E-Voting System using BlockChain

Kurakula Tanu Sri
School of Computer Science and Engineering
VIT Vellore, Tamil Nadu, India

Kurakula Rupa Sri
School of Computer Science and Engineering
VIT Vellore, Tamil Nadu, India

Nikhita Pedamallu
School of Computer Science and Engineering
VIT Vellore, Tamil Nadu, India

Abstract- In recent years, traditional elections satisfy neither citizens nor political authorities. They are not fully secure since it is easy to tamper and influence votes. It threatens the privacy and transparency of voters. Blockchain technology is one of the solutions to overcome this problem by decentralizing the information publicly by avoiding the manipulation of data and gain the trust of citizens. E-Voting system can be exceptionally useful as everybody can get to it effectively with their decisions even from the far places. In this paper, we have compared centralization and decentralization of E-Voting system using Blockchain.

Keywords – E-Voting, Blockchain, EVM, Blind Signature, TTP, Centralized e-voting, decentralized e-voting, smart contracts.

I. Introduction

The heart of democracy is voting. In order to ensure a fair and credible election process, security and reliability must be guaranteed in every stage of the process. The success of a democracy depends on the degree of fairness and reliability of its elections.

Elections initially took place via ballot boxes where in people had to mark their votes on a piece of paper and submit it in a ballot box. This was highly insecure and easily tampered. Mostly, these ballots were manually counted and this led to a considerable delay in the election process. Also, there was no guarantee of vote secrecy.

After the ballot boxes, the Electronic Voting Machines (EVM'S) were used. The electronic voting machines allowed fast declaration of the results. However, as the increase of attackers and the methods of attacking continues the hacking and tampering of such machines is highly probable and often occurred. Physical access to an EVM, even for a few minutes, is enough for it to be tampered. The above will lead to a violation of the basic functional requirements of equality and secrecy for a secure EVM.

Since software devices connected to a network are vulnerable, a security concept derived from the popular technology, blockchain, is applied in this proposed work. It is currently being implemented for the purpose of securing online monetary transactions in the digital economy. Blockchain has paved the way for cryptocurrency services such as Bitcoin and Ethereum. Blockchain is a distributed and inconvertible ledger through which data is added and updated in real time via consensus of the nodes running the software in the network. But the data cannot be removed or edited in database once it is added to the ledger. Therefore, it is not possible to tamper the votes which makes e-voting system progressively securable.

The rest of the paper is organized as follows. Literature Survey is done in section II. Objectives are presented in section III. Comparative Study is done in section IV. Conclusion and future scope is given in section V and VI.

II. Literature Survey

The use of digital technology has increased globally over the past few years. Technology in voting helps in fair elections and is cost-effective. E-Voting and I-Voting elections were held in a few countries like Estonia, Norway etc [1]. Most

E-voting systems that exist are based on centralized servers where the voters must trust the third party to tally their votes. Centralisation is also used at the phase of voter's eligibility [2]. Powerful Central authority or a trusted third party may become a vulnerable spot for the entire system as there is no transparency. So, in some countries, e-voting systems have not been widely accepted due to the security and transparency issues. But the technology like blockchain and smart contracts can solve the above issues very efficiently. In e-Voting based Blockchain, it is not possible to modify the votes once it is accepted to the database and blockchain transactions are encrypted. So, it is very hard to hack and it provides more security to the system. Smart contracts on the other hand automatically execute transactions and they are shared among the participants. Smart contracts remove the need of intermediates to validate and verify the votes. Thus, there is transparency that builds trust among voters. Smart contracts follow decentralization in e-voting [3].

Block chain under decentralization does not rely on any trusted third party (TTP) that enhances data verifiability and maintains transparency in voting. The primary goal of decentralization is to acknowledge that it has secure application using block chain innovation. Voters can compute the tally and election results on their own without TTP [4].

Decentralization at voter's eligibility verification helps to provide a secure and flexible voting mechanism which weakens the power of an election organizer [5]. Decentralization at the tallying level is transparent to voters and any third party, which allows the voters to verify their votes is indeed counted and it allows any third party to tally their votes [6][7][8][9]. Ethereum Virtual Machine (EVM) can be utilized as the Blockchain runtime condition, on which predictable, transparent and deterministic smart contracts will be conveyed by organizers for each casting a ballot event to run the democratic standards [10].

III. OBJECTIVES

The contribution of the paper can be summoned as:

- To explain the transition in voting.
- To analyse and compare the different modes of e-voting system like centralized and decentralized based e-voting at eligibility verification phase.

IV. COMPARATIVE STUDY

4.1 Transition in Voting

In order to allow an electronic voting system to compete with the most commonly used ballot system, it needed to support the same measures and mechanisms as the traditional system supports. Those are mainly security and anonymity. An e-Voting system must have higher security measures in order make sure it is available to voters but also protected against outside influencers being able to change votes that are being casted or voter's ballot from being tampered with. There are many intelligence agencies around the world that control different parts of the Internet which allow them to identify or intercept votes.

Traditional voting machines require the presence of the voter at allocated polling stations. Although this might seem simple, many drawbacks are associated. Due to physical presence at polling stations the ratio of population participation has drastically decreased. The major reason for this is migration of citizens to various states or countries, incapability of disabled or old citizens to reach till polling stations etc. Proxy, location and postal voting are the de-facto methods for remote voting, but those are inconvenient, insecure, lack privacy and do not guarantee that your vote is also being included in the election results. The drawbacks of traditional voting systems are: inaccuracy, insecurity, inconvenience, time-consumption, eligibility criteria, lack of privacy, lack of transparency, resource intensive, extensive work and human resource requirement etc.

To counter all these issues a new voting mechanism has been thought of that is the electoral voting machine. This method does not require physical presence at polling booths and allows votes to be casted from anyplace.

A robust voting system should comprise:

- In-person voting, when voters are expected to show up at a special location to cast their ballots. This may take place in an electronic voting machine or on paper ballots that can be counted electronically.
- Remote voting, when voters are allowed to cast their ballot from anywhere in the country or around the globe using a secure Internet voting platform.

The major challenge faced for electronic voting system is the matter of security and integrity. The first e-voting machine started in the early eighties. The several methods used were Estonian I-Voting System, Norwegian I-Voting System, New South Wales i-Vote System, and D.C Digital Vote-by-Mail Service.

This was the basic mechanism followed where the vote was encrypted using pubic key of government ID and private key of voters ID. However, this system proved to have drawbacks in security as keys could be intercepted and votes could be modified. This led to the usage of the Blockchain technology.

4.2 Case Study

Estonian Elections:

The Estonian I-voting solutions provided by Cybernetica is the most successful and highly trusted online voting solution. It has been used in Estonian elections since 2005.

Estonian internet voting system builds on the Estonian ID card which is a regular and mandatory national identity document for the secure authentication and legally binding the digital signatures by the Estonian supported public key infrastructure. Voters can change their electronic votes as many times but the last modified vote is taken into consideration. The voters may also cast their vote in the ballots thus invalidating their internet vote. As per the Estonian Municipal Elections (2017) a comparison is made on the cost-efficiency based on e-voting and concluded that it is the most cost-efficient voting channel provided by the Estonian government. As per the 2019 elections there is an increase in 41.9% of online voters when compared to that of 2005 elections. So, there is an increase in demand for online voting and other countries are looking forward to implementing this kind of method for the elections.

The graph is about the percentage of online voters in Estonia from the year 2005-2019.

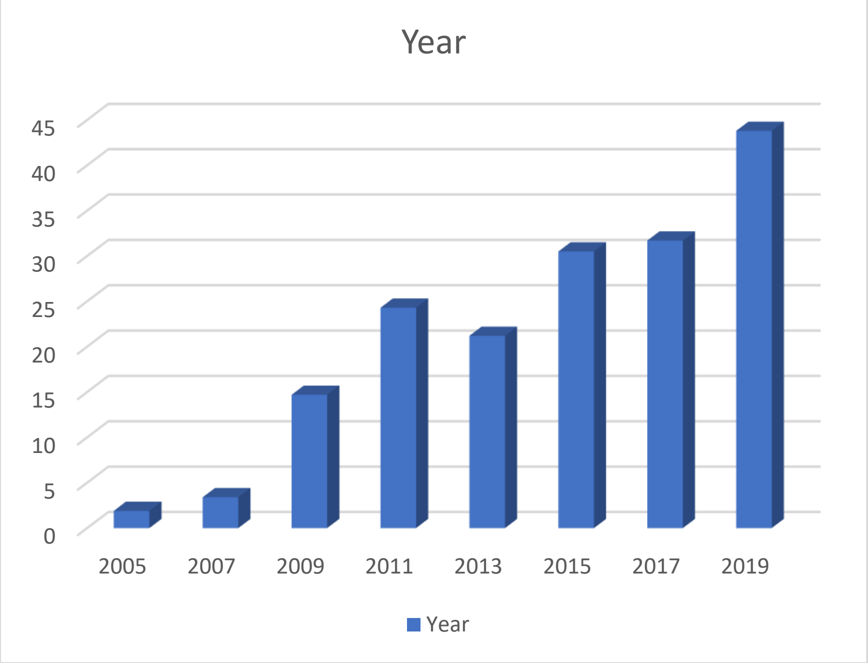

Figure 1. Percentage of online voters in Estonia

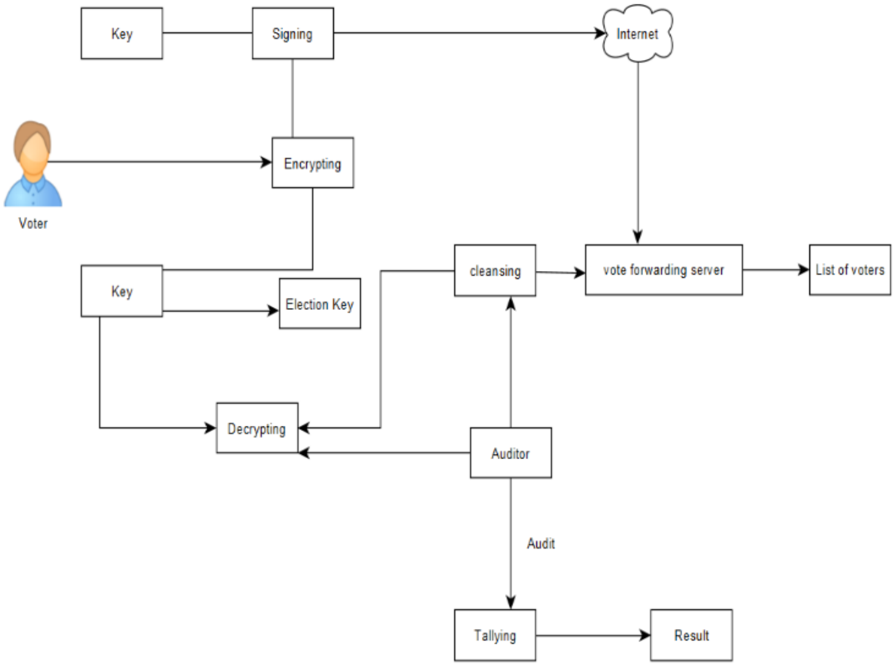

Figure 2. Estonian digital voting system

4.3 Centralized E-Voting

4.3.1 At the phase of voter's eligibility verification

There have been many proposed methods of e-voting systems using blockchain with the help of third-party verification. In order for an e-voting system deemed secure then the following properties need to be satisfied.

- Fairness: no results to be revealed before the end of the voting process which obstructs the influential votes.
- Eligibility: Only eligible voters can cast their vote and authentication is the basis of this property.
- Privacy: The identity of the voter should be kept private and should not be revealed to anyone.
- Verifiability: This property guarantees the voters and the parties whether their vote is counted in a right way. Typically, there are two types of verifiability, individual verifiability allows the individual participants to check whether one's vote has been counted and universal verifiability requires anyone can verify the election outcome.

Certain degree of centralization is needed to reach the primary goal. In order for the voting protocol to authenticate the eligible voters then a central authority is to be introduced. For a voter to be eligible he/she needs to authenticate themselves to the central authority by receiving a token that proves the eligibility of the voters. The central authority (third party) is the central point of the protocol and assumed to be trusted. The voter needs to prove his eligibility by sending his digital commitment and public key pair to the central authority and the central authority does the blind signature on the pair and sends it back to the voter and he would unblind the signed message and that would end up with an eligible valid token. If the voter is not eligible then it is dropped by the network. An additional failsafe needs to be added to provide more security in the voting system by introducing a multi signature scheme where more than one central authority would need to sign an eligibility token to produce valid signature over it. Each central authority manages to keep a part of voter's authentic information, making it impossible to steal the other person's vote. The voters use the eligibility tokens as a proof to participate in the voting process.

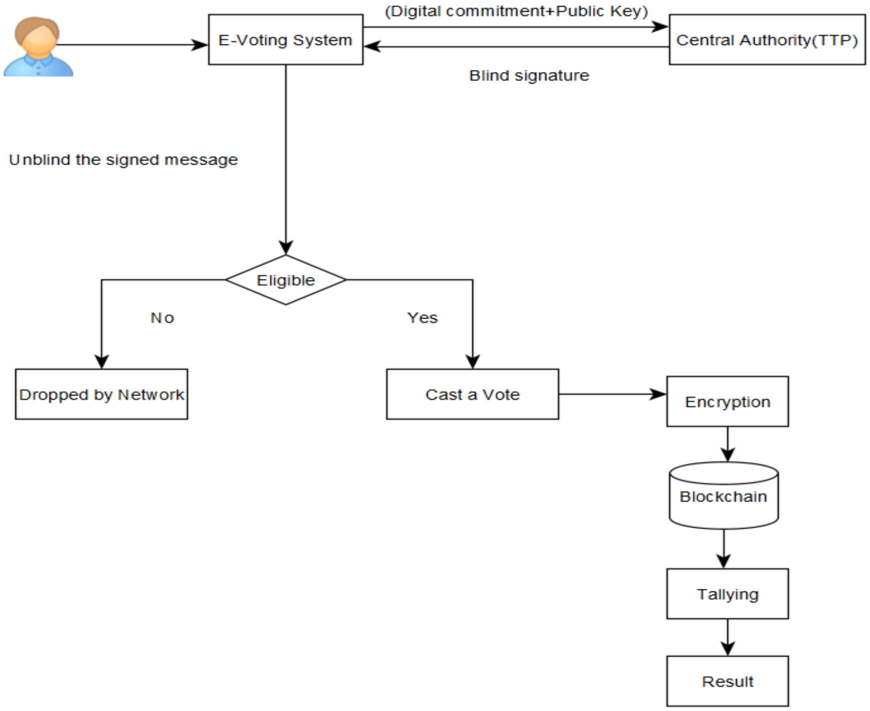

Figure 3. Centralization at voter's eligibility verification

There are different phases in voting that makes it inherently secure.

- Initialization phase: In initialization phase there is a genesis contract that contains all the information to verify and validate the users and it ensures that none of the votes is placed after a particular time.
- Voting phase: Before casting a vote, the voter must have to communicate with the central authority to verify and receive a signed token that represents their eligibility. When the submission is made then the voter must include the component parts of the signed token and the message token is to be verified to have been signed by a public key of the election, and the current time is checked whether the voter cast their vote within the allotted time.

4.4 Decentralized E-Voting

4.41 At the phase of voter's eligibility verification

There has been a lot of e -voting protocols using centralized third party to make e-voting systems easily implemented and controlled. But there are some drawbacks in using centralized trusted party as it may become the vulnerable part of the whole system. So, it is safe to use a decentralized e-voting protocol which provides a secure and flexible voting mechanism which weakens the power of an election organizer.

There are two main techniques used to preserve voter's choices are blind signature and blockchain. In decentralized e-voting systems participants are divided in to 3 categories namely voters, organizers and inspectors.

- Voters contain a set of voters that are eligible to participate in the election.
- Organizer's duty is to verify and record eligible voter's information and interact with the voters.
- Inspectors duty is to limit and inspect the organizer's power and also interact with the voters. It is better to have more than one inspector as it scales up the decentralization in e-voting.

During the pre-voting phase the voter registers as an eligible voter by submitting personal information and a public key of the voter in the channel that an organizer provides. After the registration, the organizer adds voter's information in to eligible voters list.

During the voting phase the voter sends their vote by applying a hash function and a function for blind signature and sends it to the organizer. The organizer in turn does the blind signature the function sent by the voter and it is returned to the voter. The same procedure goes with the voter and inspectors. The inspector check whether the voter has sent the same hashed message to organizer and in the voters list. If both are true then inspector signs the message and it is returned to the voter. The two signatures by the organizer and inspector indicate that the voter is an eligible voter and the voter’s choice have been confirmed by both the organizer and the inspectors.

The ballot is considered to be valid if the voting string is in format together with both the organizer and inspector signatures and it should be casted on time.

In post-voting phase the organizer collects all the valid ballots that he has received and starts to tally, which produces the result of the election. The verification can be done by all the participants who have permission to see the blockchain.

Consider:

V: Voting String

C_{Voters}: Voter function for blind signature.

$S'_{Organizer}$,$S'_{Inspectors}$: Functions used for signing the ballots.

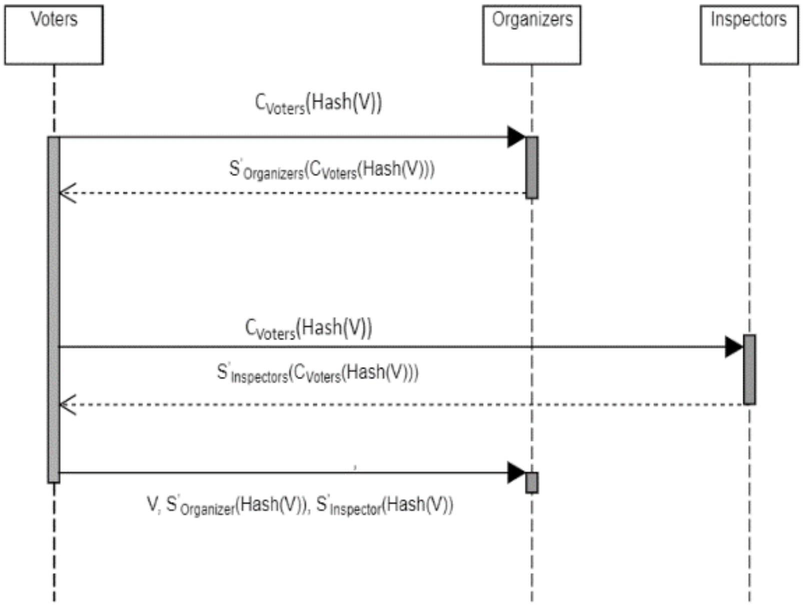
Voters
Organizers
Inspectors
C_Voters(Hash(V))
S'Organizers(CVoters(Hash(V)))
CVoters(Hash(V))
S'Inspectors(CVoters(Hash(V)))
V, S'Organizer(Hash(V)), S'Inspector(Hash(V))

Figure 4. Decentralization at voter’s eligibility verification

V. CONCLUSION

In some countries like Germany, Kazakhstan and Netherlands the e-voting system is rejected due to the lack of universal verifiability. So, in order to overcome that problem decentralised e-voting by using blockchain is used. Decentralization allows the voters to view their vote being counted correctly as almost all the participants in the blockchain have roughly the same database and it is possible for the voters and third parties to tally and verify the election results.

In the above methodology, as we compared the e-voting system using blockchain that has centralization and decentralization at the voter’s eligibility verification phase, it is more secure if the decentralization at different phases of e-voting is used to make the system more decentralised and secure.

VI. FUTURE SCOPE

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. In this paper we discuss and compare between the centralized and de-centralized voting methods.

The combination of both traditional voting and e-voting systems together prevents the encounter with issues of physical presence, requirement of electronic machine, etc. For future scope, it is seen to develop an encryption methodology, while using hybrid techniques, to increase the security of existing models and improve its resistance to vulnerable attacks. It is also seen to upgrade the system to allow it to handle a large number of connected devices and also to improve the concurrency of the model. The model will be enhanced to reduce the time taken for registration of votes and for verifying the transactions. Alternative biometric authentication mechanisms such as iris scanning, voice and face recognition can be used to replace the functionality of the fingerprint authentication system or the physical identity proof.

REFERENCES

[1] Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications, 9(3), 01-09.

[2] Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K. (2018, July). E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In 2018 IEEE International Conference onInternet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1561-1567). IEEE.

[3] Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 983-986). IEEE.

[4] Hsiao, J. H., Tso, R., Chen, C. M., & Wu, M. E. (2017). Decentralized E-voting systems based on the blockchain technology. In Advances in Computer Science and Ubiquitous Computing (pp. 305-309). Springer, Singa.

[5] Liu, Y., & Wang, Q. (2017). An E-voting Protocol Based on Blockchain. IACR Cryptology ePrint Archive, 2017, 1043.

[6] Zou, X., Li, H., Sui, Y., Peng, W., & Li, F. (2014, April). Assurable, transparent, and mutual restraining e-voting involving multiple conflicting parties. In IEEE INFOCOM 2014-IEEE Conference on Computer Communications (pp. 136-144). IEEE.

[7] McCorry, P., Shahandashti, S. F., & Hao, F. (2017, April). A smart contract for boardroom voting with maximum voter privacy. In International Conference on Financial Cryptography and Data Security (pp. 357-375).Springer, Cham.

[8] Panja, S., & Roy, B. K. (2018). A secure end-to-end verifiable e-voting system using zero knowledge based blockchain. IACR Cryptology ePrint Archive, 2018, 466.

[9] Adiputra, C. K., Hjort, R., & Sato, H. (2018, October). A proposal of blockchain-based electronic voting system. In 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4) (pp. 22-27). IEEE.

[10] Khoury, D., Kfoury, E. F., Kassem, A., & Harb, H. (2018, November). Decentralized voting platform based on ethereum blockchain. In 2018 IEEE International Multidisciplinary Conferenceon Engineering Technology (IMCET) (pp. 1-6). IEEE.