Decentralized E-Voting System Using Blockchain

[1]GEETHA M,[2]VENKTESHA NAIK R

[1]Assistant Professor,Deparment of Master of Computer Applications,BIET,Davanagere

[2]Student,Department of MCA,BIET,Davanagere

Abstract: Voting is a primary right of every citizen living ina country. Traditional methods used for voting includes paper ballot system, EVMs (Electronic Voting Machines), etc. which are still followed and trusted by every voter or citizen blindly. These voting systems can have ambiguity as the data is maintainedunder a centralized environment whether it is counting the paper ballots or storing the vote caste on a computer server. Thisuse of a centralized database for the voting system has some security issues such as Data modification through the third party in the network due to the use of the central database systemas well as the result of the voting is not shown in real-time, or manipulation with the data which can hamper the result and thus have an impact on not only system integrity but also lose faith in democracy, government, nation, etc. The votingmethods used in an election should be legal, accurate, safe,and convenient.

Keywords: ***Blockchain Technology, EVM(ElectronicVotingSystem), Smart Contracts, Ethereum, Solidity, etc.s***

I INTRODUCTION

The most fundamental aspect of a democracy is the avail- ability for citizens to not only share ideas, opinions, and beliefsbut to make their individual voices heard by deciding thecollective future by vote. However, for the voting to proceed as intended, there needs tobe a transparent and secure processwhere also the voters knowingly keep their privacy. The chal- lenge is to find a solution that prevents unlawful manipulation of the collected data and achieve desired transparency in the security measures, taken to protect voter privacy and the collected results and therefore democracy itself. By using blockchain our proposed system has the features like security, privacy, and integrity. In blockchain every node or user is anonymous and every action performed is a transaction which is hashed and then stored into the network.

To test our pro- tocol, we put it on Ethereum a blockchain platform that uses Solidity as a programming language to create smart contracts. Smart Contracts are backbone of Blockchain System. Theusage of smart contracts ensures a safe means for performing voter verification, ensuring the correctness of voting results, making the counting system public, and protecting againstfraudulent activities. Blockchain Technology eliminates the risk of single point of failure, whichis usually seen in traditional approaches as discussed above, making our voting system tamperproof and trustworthy which not only provides integrity to voters or citizens, but also supports transparency among voters and candidates and it also strengthens the actual meaning of democracy and create a sense of belief among them and thus making the system moresecured and reducing the cost for infrastructure management as well. Votingis a process which is defined as the right of people to choose their leaders. Voting is a important process that enables people to handpick their government leader.

The voting system should be democratic, independent, and unprejudiced. As a result, it must be a transparent and secure procedure that allowseveryone to partake their standpoint freely. A lot of peoplein the world do not keep faith in the election system.

The Traditional voting is controlled and full of mediators.Furthermore, people are dealing with a variety of issues,suchas booth capture, dummy voting and the problem of proper monitoring, a massive line of people in front of the polling booths, false voting, pre-vote casting, redundant vote,lack of awareness, polling booths are located a long distance away from the house, etc. Theabove problems can be solved using Blockchain technology which will provide a reliable system, where one can trust the system with integrity. Blockchain is a decentralized network in which the node members exchange data, but each user maintains the identical data replication. Blockchain technology provides characteristics such as pri- vacy, and data accuracy, etc.

II LITERATURE SURVEY

A. Related Works

Decentralized E-Voting Portal Using Blockchain. M D.Castillo In this paper proposes an e-voting system based on blockchain that eliminates some of the limitations in existing voting systems. The paper 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. [1]

Decentralized E-voting system based on Smart Contractby using Blockchain Technology. Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, and Kyung- Hyune Rhee.

Thispaper aims to provide an E-voting system with highsecurity by using blockchain. Blockchain provides a decentralized model that makes the network Reliable, safe, flexible, andable to support real-time services.[2]

DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. Andrew Barnes, Christopher Brake and Thomas Perry,. The system in this paper provides voter anonymity bykeeping the voter information as a hash in the blockchain.[3]

Decentralized E-Voting Systems Based on the Blockchain Technology. Jen-Ho Hsiao1, Raylin Tso1, Chien-Ming Chen2and Mu-En Wu. This paper is aimed to design a decentralized e-voting system.[4]

Decentralized E-Voting System UsingBlockchain. Dr S.Sekar, C.Vigneshwar, J.Thiyagarajan, V.B.Soorya Narayanan, M.Vijay. The purpose of this paper is to overcome the limitation of existing e-voting system by implementing voter validation using Biometric, Dynamic Ballot loading and Acknowledgement after casting votes with the help of Blockchain technology.[5] Blockchain Based E- Voting Recording System Design. Zibin Zheng, Shaoan Xie,Hongning Dai, Xiangping Chen,and Huaimin Wang. Thispaper provides an overview of blockchain architechture firstly and compare some typical consensus algorithms used in different blockchain.[6]

Secure Digital Voting System based on BlockchainTechnology. Rifa Hanifatunnisa, Budi Rahardjo. This research discusses the recording of voting result using blockchain algorithm from every place of election.[7]

Decentralized Electronic Voting System Based on Blockchain Technology Developing Principals. Kateryna Isirova, Anastasiia Kiian, Mariia Rodinko and Alexandr Kuznetsov. Inthe paper, the new concept for developinga decentralized electronic voting system using blockchain technology is proposed.[8]

An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Syada Tasmia Alvl, Mohammed Nasir Uddin, LintaIslam, Sajib Ahamed. In this paper, by using blockchain the proposed system ensures security, privacy, and integrity of voting system.

This system provides voter anonymity by keeping the voter informationas a hash in the blockchain.[9]

A Decentralized Voting System. Jack Ahlkvist, Anton Gustafsson, Carl Lundborg, Joakim Mattsson Thorell, Aron Sandstedt Sanjin Slavnic. This thesis investigates the possibility of a decentralized voting system and explores the possible challenges regarding privacy, correctness andintegrity.[10]

An efficient and effective Decentralized Anonymous VotingSystem. Wei-Jr Lai, Ja-Ling Wu. In this work, a lightweight E-voting system is proposed for voters to minimize their trust in the authority or government. We ensure the transparency of election by putting all message on the Ethereum blockchain,in the meantime, the privacy of individual voter is protected via an efficient and effective ring signature mechanism.[11]

Blockchain based E-voting System. Albin Benny, Aparna Ashok Kumar, Abdul Basit, Betina Cherian and Amol Kharat. In this project, we have implemented and tested an e-voting application as a smart contract for the Ethereum network using the Ethereum and the Solidity language.[12]

A Review on Distributed Blockchain Technology for E- voting Systems. Rihab H Sahib and Eman S. Al-Shamery. This paper introduced many different ideas for implementing e- voting systems based on Blockchain and how the users (votersand candidates) interact with the system showing the voting process from the first step of registration to authentication till showing the final results.Users are authenticated through their mobile phone numbers without the need of a third party server. Results showed that the system is feasible and may offer a step towards ideal environments for such experience.[13]

Blockchain for Electronic Voting System—Review and Open Research Challenges. Uzma Jafar, Mohd Juzaiddin Ab Aziz and Zarina ShukurThe following article gives anoverview of electronic voting systems based on blockchain technology. The main goal of this analysis was to examinethe current status of blockchain-based voting research andonline voting systemsand any related difficulties to predict future developments.[14]

Decentralized Voting Platform Based on Ethereum Blockchain. David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb. In this paper we propose a novel approach for a decentralized trustless voting platform that relies onBlockchain technology to solve the trust issues. The main features of this system include ensuring data integrity andtransparency, and enforcing one vote per mobile phone number for every poll with ensured privacy.[15]

III Existing System

The voting system currently being used by the University's student union is a paper based system, in which the voter simply picks up ballots sheets from electoral officials, tick off who they would like to vote for, and then cast their votes by merely handing over the ballot sheet back to electoral official. The electoral officials gather all the votes being cast into a ballot box. At the end of the elections, the electoral officials converge and count the votes cast for each candidate and determine the winner of each election category.

IV PROPOSED SYSTEM ARCHITECTURE

The system architecture comprises of Client side,Blockchain network and Middleware edge technology by removing the barrier of dependency, whichwill be adopted by the tech industry very soon and then furtherby customers.

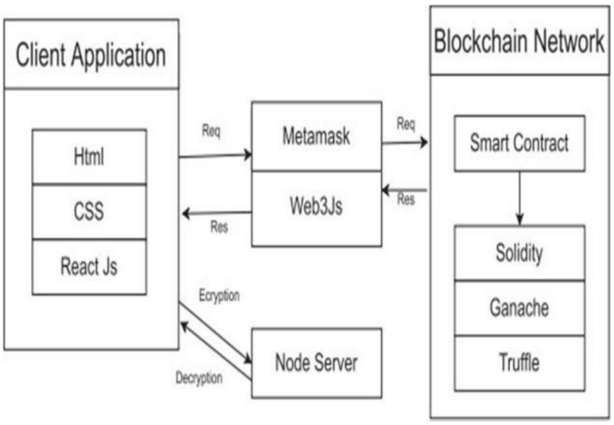


Fig1 : System Architecture E-Voting.

1) *Client Side Application:* The client side application is build using HTML,CSS, React.js Library.
2) *Blockchain Network:* The Smart Contracts are written using the Solidity programming language. Ganache is used as Ethereum client for testing. Truffle framework is used for development, testing and deploying smart contracts.
3) *Middleware:* Meta-mask is used as browser wallet. Web3.js a collection of libraries is used for connection between user interface and blockchain database(network), and A small node server is used in our system. It acts asa cryptographic server which is named as a crypto server. This server is used for storing the public private keys for encryption and decryption, respectively.

V IMPLEMENTATION

(HOMOMORPHIC) Encryption Algorithm:

The HOMOMORPHIC encryption algorithm is mainly an internet based encryption algorithm, which can be used for authentication. The HOMOMORPHIC encryption algorithmuses the public/private key cryptography technique to encrypt and decrypt data being transported between users. In order to generate the public key and private key to be used to encrypt and decrypt the data to be sent to the user, two prime numbers have to be utilised.

A complex process of mathematical calculations have to take place to acquire a set of two prime numbers that wouldrepresent the public key used to encrypt the data and the private key used to decrypt the data once received by the receiver.

The HOMOMORPHIC algorithm works as follows: take two large primes, p and q, and compute their product $n = pq$; n is called the modulus. Choose a number, e, less than n and relatively prime to $(p-1)(q-1)$, which means e and $(p-1)(q-1)$ have no common factors except 1. Find another number d such that $(ed - 1)$ is divisible by $(p-1)(q-1)$. The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e); the private key is (n, d). Thefactors p and q may be destroyed or kept with the private key.[42]

The HOMOMORPHIC encryption algorithm is used by the Secure Socket Layer (SSL) for encrypting data being transmitted over a secure connection.

Python Cryptography Extension :

JCE is an implementation of cryptography for Python systems. The JCE package provides a framework for encryption, decryption, key generation, key agreement and Method Authentication Code algorithms on Python platforms. JCE encryption allows symmetric, asymmetric, block, and stream ciphers with additional support for securestreams on the Python platform. [47]

The JCE API was created to support a number of encryption algorithms through a number of Python classes, which a developer could use for implementing security features in a Python based system. The advantage about using the JCE API is that, the developer would not have to understand the logic behind the encrypting algorithms because the details of the encryption algorithmwould be managed by the provider. The JCE Framework provides a service provider that implements the followingencryption algorithms.

- Blow Fish
- DES

The Python encryption class to be used for the Online Voting System would make of the DES encryption algorithm.

V. RESULTS

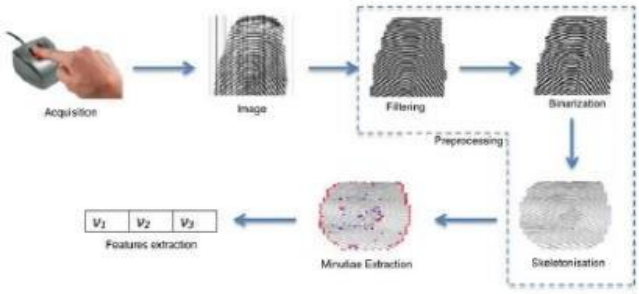
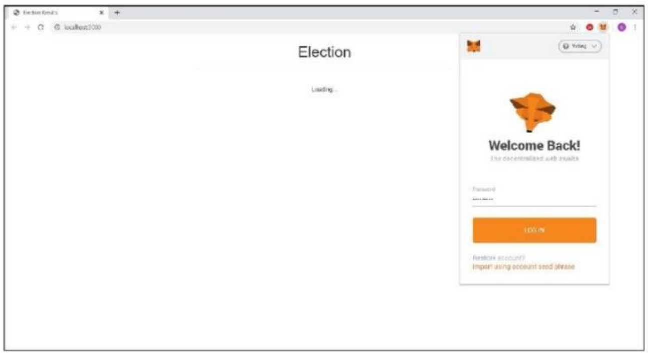


Fig2 : Anonymity and verification



Election

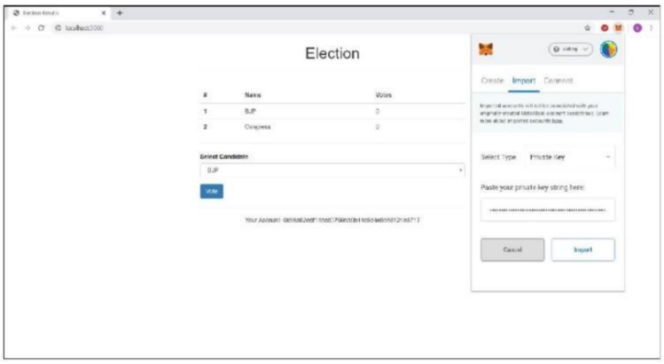
Loading...

Welcome Back!

The decentralized web awaits

Password

Fig3 : Snapshot of Loading Screen.



Election

#	Name	Votes
1	BJP	0
2	Congress	0

Select Candidate: BJP

Your Account: [illegible]

Select Type: Private Key

Paste your private key string here:

Fig4 : Constituency Logging In Via Metamask.

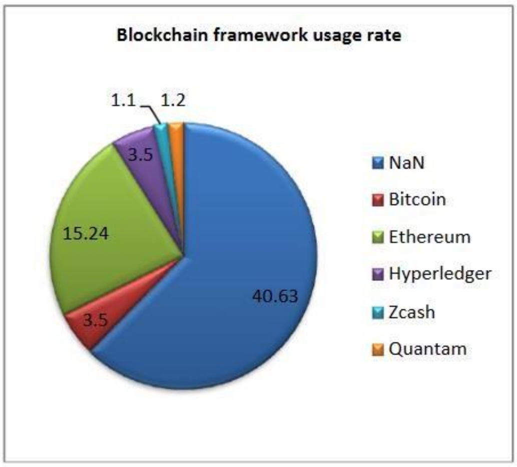


Fig5 : Gas Cost and Time Analysis

VI CONCLUSION

This paper presents a blockchain based e-voting systemthat runs on Ethereum. It shows that blockchain technology can overcome limitations of centralized voting systems. This implementation uses Ethereum blockchain as a network as well as database for storing voter's accounts, candidate de- tails and votes. This implementation makes use of smart contracts. Blockchain as a technology carries a great futureahead where many real world problems of depending onthird party centralized authority in day-to-day life can be resolved, people want an less ambiguous system where everything is crystal clear and at the same time making sure that their(users) data is safe and secure. Voting system using Blockchain will for sure solve all these circumstances faced by people or citizens of a country and will provide them with a system where we no longer they need to depend and follow on to these old aged traditional approaches. World is moving faster and it will move faster in terms of Technology, when we noticed a boom in Web 2 Era that is the dot com era every- thing was digitalized but centralized at the same time, but thisrevolution of Web3 Era brings a lot of exciting and one step ahead cutting

REFERENCES

[1] M.D. Castillo, "Russia Is Leading the Push for Blockchain Democracy,"CoinDesk, 2018; https://www .coindesk.com/russias capital -leading-charge- blockchain–democracy, 2018.

[2] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, and Kyung- Hyune Rhee, "A Critical Review of Blockchain and Its Current Applica-tions," in IEEE International Conference on Electrical Engineering and Computer Science (ICECOS) 2017, pp. 109-113, 2017.

[3] Andrew Barnes, Christopher Brake and Thomas Perry, "Digital Voting with the use ofBlockchain Technology", https://www.economist.com/sites/default/files/plymout h.pdf, 2016.

[4] Friorik P. Hjalmarsson, Gunnlaugur K. Hreioarsson, Mohammad Ham- daqa, and Gisli Hjalmtysson, "Blockchain-Based E-Voting System," in IEEE 11th International Conference on Cloud Computing, pp. 983-986, 2018.

[5] Patrick McCorry, Siamak F. Shahandashti and Feng Hao, "A Smart Con- tract for Boardroom Voting with Maximum Voter Privacy", Published in: Financial Cryptography and Data Security, Springer, 2017.

[6] Jonathan Alexander, Steven Landers and Ben How-erton, "Netvote: A Decentralized Voting Network",https://netvote.io/wpcontent/uploads/2018/02/ Netvote-White-Paper- v7.pdf, 2018.

[7] D. Khader, B. Smyth, P. Y. Ryan, and F. Hao, "A fair androbust votingsystem by broadcast", in 5th Internatio

[8] Yiyun Zhou, Meng Han, Liyuan Liu, and Wang Yan, "Improving IoT Services in Smart-Home Using Blockchain Smart Contract," in IEEE Confs. on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Com- puter and Information Technology, Congress on Cybermatics, pp. 81-87,2018.

[9] M. Hochstein, "Moscow's Blockchain Voting Platform Adds Service for High-Rise Neighbors,"CoinDesk, 15 Mar. 2018; https://www.coindesk.com/moscows-blockchain- voting-platform adds-service-for-high-rise-neighbors,2018.

[10] Francesco Restuccia, Salvatore D'Oro, Salil S. Kanhere, TommasoMelodia, and Sajal K. Das, "Blockchain for the Internet of Things: Present and Future," IEEE Internet of Things Journal, vol. 1, no. 1,pp. 1-8, January 2018.

[11] Nir Kshetri and Jeffrey Voas, "Blockchain-Enabled E-Voting," IEEE Software, pp. 95-99, 2018.

[12] Truffle : https://truffleframework.com

[13] Ethereum project : https://ethereum.org

[14] Ganache : https://truffleframework.com/ganache

[15] D. Khader, B. Smyth, P. Y. Ryan, and F. Hao, "A fair and robust voting system by broadcast", in 5th International Conference on Electronic Voting, Vol. 205, pp 285-299, 2012.