Features of Blockchain Voting: A Survey

Dr. S. F. Sayyad
Department of Computer Engineering
AISSMS COE, SPPU Pune, India

Mangesh Pawar
Department of Computer Engineering
AISSMS COE, SPPU Pune, India

Ashutosh Patil
Department of Computer Engineering
AISSMS COE, SPPU Pune, India

Vandana Pathare
Department of Computer Engineering
AISSMS COE, SPPU Pune, India

Prayag Poduval
Department of Computer Engineering
AISSMS COE, SPPU Pune, India

Abstract

Since people have recognized the potential of Blockchain technology, many researchers tried to find real-life applications of Blockchain. Blockchain has become famous after its first application which was Bitcoin, a digital currency based on Blockchain technology, inheriting its potential from the decentralized network. After Bitcoin, many digital currencies incepted. For many years Blockchain has been misunderstood as the public ledger which can be used for maintaining the online currency transaction record. People were less aware of the other features and so the applications of Blockchain. One of the most suitable example inheriting many features of the Blockchain is online Voting or decentralized Voting. Many researchers have proposed several solutions inheriting the diverse features of the Blockchain. Understanding the features and their importance in Blockchain Voting is an important topic that we need to concern. This features will then be used to develop a more secure and transparent voting solution.
Keywords: Blockchain, Ethereum, Online Voting, Encryption, Blockchain voting features

I. INTRODUCTION

Online voting is considered the most glitchy use of modern technology because of its major security issues. Developing the online voting system is a nightmare for many researchers. It's been challenging to develop an online voting system which can satisfy the legal requirements of a democratic country. The Mystic advancement is needed in the existing Information Technology world. Blockchain technology has come up with interesting features which can make the impossible looking process a cakewalk. Blockchain offers an infinite range of applications among which online voting is the one.

People have got used to the pen and paper, ballot based voting system. There should be an extraordinary feature possessed by new technology to replace the current system. Blockchain technology offers the diverse features which can make the change. As the population increases maintaining democracy become more complex, satisfying people become harder. We can solve this problem by building a more transparent system through which people can vote. Blockchain can be that technology that can help us lower our uncertainties about identity and what we mean about transparency in long distances and complex trades, like in election systems. Blockchain posses many features which can help build a better online voting solution. In this paper, we will have a quick look at the features of the different system based on blockchain voting.

II. DEFINITION

Blockchain voting is an alternative solution for the traditional paper ballot voting. It is cryptographically secured, transparent, public ledger technology which can remove the trust gap between central authority and voters, thus providing the more democratic and portable voting solution which a person who knows how to use cellphone can understand.

A. What is Blockchain?

A blockchain is a "cryptographically secure transactional singleton machine with shared-state." "Cryptographically secure" means that the creation of digital currency is secured by complex mathematical algorithms that are obscenely hard to break.

"Transactional singleton machine" means that there's a single canonical instance of the machine responsible for all the transactions being created in the system. In other words, there's a single global truth that everyone believes in.

"With shared-state" means that the state stored on this machine is shared and open to everyone.[6]

B. How Blockchain works?

The blockchain is based on a decentralized network which maintains the transactional records in the form of blocks in chronological order. The first block is known as a genesis block. Every other block is linked to the previous block. Hash of the previous block is

stored in every block thus linking all the blocks together. Hash is generated based on the transaction records in the block. Changing the record in block changes the hash and thus makes the chain invalid. This makes the Blockchain immutable.

[1]Smart contracts are blocks of code(has function or event) on the blockchain. They are stored on blockchain and are made available for use by the nodes. The block has an append-only structure which is why computational power is 51% on the network and would collude to rewrite only a part on the block.

Miners are the people who are able to store or add the transaction on the blocks. They do proof-of-work or proof-of-state. To protect the system against malicious users and compensate miners, execution of transactions include a transaction fee, called as gas in Ethereum. So, gas is a unit of measure for the amount of work done and gas price is measured in terms of ether in Ethereum.

[13]SHA-256 stands for Secure Hash Algorithm – 256 bit and is a type of hash function commonly used in Blockchain. A hash function is a type of mathematical function which turns data into a fingerprint of that data called a hash. It's like a formula or algorithm which takes the input data and turns it into an output of a fixed length, which represents the fingerprint of the data.

C. *Features of Blockchain voting:[2][12]*

1) Eligibility: This property states that only eligible users can vote. Eligibility criteria can be different for different countries. One of the criteria is the age of the user who is casting the vote. In India person who is above 18 yrs old is allowed to cast the vote.
2) Privacy: Privacy is one of the most important aspects of democratic voting. Voters 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) Physical verification: Physical verification is necessary to know whether the actual voter voted or the bogus person voted on the identity of another voter.
5) Forgiveness: The voter should be able to alter the vote at any time before the election ends. This is related to the coercion resistance. Even if the coercer forced the voter, a voter should be able to change the vote afterward.
6) 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.
7) 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.

III. IMPLEMENTATION OF BLOCKCHAIN VOTING

There are many platforms to implement Blockchain voting but the most used platform is Ethereum. [4]Ethereum is open-source, public, Blockchain based distributed computing platform and operating system featuring smart contract (scripting) functionality. When using Ethereum, computational expenses are manifested as gas price. An initial gas value is set, which can be used to perform the operations. Blockchain voting can be implemented in various phases. Most common phases are as follows: [2]Initialization, Registration, Ballot casting, verification, Tallying results, Revealing results.

[8]Different systems use a different approach by combining a few phases together. The system is proposed using the following phases, 1) Voter registration is the phase in which voter provides personal information. The information is verified by authorized personnel and stored into the blockchain. 2) Creating private Blockchain for voter registration information is the step in which a new Blockchain combined with Merkle hash tree is created to store the voter's information. [7]Merkle hash tree is also known as a binary hash tree. Merkle hash tree is used to store a large set of data and to efficiently summarize and verify the integrity of that large data set. Merkle tree has the following features: i) Ability to verify whether a transaction is included in a block ii) Light-clients. iii) Overall performance and scalability iv) Simplified Payment Verification or (SPV). 3) Voter Authentication is the step in which the physical verification of voter is done based on the record stored in private Blockchain. 4) Voting and tallying phase is the last step where actual voting is done and the results are tallied and displayed to the voters.

We will concern about the features achieved by implementing Blockchain voting this way. Since our voting is based on Blockchain, many features get inherited from the Blockchain itself, such as End-to-end verifiability, transparency, immutability etc. This features of Blockchain solves some of the legal requirements of democratic voting. But with this advancement there comes some possible threats such as maintaining anonymity becomes harder. Different research papers have proposed various implementation to solve these problems. Those implementations are as follows.

[5][10]Shamir's secret sharing scheme is used by polys voting system. The idea is based on the concept that one will need k points to interpolate the polynomial of degree k-1. for e.g, 2 points are must for drawing a line segment or 3 points are must for drawing a curve. So one can share a secret among n person in such a way that it can only be recovered by k people(k<=n), we need to hide that secret in the formula of a polynomial of degree k-1. This implementation maintains the privacy of every user even if the data is visible to everyone. So the problem of transparency and privacy is solved at the same time.

[2]Homomorphic encryption is another concept which can be used to provide anonymity. Homomorphic encryption is the encryption technology which can be implemented using the exponential ElGamal cryptosystem. The basic idea is to allow the authorities to tally the ballots without actually decrypting them thus providing the privacy and security to the system. Exponential ElGamal is a cryptosystem which is used for encryption of the voter data and provides the additive Homomorphic property to the system.

[1]Another way of implementing homomorphic encryption is Pallier encryption. Homomorphic encryption is nothing but to perform computation on encrypted data such that computations are performed originally on decrypted data. Doing a fully modular form of multiplication in fully homomorphic encryption is computationally intensive and slow. So, partial homomorphic encryption scheme such as pallier encryption is used. This adds two ciphertexts and multiplies one ciphertext with another plain ciphertext.

[3]One-time Ring Signature techniques can also be used to protect anonymity. Un-linkable signature is used at the receiver end. In this scheme, no observer can determine whether the transactions are sent to a particular receiver address or the two addresses are associated with each other. To keep the anonymity at sender side ring signature technique is used. Here the sender generates a unique ring structure with a fracture in it using the public key produced by other signers and completes the ring using the private key.

IV. COMPARISON

	Polys[5]	*Bronco Vote[1]*	*Ranked Choice Voting [2]*	*Bit Congress[4]*	*Follow My Vote [4]*
Eligibility	*yes*	*yes*	*yes*	*no*	*yes*
Anonymity	*yes*	*yes*	*yes*	*yes*	*yes*
Verifiability	*yes*	*yes*	*yes*	*yes*	*yes*
Integrity	*yes*	*yes*	*yes*	*yes*	*yes*
Physical	-	*no*	*no*	-	-
Verification					
Forgiveness	-	-	*yes*	*yes*	*yes*

V. LIMITAIONS AND CHALLENGES

Even though Blockchain provides many features, there are some limitations and issues of Blockchain. The first issue is of majority attack[10], which is nothing but, if someone has more than 51% of computational power then he/she can modify the transaction data. Another issue related Blockchain is Fork Problem[11]. When the system comes to a new agreement or new version, then the Blockchain network is divided into two types, new nodes, and old nodes, so after version change, old nodes couldn't agree with the new nodes and thus a problem occurs.

VI. CONCLUSION

In this paper, we have presented the features of the online voting system and how different systems have addressed those features. Many systems have managed to address most of the features effectively. Some of the features are inherited from the blockchain and remaining are solved by some encryption techniques like Homomorphic encryption. Although most of the systems have effectively used the features of Blockchain, there are some features of online voting which are not addressed yet.

REFERENCES

[1] Gaby G. Dagher, Praneeth Babu Marella, Matea Milojkovic, Jordan Mohler, "BroncoVote: Secure Voting System using Ethereum's Blockchain" , ICISSP 2018 - 4th International Conference on Information Systems Security and Privacy, 2018
[2] Xuechao Yang, Xun Yi, Surya Nepal, Andrei Kelarev, and Fengling Han, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption", DOI 10.1109/ACCESS.2018.2817518, 2018
[3] Baocheng Wanga, Jiawei Suna, Yunhua Hea, Dandan Panga, Ningxiao Lua, "Large-scale Election Based On Blockchain", International Conference on Identification, Information and Knowledge in the Internet of Things, Available online at www.sciencedirect.com, 2017
[4] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy",2018.
[5] Polys - Online voting system, Whitepaper. [online] Available : https://polys.me/assets/docs/Polys_whitepaper.pdf
[6] Preethi Kasireddy, "How does ethereum work anyway", [online] Available : https://medium.com/@preethikasireddy/how-does-ethereum-work-an yway-22d1df506369
[7] Andrew, "Blockchain Fundamentals #1: What is a Merkle Tree?", [online],Available : https://medium.com/byzantine-studio/blockchain-fundamentals-what-i s-a-merkle-tree-d44c529391d7
[8] Somnath Panja, Bimal Kumar Roy, "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain", [2018]
[9] Silvia Bartolucci, Pauline Bernat, Daniel Joseph, "SHARVOT: secret SHARe-based VOTing on the blockchain", ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, [2018]
[10] Iuon-Chang Lin and Tzu-Chun Liao, "A Survey of Blockchain Security Issues and Challenges", International Journal of Network Security, Vol.19, No.5, PP.653-659, [2017]
[11] Shaan Ray, "Blockchain Forks" [online] Available: https://hackernoon.com/blockchain-forks-b0dca84db0b0
[12] Lionel Dricot and Olivier Pereira, "SoK: Uncentralisable Ledgers and their Impact on Voting Systems", [2018]
[13] Cédric Bellet, "Part 5: Hashing with SHA-256", [online] Available:https://medium.com/biffures/part-5-hashing-with-sha-256-4 c2afc191c40