Web based Voting Framework using Blockchain Technology

Tanvi Shah, Sneha Kadam, Ankita Mane, Tanvi Kapdi

Atharva College of Engineering

Publication Info

Article history:
Received : 21 February 2020
Accepted : 23 May 2020

Keywords:
Blockchain, e-voting, framework, Innovation, Security.

Corresponding author:
Tanvi Shah
e-mail: *tpshah98@gmail.com*

Abstract

Public activity is one of the most profited zones by technology. Advancement in innovation has given people access to an assortment of assets and administrations through a 24 hour all around associated design. Innovation, for example, the Internet has end up being a help for developments and creating assets advantageous to mankind. One such earth-shattering advancement is Blockchain-an energizing mechanical progression conspicuously known for its application in cryptographic money. Blockchain offers an unending scope of uses which profit by the idea of shared economy. With properties, for example, unchanging nature and decentralized architecture, Blockchain introduces itself as a potential arrangement in crossing over the present equality between basic man and its government. Public Elections are one of the premises whereupon the popular government is built. Thus, doing security races and forestalling appointive extortion is of most extreme significance of security. This paper separates the necessities of building an Electoral portal using the Blockchain advancement and perceiving the authentic and particular troubles that may be stood up to while arranging the structure and give security to the framework.

1. INTRODUCTION

Building an ensured electronic popularity-based system that offers the sensibility and security of current law-based plans, while giving the straightforwardness and versatility offered by electronic structures has been a test for a long time. In relationship with the standard paper-based just, remote e-casting a ballot is naturally well disposed, continuous tallying and handling, less blunder inclined [4]. Electronic democratic (e-casting a ballot) is an electronic method for throwing and tallying votes. It is a productive and savvy route for directing a democratic system, which has normal for being unselfish information and ongoing and mentioning high safety. Blockchain advancements offer an interminable scope of utilizations profiting by sharing economies. This paper means to assess the use of blockchain as administration to actualize appropriated electronic democratic frameworks. The paper proposes an electronic web based democratic framework dependent on blockchain that tends to a portion of the impediments in existing frameworks. Blockchain was first presented by an individual or gathering of individual under the mysterious character of Satoshi Nakamoto [5]. The development from paper based democratic framework to electronic framework brings new improvement, for example, constant checking, instant result, environment friendly, transparent, anonymity, less error and decentralized.[7]

2. BLOCKCHAIN OVERVIEW:

On a fundamental level, a blockchain should be considered as an appropriated include just timestamped data structure. Blockchains license us to have a scattered circulated framework where non-accepting people can certainly associate with each without the prerequisite for a trusted in power (Christidis and Devetsikiotis, 2016) [9]. To achieve this one can, consider blockchain as a ton of interconnected parts which give unequivocal features to the structure, At the most decreased level of this establishment, we have the stamped trades between peers. These trades mean a comprehension between two individuals, which may incorporate the trading of physical or propelled assets, the zenith of a task, etc. A Blockchain permits untrusting parties with normal interests to co-create a perpetual, unchangeable and transparent record of trade and handling

Figure 1: Blockchain Overview

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

without depending on central authority.

3. BLOCKCHAIN AND SOCIETY:

Regardless of being a genuinely present innovation its first huge scaled utilization was sent with the approach of Bitcoin, the primary elective coin to turn out to be exceedingly popular - the Blockchain has quite recently been the point of convergence of a couple of electronic government looks at papers and open source adventures. In like manner, they all take advantage of Blockchain's centre qualities: a decentralized, trust less, repetitive system, which incorporates non-reversible exchanges and PC applications. Some of them advocate completely re-designing fair systems comprehensive of decisions, even as others technique opportunity casting a ballot conspires all together that its realities are made everlasting and to be had consistently to the populace. There likewise are conversations that cowl the social effect of Blockchain principally based programming. [2] Blockchain advancements can possibly affect and reform different parts of society. Indeed, it's compasses, through changing budgetary exchanges, can possibly change associations and people over the coming decades. It is important that IT chiefs comprehend the ramifications of blockchain innovation to plan.

4. BLOCKCHAIN FOR VOTING:

Proposition of casting a ballot over Blockchain systems were picking up progressively footing, with the media paying additional enthusiasm to the issue after the 2016 US races, in which there had been bits of gossip about computerized balloting machines being tempered with by far off spots programmers. President Obama's decision to oust 35 Russian negotiators over issues of Russia's impedance with the 2016 political race, among various approvals, have featured much more the uneasiness at the rear of the security of balloting techniques. Security occurrences with balloting techniques aren't new to the public, but. There had been various occasions when the legitimacy of a political race becomes introduced question in light of issues with the democratic framework. One essential case of that happened in Florida in 2000'selection among Republican chosen one George W. Shrubbery and Democrats candidate Al Gore. Both had close to cast a ballot tallies and the results of vote throwing in Florida, Oregon and New Mexico had been unequivocal to the general consequence of the political decision. After more noteworthy than half of a month, Bush changed into pronounced president-pick in a strategy that necessary relating vote in Florida. The occurrence warmed the contention of utilizing advanced deciding in favour of the inescapable decisions.[2]

5. LITERATURE REVIEW

Voting via e-voting is a modern democracy. It provides integrity, Authentication, security etc.This paper provides both its possibilities as well as its limitations. It provides the decentralized degree and places control. The vote cannot be detected & neither be changed. In the implementation details, Ethereum blockchain API network is being used. Various phase wise slotting is being mentioned due to which the systematic process gets defined Non fraudulent representative elections are important for the democracy of the government .Methods used for these public elections range from offline systems like Ballot based voting and purely electronic system like Electronic Voting Machines .Electronic methods pose certain problems, like voter confidence.Moura and Gomes explore the use of Blockchain to counter some e-voting issues. Liu and Wang (2017) investigated the use of blockchain in e-voting. E-voting

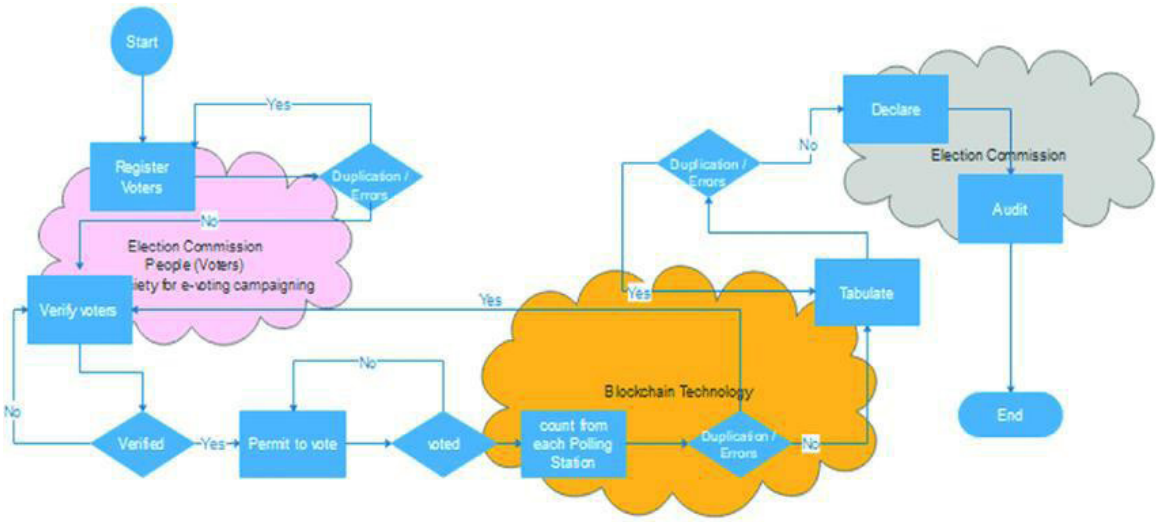

Figure 2: The electronic voting process with institutions involved.[8]

is environment friendly, real-time counting as well as processing and minor error-prone. However, it has been objected to criticism because of a lack of security. Many e-voting protocols use cryptographic tools. Some use a trusted third party (TTP) such that e-voting systems could be easily implemented and controlled. Liu and Wang develop a protocol which eliminates the need for a TTP so that anonymity and verifiability can be maintained. The protocol involves three phases and requires three participants—voter, organizer, and inspector. The *Pre-voting phase* involves registration if the voter is eligible. The V*oting phase* has two sub-phases - ballot preparation and ballot casting. The voter's two blind signatures indicate that he or she has been confirmed as an eligible voter and his or her choice has been recorded by both the organiser and the inspector. In the Post-voting phase, the organizer collects all valid ballots, which take the form of the election result. Singh and Chatterjee (2018) developed SecEVS (Secure Electronic Voting System) via blockchain technology. They identified some common issues in electronic voting systems and developed a secure voting system for university election. They ensured that the voting procedure did not involve any human interaction and was validated by the federation of system security analysis. SecEVS is made up of two concepts— hashing and encryption. It has the following components: participants (voters), organisers (in this case colleges under the university), inspectors (university election commission), encryption algorithms (AES, DES), hash algorithm (SHA-256), and voting server. In the system, a voter registers with the voting system and receives a voter ID. If the voter is eligible, a second page opens with the details of the contestants. The voter gives his or her vote which is encrypted by a public key and signed by the voter private key. The encrypted voter information is stored in the voter server where other votes are stored as well, creating one block of the blockchain. After the election is terminated at one college, blocks of individual college are joined together in collaboration for the zone level blockchain. The zone level blockchain join together for the university level blockchain, where the election committee checks all the votes and declares the final result. Blockchain is immune against different attacks and this system is encrypted using the vital SHA-256 hash algorithm and encryption algorithm for betterment. This system also resists duplication and forgery as the blockchain contains the hash of the previous block, signature and merkle root hash. For the storage of one block, 84 bytes are needed in which voter ID, signature, hash of previous data, timestamp, merkle root hash, and encrypted voting transaction data are stored.Zheng et al (2019) explored the use of Blockchain technology while controlling its high maintenance. Even though it provides decentralization, persistency, anonymity, and auditability; blockchain-based applications are complex to understand. BaaS (Blockchain-as-a-Service) are developed to embed the blockchain framework into the profound cloud computing platform. Various companies, like IBM and Microsoft, have released their own BaaS platforms which significantly reduce the difficulty of deployment and development. To respond to these shortcomings, Zheng et al developed NutBaaS (which means creating a hard barrier like a nutshell to protect blockchain applications). The architecture of NutBaaS is divided into four layers—the lowest being *Resource layer* (which provides storage, database, networks for blockchain services), followed by *Service layer* (where all basic and advanced blockchain services are implemented), *Application layer* (where appropriate applications are provided to find solutions to different business scenarios), and at the top is *Business layer* (where more business scenarios applicable for the use of blockchain technology are explored and invented).Garg et al (2019) reviewed the use of blockchain in e-voting systems. They identified trust, integrity and intermediaries as the three large problems in e-voting. These can be solved by blockchain as applications build on blockchain use multiple that is highly quantitative parties and no one can change either the minor part or update the data in it. This makes blockchain completely assurable and trustable. Since there is no single owner of blockchain, it provides autonomy to the users. Blockchain as a operation can be performed is a read and write only database and involves the formation of both encryption and decryption of data. This eliminates the need of intermediaries and makes it suitable for e-voting. In their literature review, Garg et al found that there is always a concern of authentication of the user that will require some biometric device or unique id. Blockchain based solutions provide a secure and reliable system irrespective of the platform and makes the voting system more transparent and error-free and issue free for the user as well.Shahzad and Crowcroft (2019) examined the issues causing mistrust in voting systems. Pre-polling rigging is an error to help certain parties and to hinder other parties. Another problem is casting of duplicate votes since there is no biometric authentication on the polling stations. Sometimes, power is used to influence the voters by giving them incentives or threats. For parties which have a weak representation in a region, their votes might be miscounted. Hearing of appeals on such issues is so slow that courts are generally avoided. Instead, parties take it on to streets instead of going to the constitutional bodies. Because of the lack of trust of voting systems in public, they generally do not participate in voting. The polling process proposed includes the physical and logical verification of the voter and the voter's data. The electronic voting process is verifiable by its physical record (that is the national identification and biometric authentication).

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

6. CHALLENGES OF VOTING

Governments and other stakeholders should address a few significant difficulties before blockchains see broad use for e-casting a ballot.[3]

- *Protection:* There will be no outsider intercession of any sort with respect to Election. Just Voter is permitted to see his/her subtleties and to whom casted a ballot. The main uncovered data in political race is all out votes to competitors just as in whole political decision.
- *Absence of Evidence:* Although protection with obscurity can guarantee shields against constituent misrepresentation. It is extremely unlikely to guarantee that votes are being casted under impact of fixes or any type of discretionary misrepresentation.
- *Extortion-Resistance:* Each certified voter ought to have the option to cast a ballot precisely once and no different people ought to have the option to cast a ballot. The framework must check the character of every potential voter and decide their status, yet should not permit this data to become related with their vote.
- *Ease-of-Utilization:* Elections must serve the whole open. It must be structure so that it very well may be utilized with negligible preparing and some specialized abilities.
- *Scalability:* Election is an approach to serve an enormous populace. It must be sufficiently adaptable to work everywhere.
- *Speed in service:* In this period, it must be ensuring that results is articulated inside not many long stretches of political race method closes.
- *Minimum Cost:* Cost is one of the majors for any structure plan. The System must be cost capable, having incredible adequacy and require least help as could sensibly be normal. [6]

7. PROS AND CONS

The utilization of Blockchain brings many capacity points of interest for vote throwing frameworks yet in addition experiences difficulties about which adopters should be cognizant. Straightforwardness, permanence, high accessibility, unwavering quality, auditability and voter certainty are some of gifts brought through its acknowledge as valid with less, conveyed and decentralized engineering. Be that as it may, Block chain time is a twofold edged sword. So as to convey to various hubs on a distributed system, vote throwing structures should be connected to that arrange. Thusly, hubs are without a moment's delay defenceless to digital insurance inconveniences and dangers. [2]

8. CONCLUSION

E-casting a polling form, as inspected, is an indispensable factor in improving the interest and participation of youth among the technically knowledgeable people. Late choices have given us how much the present election technique can improve to give a direct, solid and a lion's share rule condition. Apparatus of overview slow down, nonappearance of transparent, populism, etc are a part of the various issues that the present election process faces. Accordingly, making an electronic vote-based stage will bolster an increasingly conspicuous turnout during election process and extended voter's conviction. A potential response for deal with the recently referenced issues is Blockchain based law-based system. This paper examines the substantiality of Blockchain based voting system and its support in overcoming the weaknesses of the current structure. We acknowledge that the coursed record feature of Blockchain advancement will help us with conquering the shortcomings of the current structure and defeat the needfulness of Blockchain Technology.

9. REFERENCES

[1] Hardwick,Gioulis,Akram,Markantonakis(2018).E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy,IEEE.University of London, Egham, United Kingdom.

[2] Gomes(2006).Blockchain Voting and its effect on Election Transparency and Voter Confidence,IEEE Security and Privacy,Volume:4,Issue 1, Universidade de Brasilia,Brazil.

[3] Kshetri,Voas(2009).Blockchain-Enabled E-Voting, IDAACS , University of North Carolina at Greensboro.

[4] Wang(2009).An E-voting Protocol Based on Blockchain, ICAST, University of Science and Technology, Shenzhen, China.

[5] Zheng,Zheng1,2,Chen(2019).NutBaaS:A Blockchain-as-a-Service Platform, IEEEAccess,Sun Yat-sen University, Guangzhou 510006, China.

[6] Garg, Saraswat,Bisht (2019).A Comparitive Analysis on E-Voting System Using Blockchain IEEEAccess, AKTU, Uttar Pradesh, India.

[7] Singh, Chatterjee(2018).SecEVS : Secure ElectronicVoting System Using Blockchain Technology,International Conference on Computing, Power and Communication Technologies(GUCON),Greater Noida, Uttar Pradesh, India, India

[8] Shahzad,Crowcroft(2019).Trustworthy Electronic Voting Using Adjusted Blockchain Technology,IEEEAccess,University of Cambridge, Cambridge CB3 0FD, U.K

[9] http://people.cs.pitt.edu/~mosse/courses/cs3720/ blockchain-iot.pdf

[10] https://longvan.net/blockchain-la-gi-ung-dung-cua-cong-nghe-blockchain.html

 2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

AUTHORS

Ms Tanvi Shah has obtained Diploma in computer engineering in 2017.She is currently pursuing Bachelors in Engineering from Atharva College of Engineering.

Ms Sneha Kadam has obtained Diploma in computer engineering in 2017.She is currently pursuing Bachelors in Engineering from Atharva College of Engineering.

Ms Ankita Mane has obtained Diploma in computer engineering in 2017.She is currently pursuing Bachelors in Engineering from Atharva College of Engineering

Ms Tanvi Kapdi working as an Assistant Professor at Atharva College of Engineering.
Her area of specialization is network security.

2010-2019 S-JPSET : Vol. 12, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)