voting system, one must analyse why an electronic voting system is preferred over a traditional ballot voting paper. It not only enhances the effectiveness and efficiency of democracy, [3], but it is also expected to be a solution to several problems, such as enhancing election accessibility, allowing the elderly and disabled to vote, increasing election turnout, and being simple. However, it is common knowledge that operating e-voting systems under stringent security standards is critical, especially when modern encryption techniques are used. Determining which difficulties should be addressed in the design of a blockchain-based voting system is critical in this regard.

RELATED WORK

The electronic voting system was a significant improvement over the previous pen-and-paper method, and it quickly gained popularity and being implemented in several countries for their electoral processes. [4] Although it had some advantages, such as improved security, easy accessibility, time-efficient etc., it also faces several significant challenges in its implementation. The research in the field of secure blockchain based e-voting constantly growing. In this section, we discussed some of the works proposing e-voting protocols and systems. In their work, Diego F. Aranhaet al. [5] proposed an improved transparent e-voting system with improved voter participation and verifiable outcomes. The proposed system was based on the crowdsourced comparison of poll tape pictures with electronic results published by the electoral authority. The authors [6] proposed a secure decentralized blockchain based e-voting protocol which deals with vote-coercion and vote-selling issues and ensures transparency and full auditability of the process. The authors also addressed the general requirements of the electronic voting such as Correctness, Fairness, Transparency, verifiability, and privacy. The proposed system follows the two vote protocol where the voter can possess two voting tokens. [7] proposed permissioned blockchain based crypto e-voting system by using sidechain. In this work, the authors used two separate linked blockchains one for listing the voting procedures and second for counting the votes. The authors wanted to increase traceability and auditing mechanisms for voting operations without using a middleman. [8]

The authors addressed the security and fairness issues which desirable in any election process. The authors proposed an e-voting model with double layer encryption and denial of administrators to preview the results to prevent the manipulations in the results.

PROPOSED SYSTEM

In this work we, have proposed an online e-voting system using Ethereum based on blockchain technology. The architecture for the e-voting system has been shown in Figure 1. The voter can access the voting interface with the help of any device such as mobile phone, laptop or computer desktop. First Voter comes to the UI of Voting System and via mobile or laptop which is also called Voting interface and then after Voter complete his vote to the candidate there is a encryption s encryption before it is going to store in Blockchain to protect it from external threats.

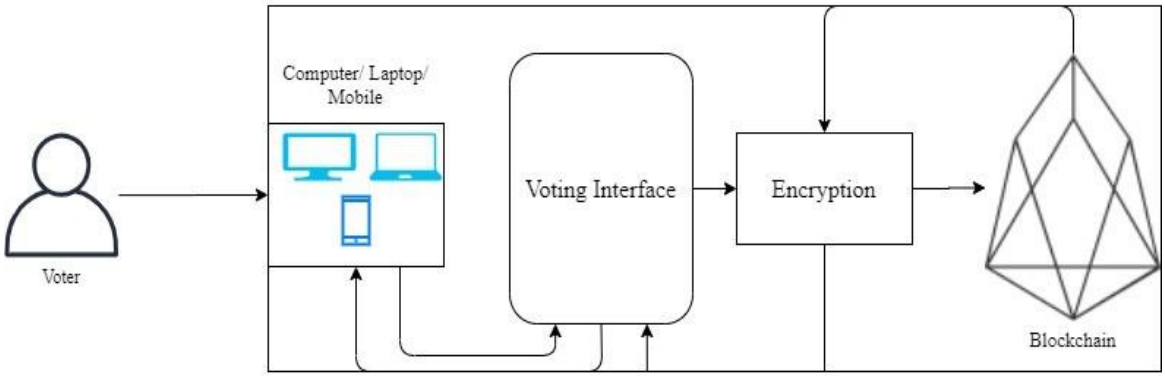


Figure 1: E-Voting Architecture using Blockchain Technology **[4]**

PRELIMINARIES

Our approach can be implemented after installing the following dependencies[4]

- Node Package Manager
- Truffle Suite
- Ganache
- Meta Mask

Metamask is a browser extension which is used to connect with Dapp. It provides UI and with the help of this we can easily connect with dapp without using command line.Solidityuses JavaScript syntax[9]. It's a way for converting EVM machinecode into basic instructions. It has the same operators as JavaScript [10], data types are Booleans, Integers, Unsigned Integers, Address,Enumsand String[9].

KEYS:

During the election process, the candidate's public and private keys are required for login and voting reasons. In this voting procedure, it serves as a login id and password. However, because it has such a high value, the voter may forget it. [10] This key is sent to the registered email or mobile number after a successful registration. It is also utilized for data encryption and decryption during the voting process. The voter uses keys to log into the system generation of both keys (public & private). The user selects his option to vote and casts his ballot for him. Every user follows similar procedure. The hash value of the preceding block connects each block to the next. Due to the decentralized nature of blockchain, it is created on every computer system in the network. As a result, data tampering and blockchain hacking are not conceivable. When the election process is completed, all votes are counted and the results are announced.

IMPLEMENTATION METHODOLOGY

Several tools are used to implement the proposed system [11]. Truffle is used to get smart contract on blockchain, where ganache provide blockchain running on system then we connect Ganache to metamask. A voter contain eth on his account or other coin which is used in the system to vote(to made changes in Blockchain) this amount is used to made changes in blockchain and pay gas fee. To finish the transaction, these miners compete with one another. Node who completed or verify the vote get the reward in the form of coin which is paid for by users that vote. We have used ganache software instead of node. First, Ganache is

launched to start the local blockchain. There will be no transaction after setting up ganache because we haven't done any yet. Further we have discussed the steps to be followed during the process of e-voting using Ethereum.

- Smoke Test
- List Candidates
- Cast Vote
- Watch Events (Vote Counted)

Step 1: Smoke Test

In this step start the ganache with Quick start Ethereum. It give us 10 account already loaded where every account contain 100 eth. Each account contains its unique private key and account address shown in Figure 2. Each address contains a unique user as a unique identifier for vote in election.

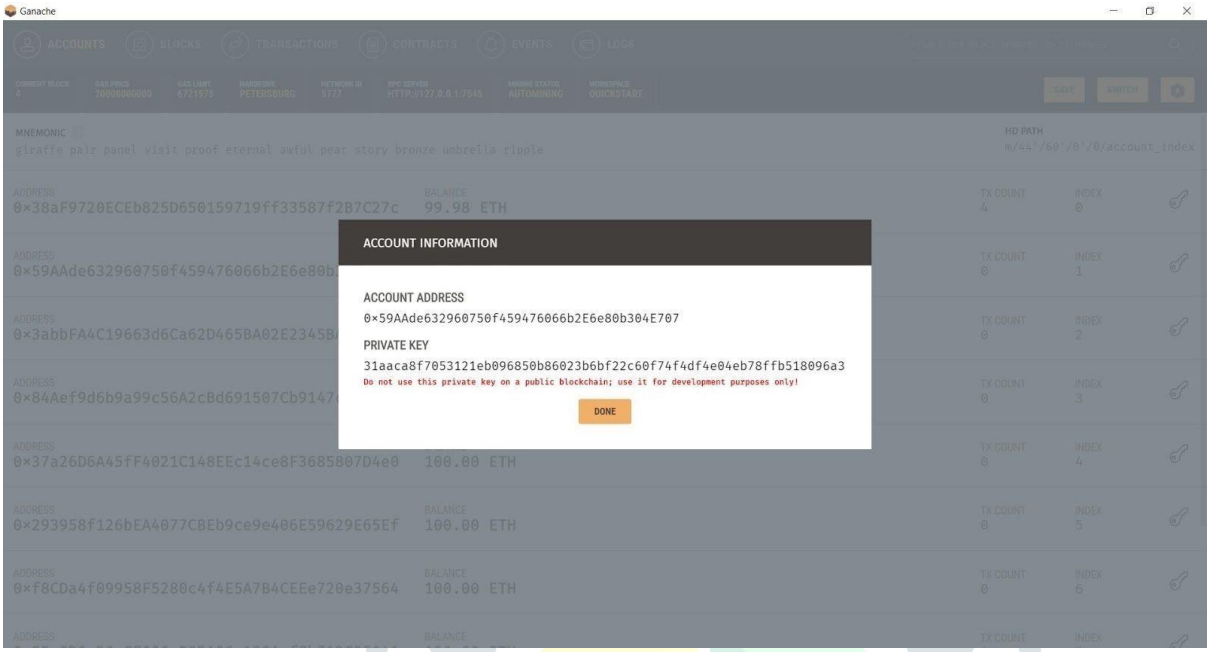


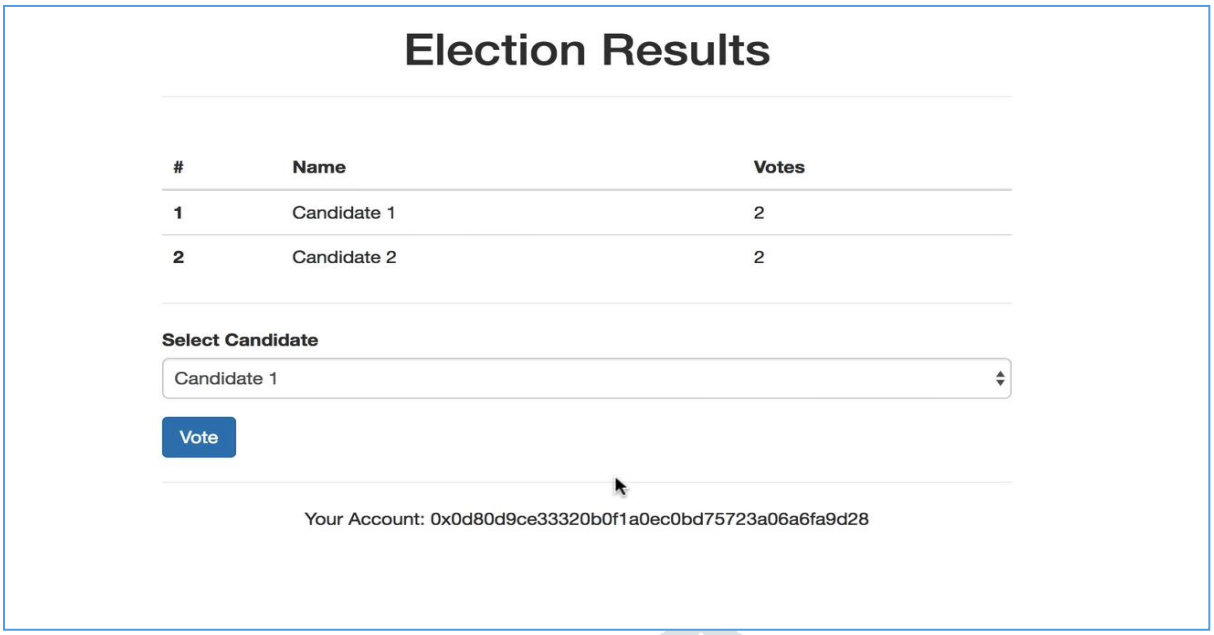
Figure2: Ganache keys

Step 2: List Candidates

We need to add multiple candidates that are taking part in election and store multiple attribute about each candidate. Now we need to store the candidate information for this we use solidity mapping and set mapping to public to get getter function. The function was created to add Candidates. For testing purpose, a new file was created to test every test case. We write file with Mocha testing framework and chai assertion library. Client Side Application UI will be shown to the voter and talk with our smart contract. Here we use following things; Set up web3.js, HTML, javascript.

Step 3: Cast Vote

Here we are going to implement the ability to cast the vote and keep track the accounts where voting is already casted and the ability to increase the vote Count by 1.



TEST VOTING FUNCTION

1. Increase the vote count for candidate.
2. Voting cannot cast vote again.

CLIENT-SIDE VOTING

1. Create a form with empty select statement.
2. User choose its candidate and click on vote button.

Step 4: Watch Events

Last step when voter gives its vote then it will be redirected to homepage and now option to cast vote for same user will be disappear and user can see that there vote is added to the candidate list.

FUTURE RESEARCH DIRECTIONS

In general, the benefits of blockchain-based e-voting will be determined by how the system is implemented[4]. One of the most pressing challenges to be addressed is the concern that election regulations contained in smart contracts or election outcomes may be violated. By definition, everyone who uses a complete Bitcoin or Ethereum node on a public blockchain can access all of the data that has been published there. A private blockchain could be a viable alternative. However, how openness will be integrated and ensured in that situation remains a concern that must be solved.Second, it is well understood that limited central authority intrusion is a desirable quality. However, it is possible that disclosing the intermittent voting results throughout the voting process is undesirable [12]. The election results must stay closed until the election process is completed to ensure that no conceivable interference is carried out based on the outcomes. As a result, a time-dependent disclosure mechanism to ensure results should be researched further.

a) Processing Overheads and Scalability: The scalability of the blockchain-based system would be further impacted by electronic voting integration. Sharding is a method of parallelizing blockchains in order to improve their scale.
b) Identify User: This methodnot guarantee perfect anonymity or privacy. Because the transactions are public, examining and analysing them may reveal the user's identity.
c) Transactions:Security and fairnessbot aremandatory to achieve in blockchain technology. However, due to the presence of transactions in an election system, transactional secrecy and anonymity are essential. A third-party authority is essential for this purpose, but it does not need to be centralised.
d) Energy Efficiency: For blockchain-based electronic voting, we need a lot of energy and a algorithm which consume less amount of energy. Researchers proposed changes to current algorithm for making system more efficient in terms of energy.
e) Immaturity:It has capacity to transform businesses. The technology's immaturity is the root of all current technical challenges with blockchain adoption.
f) Acceptability: Because of the complexity of blockchain, it is very difficult for people to adopt this system.

CONCLUSION

Blockchain is being extensively used in field of electronic voting due to its distributed, secure and transparent nature. Blockchain has become the common technology in this area of research due to providing its secure distributed data storage and transmission of data. In both political and scientific circles, e-voting is still a contentious issue. Here we are giving more efficient way for Voting there are many previous work on it but this paper gives more security to electronic system such as encryption before storage and future research directions like fingerprint authorization and face detection etc.

REFERENCES

[1] R. Sapra and P. Dhaliwal, "Blockchain: The new era of Technology," 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2018, pp. 495-499, doi: 10.1109/PDGC.2018.8745811.

[2] Sapra R, Dhaliwal P. Blockchain: the perspective future of technology. International Journal of Healthcare Information Systems and Informatics (IJHISI). 2021 Apr 1;16(2):1-20.

[3] "Challenges of Electronic Voting A Survey", ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 6, No.18 , November 2015, ISSN : 2322-5157

[4] Khan, S., Arshad, A., Mushtaq, G., Khalique, A., & Husein, T. (2020). Implementation of Decentralized Blockchain E-voting. EAI Endorsed Transactions on Smart Cities, 4(10).

[5] Aranha DF, Ribeiro H, Paraense AL. Crowdsourced integrity verification of election results. Annals of Telecommunications. 2016 Aug;71(7):287-97. DOI: 10.1007/s12243-016-0511-1

[6] Spadafora, C., Longo, R., & Sala, M. (2020). Coercion-resistant blockchain-based e-voting protocol. Cryptology ePrint Archive.

[7] Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018, September). Crypto-voting, a Blockchain based e-Voting System. In KMIS (pp. 221-225).

[8] Taş, R., & Tanrıöver, Ö. Ö. (2021). A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. Security and Communication Networks, 2021.

[9] https://decrypt.co/resources/metamask, accessed on 5/Oct/2021

[10] https://docs.soliditylang.org/en/v0.8.14/ accessed on 5/Oct/2021

[11] Prabhu, S. G., Nizarahammed, A., Prabu, S., Raghul, S., Thirrunavukkarasu, R. R., & Jayarajan, P. (2021, March). Smart Online Voting System. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 632-634). IEEE.

[12] Aakash, Aashish, Akshit, Sarthak, "Online Voting System" Available https://deliverypdf.ssrn.com/delivery.php?ID=912071094074108093078127029082020110000069085067010018086000064122074003022003103121034011107062116011014120095079079002119029015069090069028013067082101124097102077066017083097016069098117070071009080119019102099027071120066118084124095121083121114008&EXT=pdf&INDEX=TRUE accessed on 5/Oct/2021