International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST2182120

Blockchain Based E-Voting System

Prof. Mrunal Pathak[1], Amol Suradkar[2], Ajinkya Kadam[2], Akansha Ghodeswar[2], Prashant Parde[2]

[1]Assistant Professor at Information Technology Department, AISSMS Institute of Information technology, Pune, Maharashtra, India

[2]B.E. Scholar, Information Technology Department, AISSMS Institute of Information technology, Pune, Maharashtra, India

Article Info
Volume 8, Issue 3
Page Number : 134-140

Publication Issue
May-June-2021

Article History
Accepted : 07 May 2021
Published : 14 May 2021

ABSTRACT

Increasingly digital technology in the present helped many people lives. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, there is one organization that manages it. Some of the problems that can occur in traditional electoral systems is with an organization that has full control over the database and system, it is possible to tamper with the database of considerable opportunities. Blockchain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users. Blockchain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting blockchain in the distribution of databases on e-voting systems can reduce one of the cheating sources of database manipulation. This research discusses the recording of voting result using blockchain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this thesis proposed a method based on a predetermined turn on the system for each node in the built of blockchain.

Keywords : Blockchain, ethereum, smart contracts, e-voting, solidity

I. INTRODUCTION

E-voting is widely used in society life. But it is not obvious how to ensure the outcome is respected when the decision is financially or politically related. The correctness, security and privacy are always the most important characters. Secure e-voting is a kind of secure multi-party computation. In the voting process, a set of people make their choices and the choices of them could be kept secretly. Most of the e-voting schemes need a trusted public bulletin board to provide a consistent view to all voters. However, it is not clearly for election administrator to show the public bulletin board can be completely trusted. Some people realize blockchain can be used as the bulletin board because the content is publicly trusted.

Blockchain served as a decentralized database provides new tools for creating trustless and decentralized system. In the blockchain system, there is no trusted centralized coordinator. Instead, each node that is involved in the blockchain system holds the data block locally. Blockchain is maintained by a decentralized and open-membership peer to peer network. At first, this technology is designed for money transfer. With the development of it, researchers are trying to reuse Blockchain in other research areas such as coordinating the Internet of Things, carbon dating and health-care. This sparked the invention of Ethereum , which is well known as a milestone in the development of blockchain. It owns a Turing complete programming language and users can realize the function by the smart contract in the Ethereum network.

Blockchain could be used as the trusted public bullet board for the voting system. In addition, the smart contract on the blockchain served as a trusted computer whose result is public trusted. However, only replacing the bulletin board with blockchain is not a good idea. Because there will be too many transactions for voters to discern and the computation on blockchain is very hard, this could be seen in.
In this paper, proposed a decentralized trustless e-voting system based on blockchain. The decentralized system means the computation is depended on decentralized blockchain. The trustless system means voter do not need to rely on the election administrator, the trust is separated to all voters. The correctness of the system depends on the whole protocol. In addition, all voters can have cryptographic assurance that the privacy of each voter can be protected.

To ensure that anybody could not tally the election result before the end of the election, the scheme uses threshold encryption without trusted third party. In addition, even if the election administrator is malicious, the tally result will not be changed. The encryption method of it is to set up a pair of public/secret keys. The public key is known to all parties, while the secret key is separated to all parties and nobody gets the complete secret key before key reconstruction stage. When at least of n parties upload their secrets, the secret key is reconstructed.

The voting protocol is deployed on Ethereum by smart contract. The Ethereum script allows users to write the required smart contracts on Ethereum and implement powerful functions through smart contracts to implement decentralized applications. All nodes of Ethereum network run the contract code independently to ensure the credibility of the final result. The final result is public verifiable.

II. REVIEW

Technology is playing an essential role in providing solutions to worldwide problems. Likewise, it has played its part in Voting Systems. In 2011, a Web-based secure E-voting system with fingerprint authentication was developed, where the system administrator can define the election, party, village headman, polling clerks, and candidate details into the database also system administrator sets the election timings. The village headman is responsible for registering the electors with their fingerprints. Polling clerks can start the election in their authenticated areas. Electors cannot vote before the start timing of the election, also electors' would be authenticated for election based on their fingerprint match with already registered fingerprints in the database, and the voter can vote once only. The election process can be finished by the system administrator and the election results relevant to the region would be shown after the end of the election process.

In traditional voting systems, the ratio of voters is decreasing day by day therefore in 2015, the idea of an E-Voting System using mobile SMS was proposed named "Mobile-Electronic voting machine (M-EVM) or Modified Electronic voting machine(MEVM)". This

system has two different modes. First for those who don't have mobile phones, for them the solution is an old traditional system but another mode is for those who have mobile phones which is the necessary condition for using M-EVM. For successful voting using M-EVM, the voter name concerning his/her mobile number must be registered in the EVM database. Voters can vote for the specific candidate by sending the message in the required format and the result M-EVM would acknowledge the voter about the vote. After voting that person would be blocked from the list after that voter cannot vote again. In this system, all registered mobile numbers will be informed about the results of the election after the 1 hour of voting.

Another research presents, Blockchain-based Electronic Voting System (EVS) to prevent the security threats occurring at normal EVS and ballot voting which ensures transparency that even the Election Commission can't view whom the voter voted for. As the blockchain is immutable, no one can change or temper the vote once it is cast. To keep the confidentiality of data the concept of Trusted Third Party (TTP) is used, which acts as an intermediary between a voter and Election Commission to authenticate and validate voters for casting votes anonymously without security hazards. The system is multi-chain and is capable of restricting multiple vote casting per voter. Every voter has to register himself before voting starts, for which the voter has to submit their aadhar database. During voting, the voter has to submit their aadhar database i.e. fingerprint. Aadhar data is secured using cryptography to the Election Commission to make sure the voter is valid and upon validation, the voter would be navigated to the voting module. After voting ends different reports can be generated about candidate's results, party-wise results, constituency results, etc.

Studies indicate the project about a secure, decentralized blockchain-based e-voting system using private Ethereum with less or no delay considering common voting problems like vote tampering, standing in queues, and booth capturing. Smart Contact (using solidity) along with voters' national identity or One Time Password (OTP) is used to validate voters, check eligibility, and to restrict multiple votes. At the voting time, users have to log in with the same data used in registration, upon logging in he would require submit voter's fingerprint data. After verification he would be directed to the voting portal to cast his vote. After logged in once, he would no longer be able to log in again as it would be stored in the database. As a storage entity two databases are used MongoDB and Blockchain. The registration data and users' details are stored in MongoDB whereas the voting data and candidates' details are stored in Blockchain.

III. LITERATURE SURVEY

Authentication of voters:

There are various different strategies for authentication of voters. According to Kriti Patidar and Dr jain voters authentication can be done using private key cryptography that has to be provided to voters prior to election process.

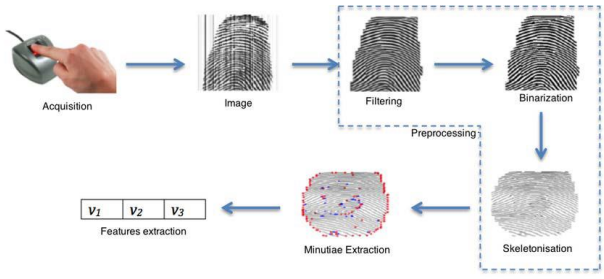
Voters should be registered by some authority, while registering the voters keys must be generated and distributes to voters in hand .

Cosmas Krisna Adiputra, has same idea for system design he also suggests that there must be an public, private key infrastructure, the electoral commission (or another election manager) generates a key-pair for the election (PE; SE) which later is used for encrypting and decrypting messages of voters. Then, each voter needs to generate their own key-pair. (PV X; SV X) denote the key pair of voter X. This key pair is later used for signing the message created by the voter herself. Voters need to register their public key PV X to the electoral commission for their voting eligibility

using a designated valid ID. The electoral commission then verifies each voter's ID and registers the corresponding public key PV X to a public list; or rejects it if the voter is not eligible. It is crucial that each voter keeps their public key secret in this scheme and only sends it to the governing body.

There is some different thought of Friðrik Þ. Hjálmarsson ,he has plan to use 6 digit pin for voter that voter can use for voter authentication, Each individual is identified and authenticated by the system by presenting an electronic ID from Auokenni and the corresponding 6-digit PIN in the voting booth. Without supervision, an individual could vote for multiple people, if the individual had knowledge of the PIN for each corresponding electronic ID he has.

Roopak proposed some unique solution of using Aadhar database for voter information. The proposed framework is an electronic voting system using virtual ID which is provided by the UIDAI which is unique. Aadhar database helps to get the demographic details including the fingerprint details of the voters/voter. The fingerprint is converted to the digital signature which can be used to ensure the security of the vote in the block while doing the encryption as shown in Fig.



Anonymity and verification

One of the primary voting conditions is being anonymous, with outsiders unable to access information on how someone voted. However, to get citizens to cast a vote, they need to be eligible, and there needs to be some way to verify that. It is a challenge to balance these two requirements. Once it is on the blockchain, we want the person to see that is their vote, but we do not want anyone else to see what is going on, because it does not help to make sure the voting is reasonable.

Nevertheless, countries are pressing along with an attempt to introduce blockchain voting; one of them is Brazil [13], which uses the Ethereum blockchain to store election data. It is a huge task to collect and validate the information of around 145 million registered voters. Therefore, to conduct an utterly blockchain-based e-voting, different issues need to be overcome.

Verifying voter identity from various angles is always a challenge; some works have tried the biometric solutions, such as facial comparison, fingerprint, Iris and retinal scan but this can be biased and easily gamed or stolen. However, we think that one way to protect the stolen biometrics data is by using a complex algorithms that are hard to crack. It can be hashed using any hashing algorithm instead of saving the biometric information as binary data and then stored as a reference string. The sample model should be converted to a hash value during the validation and identification process and then compared with the reference value.

Comparison

Literature [12] propose a concrete construction of a blockchain based self-tallying voting protocol in decentralized IoT, and prove that it satisfies fairness, dispute freeness, and maximal ballot secrecy. In this system they formalize the system model of self-tallying voting systems based on blockchain in decentralized IoT. Literature [13] propose an electronic voting system based on smart contracts to protect voters' privacy. The test results suggested that the system can effectively reduce the cost of using smart contracts to vote, and protect the privacy of voters with practicability. Literature [14]proposes an e-voting system based on blockchain that eliminates some of the limitations in existing voting systems. It also presents state of art of some blockchain

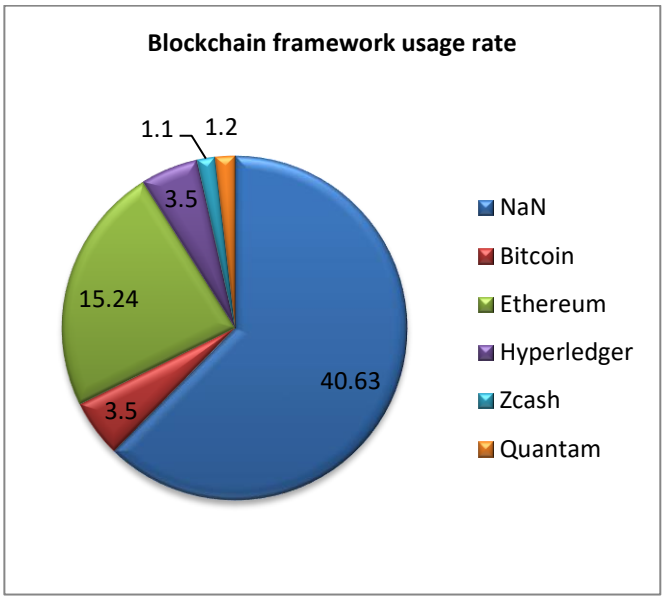
frameworks for e-voting. The presented implementation is suitable for small scale elections like inside corporate houses, board rooms etc. The implementation uses smart contract from Ethereum. Truffle framework is used for development, testing and deploying smart contracts. Ganache is used as Ethereum client for testing. Meta-mask is used as browser wallet. Literature [15]proposes a distributed blockchain electronic voting scheme with self-tally function by using blockchain. In the scheme, the voter's voting privacy information is protected by two rounds of zero knowledge proof protocol, but the voting scheme only allows voters to select two candidates (yes/no),namely 1-out-of-2 voting, which cannot satisfy the situation of multiple candidates in one voting process.

Table 2. Comparison of three types of voting schemes

Author	Cryptography /Encryption mode	Vote Counting Method	Technology Used
Yannan Li, Willy Susilo[4]	Zero knowledge proof	Self-tally	Blockchain and IOT
Friðrik Þ. Hjálmarsson, Gunnlaugur K. [1]	Public-Private Cryptography	Self-tally	Blockchain and smart contract
Kriti Patidar, Dr. Swapnil Jain[4]	RSA algorithms	Third Party counting	Blockchain and ETH
McCorry et al.	2 Round-zero knowledge proof	Self-tally	ETH and Smart Contract

Analysis

Blockchain systems allow the development of blockchain-based applications. Bitcoin, Ethereum, Hyperledger and R3 Corda are the most renowned blockchain frameworks. We tried to find out which systems are mostly preferred for analyzing the details of the selected papers. However, we found that most of the papers containing general definitions and there were insufficient information on the technical implementation details. Many of the studies tackle the overall idea of blockchain based e-voting and general issues affiliated with it. There seems to be a general consensus on the idea that blockchain can be applied in e-voting systems. However, technical details and implementation proposals are not explicitly stated. Nevertheless, based on the studies the blockchain platform usage distribution can be seen in Figure



Gas Cost and Time Analysis

Yuxian Zhang has performed gas cost and time analysis of his system they chose to deploy and test the contract in the Ethereum private chain. Consumption of Gas and money for a 40-person election. They calculate the real-time price required for the transaction based on the Gas Price provided by eth gas station and the current eth price. Gas Price = 7

gwei, 1ETH=607.76USD, A and V represent the operations of the administrator and the voter respectively. The results show that it takes about $20.49 to hold such an election, and the administrator needs to spend about $3.41. MeanwhileThe result is shown in Figure .Since their system do not use complex calculations and zero-knowledge proofs in contracts, the amount of Gas required to execute contracts is greatly reduced, and this cost is acceptable to the organizers and participants of the election.

Operation	gas Cost	gas Cost
Deploy(A)	3,328,566	6,088,493
Initialize(A)	2,705,384	22,993,368
Send Blind Message(v)	54,780	3,773,528
Send Signature(A)	1,821,960	68,149,05
Send Unblind Signature(V)	42,778	1,770,372
Send Final Whitelist(A)	1,770,372	3,773,528
Register(V)	74,352	553910
Begin Vote(A)	28 849	36796
Vote(V)	553910	146,872
Begin Tally(A)	28,476	553,910
Tally(A)	553,910	654932
Administrator Total	10,237,517	40,915,932
Voter Total	274,693	6,244,679
Election Total	21,225,237	47160611

IV. CONCLUSION

In this paper we analyzed and discussed about the traditional voting system and also the advantages of implementation blockchain based E-voting system that uses various blockchain based tools and using case study of manual voting process. After that we saw the comparison between traditional voting system used and the blockchain based e voting system.

The implementation uses blockchain as a centralized voting system. This system will use blockchain as a network as well as database to store voter's information or credentials which is going to use for their authentication. System will be using candidate's or voter's details for the voting process.

V. FUTURE WORK

In future work, we will continue on the further implementation or changes in our system and we will try to research on its further performance. However, there are still some implementation that can be applied to our system.

Basically our focus is on the development of more efficient and sophisticated system for E-voting using blockchain technology and its related variable tools.

VI. REFERENCES

[1]. F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[2]. C. K. Adiputra, R. Hjort and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, 2018, pp. 22-27, doi: 10.1109/WorldS4.2018.8611593.

[3]. K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparitive Analysis on E-Voting System Using Blockchain," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/IoT-SIU.2019.8777471.

[4]. R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th International Conference on

Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-6, doi: 10.1109/TSSA.2017.8272896.

[5]. Xiao S., Wang X.A., Wang W., Wang H. (2020) Survey on Blockchain-Based Electronic Voting. In: Barolli L., Nishino H., Miwa H. (eds) Advances in Intelligent Networking and Collaborative Systems. INCoS 2019. Advances in Intelligent Systems and Computing, vol 1035. Springer, Cham. https://doi.org/10.1007/978-3-030-29035-1_54

[6]. Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2020). A Blockchain-based Self-tallying Voting Protocol in Decentralized IoT. IEEE Transactions on Dependable and Secure Computing, 1–1. doi:10.1109/tdsc.2020.2979856

[7]. K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.

[8]. Y. Zhang, Y. Li, L. Fang, P. Chen and X. Dong, "Privacy-protected Electronic Voting System Based on Blockchin and Trusted Execution Environment," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1252-1257, doi: 10.1109/ICCC47050.2019.9064387.

[9]. T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 71-75, doi: 10.1109/ICIMIA48430.2020.9074942.

[10]. Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul, "Risks and Opportunities of Blockchain Based on E-Voting Systems," 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 2019, pp. 365-368, doi: 10.1109/ICCWAMTIP47768.2019.9067529.

Cite this article as :

Prof. Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar, Prashant Parde, "Blockchain Based E-Voting System", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 3, pp. 134-140, May-June 2021. Available at
doi : https://doi.org/10.32628/IJSRST2182120
Journal URL : https://ijsrst.com/IJSRST2182120