IRJET- A Study on Decentralized E-Voting System Using Blockchain Technology

IRJET Journal

A Study on Decentralized E-Voting System Using Blockchain Technology

Mrs. Harsha V. Patil[1], Mrs. Kanchan G. Rathi[2], Mrs. Malati V.Tribhuwan[3]

[1,2,3] *Assistant Professor, Dept. of Computer Science, Dr. D .Y. Patil ACS College, Pimpri , Pune-18, Maharashtra, India.*

Abstract - *Election is a very important event in a modern democracy but large sections of society around the world do not trust their election system which is major concern for the democracy. Even the world's largest democracies like India, United States, and Japan still suffer from a flawed electoral system. Vote rigging, hacking of the EVM (Electronic voting machine), election manipulation, and polling booth capturing are the major issues in the current voting system [10]. In this paper, we are investigating the problems in the election voting systems and trying to propose the E-voting model which can resolve these issues. Also this article aiming to evaluate the application of blockchain as service to implement distributed electronic voting systems. The section of paper will highlight some of the popular blockchain frameworks that offer blockchain as a service and associated electronic E-voting system which is based on blockchain that addresses all limitations respectively, it also preserve participant's anonymity while still being open to public inspection.*

***Key Words*: Blockchain, Decentralization, Voting scheme, Distributed System, EVM, Anonymity**.

1. INTRODUCTION

Blockchain being relatively a new technology, a representative sample of research is presented, spanning over the last ten years, starting from the early work in this field. Different types of usage of blockchain and other digital ledger techniques, their challenges, applications, security and privacy issues were investigated. Some countries have already taken the initiative to improve their voting system by using blockchain technology and decentralized peer to peer network accompanied by a public ledger. (Nakamoto, *et al*,2008) [10]. **Sierra Leone** became the first country in the world to use blockchain Technology to verify votes in an election in **March, 2018**. The inability to change or delete information from blocks makes the blockchain the best technology for voting systems. Blockchain technology is supported by a distributed network consisting of a large number of interconnected nodes. Each of these nodes have their own copy of the distributed ledger (information) that contains the full history of all transactions the network has processed. There is no single authority that controls the network. If the majority of the nodes agree, they accept a transaction. This network allows users to remain anonymous. A basic analysis of the blockchain technology (including smart contracts) suggests that it is a suitable basis for e-voting and moreover, it could have the potential to make e-voting more acceptable and reliable [7].

Modern democracies are built up on voting system, whether traditional ballot based or electronic voting (e-voting). In recent years voter apathy (lack of interest) has been increasing, especially among the younger computer/techno savvy generation. E-voting is pushed as a potential solution to attract young voters. For a robust e-voting scheme, a number of functional and security requirements are specified including transparency, accuracy, auditability, system and data integrity, secrecy/privacy, availability, and distribution of authority.

Existing works explore how blockchain can be used to improve the e-voting schemes or provide some strong guarantees of the above listed requirements. However, these papers do not discuss the implementation challenges and limitations of the blockchain (and smart contract) technologies at their current state to fully support a large scale voting scheme. In this paper we explore both the possibilities of an e-voting scheme, along with the challenges and limitation of the blockchain technology in the e-voting context.

1.1 TRADITIONAL E-VOTING SYSTEM

Recent major technical challenges regarding e-voting systems include, but not limited to secure digital identity management. Any potential voter should have been enrolled to the voting system prior to the elections. Their information should be in a digitally processable format. Besides, their identity information should be kept private in any involving database. Traditional E-voting system may face following problems:

Anonymous vote-casting: Each vote may or may not contain any choice per candidate, should be anonymous to everyone including the system administrators, after the vote is submitted through the system.

Individualized ballot processes: How a vote will be represented in the involving web applications or databases is still an open discussion. While a clear text message is the worst idea, a hashed token can be used to provide anonymity and integrity. Meanwhile, the vote should be non-reputable, which cannot be guaranteed by the token solution.

Ballot casting verifiability by (and only by) the voter: The voter should be able to see and verify his/her own vote, after he/she submitted the vote. This is important to achieve in order to prevent, or at least to notice, any potential malicious activity. This counter measure, apart from providing means of non-repudiation, will surely boost the feeling of trust of the voters. These problems are partially addressed in some recent applications. Yet, means of e-voting is currently in use in several countries including Brazil, United Kingdom, Japan, and **Estonia**. Estonia should be evaluated differently than the others, since they provide a full e-voting solution that is, said to be, equivalent of traditional paper-based elections.

High initial setup costs: Though sustaining and maintaining online voting systems is much cheaper than traditional elections, initial deployments might be expensive, especially for businesses.

Increasing security problems: Cyber attacks pose a great threat to the public polls. No one would accept the responsibility if any hacking attempt succeeds during an election. The DDoS attacks are well known and mostly not the case in the elections. The voter integrity commission of the United States gave a testimony about the state of the elections in the US recently. Accordingly; Ronald Rivest stated that "hackers have myriad ways of attacking voting machines". As an example; barcodes on ballots and smartphones in voting locations can be used in the hacking process. Apple stated that we mustn't ignore the fact that computers are hackable, and the evidences can easily be deleted. Double-voting or voters from the other regions are also some common problems.

To mitigate these threats, software mechanisms which promise the following should be deployed:

- Prevention of evidence deletion.
- Transparency with privacy.

Lack of transparency and trust: How can people surely trust the results, when everything is done online? Perceptual problems cannot be ignored.

Voting delays or inefficiencies related to remote/absentee voting: Timing is very important in voting schemes; technical capabilities and the infrastructures should be reliable and run at the highest possible performance to let remote voting be synchronous.

The blockchain technology may address many issues regarding e-voting schemes mentioned in above section and make e-voting cheaper, easier, and much more secure to implement. It is a considerably new paradigm that can help to form decentralized systems, which assure the data integrity, availability, and fault tolerance. Some state that "the blockchain technology is bringing us the Internet of value: a new, distributed platform that can help us reshape the world of business and transform the old order of human affairs for the better." .This technology aims to revolutionize the systems. The blockchain systems are formed as decentralized networked systems of computers, which are used for validating and recording the pure online transactions. They also constitute ledgers, where digital data is tied to each other, called the blockchain. The records on the blockchains are essentially immutable.

1.2 WHAT IS BLOCKCHAIN

The simple explanation is a 'chain' of blocks. A block is an aggregated set of data. Data are collected and processed to fit in a block through a process called mining. Each block could be identified using a cryptographic hash (also known as a digital fingerprint). The block formed will contain a hash of the previous block, so that blocks can form a chain from the first block ever (known as the Genesis Block) to the formed block. In this way, all the data could be connected via a linked list structure.

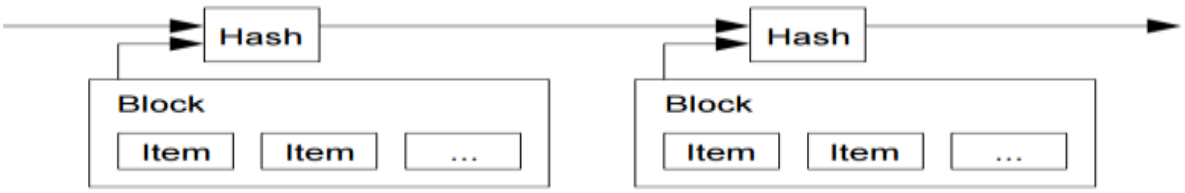


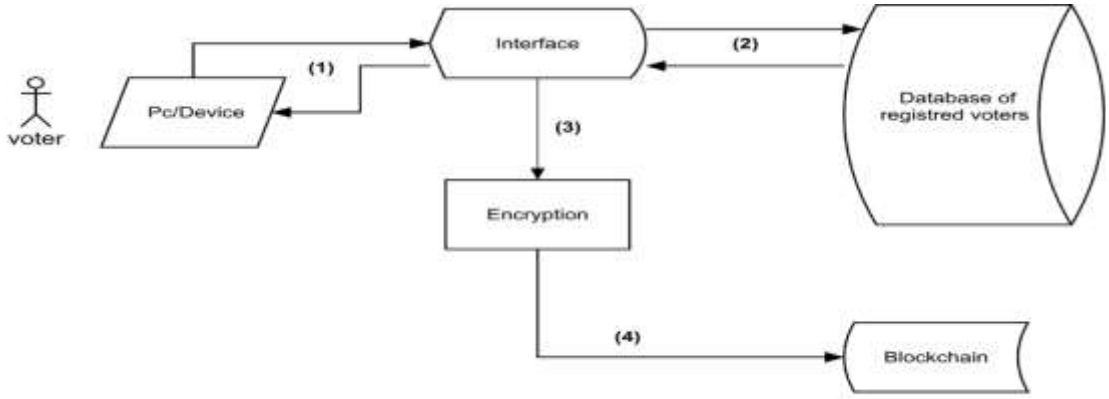
Fig 1.A Visual illustration of Blockchain

Source Bitcoin: A Peer-to-Peer Electronic Cash System, S. Nakamoto

2. WORKING OF E-VOINT USING BLOCKCHAIN

- The first transaction added to the block will be a special transaction that represents the candidate [1].
- When this transaction is created it will include the candidate's name and will serve as the foundation block, with every vote for that specific candidate placed on top of it. Unlike the other transactions, the foundation will not count as a vote, and it will only contain the name of the candidate.
- Our e-Voting system will allow a protest vote, where the voter may return a blank vote to demonstrate dissatisfaction with all candidates or a refusal of the current political system and/or election.
- Every time a person votes the transaction gets will be recorded and the blockchain will be updated.

To ensure that the system is secure, the block will contain the previous voter's information. If any of the blocks were compromised, then it would be easy to find out since all blocks are connected to each other [1].The blockchain is decentralized and cannot be corrupted, no single point of failure exists. The blockchain is where the actual voting takes place. The user's vote gets sent to one of the nodes on the system, and the node then adds the vote to the blockchain. The voting system will have a node in each district to ensure the system is decentralized.



Blockchain Based Electronic Voting System

As per the above structure the working of e-voting system using blockchain is:

(1)Requesting to vote: The user will have to log in to the voting system using his credentials- in this case, the e-voting system will use his Social Security Number, his address, and the voting confirmation number provided to registered voters by the local authorities [1]. The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote. Our e-Voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to the Sybil attack where attackers claim a large number of fake identities and stuff the ballot box with illegitimate votes.

(2) Casting a vote: Voters will have to choose to either vote for one of the candidates or cast a protest vote. Casting the vote will be done through a friendly user interface [1]. For each voter a token is generated known as Ethereum, with initial Boolean value one, once a vote is casted it becomes 0. A voter can cast a vote if and only if Ethereum value is 1.In this way revoting problem is resolved.

(3) Encrypting votes: After the user casts his vote, the system will generate an input that contains the voter identification number followed by the complete name of the voter as well as the hash of the previous vote. This way each input will be unique and ensure that the encrypted output will be unique as well. The encrypted information will be recorded in the block header of each vote cast. The information related to each vote will be encrypted using SHA one-way hash function that has no known reverse to it. The only theoretically possible way to reverse the hash would be to guess the seed data and the encryption method and then hash it to see if the results match. This way of hashing votes makes it nearly impossible to reverse engineer, therefore there would be no way voters' information could be retrieved [1].

(4) Adding the vote to the Blockchain: After a block is created, and depending on the candidate selected, the information is recorded in the corresponding blockchain. Each block gets linked to the previously cast vote.

Opportunities and Benefits of Blockchain in E-voting (BEV)

BEV provides the following opportunities and benefits.

- To address voter tampering, blockchains generate cryptographically secure voting records. Votes are recorded accurately, permanently, securely, and transparently. So, no one can modify or manipulate votes. Furthermore, blockchains preserve participant's anonymity while still being open to public inspection. Although nothing is totally secure, tampering is nearly impossible with blockchains [12].
- BEV might promote more voter participation. For instance, corporate annual general meetings can be costly events with low shareholder participation. With increasing cross border investments, companies face pressure to increase in investor engagement. BEV is a flexible solution that enables secure, cost-effective voting to facilitate shareholder participation and voting from a distance.
- Also, improved identity verification can help increase access and participation. For example, according to a federal court in Texas, 608,470 registered voters lacked verification identification. Approximately 11 percent of US citizens lack government-issued photo identification cards. BEV can improve this situation. For instance, Voatz accepts 10 different official documents including driver's licenses, state IDs, and passports to verify voter identity.
- BEV can increase the speed with which votes are tallied. For example, Agora reported that it published election results on its website five days before the official manual counts ended.
- BEV can eliminate ambiguities. For example, in the 2017 Virginia House of Delegates election, the winner was chosen from paper ballots placed in a bowl. One vote initially wasn't counted because that voter made confusing marks on the ballot. Such ambiguity is less likely to arise with BEV [12].
- BEV can promote greater transparency and clarity to voters. As of 2017, 23 countries in had adopted online voting. Current online-voting processes might be complicated for some voters. It's not easy to know whether a vote was cast as intended or whether it was counted as cast. As we already noted, blockchain results are publicly auditable.
  Some security systems in electronic and online-voting platforms were possibly developed decades ago and are vulnerable to tampering. Consider the WINVote touch screen machines made by Advanced Voting Solutions, which went out of business in 2015.25 WINVote machines were used in the 2016 US elections even though they hadn't had a security patch since April 2014. A security expert found that anyone within a half-mile of a voting machine could have altered votes without detection. Blockchain's decentralized nature makes attacks more difficult.
- Finally, with BEV, individual votes will be publicly available, while voters are masked behind an encrypted key. This offers greater privacy and security than traditional ballot boxes and could reduce voter suppression. Bad actors can't identify voters and therefore can't target them [12].

Challenges for E-Voting system using blockchain

- Governments and other stakeholders will need to address several major challenges before blockchain's see widespread use for e-voting. Although blockchain's are good at providing security and accuracy, public confidence and trust are necessary ingredients for BEV's success. Blockchain's complexity might hinder mainstream public acceptability of BEV. Broadband access and digital user skills are also concerns.
- In 2016, the nonprofit Democracy Earth Foundation used a blockchain to give Colombian expatriates a voice in the 2016 peace plebiscite that was conducted to ratify the agreement to terminate the conflict between the Colombian government and FARC guerillas. According to the foundation, a main challenge in the deployment blockchain is the technology's immaturity.
- Let's now consider software quality. Estimates have suggested that, on average, there are from 15 to 50 defects per 1,000 LOC. For Ethereum, the blockchain-based distributed-computing platform used by Moscow's Active Citizen program (which features smart contracts), the number might be twice that. This might be attributed to Ethereum's immaturity. The Economist quoted a blogger who said that Ethereum contracts are "candy for hackers."29 Also, sufficient observations haven't yet been accumulated to determine blockchain-based platforms' scalability [12].
- Traditional voting emphasizes the authority of the state. BEV emphasizes voter transparency. The BEV process is transparent, decentralized, and bottom-up. BEV might not perform well in a society whose culture and values exhibit low compatibility with these values.
- Also, blockchains require much energy to perform authentication and validation, and they're slow. So, using them for national e-voting might not be practical yet.
- Finally, BEV will shift power away from central actors such as electoral authorities and government agencies. Thus, the technology is likely to face resistance from political leaders who benefit from the status.

3. CONCLUSION

The transparency of the block-chain enables more auditing and understanding of elections. These attributes are some of the requirements of a voting system. These characteristics come from decentralized network, and can bring more democratic processes to elections, especially to direct election systems. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on blockchain technology. This paper explores the potential of the blockchain technology and its usefulness in the e-voting scheme. The blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it.

REFERENCES

[1] Ahmed Ben Ayed(2017);A Conceptual Secure Blockchain –Based Electronic Voting System; International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3,

[2] Pavel Tarasov and Hitesh Tewari(2017);The Future of E-Voting; IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165 I

[3] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3(2017);An Overview of Blockchain Technology : Architecture,Consensus, and Future Trends; IEEE 6th International Congress on Big Data.

[4] Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander3(2016); Where Is Current Research on Blockchain Technology?—A Systematic Review;PLOS-ONE.

[5] Mahdi H. Miraz1, Maaruf Ali2(2018); Applications of Blockchain Technology beyond Cryptocurrency;Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018

[6] Michael Crosby, Google,Nachiappan, *Yahoo,*Pradhan Pattanayak, Yahoo,Sanjeev Verma, Samsung Research America,Vignesh Kalyanaraman, Fairchild Semiconductor(2015);Blockchain Technology Beyond Bitcoin.

[7] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis (2018); E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy; arXiv:1805.10258v2 [cs.CR]

[8] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, Hyoung Joong Kim(2016); Electronic Voting Service Using Block-Chain; Journal of Digital Forensics, Security and Law.

[9] Aayushi Gupta1*, Jyotirmay Patel2, Mansi Gupta1, Harshit Gupta1(2017); Issues and Effectiveness of Blockchain Technology on Digital Voting; International Journal of Engineering and Manufacturing Science. ISSN 2249-3115 Vol. 7, No. 1 (2017)

[10] Gautam Srivastava1, Ashutosh Dhar Dwivedi2 and Rajani Singh2(2018); Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology.

[11] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson(2018);Blockchain-Based E-Voting System.

[12] Nir Kshetri and Jeffrey voas(2018);Blockchain Enabled E-Voting;www.computer.org/software.

[13] Umut Can Çabuk1, Eylül Adıgüzel2, Enis Karaarslan2(2018); A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems; International Journal of Advanced Research in Computer and Communication Engineering.

[14] Madise, Ü. & Martens, T. (2006). E-voting in Estonia 2005. The first practice of countrywide binding Internet voting in the world. Electronic Voting, 86.

[15] S. Raval, "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology." O'Reilly Media, Inc. Sebastopol, California (2016).

[16] Jason Paul Cruz1,a) Yuichi Kaji2,b)(2017);E-voting System Based on the Bitcoin Protocol and Blind Signatures ; IPSJ Transactions on Mathematical Modeling and Its Applications Vol.10 No.1 14–22.

[17]https://www.google.com/A+Simple+Representation+of+the+Blockchain+Structure+of+each+Candidate+in+e+voting

[18] http://www.doc.ic.ac.uk/~ma7614/topics_website/tech.html

AUTHORS

Mrs.Harsha V. Patil ,M.Sc.(CS),NET
Working as Assist. prof in Dr. D.Y. Patil ACS college, Pimpri, Pune

Mrs.Kanchan G.Rathi, MMS(comp mgmt) Working as Assist. prof in Dr. D. Y. Patil ACS college, Pimpri, Pune

Mrs.Malati V. Tribhuwan, M.Sc(CS), Working as Assist. prof in Dr. D.Y . Patil ACS college, Pimpri, Pune