International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

An Analysis on Hyperledger based Secure E-Voting

Priyanka S[1], G Maria Kalavathy[2]

[1]Student, Dept. of Computer Science and Engineering, St Joseph's College of Engineering, Chennai, India
[2]Head of Department, Dept. of Computer Science and Engineering, St Joseph's College of Engineering, Chennai, India

---

Abstract - *Voting plays a vital role in choosing of government authorities to take up decisions and also a representative on behalf of the people to express their voice .As years passed it was difficult to handle the centralized voting system and to make it more transparent, anonymous, reliable and secured, for preventing data change and multiple vote casting for a single id. Even in e-voting, the electronic medium of voting has lots of disadvantage such as physical attack, mis using the input keys used to cast vote, black voting and no transparency in the voting process. As of from a voter point of view it as to be assured and know the vote reaches safely and secured. Presently, various researches are being conducted to make a secured and transparent voting system to overcome the issues of anonymity and security issues. In decentralized system, the purpose of the voting process is to make it transparent, simple, secure and anonymity for user interface. This paper provides an E-voting system that are used to manage the voting system and its challenges using a private blockchain Hyperledger in a highly secured manner and medium of voting is through mobile application.*

Key Words: **Blockchain, Hyperledger, Smart Contract, Voting. Secure Voting, Mobile Voting**

1. Introduction

Electronic Voting (E-Voting) is a one of the ways to cast votes by the electronic systems being built to cast and counting of votes in an election using the cryptography concept. It secures the system since its properties such as transparency, decentralization, irreversibility non-repudiation is the various featured provided by the blockchain to secure the system. In general, there are two main types of e-voting namely:

1. E-voting is the method of monitoring physically by the representatives of governmental or electoral authorities e.g. Electronic voting machines at polling booth
2. Remote electronic voting system through Internet in this system the voter can cast and submit their votes electronically to the election authorities, from anywhere since it is be managed when it comes to large number systems of process and it can be made secured through blockchain.

Trust, Security, Autonomy and transparency are drawbacks being faced in present time. We are forced to trust the banks for securing our money for our transactions and receive for our purpose. When it comes to bank the third party's dependence is mostly common for ensuring our privacy and secured based upon terms of our data. So, the trust and dependence on intermediaries is compulsory. These issues can be resolved using blockchain. The applications that are being built using blockchain technology are decentralised and being owned by multiple persons and no one can alter or upload any data in the blockchain without the knowledge of ownership owned member. If anyone tries to alter or upload any data that has to be accepted by the interconnected people. So, blockchain can be completely trusted and it provides the utmost security to data being transferred and received. The ownerships keep on changing as the data is being transmitted to each segment and no single authority is controlling the function, anybody can join in the network who has being authenticated to join the network, based on the request and also other factors like type of blockchain i.e public, private and consortium.

Blockchain will read and write only in database once if the data being written in blockchain based database it cannot be altered or changed at any cause. This kinds of advantages of blockchain can be very used in building a e-voting system since it manages huge amount of data also it provides security for each and every vote so it can be also said has highly secured system when the system is build using blockchain. It involves both the encryption and decryption of data. By this it enables to send the data more securely over the network even if it is unsecured. Encryption is using key to a plain text for converting it into cipher text and decryption is vice versa process of encryption.

1.1 Existing System

An Electronic Voting Machine has two units, one is control unit and the other is balloting unit which are combined by a cable. Balloting unit facilitates voting process by the voter through the provided labelled buttons. The control unit controls the ballot units which stores the casted vote, the voting counts and shows the results on 7 segment LED displays. An Electronic Voting Machine can record and collect a maximum range of 3840 votes and can cater to a maximum range of 64 candidates. There is provision for 16 candidates in a single balloting unit and can extend up to a maximum of 4 units which can be connected in parallel. As soon as a specific button on the balloting unit is being pressed, the vote is recorded for that particular candidate and the machine gets locked up. It is not possible to cast vote

more than once by pressing the button again. This way the Electronic Voting Machine ensure that the concept of "one person, one vote". The drawbacks are that is expensive and more time consuming. Also, too much paper work, Errors during data entry, loss of registration forms, very short time is being provided to view the voter's register, number of voters end up being locked out from voting and security issues.

1.2 Challenges of Existing System

Electronic Voting (E-Voting) is a one of the ways to cast votes by the electronic systems being built to cast and counting of votes in an election using the cryptography concept. But these systems possess following challenges as described below.

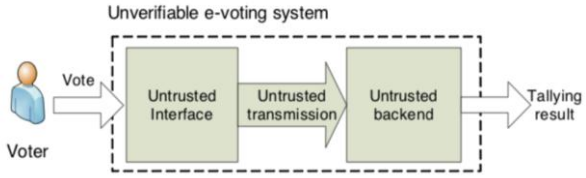

Fig 1: Typical E-Voting Process

1. Physical method of voting

The physical method that is casting the vote through a physical machine (EVMs) which may get failure when multiple votes are being recorded. There are even chances of vote missing, physical attack which does not provide a secured way for voting and even no high security for each stages of the voting process. Even after casting the vote there are no guarantee that casted vote is being highly secured such that once the data received can't be altered in case of physical manner of voting through EVMs. This is one of challenge that can be rectified using blockchain since it has the feature of providing high secured database and security to each stages of the voting process and to the vote.

2. Privacy

The vote that has been casted has be known only to the voter (particular individual) and also the details that are being furnished. The third-party involvement is strictly restricted. So, the voting process and details of voter are being secured.

3. Transparency

The internal process that is being made is has to be known to the voter. The voter has to know the details like time and date of casting vote for their particular id number (Time stamp). Each stages of voting process from the registration till the vote reaching to the ballot the process has to be known by the voter.

4. Speed

In this high technology world, it must ensure that results are declared within few hours of election procedure ends which means that the counting of vote is very easier compared to the previous years.

5. Low cost

Cost is one of the major factors to be analysed before building any system design. The System must be cost efficient, reliable and require maintenance as possible to rectify if any error occurs.

6. Easy to use

Elections has to serve the entire public. So, it must be designed in such a way that it can be used with minimal training and some technical skills to manage for large scale voting process.

7. Scalable

Election means to serve for a large scale of population. So, it must be flexible enough to work at large scale. And also record all the data without any data loss.

2. Proposed System using Hyperledger

In the proposed system an architecture for client server integrated with Hyperledger blockchain which provides the fundamental requirements like integrity, security, auditability and sustainability for a building trustable E-Voting platform. But other requirements like authentication, authorization and confidentiality has to be bolted-on over the blockchain platform to provide an end-to-end solution for E-Voting. Accordingly, a wrapper has to be built around the blockchain network using microservices to expose only the services through which data flow is restricted. As E-Voting is a public domain application, necessary guard rails have to be built upon the user interface to the blockchain networks. Thus, we are proposing a three-tiered architecture for building a trustable E-Voting platform that can provided over the mobile interface for the voters to cast their votes securely. It takes very less time to cast the vote and in secured manner.

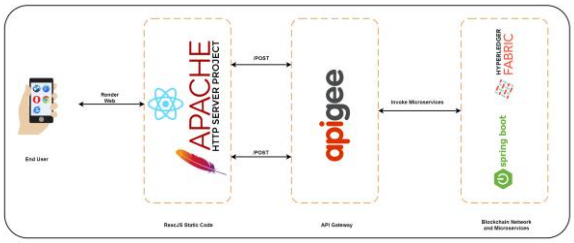

Fig 2: Proposed 3-tier architecture

2.1 Blockchain

The blockchain is a series of time-stamped immutable data records of which is managed by a cluster of nodes like a server and is not owned or manged by any single entity. Each of the data blocks are secured and linked using a cryptographic method called chaining. Which means there is no central authority for the blockchain network. The

information in the immutable ledger is visible for anyone as it is shared. Hence, any business login that is built upon blockchain has transparency and all are accountable for their actions involved. A shared distributed ledger is the heart of a blockchain network which records all the transactions that occurs on the network.

A blockchain ledger is decentralized because, the data is replication across all the nodes and collaborate among themselves to ensure integrity. In addition to this, blockchain allows information's to be recorded in append only mode. Once a transaction has been added to the ledger it cannot be modified which is guaranteed by cryptographic techniques. This property is called "immutability" and makes it simple to determine the integrity of information because participants or nodes in the network can be sure that no information has not been changed post the inception of the fact. That's why blockchains are sometimes called as systems of proof.

2.2 Features of Hyperledger

The blockchain distributes ledger technology primarily provides following features,

1. Distributed – All the systems within the network have a copy information for complete transparency
2. Immutable – All the records or ledgers within the network that are validated become irreversible and can't be tampered
3. Timestamped – All the transactions that happen within the network are timestamped
4. Secure – All the records within the network are encrypted
5. Unanimous – All the systems within the network consensus to the validity of each information present within the network
6. Programmable – The blockchain network can be programmed to meet the business requirements

2.3 Choosing Right Block Chain

Primarily there are three types of blockchain that are available in the market,

1. Public blockchains like Bitcoin and Ethereum
2. Private blockchains like Hyperledger and R3 Corda
3. Hybrid blockchains like Dragon chain

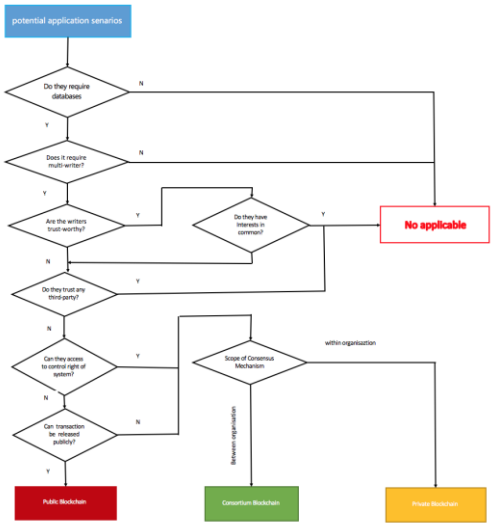

Fig 3: Flow chart for choosing Blockchain type

In order to choose the right blockchain platform for E-voting, we have to follow the simple decision tree. Accordingly, based on the decision tree from, a public blockchain like Hyperledger would meet the requirement for building a trustable platform for E-voting.

2.4 Block Chain Network Architecture Design

The core Business Network Achieve (BNA) is deployed using the Hyperledger composer. The business network definition primarily consists of a Model (cto), Scripts (js), ACLs (acl) and a Query (qry) file. The model files define the assets, participants and transactions. The scripts file defines the transaction functions. The ACL files define the access control rules with in the network. The query files define the querying definition for the smart contract. The data points defined in the model is shown in the Fig 5.

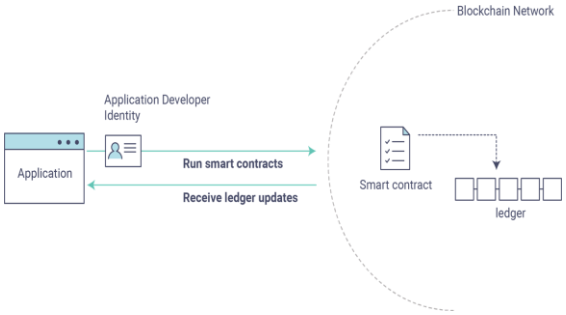

Fig 4: BNA Network Design

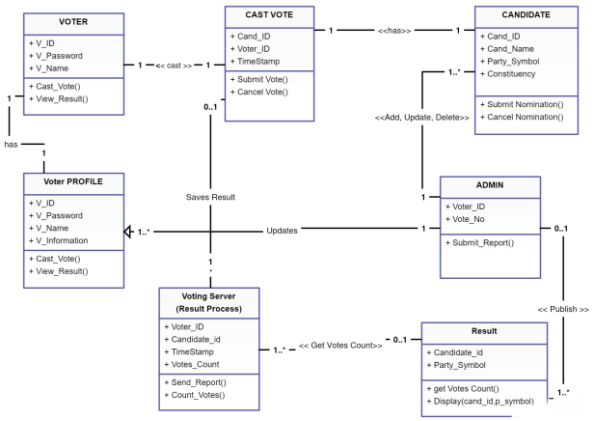

Fig 5: BNA Data Points

2.4 API Management

Apigee, helps to build API proxies—RESTful, HTTP-based APIs that interact with backend microservices services. API proxies provides capability to secure API calls, control traffic, mediate messages, handle errors, analyze API traffic data, make money on the use of APIs, protect against bad bots, and etc. Apigee helps to Design, secure, analyze, and scale APIs with visibility and control. It also helps to implements 2-way-ssl for application authorization by which strong trust is established between the systems. API management also Implements OAuth for application authentication.

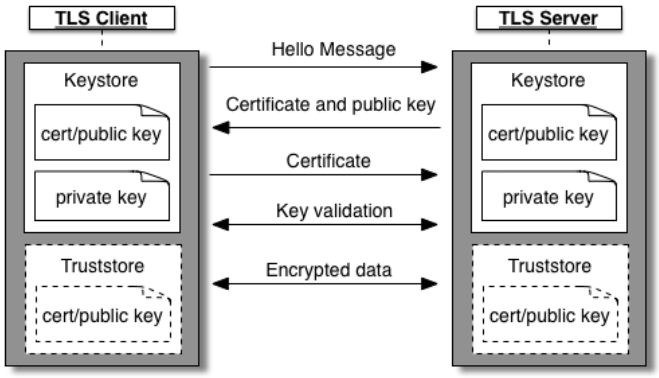

Fig 6: 2-Way-SSL

2.5. Mobile Application

A mobile application has been developed for iOS platform. iOS has inbuilt security because of which application can't be tampered. Feasibility of Android has been studied; but rooted phones have the capability to tamper the application. 2-way-ssl has been implemented in the application to ensure there is a trusted communication between the application and APIs. OAuth based access delegation is used when accessing the APIs to ensure no password or confidential information's are passed. End to end data encryption is used both at rest and during at transit. Application is built using ReatJS which provides a rich user experience.

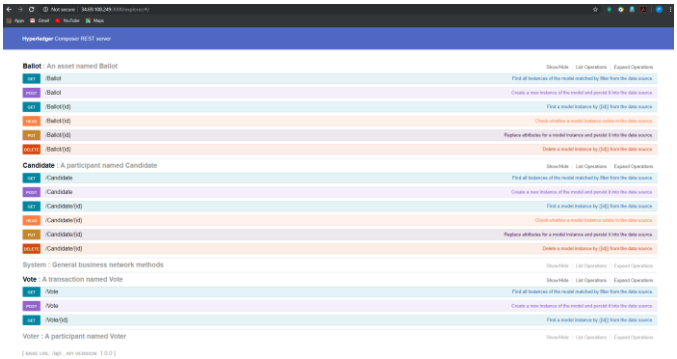

Fig 7: API Output

Fig 7: Mobile Application welcome screen

3. Conclusions

The proposed e-voting system is based on the Blockchain technology by using the web interface method. An eligible registered voter will have the ability to cast their vote using any device at any location connected to the Internet. The Blockchain based system will provide secure, reliable, anonymous. Also help increase the number of voters as well as the trust of people in their governments and the vote cast. The current existing system has multiple issues. Hence, it is one that have a transparent voting system. Considering all these factors, challenges the proposed system is a best solution that satisfies all the Requirements with less cost.

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 & ItsApplications (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] Harsha V. Patil , KanchanG. Rathi, malati V.Tribhuwan", in International Conference on International Research Journal of Engineering and Technology.

[6] SriRaksha S Arun1, Shibani2, Spoorthi S3, Vaishnovi R Kamath4, Dr. C Vidya Raj5, "Blockchain Enabled E-Voting System", International Journal of Advanced Research in Computer and Communication Engineering