

Blockvote - Blockchain based E-Voting System

Rajesh Kumar Yadav¹, Santosh Kumar Mishra², Avadh Narayan Yadav³ and Sachin Kumar Kamat⁴

¹⁻⁴Department of Computer Science and Engineering, Delhi Technological University, New Delhi, INDIA

Email: rkyadav@dtu.ac.in, santosh.mishra7@yahoo.com, avadhnarayan537@gmail.com,

Sachinkamat730@gmail.com

Abstract—In this venture, the idea of building up an electronic democratic framework utilizing blockchain innovation is executed. The two-level design gives a safe democratic cycle without excess of existing (not founded on blockchain) frameworks. The blockchain-based democratic undertaking has two modules to make the entire task coordinated and work along. One will be the Election Commission who will be liable for making races, adding enlisted gatherings and up-and-comers challenging for the political decision added under the brilliant agreements. The opposite end will be the citizen's module where every individual can make a choice for their particular Assembly Constituency and the vote will be enlisted on the blockchain to make it carefully designed.

Index Terms— Blockchain, Election, Election Commission, Voting Process.

I. INTRODUCTION

Casting a ballot is essential and appropriate for each country. An Electronic Voting (E-Voting) framework is a democratic framework where the political race measure is recorded, saved, put away, and prepared carefully, which makes the democratic administration task better compared to the customary paper-based technique. Blockchain is offering new freedoms to grow new kinds of computerized administrations. While research on the theme is as yet arising, it has for the most part centered on the specialized and lawful issues as opposed to exploiting this novel idea and making progress in computerized administrations. Blockchain-empowered e-casting a ballot (BEV) could lessen citizen extortion and increment elector access. Qualified electors cast a polling form namelessly utilizing a PC or cell phone. BEV utilizes a scrambled key and sealed individual IDs. Electronic believability administrations have become an indispensable piece of the data space. With the solid execution of fundamental administrations as an electronic signature and electronic confirmation, it is feasible to fabricate more mind boggling frameworks that depend on them, especially the electronic democratic framework.

A. Overview

Current popular governments are based upon customary polling form or electronic democratic (e-casting a ballot). In these new years, gadgets which are known as EVMs are enormously condemned because of sporadic reports of the political race results. There have been numerous inquiries in regards to the plan and inward design of these gadgets and how it very well may be defenseless to assaults. This [1] paper has examined various procedures of altering the EVMs. Web based democratic is pushed as a possible answer for draw in the youthful residents and the non-inhabitant of the country. For a vigorous online political decision conspire, various useful

and security necessities are to be met like straightforwardness, exactness, auditability, information protection, and so forth.

We have worked the accompanying thoughts by having the two distinctive arrangements of modules: political decision commission and the voter(s). The Political decision Commission makes races and adds enrolled up-and-comers alongside the gatherings for challenging the political race. Utilizing a political race's REST API facilitated on Ethereum's Blockchain, the subtleties are appeared at the front-finish of the elector for making the choice. At that point, while surveying the vote is put away on our blockchain structure of which the Election Commission gets the vote tally. The limit which we have looked because of not utilizing the customary method of brilliant agreements is that the blockchain system which we have coded can't run on the principle net as it should be facilitated and a different web3 supplier must be utilized for connecting with it and not having a public API of citizen ID makes a disadvantage of not having verification of an elector. The main factor of this application is to coordinate the blockchain structure with both the modules for consistent democratic.

B. Existing System

In India, before 2003 there was a paper-based democratic framework. This is called as voting form Paper framework. Citizens needed to go to surveying corner and cast their vote by stamping on seal before the image of a contender for which they needed to project their decisions on voting form paper. Results were reported by tallying the votes. The most extreme vote gainer was announced as victor. India has populace in excess of 120 crores the polling form paper casting a ballot isn't a lot of dependable, tedious and exceptionally hard to check the vote and there are additionally issues like supplanting of polling form paper boxes with copy, harm of voting form paper, stamping stamp seal for more than one competitor henceforth there is a solid need to beat these issues. To conquer these issues Electronic Voting Machines Were presented. Electronic Voting Machine (EVM's) principally comprises of two parts:

1) Control Unit 2) Ballot Unit

Both the units are associated through 5m link and one finish of the link is forever fixed to polling form unit. The control unit has a battery pack inside, which mechanizes the framework. The polling form unit has 16 competitor button and the unused catches are covered with a plastic concealing tab inside the unit. An extra polling form unit can be associated when there are in excess of 16 competitors. The extra voting form unit can be associated with a port on the underside of the main voting form unit. EVM's are globally known as DRE's (Direct Chronicle Electronic). EVM's are all around utilized in India since the overall appointment of 2004, when voting forms were totally out of pattern. They have been utilized taking all things together the gathering surveys and general appointment of 2009. By utilizing EVM's, Votes are accurately recorded and there is no issue in tallying, adaptability, Accuracy, quick presentation of results and power of framework. Fundamental Problem lies in confirmation, the individual who is casting a ballot may not be the real individual. Different issues like catching of corner by ideological groups, projecting of votes by underage individuals and extortion casting a ballot may happen. An individual is given the elector id card as a proof of personality, given by Indian government. Part of issues are found in citizen id cards like name misprinting, missing of name, no reasonable photograph on picture id card, and so forth.

C. Proposed System

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: 1) Users' can vote from anywhere in the world until he possess a citizenship of the country. 2) The voting is stored in the Blockchain which makes it tamper proof. 3) As there's no standing in queue for casting vote it will save a lot of time and reduce the workload.

II. LITERATURE REVIEW

In this paper [2], it has featured about the serious issue in casting a ballot security where in the 2016 US Presidential Elections, EVM's were probably going to be blocked and casts of ballots were altered. The investigation tracked down that this old democratic hardware isn't simply more inclined to disappointments and crashes but at the same time is famously simple to hack and alter. In this examination [3] by Ayed, Ahmed, et al., it has been proposed as an electronic democratic framework dependent on Blockchain innovation. The framework is decentralized and doesn't depend on trust. Any enlisted elector can cast a ballot utilizing any

gadget associated with the Internet. The Blockchain will be openly obvious and circulated such that nobody will actually want to ruin it. Rifa and Budi has reached a resolution that in the event that we utilization of hash esteems in recording the democratic aftereffects of each surveying station connected to one another makes this account framework safer and the utilization of advanced marks makes the framework more dependable. The utilization of the succession proposed in the blockchain creation measure in this framework thinks about that in a constituent framework not needed for mining as in the Bitcoin framework in light of the fact that the elector information and numbers are clear and are not permitted to choose more than once, the proposed arrangement guarantees that all hubs Which is lawfully associated and can keep away from crash in transportation [4]. Container, Joseph, et al., has reached a resolution that the current blockchain casting a ballot framework can't give the complete security highlights, and the vast majority of them are stage subordinate, we have proposed a blockchain-based democratic framework that the citizens' protection and casting a ballot rightness are ensured by homomorphic encryption, linkable ring mark, and PoKs between the elector and blockchain [5].

III. MOTIVATION

The goals for building up the venture are as per the following: 1) To improve the current internet casting a ballot framework utilizing Blockchain innovation. 2) To decrease the responsibility of setting up a political decision corner and leading races in actual structure. 3) Non-Resident Indian can give their votes as it is absolutely on the web. 4) We should become familiar with the idea of Blockchain and how it tends to be used to chip away at various areas.

IV. PROBLEM DEFINITION

Distinguishing likely issues before the beginning of a task can save the association huge measures of time and cash. Issue examination is quite possibly the most basic phase of undertaking arranging since this stage assists with managing all ensuing investigation and dynamics. In the event that the undertaking doesn't progress past this stage with arrangements that the association can execute, the task ought not go ahead in its present structure.

V. STATEMENT

This project is for the creation of an online election system using Blockchain technology. There will be a website for Election Commission and for the voters. The user interface will be designed as part of the project which will contain necessary details at both the end.

VI. DESIGN

i) Planning Requirements :

The first step, as with most improvement projects, is to go through an underlying planning stage to outline the basic reports, set up programming or equipment specifications, and generally get ready for the next stages of the cycle.

ii) Analysis Design:

Following the conclusion of the planning process, an investigation is carried out to evaluate the required business theory, database models, and other elements that will be expected at this stage of the project. The design stage takes place here as well, and it defines any technical specifications (languages, data layers, facilities, and so on) that will be used to fulfil the analysis stage's requirements.

iii) Implementation:

After the arranging and analysis are completed, the actual execution and coding interaction will begin. All arranging, particular, and scheme documents are yet to be coded and carried out into the venture's underlying focus.

iv) Testing:

Since this new type focus has been coded and introduced, the next move is to go through a set of testing systems to detect and fix any existing bugs or problems that have occurred.

v) Evaluation:

When all of the previous steps have been completed, now is the perfect time to perform an in-depth review of success to this phase. This allows the whole community, as well as clients or other external groups, to assess where the project is, where it can be, what can or can improve, and so on.

VII. SOLUTION METHODOLOGIES

i) Qualification: This property expresses that lone qualified clients can cast a ballot. The individuals who are given validation by the Election Commission. ii) Protection: Privacy is quite possibly the main parts of vote based democratic. Citizens protection ought to be kept up. Nobody ought to have the option to realize how a specific individual casted a ballot or to whom the specific elector casted a ballot. iii) Intimidation opposition: No one ought to have the option to constrain the citizen and ought not can recognize whether the elector cast a ballot in a similar way he/she was told to cast a ballot. iv) Certainty: This property expresses that everybody engaged with the democratic cycle ought to have the option to check the outcomes. This acquires straightforwardness in the political race. Additionally, an individual citizen ought to have the option to check whether his/her vote is tallied or not.

Changelessness: The citizen's vote ought to be permanent. Nobody ought to have the option to change the vote of any citizen without appropriate worry of the elector. Every one of the records ought to be unchanging.

VIII. DATA MODELS

The project has been divided into many modules in which for every functionality we have designated modules. Any software comprises of many systems which contains several sub-systems and those sub-systems further contains their sub- systems. So, designing a complete system in one go comprising of each and every required functionality is a hectic work and the process can have many errors because of its vast size. Effective modular design can be achieved if the partitioned modules are separately solvable, modifiable as well as compliable. Following are the project modules:

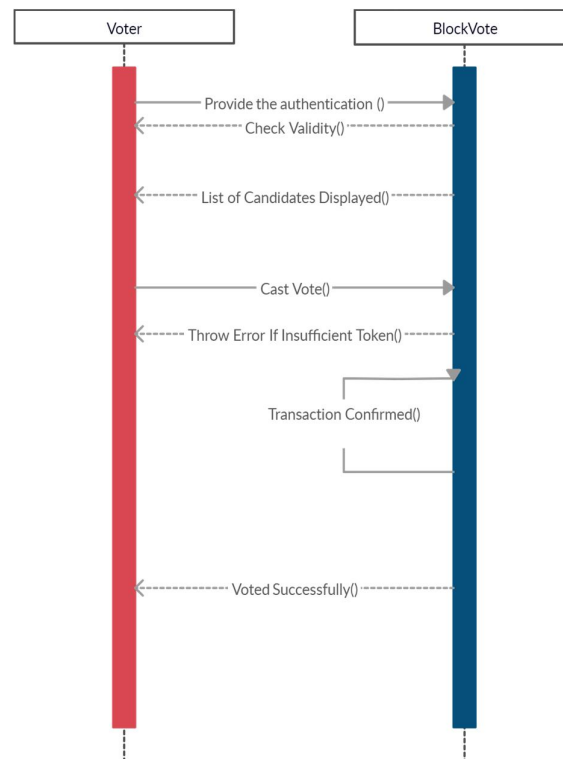


Fig. 1. Sequence Diagram

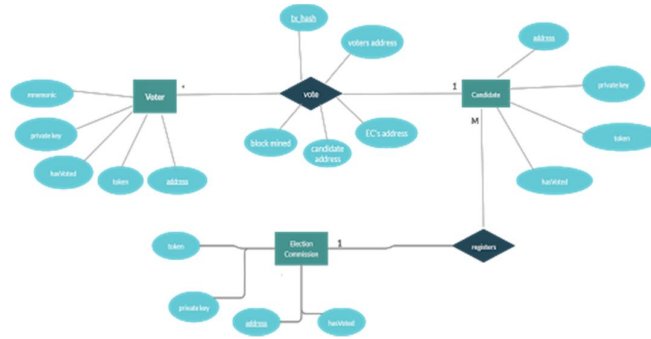


Fig. 2. Entity Relationship Diagram

(i) Election Commission: In this module, an entity named Election Commission will be responsible to setup the smart contract and register candidates, parties and start off an election.

(ii) Election Test: This is the module to test our smartcontract where we use Mocha Framework to perform unit test on our application.

Voter Module: In this module, voters who have been provided with the personal ETH wallet will import onto the voting portal using the Metamask extension and cast their vote. 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: 1) 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. 2) Ganache: It is a personal blockchain for rapid Ethereum and Corda distributed application development. 3) 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. 4) NodeJS: It is a JavaScript runtime built on Chrome's V8 JavaScript engine.

IX. COST ESTIMATION OF PROPOSED SYSTEM

The people who do the cost estimates could be either directly or indirectly responsible for the implementation for a project, such as a developer or manager, respectively. Someone who has knowledge of the organization and previous projects could use an analogy-based approach to compare the current project with previous projects, which is a common method of estimation for small organizations and small projects. The historical data is often limited to the memory of the estimator. In this case, the estimator would need to be experienced and would likely have been with the company for a while. Some people believe it is better if the estimates are done by outsiders so that there is less chance of bias. It is true that people outside an organization will likely have to deal with fewer company politics than people within the organization. For example, the developer for a company may want to please the manager and so give an estimate that is overly-optimistic. The disadvantage of having an outside estimate is that the person would have less knowledge of the development environment, especially if the person is from outside the company. An empirical method of estimation would then be required, such as the Constructive Cost Model (COCOMO). Empirical methods of estimation can be used by all types of estimators. There may be some resistance to using an empirical method of estimation because there may be some question on whether a model could outperform an expert. People who are accurate estimators are rare in our experience, and so it is best to get the opinion of several people or tools. In the actual cost estimation process, there are other inputs and constraints that needed to be considered besides the cost drivers. One of the primary constraints of the software cost estimate is the financial constraint, which are the amount of the money that can be budgeted or allocated to the project. There are other constraints such as manpower constraints, and date constraints. Other input such as architecture, which defines the components that made up the system and the interrelationships between these components. Some company will have certain software process or an existing architecture in place; hence for these companies the software cost estimation must base their estimates on these criteria. There are only very few cases where the software requirements stay fixed. Hence, how do we deal with software requirement changes, ambiguities or inconsistencies? During the estimation process, an experienced estimator will detect the ambiguities and inconsistency in the requirements. As part of the estimation process,

the estimator will try to solve all these ambiguities by modifying the requirements. If the ambiguities or inconsistent requirements stay unsolved, which will correspondingly affect the estimation accuracy.

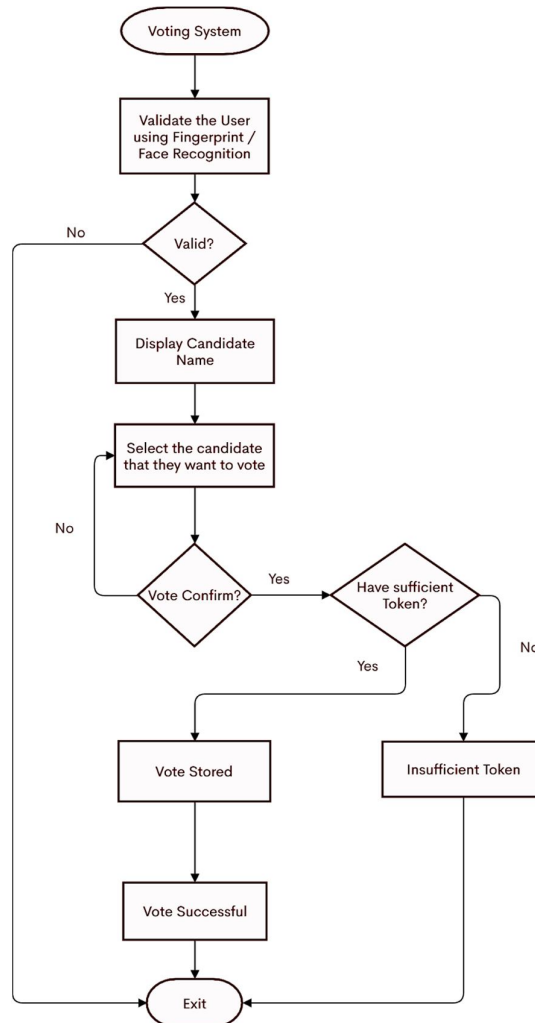


Fig. 3. Flowchart

X. BLOCKCHAIN SECURITY THREAT MODELS

Blockchain applications often incorporate external components — Identity and access management (IAM) systems, multi-factor authentication (MFA), public key infrastructure (PKI), and regulatory and audit systems — that are owned and managed by actors. These systems need to be carefully scrutinized before they can become part of the overall solution as they are developed or controlled by third parties. These should be taken into consideration for the threat model in a blockchain solution.

XI. ADVANTAGES OF PROPOSED SYSTEM

A. Inherent Versioning

Most programming improvement life cycles will, without a doubt, include some sort of shaping that depicts the product's delivery process at a specific level. However, the iterative model makes this much easier by ensuring that more recent cycles are continuously modified versions of previous emphases. In addition, if

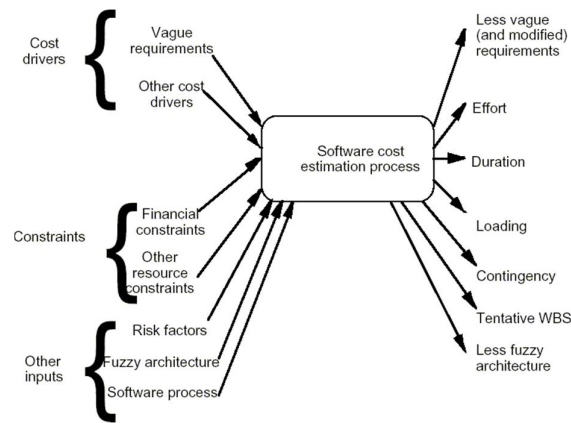


Fig. 4. Actual Cost Estimation Process

another focus in general destroys a system in a cataclysmic way, a previous cycle may be easily and efficiently executed or "moved back," with minimal consequences; this is especially useful for post-discharge upkeep or web applications.

B. Rapid Turnaround

Although it might seem that each step of the iterative cycle isn't exactly the same as the stages of a more conventional model like the cascade strategy — and therefore the interaction can take a long time — the excellence of the iterative interaction is that each stage can be sufficiently thinned down into more modest and more modest time periods; whatever is required to fulfil the needs of the iterative interaction. While the overall process of all stages which take some time, each subsequent concentration would be faster and faster, fitting the dexterous nickname so well overall, and allowing the life pattern of each new period to be handled down to only a few days.

C. Suited for Agile Organizations

While a piecemeal approach like the cascade model can work well for large groups of several collaborators, the iterative model really shines when it's in the hands of a smaller, more organised community. A complete "cycle measure" can be adequately performed by various individual colleagues, from arranging and configuration to execution and testing, with virtually no outside input or support, particularly when combined with the force of modern form control frameworks.

D. Easy Adaptability

Another important advantage of the iterative model is the ability to rapidly respond to the constantly evolving needs of the venture or the impulses of the consumer, which is based on the central intensity of continuous, incessant focus coming out consistently. Indeed, even major improvements to the basic code design or executions (such as a new database system or administration execution) can often be made in a short amount of time and at a reasonable cost, since any negative changes can be detected and restored to a previous focus in a short amount of time.

XII. SECURITY CONTROLS UNIQUE TO BLOCKCHAIN

- 1) Programming interface security best practices are utilized to defend API-based exchanges.
- 2) Information arrangements are received for the way to deal with defending information/data.
- 3) The suitable underwriting arrangements are characterized and embraced dependent on business contracts.
- 4) Mysteries store for both application and restricted admit-tance is utilized.

XIII. CONCLUSION

Democracies depend on trusted elections and citizens should trust the election system for a strong democracy. However traditional paper-based elections do not provide trustworthiness. The idea of adapting digital voting

systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. This project has been developed to a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. It outlines the systems architecture, the design, and a security analysis of the system. In the next build of this application, it has been proposed to create separate client designs for various roles such as one for election commission and one for candidates registered to a certain party with the existing voting client design. Also, the current versions lack authentication as we don't have access to current Aadhar's or Voter SDK to integrate in our application. Also, it is planned that in the next build notification prompt will be given on the day of voting to all the voters to cast their vote so that the voter turnout is maximum for that election.

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 blockchain-based electronic voting system." *International Journal of Network Security Its Applications* 9.3 (2017): 01-09.
- [4] Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain 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 blockchain-based voting system." *International Conference on Information Security*. Springer, Cham, 2018.