IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Blockchain Enabled E-Voting System

[1]Kaushiki kumari [2] Dr Anuranjan Mishra

M. Tech Student, Department of CSE, Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University, Lucknow, India[1]

Asst. Professor, Department of CSE Greater Noida Institute of Technology, Greater Noida, Dr. APJ Abdul Kalam Technical University, Lucknow, India[2]

ABSTRACT: The Blockchain-Enabled E-Voting uses a digital-currency comparison, where a ballot can be cast anonymously using a network system in qualifying voters. BEV uses encrypted key, smart biometrics, and real-time tamperproof personal ID authentication. Blockchain allows for the development of tamper-proof voting audit trails. The idea of integrating digital voting systems to make the public election process cheaper, quicker and easier is a convincing one in modern society that normalizes it in the eyes of voters, eliminates a certain barrier of control between the elector and the elected candidate, making it an efficient way to cast votes in this technology age.

KEYWORDS: Blockchain, E-Voting System, Ether, Ethereum, Paillier Encryption, Smart Contract

I.INTRODUCTION

Electronic Voting (E-Voting) is one of the voting methods that uses electronic mechanisms to help cast and count votes in a cryptographic election. It secures Multi-Party Computation (MPC) due to properties like openness, decentralization, nonrepudiation and irreversibility. Two principal forms of e-voting can generally be defined:

1. E-voting that is monitored physically by members of governmental or autonomous electoral authorities (e.g.

Electronic voting machines at polling sites)

2. Remote e-voting from any location via the Internet (also known as I where the elector submits their votes electronically to the election authorities. Blockchain has a great potential when built into many areas.

Blockchain Technology: A blockchain is a increasing list of blocks that are connected using cryptography, called records. Each block includes the previous block's cryptographic hash, timestamp and transaction data and has features such as longevity, robustness, improved network security and decentralization. The database ledger is not located at any single location. The documents are kept public, and are easy to check. There is no centralized version of the information for a crooked hacker.

Ethereum Platform: Ethereum is an open-source, public , blockchain-based distributed computing platform, and a smart contract operating system. The Ethereum Wallet is a portal to decentralized applications on the Ethereum blockchain, in which miners work to gain Ether instead of mining for bitcoin.

Ether: Ether is a type of crypto token that is a digital asset to issuer that power the network. In addition to a tradable cryptocurrency, the application developers can use Ether to pay transaction fees and utilities on the Ethereum network. Like cash, a third party need not process or authorize a transaction.

Node Package Manager: The Node Package Manager or NPM is a dependency of JavaScript software globally enabled, which comes with Node.js. It consists of a client command line, npm and an online public and paid private package database, npm registry accessed via client and operated by npm, Inc.

Truffle Framework: Dependence on the Truffle Platform enables the development of decentralized applications on the blockchain Ethereum. It offers a suite of tools that enables smart contacts to be written, checked and deployed in order to blockchain with the Solidity programming language.

Ganache: The Ganache dependency, a local in-memory blockchain is downloaded from the Truffle Framework website. It gives 10 external accounts with addresses on local Ethereum blockchain to run tests, execute commands and inspect state

while controlling how the chain operates. Each account is preloaded with 100 fake ether. It is used for developing and deploying of DAPP on ethereum.

Metamask: MetaMask acts as an Ethereum browser through a plug-in for Chrome allowing users to manage their Ethereum wallet with multiple accounts, switch between different networks and interact with decentralized applications and smart contracts without running a full node. The transactions are signed using the sender's private key [5].

Paillier Encryption: Full homomorphic encryption enables users to perform computations on encrypted data that can be decrypted and yield the same result as if the computation had been originally performed on decrypted data. This probabilistic public-key encryption method supports addition and multiplication. Paillier system can homomorphically add two ciphertexts but it can only multiply a ciphertext with a plaintext integer. Hence, it is considered partially homomorphic thus achieving the advantages of homomorphic encryption without the substantial reduction in processing speed [5].

II.LITERATURE SURVEY

According to **Nir Kshetri et.al** [1], E-Voting is among the key public sectors that can be disrupted by blockchain technology. To use a digital-currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the voter's coin to a candidate's wallet. A voter can spend his or her coin only once.

According to **Fridrik P Hjalmarsson et.al** [2], this paper aims to evaluate the application of blockchain as service to implement distributed electronic voting systems. The paper starts by evaluating some of the popular blockchain frameworks that offer blockchain as a service. More generally this paper evaluates the potential of distributed ledger technologies through the description of a case study, namely the process of an election and implementing a blockchain- based application which improves the security and decreases the cost of hosting a nationwide election.

According to **Ahmed Ben Ayed** [3], Blockchain is offering new opportunities to develop new types of digital services. In this paper, we are going to leverage the open source Blockchain technology to propose a design for a new electronic voting system that could be used in local or national elections. The Blockchain-based system will be secure, reliable, and anonymous and will help increase the number of voters as well as the trust of people in their governments.

According to **Freya Sheer Hardwick et.al** [4], the objective of such a scheme would be to provide a decentralized architecture to run and support a voting scheme that is open, fair, and independently verifiable. In this paper, we propose a potential new e-voting protocol that utilises the blockchain as a transparent ballot box. The protocol has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralisation.

III.RESEARCH METHODOLOGY

The proposed system involves a client server architecture integrated with a block chain system. The minimum requirements needed by a voter is a smartphone or a computer. BEV issues each voter a "wallet" containing a user credential. Each voter gets a "digital coin" as ether representing one opportunity to vote. Voters can cast their vote before a preset deadline.

The objectives of the adoption of the Blockchain technology in the solution are - To provide a decentralized architecture; To support a voting scheme that is open, fair and independently verifiable; To optimize the electoral process that enables secure, quick, cost effective, transparency and improved identity verification.

A. SYSTEM ARCHITECTURE:

The Fig 1 shows how the user interacts with the different parts of the system. The system has two parts – functionality of each part and the processes associated with the system

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

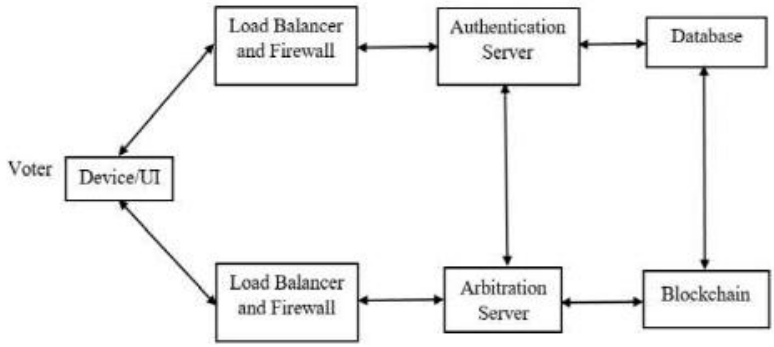

Fig 1: System Architecture

i. System Parts:

- User - The voter can have any digital device with internet to register and vote.
- Authentication Server (AS) - The Authentication Server is a traditional centralized web server. It has a backend database connected which has voter's details. This system is used by people to register to vote for their elections. It creates accounts on the blockchain system when people register. The AS also authenticates the token provided by the voter while voting.
- Arbitration Server (AR) - The Arbitration Server acts as an intermediary between a user and the Blockchain voting system. It verifies the voter while voting using the Authentication Server. The AR is a blockchain thin client

that sends the users' vote to a blockchain node and sends the voter the key to encrypt their vote.

- Blockchain System - The actual voting takes place in the blockchain system. The users' vote is sent to the one of the nodes on the system depending on each node's load to ensure a distributed network traffic on the system. Then the node adds the transaction to the blockchain depending on the smart contracts that exist on each node. The smart contracts are the rules that the nodes follow to not only verify but also add the vote in the system.

ii. System Processes:

- Registering to vote - The voter will log in to the E-Voting System using the credentials interacting with the Authentication Server via a website. The system will use private key provided to registered voters by the ethereum wallet. Also an entry is made next to the voters' database entry storing whether user has registered to vote. The system will check all information entered, if it is valid, the voter will be authorized to cast a vote.
- Casting a vote - Voters will choose to vote for one of the candidates through user interface. A specific amount of ether is added to the voters' account which enables them to vote.
- Encrypting votes - After the voter casts the vote, the system will generate an input that contains the voter identification number followed by the complete details of the voter as well as the hash of the previous vote. This way each input and encrypted output will be unique. The encrypted information will be recorded in the block header of each vote cast. The information related to each vote will be encrypted using SHA-256, which is a one- way hash function that has no known reverse to it. Therefore there would be no way voters' information could be retrieved.
- Adding the vote to the Blockchain and counting votes - After a block is created and depending on the candidate selected, the information is recorded in the corresponding Blockchain. Each block gets linked to the previously casted vote. The candidate with the highest amount of ether in their account wins the election.

B. Implementation Results:

Table 1 compares decentralized e-voting and normal voting based on different criteria and gives an overview of both the voting process.

Table 1: Comparative Analysis

Sl.No.	Features	E-Voting	Existing Voting
1.	Verification	Machine and Vote cannot be tampered	Machine and vote can be tampered
2.	Update	One can change vote	Not possible
3.	Authentication	Each user is verified using unique Id	Not possible
4.	Ease of Accessibility	One can vote from anywhere. No need to be physical present at voting area	One need to be present at the vote area
5.	Result calculation	Less time required(approx. hour)	More time required(approx. day)
6.	Live Update	Possible	Not Possible
7.	Technology Used	Smart contract	Logical contract
8.	Cost	One time set up cost	Cost varies on several factor

Table 2 : shows all the contracts being executed and time taken to execute each contract individually

Sl.No.	Contract	Avg Time(ms)
1	Initializes with candidates	125
2	Initializes the candidates with correct values	143
3	Allows a voter to cast a vote	230
4	Throws an exception for invalid candidates	243
5	Throws an exception for double voting	592

The implementation is based on a private network that uses the Ethereum blockchain API. With Ethereum, the computational expense is exhibited in the form of 'gas' which is a unit of measure of a contract. Gas is priced by the node to push the node to the wider chain and this price will be paid to the node that mines that transaction. Therefore, nodes are attempting to maximise profits by determining the worth of a transaction verses the computational cost. Hence, the computational expense is minimised to make a blockchain application viable.

IV.CONCLUSION

The proposed e-voting system is based on the Blockchain technology. Any registered voter will have the ability to vote using any device connected to the Internet. The Blockchain based system will be secure, reliable, anonymous and will help increase the number of voters as well as the trust of people in their governments. The current existing system has large number of issues. Hence, it is vital to have a transparent voting system that must have the least number of obstacles. Considering all these factors, the proposed system is a comprehensive solution that satisfies all the requirements.

REFERENCES

[1] Ahmed Ben Ayed(2017);A Conceptual Secure Blockchain –Based Electronic Voting System; International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3,
[2] Pavel Tarasov and Hitesh Tewari(2017);The Future of E-Voting; IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165 I
[3] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3(2017);An Overview of Blockchain Technology : Architecture,Consensus, and Future Trends; IEEE 6th International Congress on Big Data.
[4] Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander3(2016); Where Is Current Research on Blockchain Technology?—A Systematic Review;PLOS-ONE.
[5] Mahdi H. Miraz1, Maaruf Ali2(2018); Applications of Blockchain Technology beyond Cryptocurrency;Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018

[6] Michael Crosby, Google,Nachiappan, *Yahoo*,Pradhan Pattanayak, Yahoo,Sanjeev Verma, Samsung Research America,Vignesh Kalyanaraman, Fairchild Semiconductor(2015);Blockchain Technology Beyond Bitcoin.
[7] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis (2018); E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy; arXiv:1805.10258v2 [cs.CR]
[8] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, Hyoung Joong Kim(2016); Electronic Voting Service Using Block-Chain; Journal of Digital Forensics, Security and Law.
[9] Aayushi Gupta1*, Jyotirmay Patel2, Mansi Gupta1, Harshit Gupta1(2017); Issues and Effectiveness of Blockchain Technology on Digital Voting; International Journal of Engineering and Manufacturing Science. ISSN 2249-3115 Vol. 7, No. 1 (2017)
[10] Gautam Srivastava1, Ashutosh Dhar Dwivedi2 and Rajani Singh2(2018); Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology.
[11] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson(2018);Blockchain-Based E-Voting System.
[12] Nir Kshetri and Jeffrey voas(2018);Blockchain Enabled E-Voting;www.computer.org/software.
[13] Umut Can Çabuk1, Eylül Adıgüzel2, Enis Karaarslan2(2018); A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems; International Journal of Advanced Research in Computer and Communication Engineering.
[14] Madise, Ü. & Martens, T. (2006). E-voting in Estonia 2005. The first practice of countrywide binding Internet voting in the world. Electronic Voting, 86.
[15] S. Raval, "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology." O'Reilly Media, Inc. Sebastopol, California (2016).
[16] Jason Paul Cruz1,a) Yuichi Kaji2,b)(2017);E-voting System Based on the Bitcoin Protocol and Blind Signatures ; IPSJ Transactions on Mathematical Modeling and Its Applications Vol.10 No.1 14–22.
[17]https://www.google.com/A+Simple+Representation+of+the+Blockchain+Structure+of+each+Candidate+in+e+voting

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details