Election System Using Blockchain Technology

Mr. Aviraj Hanumant Shinde [1], Mr. Chaitanya Suryakant Urane[2], Mr. Akash Shrimant Waghmare[3], Mr. KiranKumar Vikram Kalel[4],Prof. S. R.Vasekar [5], Prof. S. D.Pandhare [6]

[1, 2, 3, 4, 5, 6]Dept of Computer Science & Engineering

[1, 2, 3, 4, 5, 6]SMSMP Institute of Technology & Research, Akluj, India

Abstract- *Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. However, there remain challenges to achieve wide spread adoption of such systems especially with respect to improving their resilience against potential faults. Blockchain is a disruptive technology of current era and promises to improve the overall resilience of e-voting systems. The idea presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for e-voting. The proposed scheme confirms to the fundamental requirements for e-voting schemes and achieves end-to-end verifiability. The paper presents details of the proposed e-voting scheme along with its implementation using multichain platform. The paper presents in-depth evaluation of the scheme which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme.*

Keywords- E-voting, Online Voting System

I. INTRODUCTION

Elections are fundamental pillar of a democratic system enabling the general public to express their views in the form of a vote. Due to their significance to our society, the election process should be transparent and reliable so as to ensure participants of its credibility. Within this context, the approach to voting has been an ever evolving domain. This evolution is primarily driven by the efforts to make the system secure, verifiable and transparent Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions.

A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Each block is assigned a cryptographic hash (which may also be treated as a finger print of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domain.

Bitcoin remains the most distinguished application of blockchain however researchers are keen to explore the use of blockchain technology to facilitate applications across different domains leveraging benefits such as non-repudiation, integrity and anonymity. In this project, we explore the use of blockchain to facilitate e-voting applications with the ability to assure voter anonymity, vote integrity and end-to-verification. We believe e-voting can leverage from fundamental blockchain features such as self-cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records. The blockchain technology can play key role in the domain of electronic voting due to inherent nature of preserving anonymity, maintaining decentralized and publicly distributed ledger of transactions across all the nodes.

II. RELATEDWORK

An online voting system for Indian election is proposed for the first time in this paper. The proposed model has a greater security in the sense that voter high security password is confirmed before the vote is accepted in the main database of Election Commission of India. The additional feature of the model is that the voter can confirm if his/her vote has gone to correct candidate/party.[1]

The voting system is the backbone of every democracy and organization. The voting system has experienced many efficient changes in the past few decades. There are various voting techniques used such as Paper Ballot Voting System, E-Voting System also known as Electronic Voting System, Internet Voting System, SMS and Miss Calls Voting System.[2]

The main objective of the democracy is “vote” by which the people can elect the candidates for forming an efficient government to satisfy their needs and requests such

that their standard living can be improved. In developing countries like "INDIA" the election commission follows manual voting mechanism which is done by electronic voting machine. This machine is placed in the poll booth centre and is monitored by higher officials. [3]

Building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge for a long time. In this work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. [4]

III. PROPOSEDSYSTEM

The proposed e-voting system architecture is presented in following Fig. 1 and has been divided into several layers to achieve modular design. These layers are described below:

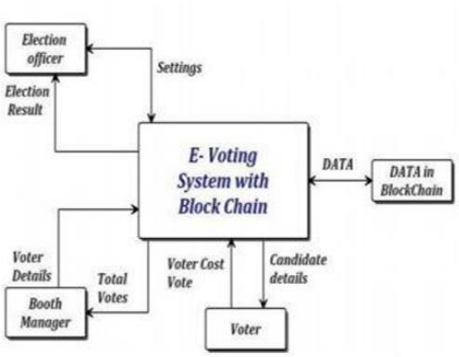

Fig. 1 System Architecture

User Interaction and Front-end Security layer is responsible for interacting with a voter (to support vote casting functions) and the administrator (to support functions pertaining to administering the election process). It encapsulates two key functions i.e. authentication and authorization of the users (voters and administrators) to ensure that the access to the system is restricted to legitimate users in accordance with the predefined access control policies.

A number of different methods can be applied to achieve this function ranging from basic username/password to more advance such as fingerprinting or iris recognition. Therefore these are rendered specific to individual implementation of the proposed architecture. Overall, this layer serves as the first point of contact with the users and is responsible for validating user credentials as governed by the system-specific policies.

Access Control Management layer is envisaged to facilitate layer 1 and layer 3 by providing services required for these layers to achieve their expected functions. These services include roles definition, their respective access control policies and voting transaction definitions. The role definition and management provides core support for the access control functions implemented by layer 1 whereas the voting transaction definitions support the blockchain based transaction mapping and mining performed at the layer 3. Overall, this layer enables a coherent function of the proposed system by providing the providing the foundation required by individual layers.

IV. METHODOLOGY

The proposed system involves a client server architecture integrated with a block chain system. The minimum requirement needed by a voter is a smartphone or a computer. If these are not met alternate arrangements such as pop up cyber cafes and computers at public buildings must provide access to disadvantaged voters.

Architecture Shown below is the network architecture of the proposed system.

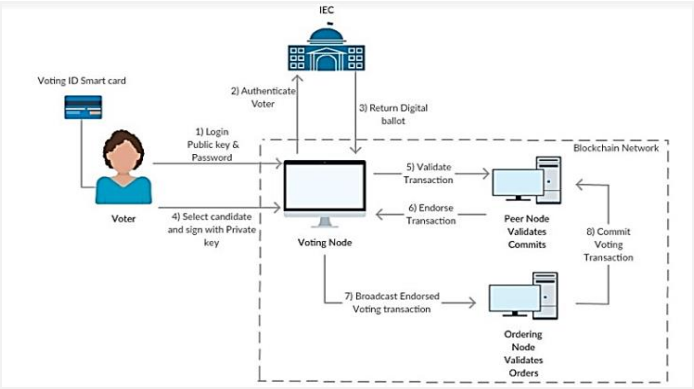

Fig. 2 Network Architecture of Proposed System

The above Fig. 2 shows how the user interacts with the different parts of the system. The system will be explained in two parts – explaining the functionality of each part and the processes associated with the system.

Parts of the system: main parts to the system. Each of them will be explained in detail below.

Voters: The voter must have a smartphone, laptop or any device with a browser and a front facing camera. The user must also have an internet connection to register and vote as well. If the user does not have a computer or an internet connection, he/she could go to a public building such as a library or a school which does have computers to register to

vote. These could be kept open all day during voting registration and voting days to ensure people with low sources of income do not get left out.

Election Authority (**EA**): The election authority is responsible for tallying the votes

Authentication Server: The Authentication Server is a traditional centralized web server. It has a backend database connected to it which has the information of all the citizens in the country. This system is used by people to register to vote for their elections. People create login accounts when they register. It also creates accounts on the blockchain system for the users when they vote. The blockchain account is used by the Arbitration Server to vote for a candidate of the user's choice. The AS also authenticates the token provided to the Authorization Server by the user while voting.

Arbitration Server: The Arbitration Server acts as an intermediary between a user and the Blockchain voting system. It verifies the user while voting using the Authentication Server. The AR is a blockchain thin client that sends the users vote to a blockchain node. It also sends the user the key to encrypt their vote. The AR sends the users vote to the appropriate node to be added to the blockchain. The user can verify their vote using the AR as an intermediary.

Blockchain System: The blockchain system is the system on which the actual voting takes place. The users' vote is sent to the one of the nodes on the system depending on the load on each node. The node then 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. Each node follows the smart contract to verify the vote. The blockchain is a private system and is not accessible to the public directly. The system will currently have node server in each state to ensure distributed network traffic on the system.

The Processes in the System: The process of voting has two steps in the old process, i.e. registering to vote and the process of voting itself. This is an important step where the user can get a confirmation of their vote. The other steps include counting the votes by the organizer and recounting in case of any discrepancies.

Registering to Vote: The process of registering to vote begins with the user interacting with the Authentication Server via a website. The AS contains information about voters in a database. The user enters his/her Personally Identifiable Information (PII) and scans supporting documentation to upload into the system along with an email address. The users' picture is also taken for verification. If the information is verified and is correct, the user is allowed to create an account. The user enters a username of their choice and a password to log in If the users' information cannot be verified, he/she is not allowed to create an account.

Voting: The process of voting is a multi-step process. It involves verifying your identity with the AS and then voting using the AR. On the day of voting each candidate is given an account on the blockchain system so they can get votes. During voting day, the user logs in to the authentication server using the username and password created in the previous step. An image of the user is taken to ensure that the user is the owner of the account. This image is compared with the image taken during registration.

Verifying the Vote: The process of verifying the vote depends on the type of election it is. Some elections allow for interim results and some do not. In either case the voter must get a confirmation that his/her transaction has been approved by the blockchain system. In case of the election that allows interim results, one of the nodes of the blockchain could be made publicly accessible.

Counting Votes: The process of counting votes of a candidate can be very simple. Each voter has a fixed amount of ether or currency value that they use to vote for a candidate of their choice. The candidate with the highest amount of ether in their account wins the election. For users who abstained from voting, their ether will be sent to an Abstain Account. This ensures their vote does not get misused.

V. RESULT ANDDISCUSSION

E-voting (also known as e-voting) is voting that uses electronic means to either aid or take care of casting and counting votes.

Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results.

A worthy e-voting system must perform most of these tasks while complying with a set of standards established by regulatory bodies, and must also be capable to deal

successfully with strong requirements associated with security, accuracy,integrity,swiftness, privacy, auditabilit y, accessibility, costeffectiveness, scalability and ecological su stainability.

Electronic voting technology can include punched cards, optical scan voting systemsand specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.

In figure 3 shows the login window and after successful login with credentials he/she will get a dashboard window followed by all other windows like Voter List, Candidate to be selected, Candidate List, Convassing Report (Result)

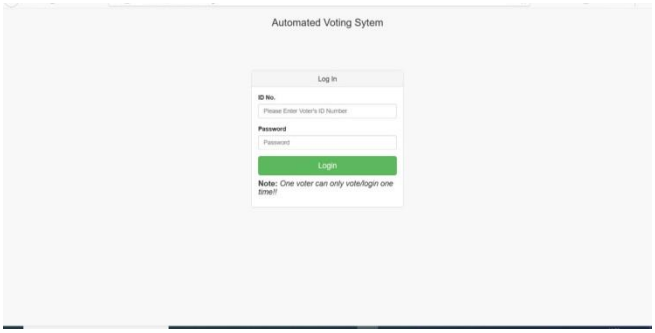

Fig 3. User Login

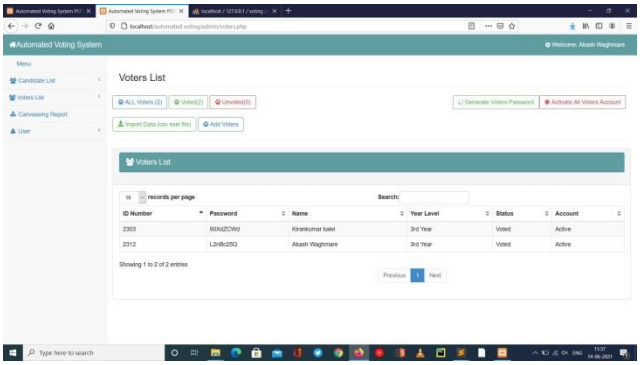

Fig 4. Voter List

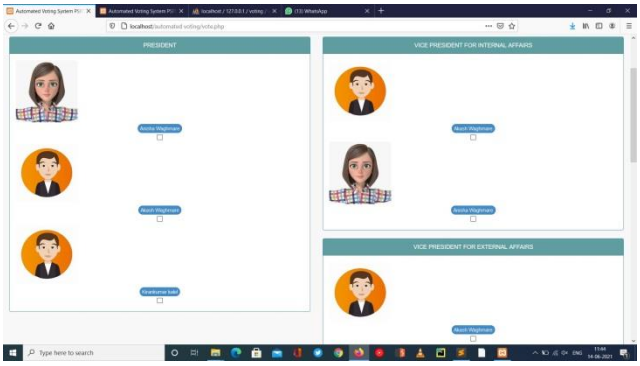

Fig 5. Candidate to be Selected

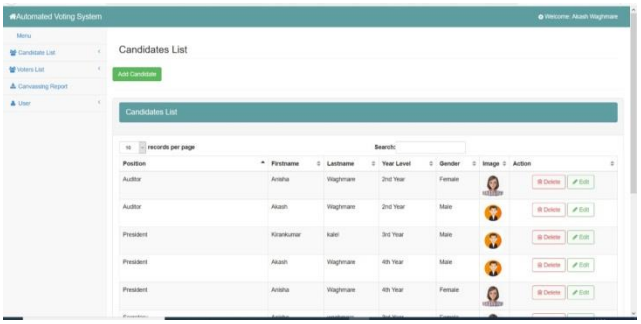

Fig 6. Candidate List

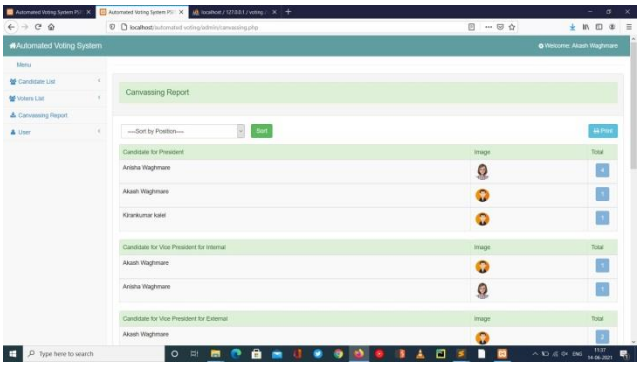

Fig 7. Convassing Report

VI. REQUIRMENTANALYSIS

Hardware requirement specification:

- Hard Disk : At least 20 GB
- Processor : More than 1GHz
- RAM : 512 MB

Software requirement specification:

- Operating system : windows and linux based system
- Database : MySQL DBMS
- Server : Xampp Server
- Programming language : PHP, JAVA

VII. CONCLUSION AND FUTURESCOPE

In this way the proposed approach has been implemented with multi-chain and in depth evaluation of approach highlight its effectiveness with respective to achieving fundamental requirements for e-voting scheme.

Scope of application:

The Same system can be extended to perform the function of counting the number of votes casted and announcing the results immediately.We can include an

administrator mode in which the user details can be updated dynamically through the application only .In near future we can even implement the system in mobile phones. The user can access the website through mobile phone and the vote.

REFERENCES

[1] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa and G. Hjalmtysson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco.

[2] Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers –Plymouth University Andrew Barnes, Christopher Brake and Thomas Perry, "Digital Voting with the use of Blockchain Technology," [Nov. 20, 2018] The Economist.

[3] Zhang, S.; Wang, L.; Xiong, H. Chaintegrity: "Blockchain-enabled large-scale e-voting system with robustness and universal verifiability". Int. J. Inf. Secur. 2020, 19, 323–341.

[4] P. Tarasov and H. Tewari, School of Computer Science and Statistics, Trinity College Dublin, University of Dublin, Ireland "The Future of E-voting," IADIS International Journal on Computer Science and Information Systems, vol. 12, no. 2, pp. 148-165