EFFCTIVE IN-HOUSE VOTING AND IMPLEMENTATION USING BLOCK-CHAIN VERIFICATION

S. Gopi[1], B.Giridharan[2], R. Mohamed Rifoy[3], S. Sivachidambaram[4], S.Yuvaraja[5]

[1] Assistant Professor, Department of Information Technology, Panimalar Engineering College, Chennai, Tamil Nadu, India.

[2,3,4,5]Student, Department of Information Technology, Panimalar Engineering College, Chennai, Tamil Nadu, India.

***

Abstract - *In Ballot based Voting is present, but still there is no system to avoid Proxy Casting and Recasting is implemented. We do not have an option to see our casted Vote also. There is no security in this current application. In a novel electronic voting system based on Block-chain that addresses some of the limitations in existing systems and evaluates some of the popular block-chain frameworks for the purpose of constructing a block-chain-based e-voting system, we integrate Aadhar card linked Mobile number is used for OTP Generation, only then the voter can cast the vote, This system will avoid Proxy casting and Recasting.*

***Key Words*: Block chain, Aadhar card, OTP generation, Block chain framework, Proxy Casting and Recasting.**

1. INTRODUCTION

Electronic voting systems have been the subject of active research for decades, with the goal to minimize the cost of running an election, while ensuring the election integrity by fulfilling the security, privacy and compliance requirements [1]. Replacing the traditional pen and paper scheme with a new election system has the potential to limit fraud while making the voting process traceable and verifiable [2]. Block Chain is a distributed, immutable, incontrovertible, public ledger. This new technology has three main features: (i) Immutability: Any proposed "new block" to the ledger must reference the previous version of the ledger.

This creates an immutable chain, which is where the Block Chain gets its name from, and prevents tampering with the integrity of the previous entries. (ii) Verifiability: The ledger is decentralized, replicated and distributed over multiple locations. This ensures high availability (by eliminating a single point of failure) and provides third-party verifiability as all nodes maintain the consensus version of the ledger. (iii) Distributed Consensus: A distributed consensus protocol to determine who can append the next new transaction to the ledger. A majority of the network nodes must reach a consensus before any new proposed block of entries becomes a permanent part of the ledger.

1.1 Scope

The main scope of the project is to verify the casting of the voter has registered correctly. We deploy Block chain for this concept. The main advantage of the project is to provide an opportunity to cast their vote from home itself.

1.2 Objective

The objective of the project is to protect the people voting using Block chain technology. The main objective of the project is to avoid Proxy casting and Recasting.

2. LITERATURE SURVEY

2.1 Performance Assessment of an Imperceptible and Robust Secured E-Voting Model

In this paper, we present the performance assessment of an imperceptible and robust secured stegano-cryptographic model of electronic voting. The Performance analysis was achieved based on the degree to which the model meets the generic and functional requirements of secured evoting system: authentication, integrity, confidentiality and verifiability as well as other functional security requirements of a secured voting using fivepoint psychometric analysis. The result of the quantitative evaluation of the model assert that the model possessed capacity to guarantee and validate voter's for who they said they are, guarantees the integrity of elections, ensures privacy of the voters, guarantees the confidentiality of the vote and provide mechanism for fraud detection after the electioneering process in developing country where digital divide is significant.

2.2 Towards a Fraud Prevention E-Voting System

Election falsification is one of the biggest problems facing third world countries as well as developed countries with respect to cost and time. In this paper, the guidelines for building a legally binding fraud-proof Electronic-Voting are presented. Also, the limitations are discussed.

2.3 Secure E-Voting System

With the rapid growth of the internet and technologies, E- voting appears to be a reasonable alternative to conventional elections. Various Information Security and Privacy Technologies including cryptography, steganography, and combination of both have been formulated in literatures to make democratic decision through e-voting systems to be fair and credible. In practice, different data cryptographic standards like Data Encryption Standard (DES), and Advanced Encryption Standard (AES), Rivest, Sharim and Adleman (RSA) is needed to ensure the security of the votes and maintain the confidentiality and integrity. Homomorphic encryption scheme is used to encrypt all the votes and perform the calculation of the votes without revealing any information about them.

Current research focuses on designing and building "electronic voting protocols" such as zero knowledge authentication protocol, based on Diffie-Hellman key exchange algorithm, to ensure a mutual authentication between the election authority server and the voters. This thesis proposes a new protocol that covers and maintains the security requirements which are: (authentication, privacy, integrity, Anonymity and non-repetition) of the voting process.

2.4 Online voting application using Ethereum Block Chain

Voting is an important part of the administration of a country. Votes are still being carried out by physically going to voting booths. This process doesn't guarantee security and cases of tampering has been observed. This paper aims at removing these issues in the voting process by making it online and using the technology, Block Chain. Block Chain uses encryption and hashing to make every vote secure. In this case, one vote is considered as a transaction. A peer to peer network is created to create a private Block Chain that share this distributed ledger having voting transaction. The application is designed in such a way so that the intricacies of the underlying architecture are hidden from the user. Each voter is uniquely identified by Government approved Aadhar number. The application makes use of this number to make sure that each voter gets only one chance to vote. When the vote gets submitted as a transaction then all the peers get synch up. Since each peer is associated with a public and private key the votes are encrypted and hashed and added to the Block Chain to increase security and form a chain of blocks. Votes cannot be tracked back to the voter. In this paper, a peer to peer network is created having minimum three peers. Since voting is made online, it is expected that this paper will increase the voter turnouts. The scalability of the Block Chain application depends on the secondary memory limit of the peer.

2.5 Secret Suffrage in Remote Electronic Voting Systems

Can the principle of secret suffrage be ensured when voters are offered the possibility to cast their votes using internet voting? With the steady introduction of different forms of remote electronic voting since 2000, it has become apparent that internet voting fails at providing the privacy guarantees offered by traditional paper-based voting systems. Against this assumption, the current proposal suggests reviewing the traditional configuration of the principle of vote secrecy. With this in mind, the proposal will: (1) assess current accepted standards on voters' anonymity for traditional and internet-based voting systems; (2) evaluate the core elements of lawful relaxations to the principle of secret suffrage, and especially those traditionally associated to different forms of remote voting, and assess whether they can be applied to internet voting; and (3) study how current technical developments in the field of elections (and more broadly, in the field of e-governance and e-democracy) may result in further relaxations of the principle of secret suffrage in the future. Overall, the goal of the proposal is to approach the principle of secret suffrage against the specificities of internet voting and, instead of evaluating electronic voting systems using traditional standards for voters' privacy and anonymity, evaluate how specific proposals aimed at ensuring voters' secrecy in internet voting comply with the very end that the principle of secret suffrage is aimed at protecting, namely: voters' freedom.

2.6 The Council of Europe and e-voting

When the Council of Europe started to deal with the subject of electronic voting in 2002, the impact of its work was not foreseeable. What followed, however, was basically a "success story": The Recommendation on legal, operational and technical standards for e-voting (Rec(2004)11), which was adopted by the Council of Ministers on 30 September 2004, has been the most relevant international document and reference regarding e-voting for a decade. Since 2010, the role of the Council of Europe with regard to e-voting has shrunk. Nevertheless various Member States expressed the desire to further review the Recommendation in the forthcoming years. Following an informal experts' meeting in Vienna on 19 December 2013, the Committee of Ministers was confronted with the suggestion to formally update the Recommendation in order to keep up with the latest technical, legal and political developments. The forthcoming Review Meeting on 28 October 2014 may help set the course for future e-voting activities of the Council of Europe.

2.7 Enhancing Electronic Voting Machines on the Example of Bingo Voting

The main purpose of cryptographic voting schemes is to provide transparency while protecting ballot secrecy and to enable a fast tally. In this paper, we address three major issues of cryptographic voting schemes. First we discuss the problem of secrecy and coercion resistance in the situation of a corrupted voting machine. While hard to obtain in general, we propose and analyze a novel approach that uses encapsulated design and minimizes the information that can compromise ballot secrecy. The second issue we address is the assumption that an adversary does not know which receipts are checked and the problem of receipt stealing. Many voting schemes with receipts share this vulnerability. We provide a solution that increases protection of each vote and which can be generalized for voting schemes that use computers to form the receipt. The last issue discussed in this paper is the question of how an election can be contested. For this, an error or a manipulation must not only be detected but also proven. While the problems and solutions are described for Bingo Voting, we argue that the problems are shared by many cryptographic voting schemes and that the solutions presented in this work give insight in the prerequisites needed for a secure election.

3. SYSTEM DESIGN AND IMPLEMENTATION

The overall architecture describes about, First the admin will register the user and candidate details with their aadhar number on user interface. Those details will be stored on data base.

3.1 ARCHITECTURE

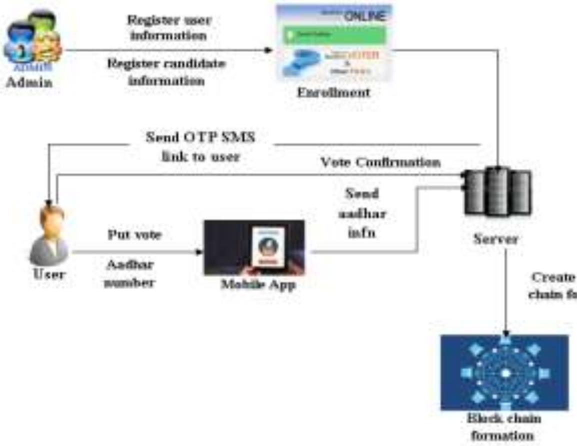

Fig -1: Architecture Diagram

From user side they have a mobile application on their mobile. They will login into application and give their aadhar number on that application after system will send OTP to the registered mobile number. User has to share that OTP for confirmation of vote. Finally vote details will create as a block and stored on block chain.

3.2 ABOUT BLOCK CHAIN

The Block Chain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something greater, and the main question every single person is asking is: What is Block Chain?

What is Block Chain Technology?

"The Block Chain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

How Does Block Chain Work?

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the Block Chain.

Information held on a Block Chain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The Block Chain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

Block Chain Durability and robustness

Block Chain technology is like the internet in that it has a built-in robustness. By storing blocks of information that are identical across its network, the Block Chain cannot:

1. Be controlled by any single entity.
2. Has no single point of failure.

3.5 LANGUAGE SPECIFICATION

Solidity

Solidity is a brand new programming language native to Ethereum, the second largest crypto currency by market capitalization, initially released in 2015. Ethereum is not only a crypto currency capable of storing value or making payments, but a fully-fledged platform for creating what's known as a **smart contract**.

"Solidity is known as a contract-based, high-level programming language. This platform has similar syntax to the scripting language of JavaScript. Solidity as a programming language is made to enhance the Ethereum Virtual Machine. Solidity is statically typed scripting language which does the process of verifying and enforcing the constraints at compile-time as opposed to run-time."

3.5.1 BACK END

WHAT IS MYSQL?

MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation. MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by MySQL AB. MySQL AB is a commercial company, founded in 1995 by the MySQL developers. It is a second generation Open Source company that unites Open Source values and methodology with a successful business model. The MySQL Database Software is a client/server system that consists of a multi-threaded SQL server that supports different backend, several different client programs and libraries, administrative tools, and a wide range of application programming interfaces (APIs).

MySQL Cluster Overview

MySQL Cluster is a technology that enables clustering of in-memory databases in a shared-nothing system. The shared-nothing architecture enables the system to work with very inexpensive hardware, and with a minimum of specific requirements for hardware or software.

MySQL Cluster is designed not to have any single point of failure. In a shared-nothing system, each component is expected to have its own memory and disk, and the use of shared storage mechanisms such as network shares, network file systems, and SANs is not recommended or supported.

3.5.2 JSON

JSON (JavaScript Object Notation) is a lightweight format that is used for data inter-change . It is based on a subset of JavaScript language (the way objects are built in JavaScript). As stated in the MDN, some JavaScript is not JSON, and some JSON is not JavaScript.

JSON is built on two structures:

- A collection of name/value pairs. In various languages, this is realized as an object, record, struct, dictionary, hash table, keyed list, or associative array.
- An ordered list of values. In most languages, this is realized as an array, vector, list, or sequence.

4. MODULE DESCRIPTION

A modular design reduces complexity, facilities change (a critical aspect of software maintainability), and results in easier implementation by encouraging parallel development of different part of system. Software with effective modularity is easier to develop because function may be compartmentalized and interfaces are simplified. Software architecture embodies modularity that is software is divided into separately named and addressable components called modules that are integrated to satisfy problem requirements.

Modularity is the single attribute of software that allows a program to be intellectually manageable. The five important criteria that enable us to evaluate a design method with respect to its ability to define an effective modular design are: Modular decomposability, Modular Comps ability, Modular Understandability, Modular continuity, Modular Protection.

The following are the modules of the project, which is planned in aid to complete the project with respect to the proposed system, while overcoming existing system and also providing the support for the future enhancement.

4.1 MODULE LIST:

1. User Registration
2. Voting server
3. Candidate registration
4. Block chain formation
5. Verification

4.1.1 User Registration

Once the User creates an account, they are allowed to login into their account to access the application. Based on the User's request, the Server will respond to the User. All the User details will be stored in the Database of the Server. User and candidate have to register their details along with aadhar number.

4.1.2 Voting Server

The Server will store the entire voter's information in their database and verify them if required. Also the Server will store the entire voter's information in their database. Also the Server has to establish the connection to communicate with the Users. The Server will update the each new voter's updating in its database. The Server will authenticate each voter by aadhar before they access the Application. So that the user can access the Application.

4.1.3 Candidate Registration

In this module admin will register the candidate using their aadhar number. Candidate registration will be made using aadhar number and constituency of that candidate. If user candidate provide improper information system will discard those registration process.

4.1.4 Block chain Formation

A block is a container data structure. The average size of a block seems to be 1MB (source). Here every certificates number will be created as a block. For every block a hash code will generate for security. Here all voting information will be stored on block chain. If we store the information on block-chain it is more secured and every block is created based on constituency.

4.1.5 Verification

In this user will get OTP after they polled the vote. OTP is the purpose for confirmation of vote. When user poll the vote OTP will be send to the user verification, after that confirmation of OTP, System will update vote on database.

5. RESULT

The Candidate details are shown to the User in the mobile application. Using that the User can poll the vote to the candidate to whom they want to vote. After the user polling the vote the message is send to the user to verify their voting details.

6. CONCLUSION AND FUTURE ENHANCEMENT

Thus the paper infers that every people can poll their vote through mobile application. Aadhar number is the authentication number to poll the vote on application and for confirmation we use OTP. For future enhancement, the Fingerprint mechanism will give more security for user to poll the vote.

REFERENCES

[1] S. Shah, Q. Kanchwala, H. Mi, Block Chain Voting System, 2016.

[2] Christian, "Desain Dan Implementasi Visual Cryptography Pada Sistem E-Voting Untuk Meningkatkan Anonymity", Institut Teknologi Bandung, 2017.

[3] C. Dougherty, Vote Chain: Secure Democratic Voting, 2016.

[4] "Why Online Voting", Follow My Vote, Jan 2017.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", pp. 9, 2008.

[6] D. A. Wijaya, Bitcoin Tingkat Lanjut., 2016.

[7] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. J. Kishigami, "Blockchain contract: A complete consensus using blockchain", 2015 IEEE 4th Glob. Conf. Consum. Electron. GCCE 2015, pp. 577-578, 2016.

[8] C. Cachin, M. Vukolić, Blockchain Consensus Protocols in the Wild, 2017.