JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Study of Techno-Economic aspects of Electronic voting and proposed Online Voting System

***Dr Rajeev Singh**

*Associate Professor

(Business Management)

*B.S.Dr.B.R.A. College of Agril.Engg. & Technology Etawah

(*Faculty of Technology of C.S.Azad University of Agriculture & Technology Kanpur

ABSTRACT

Online voting is a trend that is gaining momentum in modern society. It has great potential to decrease organizational costs and increase voter turnout. It eliminates the need to print ballot papers or open polling station voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they introduce new threats. A single vulnerability can lead to large-scale manipulations of votes. *Electronic voting systems* must be legitimate, accurate, safe, and convenient when used for elections. Nonetheless, adoption may be limited by potential problems associated with electronic voting systems. *Block chain* technology came into the ground to overcome these issues and an offer decentralized nodes for electronic voting and is used to produce electronic voting systems mainly because of their end-to-end verification advantages. This *technology* is a beautiful replacement for traditional electronic voting solutions with distributed, non-repudiation, and security protection characteristics.

Key words: *Online voting Electronic voting systems Block chain technology*

Introduction

Voting is the fundamental right for every nation. An Electronic Voting (E-Voting) system is a voting system in which the election process is notated, saved, stored, and processed digitally, which makes the voting management task better than the traditional paper-based method. Blockchain is offering new opportunities to develop new types of digital services. While research on the topic is still emerging, it has mostly focused on the technical and legal issues instead of taking advantage of this novel concept and creating advanced digital services. Blockchain-enabled e-Voting (BEV) could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV uses an encrypted key and tamper-proof personal IDs.

Electronic credibility services have become an integral part of the information space. With the reliable implementation of basic services as an electronic signature and electronic authentication, it is possible to build more complex systems that rely on them, particularly the electronic voting system. In this project, the concept of developing an electronic voting system using blockchain technology is implemented. The two-level architecture provides a secure voting process without redundancy of existing (not based on blockchain) systems. The blockchain-based voting project has two modules to make the whole project integrated and work along. One will be the Election Commission who will be responsible for creating elections, adding registered parties and candidates contesting for the election added under the smart contracts. The other end will be the voter's module where each individual can cast a vote for their respective Assembly Constituency and the vote will be registered on the blockchain to make it tamper proof.

Modern democracies are built upon traditional ballot or electronic voting (e-Voting). In these recent years, devices which is known as EVMs are hugely criticized due to irregular reports of the election results. There have been many questions regarding the design and internal architecture of these devices and how it might be susceptible to attacks. This paper has analysed different techniques of tampering the EVMs. Online-voting is pushed as a potential solution to attract the young citizens and the non-resident of the country. For a robust online election scheme, a number of functional and security requirements are to be met such as transparency, accuracy, auditability, data privacy, etc. We have worked the following ideas by having the two different set of modules: election commission and the voter(s). Election Commission creates elections and adds registered candidates along with the parties for contesting the election. Using an election's REST API hosted on Ethereum's Blockchain, the details are shown at the front-end of the voter for casting the vote. Then, while polling the vote is stored on our blockchain framework of which the Election Commission fetches the vote count. The limitation which we have faced due to not using the traditional way of smart contracts is that the blockchain framework which we have coded cannot run on the main net as it needs to be hosted and a separate web3 provider have to be used for interacting with it and not having a public API of voter ID creates a drawback of not having authentication of a voter. The most important factor of this application is to integrate the blockchain framework with both the modules for seamless voting.

Objectives

The objectives for developing the project are as follows:

1) To improve the existing online voting system using Block chain technology.
2) To reduce the workload of setting up an election booth and conducting elections in physical form.
3) Non-Resident Indian can cast their votes as it is totally online.
4) To learn the concept of Block chain and how it can be utilized in different sectors.

Review of literature

In this paper it has been highlighted about the major problem in voting security where in the 2016 US Presidential Elections, EVM's were likely to be intercepted and votes were tampered. The study found that this old voting equipment is not only more prone to failures and crashes but is also notoriously easy to hack and tamper with.

In the study done by Ayed, Ahmed, et al., it has been proposed an electronic voting system based on the Block chain technology. The system is decentralized and does not rely on trust. Any registered voter will have the ability to vote using any device connected to the Internet. The Block chain will be publicly verifiable and distributed in a way that no one will be able to corrupt it. Rifa and Budi has come to a conclusion that if we use of hash values in recording the voting results of each polling station linked to each other makes this recording system more secure and the use of digital signatures makes the system more reliable. The use of the sequence proposed in the block chain creation process in this system considers that in an electoral system not required for mining as in the Bit coin system because the voter data and numbers are clear and are not allowed to select more than once, the proposed sequence ensures that all nodes Which is legally connected and can avoid collision in transportation Bin, Joseph, et al., has come to a conclusion that the current block chain voting system cannot provide the comprehensive security features, and most of them are platform dependent, we have proposed a block chain based voting system that the voters' privacy and voting correctness are guaranteed by homomorphism encryption, linkable ring signature, and PoKs between the voter and block chain [5].

Existing Electronic Voting System

In India, before 2004 there was a paper-based voting system. This is called as ballot Paper system. Voters had to go to polling booth and cast their vote by marking on seal in front of the symbol of a candidate for which they wanted to cast their votes on ballot paper. Results were announced by counting the votes. The maximum vote gainer was declared as winner. India has population more than 120 crores the ballot paper voting is not much reliable, time consuming and very difficult to count the vote and there are also problems like replacement of ballot paper boxes with duplicate, damage of ballot paper, marking stamp seal for more than one candidate hence there is a strong need to overcome these problems. In order to overcome these problems Electronic Voting Machines Were introduced. Electronic Voting Machine (EVM's) mainly consists of two components:

1. Control Unit: It stores and assembles votes, used by poll workers.

2. Ballot Unit: It is placed in the election booth and is used the voters.

Both the units are connected via 5m cable and one end of the cable is permanently fixed to ballot unit. The control unit has a battery pack inside, which motorizes the system. The ballot unit has 16 candidate button and the unused buttons are covered with a plastic masking tab inside the unit. An additional ballot unit can be connected when there are more than 16 candidates. The additional ballot unit can be connected to a port on the underside of the first ballot unit. EVM's are internationally known as DRE's (Direct recording Electronic). EVM's are universally used in India since the general elections of 2004, when ballots were completely out of trend. They have been used in all the assembly polls and general elections of 2009.

Drawbacks of Existing Electronic Voting System

By using EVM's, Votes are correctly recorded and there is no problem in counting, scalability, Accuracy, fast declaration of results and robustness of system. Main Problem lies in authentication, the person who is voting may not be the legitimate person. Other problems like capturing of booth by political parties, casting of votes by underage people and fraud voting may occur. A person is provided with the voter id card as a proof of identity, issued by Indian government. Lot of problems are seen in voter id cards like name misprinting, missing of name, no clear photo on photo id card, etc. It consumes a lot of time to stand in a que to vote and there is no such remote facility available to cast your vote from anywhere in the world.

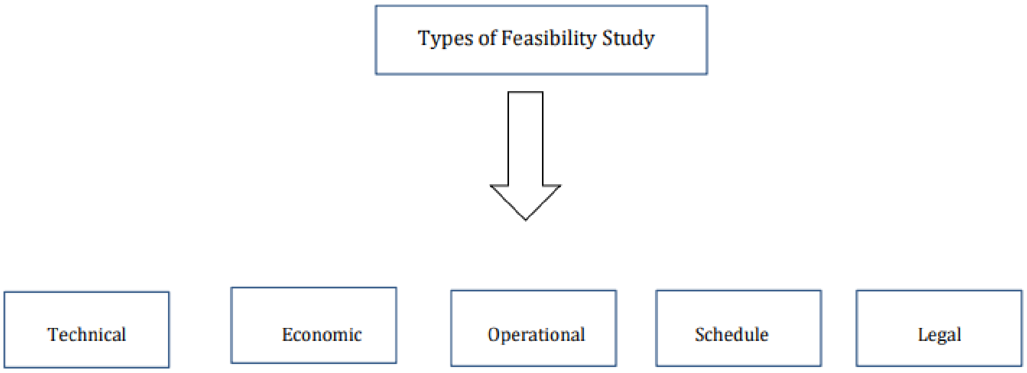
Proposed System

Several studies have been done on using computer technologies to improve elections. These studies tell about the risks of adopting electronic voting system, because of the software challenges, insider threats, network vulnerabilities, and the challenges of auditing. We've proposed to design the existing online voting system which is integrated with the Blockchain technology. The proposed system has the following advantages as compared to the existing system:

- Users' can vote from anywhere in the world until he possess a citizenship of the country.
- The voting is stored in the Blockchain which makes it tamper proof.
- As there's no standing in queue for casting vote it will save a lot of time and reduce the workload.

Feasibility Study

A feasibility study is a high-level capsule version of the entire system analysis and design process. The study begins by classifying the problem definition. The purpose of feasibility study is not to solve the problem, but to determine whether the problem is worth solving. It is a preliminary study which is conducted before the real development of the project commences not keeping the factor of project's success. It creates a roadmap of what are the possible solutions if we choose a certain path. The feasibility study concentrates on the following areas:



Technical Feasibility

Evaluating the technical feasibility study is the trickiest part of a feasibility study. This is because, at this point in time, not too many detailed designs of the system, making it difficult to access issues like performance, costs on (on account of the kind of technology to be deployed) etc. A number of issues have to be considered while doing a technical analysis. Understand the different technologies involved in the proposed system before commencing the project we have to be very clear about what are the technologies that are to be required for the development of the new system. Overall, this study needs to demonstrate that the proposed system which is need to be developed is technically feasible.

This requires:

- An outline of the requirements,
- A possible system design,
- Possible choices of software to be used or developed,
- Estimates on number of users, data, etc.

Economic Feasibility

The economic feasibility study evaluates the cost of the software development against the ultimate income or benefits gets from the developed system. There must be scopes for profit after the successful Completion of the project. The life cycle of an engineering project or product contains of several stages, namely: (i) Planning and design; (ii) Development; (iii) Operation and maintenance. It should be performed to identify the financial risk associated with the project. Various techniques like net present value (NPV), payback period, return on investment (ROI) are employed. Techno-Economic Assessment (TEA) is a cost-benefit comparison using different methods. These assessments are used for tasks such as:

- Evaluate the economic feasibility of a project.
- Investigate cash flows over the lifetime of the project.
- Evaluate the likelihood of different technology scales and applications.
- Compare the economic quality of different technology application providing the same service.

Operational Feasibility

The operational feasibility study focuses on the degree to which the proposed development project fits in with the existing business environment and objectives with regard to development schedule, delivery date, corporate culture, and existing business processes. It is also the measure of how well the solution will work in the organization after it is deployed. As we are dealing with blockchain voting system, which indirectly targets the country's or state's election process protocol, so there will be a detailed comparison between these two to check which one dominates the other. It is also the measure how people will feel about the project as in will people be accustomed to use this in a proper way or it will be too complex to deal with. There are two aspects of operational feasibility to be considered:

- Is the problem worth solving?

- How do the end user (voters in this case) and management (Election Commission) feel in this case?

Schedule Feasibility

It means that the project can be implemented in an acceptable time frame. When assessing schedule feasibility, a systems analyst must consider the interaction between time and costs. For example, speeding up a project schedule might make a project feasible, but much more expensive.

Other issues that relate to schedule feasibility include the following:

- Can the company control the factors that affect schedule feasibility?

- Has management established a firm timetable for the project?

- What conditions must be satisfied during the development of the system?

- Will an accelerated schedule pose any risks? If so, are the risks acceptable?

- Will project management techniques be available to coordinate and control the project?

- Will a project manager be appointed?

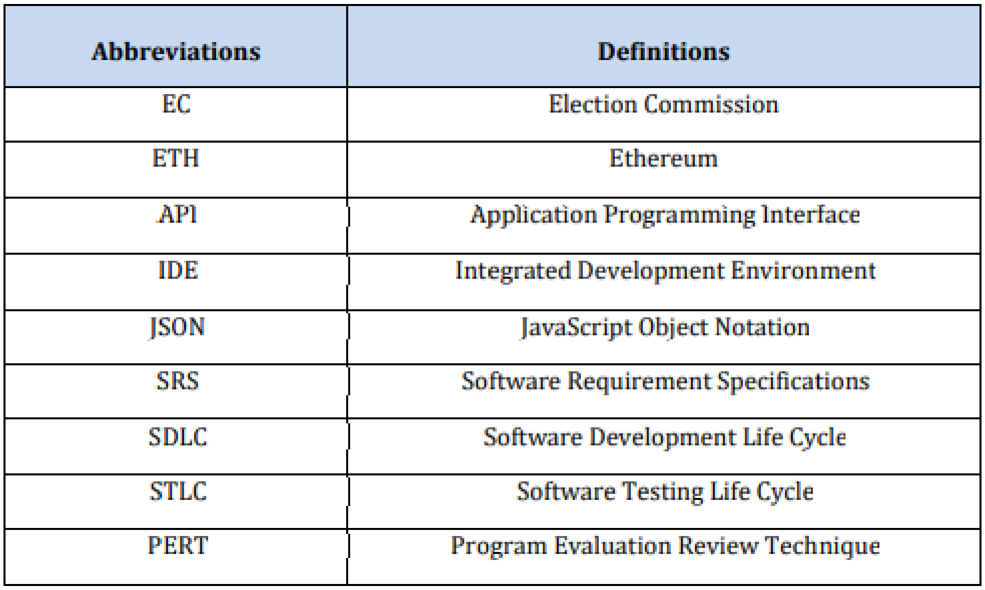
It is also the likelihood that timeframes can be met and that this is adequate to meet organization's needs.

Legal Feasibility

It determines whether the proposed system conflicts with the legal requirements, in this case as we didn't try to execute anything on the public domain, hence this project is legal feasible. It is important that the project is following the requirements needed to start a project including certificates, copyrights, business insurance, tax number, health and safety measures and many more. There are some things to consider in legal feasibility study including ethical issues and some social issues. These issues are the privacy and accountability. In this project, everything is designed keeping in mind all the legal terms and no real-world data or privacy has been breached of any person of this country to use it as a sample voter to implement this application.

Conclusion: Manual voting system has been deployed for many years in our country. However, in many parts of our country people cannot attend the voting because of several reasons. To illustrate, sometimes people may not be in their own registration region and due to this fact, they cannot fulfill their voting duties. In order to solve these problems, there is a need of online election voting system with this keeping in mind that EVM votes tampering issues are also encountered, so this online election system will be integrated with Block chain Technology to make it tamper proof. The purpose of this document is to make the functional and non-functional requirements of the 'Voting Blocks'- A Block chain based e-Voting Application System easy to comprehend. It also serves the purpose of making the functionality clear to end users. This SRS document applies to the initial version (release 1.0) of the 'VotingBlocks'- A Blockchain based e-Voting Application System software package. This document describes the modelling and the requirement analysis of the system. The main aim of the system is to provide a set of protocols that allow voters to cast votes while the election commission is responsible for creating elections and adding candidates. The remainder of this document identifies the actors, use-cases, use-case scenarios, activity diagrams, assumptions and dependencies needed for the analysis and design of the Online Election software package. The rest of the document contains the overall description of the system, requirements, data model and behavioural description of the system and project planning.

The following is a list of terms, acronyms and abbreviations used by the Online Election System using Blockchain software package and related documentation.



Abbreviations	Definitions
EC	Election Commission
ETH	Ethereum
API	Application Programming Interface
IDE	Integrated Development Environment
JSON	JavaScript Object Notation
SRS	Software Requirement Specifications
SDLC	Software Development Life Cycle
STLC	Software Testing Life Cycle
PERT	Program Evaluation Review Technique

Overall Description

The Online Election System is a web-based system so fundamental features related with web-based technologies such as client-server and database properties determine the software requirements of that project along with the addition of blockchain framework.

Product Perspective

The software product is a standalone system and not a part of a larger system. The system will be made up of two parts. One will be used for general purposes by the EC, such as viewing candidates, registered parties and past years' election results. The voters will reach the system connected to another module through web pages by using web-browsers such as Mozilla, Internet Explorer and Google Chrome. On the election day, the voter needs to import his/her Ethereum's wallet and get authenticated accordingly. The voters cast their votes using the interface that is provided. These votes are accepted by the blockchain and then thrown into the server. The EC configures the whole system according to its needs on the server.

Product Features

1. Eligibility: This property states that only eligible users can vote. Those who are provided with authentication by the Election Commission.

2. Privacy: Privacy is one of the most important aspects of democratic voting. Voter's privacy should be maintained. No one should be able to know how a particular person voted or to whom the particular voter voted.

3. Coercion resistance: No one should be able to force the voter and should not have the ability to distinguish between whether the voter voted the same way he/she was instructed to vote.

4. Verifiability: This property states that everyone involved in the voting process should be able to verify the results. This brings transparency in the election. Also, an individual voter should be able to verify whether his/her vote is counted or not.

5. Immutability: The voter's vote should be immutable. No one should be able to change the vote of any voter without proper concern of the voter. All the records should be immutable.

Constraints, Assumptions and Dependencies

The system enables voters to cast their vote from anywhere and is authenticated by EC and provided with the ETH wallet address and private key. Security and anonymity are the most crucial fundamentals of this blockchain voting system.

For the proper working of the system, we can list our assumptions and dependencies as follows:

- **Metamask Browser Extension**: Metamask allows users to manage accounts and their keys in a variety of ways, including hardware wallets, while isolating them from the site context.

- **Ganache**: It is a personal blockchain for rapid Ethereum and Corda distributed application development.

- **Truffle**: A world class development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM), aiming to make life as a developer easier.

- **NodeJS**: It is a JavaScript runtime built on Chrome's V8 JavaScript engine.

Functional Requirements and Software Requirements

Software	Type	Version
Ganache	Ethereum Blockchain Server	2.4.0
Metamask	Ethereum Wallet	7.7.9
Truffle	Development framework for ETH	5.1.31
Node	JavaScript Runtime	12.17.0
Visual Studio Code	Integrated development environment	1.46
Remix	Solidity's IDE	0.10.1
Windows 10	Operating System	1809

Table 3.2 Software Requirements

Minimum Hardware Requirements

Processor	:	intel i3
RAM	:	8GB
Hard Disk	:	1TB

Non-functional Requirements

Performance Requirements

The system is expected to have a reasonable short time of response. The voter should be able to import his/her wallet provided by the Election Commission within few seconds keeping in the mind the condition of network stability. The system's performance is different according to its modes:

(i) Election Mode:

In this phase, the expected time to deploy the smart contracts totally depends upon the miners connected to the blockchain and the amount of GAS we decide to sign off the transaction to marked as validated one but as we are working locally, it is just a matter of half a minute or so.

(ii) Voting Mode:

In this phase, the system will be responding within seconds as we don't have to sign off transaction just to fetch the list of candidates for the elections but depending on the network stability and web3 connection the above performance might be delayed. Next, after casting the vote it might take a minute or two to sign off the transaction depending upon the miners and GAS limit.

Security Requirements

- The data transaction between client and the blockchain server must be done over https to avoid mixed content attack.

- The re-entrancy on a single function has to be minimized while deploying the smart contract.

- To address the integer overflow error, the idea of counting the votes have been done within a specific event responsible for it.

Reliability

- **In Election Mode**: The system needs to be maintained time to time as if the smart contract which is to be deployed encounters any bugs, it needs to be fixed to prevent votes miscalculation and transaction error handling.

- **In Voting Mode**: As the maintaining part is in the Election Mode, if there's any error in web3 connection the interoperability status might change otherwise the system will work flawlessly all the time.

Usability

- The system will have a minimal and simple User Interface.

- To guide the users for the first time using it, there will be a guidance related to the usage of the system.

Block chain

A **block chain** is a growing list of records, called **blocks**, that are securely linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). The timestamp proves that the transaction data existed when the block was published to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Block chains are typically managed by a peer-to-peer network for use as a publicly distributed ledger, where nodes collectively adhere to a protocol to communicate and validate new blocks. Although block chain records are not unalterable as forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance.

The block chain was popularized by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the crypto currency bitcoin, based on work by Stuart Haber, W. Scott Stornetta, and Dave Bayer. The identity of Satoshi Nakamoto remains unknown to date. The implementation of the block chain within bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications and block chains that are readable by the public and are widely used by cryptocurrencies. The blockchain is considered a type of payment rail.

Private block chains have been proposed for business use. Computerworld called the marketing of such privatized block chains without a proper security model “snake oil”; however, others have argued that permissioned block chains, if carefully designed, may be more decentralized and therefore more secure in practice than permissionless ones.

Cost estimation can be defined as the approximate judgement of the costs for a project. Cost estimation will never be an exact science because there are too many variables involved in the calculation for a cost estimate, such as human, technical, environmental, and political. Furthermore, any process that involves a significant human factor can never be exact because humans are far too complex to be entirely predictable. Furthermore, software development for any fair-sized project will inevitably include a number of tasks that have complexities that are difficult to judge because of the complexity of software systems.

Cost estimation is usually measured in terms of effort. The most common metric used is person months or years (or man months or years). The effort is the amount of time for one person to work for a certain period of time. It is important that the specific characteristics of the development environment are taking into account when comparing the effort of two or more projects because no two development environments are the same. A clear example of differences in development environments are the amount of time people work in different countries; the typical workweek in North America is 40 hours per week, while in Europe the typical workweek is 35 hours per week. Thus, when comparing a project from North America with a project from Europe, a conversion factor would have to be used to all for an accurate comparison. Different variables can be used for cost estimation, which leads to a difficulty when comparing projects if standard models or tools are not used. For example, a cost estimate can include factors from management, development (e.g., training, quality assurance), and other areas specific to an organization.

References

[1] Wolchok, Scott, et al. "Security analysis of India's electronic voting machines." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.

[2] Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law." Tex. L. Rev. 95 (2016): 1579.

[3] Ayed, Ahmed Ben. "A conceptual secure block chain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2017): 01-09.

[4] Hanifatunnisa, Rifa, and Budi Rahardjo. "Block chain based e-voting recording system design." 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). IEEE, 2017.

[5] Yu, Bin, et al. "Platform-independent secure block chain-based voting system." International Conference on Information Security. Springer, Cham, 2018.

[6] Block chain | Binance Academy.

[7] Ethereum Development Tutorials | ethereum.org.

[8] Smart Contracts Explained | The Ultimate Beginner's Guide (imiblockchain.com).

[9] Intro to Web3.js · Ethereum Blockchain Developer Crash Course | Dapp University.