IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

Blockchain Enabled E-Voting System

SriRaksha S Arun[1], Shibani[2], Spoorthi S[3], Vaishnovi R Kamath[4], Dr. C Vidya Raj[5]

Department of Computer Science and Engineering,

The National Institute of Engineering Mananthavadi Road, Mysuru, India[1,2,3,4,5]

Abstract: The Blockchain-Enabled E-Voting uses a digital-currency analogy where in eligible voters can cast a ballot anonymously using a computing environment. BEV employs an encrypted key, smart biometrics and tamperproof real-time personal ID verification. Blockchain enable the creation of tamper-proof audit trails for voting. The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society which normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected candidate, thus making it an effective way for casting vote in this generation of technology.

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

I. INTRODUCTION

Electronic Voting (E-Voting) is a one of the method of casting votes which uses electronic systems to aid casting and counting votes in an election in cryptography. It secures Multi-Party Computation (MPC) because of the properties such as transparency, decentralization, irreversibility nonrepudiation. In general, two main types of e-voting can be identified:

1. E-voting which is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations)
2. Remote e-voting via the Internet (also called i-voting) where the voter submits their votes electronically to the election authorities, from any location. Blockchain has a large potential when integrated into many areas.

Blockchain Technology: A blockchain is a growing list of records called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp and transaction data and has properties such as durability, robustness, Enhanced security and decentralisation of network. The blockchain database isn't stored in any single location. The records are kept public and easily verifiable. No centralized version of this information exists for a hacker to corrupt.

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

Ether: Ether is a type of crypto token which is a digital bearer asset that fuels the network. Beyond a tradable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the Ethereum network. Just like cash, it doesn't require a third party to process or approve a transaction.

Node Package Manager: The Node Package Manager or NPM is a dependency of globally-installed JavaScript tools, which comes with Node.js. It consists of a command line client, npm and an online database of public and paid-for private packages, npm registry which is accessed via client and are managed by npm, Inc.

Truffle Framework: The Truffle Framework dependency allows to build decentralized applications on the Ethereum blockchain. It provides a suite of tools that allows to write, test and deploy smart contacts to blockchain with the Solidity programming language giving a place to develop client-side application.

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. RELATED WORK

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 decentralised 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. EXISTING SYSTEM

An EVM consists of two units, control unit and balloting unit which are joined by a cable. Balloting unit facilitates voting by voter via labelled buttons while control unit controls the ballot units, stores voting counts and displays the results on 7 segment LED displays.
An EVM can record a maximum of 3840 votes and can cater to a maximum of 64 candidates. There is provision for 16 candidates in a single balloting unit and up to a maximum of 4 units can be connected in parallel. As soon as a particular button on the balloting unit is pressed, the vote is recorded for that particular candidate and the machine gets locked. It is not possible to vote more than once by pressing the button again. This way the EVMs ensure the principle of "one person, one vote".
The drawbacks are – Expensive; Time consuming; Too much paper work; Errors during data entry; Loss of registration forms; Short time provided to view voter's register; Number of voters end up being locked out from voting; Security issues

IV. E-VOTING SYSTEM

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 decentralised 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.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

V. DESIGN AND IMPLEMENTATION

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.

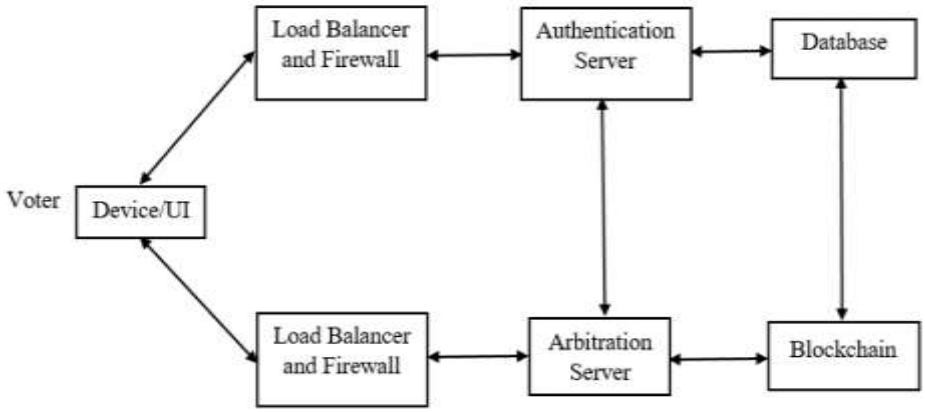

Fig 1: System Architecture

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.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

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.

Table 2: Contract Execution Time

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

Table 3 evaluates average time taken and cost that is gas used to deploy the contracts. Each time a contract is deployed, its execution time and cost of deployment that is gas used is noted. Five observations are taken and average of these values are calculated. Execution time varies at each deployment but the gas used for deployment always remains the same.

Table 3: Contract Deployment

Contract	Time(ms)	Cost(gas)
1	1333	746943
2	1111	746943
3	1001	746943
4	1135	746943
5	1323	746943
Average	1180.6	746943

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.

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

VI. 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]. Nir Kshetri and Jeffrey Voas, "Blockchain-Enabled E-Voting", in IEEE Software, DOI: 10.1109/MS.2018.2801546, JULY/AUGUST 2018
[2]. Fridrik .P. Hjalmarsson, Gunnlaugur .K. Hreidarsson, "Blockchain-Based E-Voting System", in School of Computer Science Reykjavik University, Iceland, JUNE 2018
[3]. Ahmed Ben Ayed, "A Conceptual Secure Blockchain- Based Electronic Voting System", in International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, MAY 2017
[4]. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy", in ISG-SCC, Royal Holloway, University of London, Egham, United Kingdom, JULY 2018
[5]. Gaby G. Dagher, Praneeth Babu Marella, Matea Milojkovic and Jordan Mohler, "BroncoVote: Secure Voting System using Ethereum's Blockchain", DOI: 10.5220/0006609700960107, in Proceedings of the 4th International Conference on Information Systems Security and Privacy, pages 96-107, ISBN: 978-989-758-282-0, 2018