Blockchain Technology- How it can transform the Voting system

Medhavi Gupta

Abstract- The shift from ballot paper voting system to e-voting using EVM (Electronic Voting Machine) has had fundamental benefits such as increased efficiency and reduced errors. However, this system is not completely immune from real world problems and there still remain challenges especially with respect to improving resilience against potential faults and alleged frauds. Blockchain technology holds the potential to completely reform the way elections are being held in the present day and improve the overall resilience of e-voting system. This paper presents an attempt to leverage benefits of blockchain technology such as accessibility, cryptography and transparency to build an effective e-voting system. The proposed model conforms to the fundamental requirements of e-voting and ensures voter anonymity while still being open to public inspection. The paper presents details of the proposed e-voting model along with its implementation.

Index Terms- Blockchain, e-Voting**,** decentralization, election commission, hash-code, fingerprint, voter-anonymity

Introduction

What is Blockchain?
A blockchain is a basically a distributed ledger that is open to anyone. Blockchain technology, by using cryptography, provides an open de-centralised database of any transaction involving value that can be money, goods, property, work and even votes. It creates a record of the transaction whose authenticity can be verified by the entire community because once a data is recorded inside a blockchain, it is almost impossible to change it.

How does it work?
Each block of a blockchain contains a data, hash of the block and hash of the previous block. The data stored inside the block depends on the type of blockchain. In the voting blockchain, for example, a block will store details about the voter who casts the vote and recipient candidate who receives the vote. A block also has a hash which identifies the block and all the contents. The hash of each block is unique like a fingerprint. The hash gets calculated when a block is created and making any change to the block later, changes the hash altogether. Any such activity immediately comes to notice because when the block print changes, it no longer remains the same block. The third element inside a block is the hash of the previous block, which effectively creates a chain of blocks chronologically and thus cannot be modified, deleted or tampered with under any circumstances.

Types of Blockchain
There are mainly three types of blockchains-

1. Public Blockchain
2. Private Blockchain
3. Consortium Blockchain

1. Public Blockchain- As the name suggests, a public blockchain is for the public, where anyone can participate because it is open and transparent. No one is actually in-charge of the process and everyone has the right to read, write or audit the information available on the blockchain. As there is no sole owner, decision making happens by various decentralized consensus mechanisms such as Proof of Work (POW), Proof of Stake(POS) etc.

2. Private Blockchain- This type of blockchain has a sole owner who looks after and handles the processes of the blockchain. Here, the blockchain is private property of the owner and he holds all the decision-making rights.

3.Consortium Blockchain- This type of blockchain allows joint ownership to make joint decisions on any topic. Here there is no one person in-charge but a group of companies or representative individuals, who come together and make decisions in the best interests of the whole network.

These can be further divided as public-permissioned blockchain, private-permissioned blockchain etc. on the basis of the requirements.

Permissioned blockchains are built such that they grant special permissions to each participant for specific functions to be performed. These can be customized as per

specific requirements. The available customization options include allowing anyone to join the permissioned network after suitable verification of their identity, and allocation of select and designated permissions to perform only certain activities on the network.

Voting System in India

India used the traditional ballot paper voting system during elections, but this system had its fair share of problems such as booth capturing, identity theft, vote tampering etc. on a large scale. This caused the government to take notice and look for safer alternatives.
India adopted electronic voting and started using EVM's from Lok Sabha elections 2004 instead of the paper ballot system but that didn't make the system immune from the other problems. Identity thefts were reported from many parts of the country where the goons threatened people and voted in place of them. The present system of electronic voting using EVM (Electronic Voting Machine) also has constantly been at the center of tampering allegations. Even though there is no certain proof for that, a decentralized voting system operated via a public blockchain will leave no scope for any such allegations.

Blockchain Technology in e-Voting

The Voting System is in dire need of an upgradation or complete technological transformation in the present situation. Blockchain technology, as it has proved so far, is very much capable of bringing about this change in the way elections are held and votes are cast as blockchain is a constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure, chronological and immutable way that makes peer to peer value transfer possible. Value can be anything. In this case, value can take the form of a vote.

India is the largest democracy of the world and elections play a very important role in government formation at every level, be it as big as the National election where people elect the next government or as basic as the Panchayat election where they elect their village leader. One cannot imagine a democracy this big running peacefully if these elections were not held properly. Even though it holds such

importance the sad reality of today is that given the way the elections are conducted, only about 67.11% voter turn-out was registered during the 2019 Loksabha elections. This means out of the 900 million eligible voters, 296 million voters did not or could not vote. It is a huge number as can be known from the fact that total eligible voters in the US are estimated to be about 230-240 million.

The reasons could be many but the main reason can be attributed to the lack of technological advancement which would have allowed these people who were deprived of their basic constitutional right only because they could not be there at a particular place of voting on a particular date. This would definitely not have been the case if everyone could just access a portal and cast their vote during a particular window as and when it was convenient for them.

Blockchain technology in Voting is the need of the hour. It not only has the potential to overcome the listed problems but also can become the true definition of 'free-and-fair' elections in its true right.
The focus of our research will be to envisage a secure and robust system that would ensure transparency, voter anonymity and seamless functioning. We will review blockchain technologies that would be best suited for Electronic Voting Application in terms of security and scalability.

Blockchain Model

We can start by developing a private permissioned network which will render the voting system more robust and secure.

Steps involved-

1. Voter Registration- The voter will need to first register with unique identifiers such as government issued documents to verify their eligibility for voting. Additionally, the system will be based on finger-print technology which will make the authentication mechanism unbreakable. During registration, each voter will be assigned exactly one vote on the system which the voter will be able to access with his/her fingerprint. The biometric authentication will ensure that only registered voters cast their

votes and this will eliminate the possibility of identity theft.

The Election commission will be the governing body for the entire process. In a similar way but with additional documents the candidates contesting the election will file their nomination with the commission and there-by a list of candidates will be generated on the election portal. The candidates contesting the election will have to register separately for exercising their voting rights.

2. Casting Vote- After registration when the voter's documents are duly verified and fingerprint is registered on the system, the voter will be able to access the voting portal with his fingerprint and serial number of the government document used during registration during a specific voting window which will be decided by the election commission. A registered voter will be able to access the portal from any device, at his convenience, and will not be required to visit the polling booths unlike now. After accessing the portal, the voter will come across a list of all the contesting candidates and will be able to then vote for one candidate only, depending on his choice. After casting the vote, the voter will receive a confirmation message on his registered phone number as a confirmation of his vote and the portal will be closed for the voter which will completely rule-out any instances of double voting.

3. After Voting- Once the participant has voted, the data will get converted in a block with a hash function and the server will transfer that block (vote) from voter's account to the candidate's account which then gets added to the previous block of the blockchain node. Once a block is created, the system identifies the hash and any changes if made to the block later will change the hash altogether. Thus, this encryption technology will ensure voter anonymity and security during election. Since, electronic voting is capable of generating results in real-time, it is required that the blockchain platform used is private with restricted access only to the governing body, in this case the Election Commission. But as it will be a distributed and decentralized network, no person will be able to tamper or delete any blocks, thereby making the system very secure and reliable. At the end of the election, all the blocks in the candidates' accounts will be counted by the system and the winner will be declared accordingly. This system if implemented successfully, will leave no scope for any allegations and elections will be carried out peacefully thus giving everyone the opportunity to exercise their voting right.

Before Voting

HASH code is generated for a combination of fingerprint and document serial number.
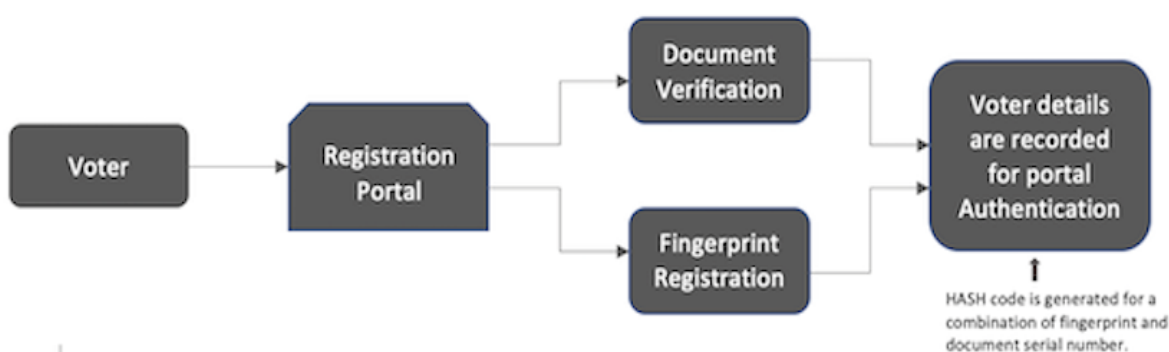
During Voting
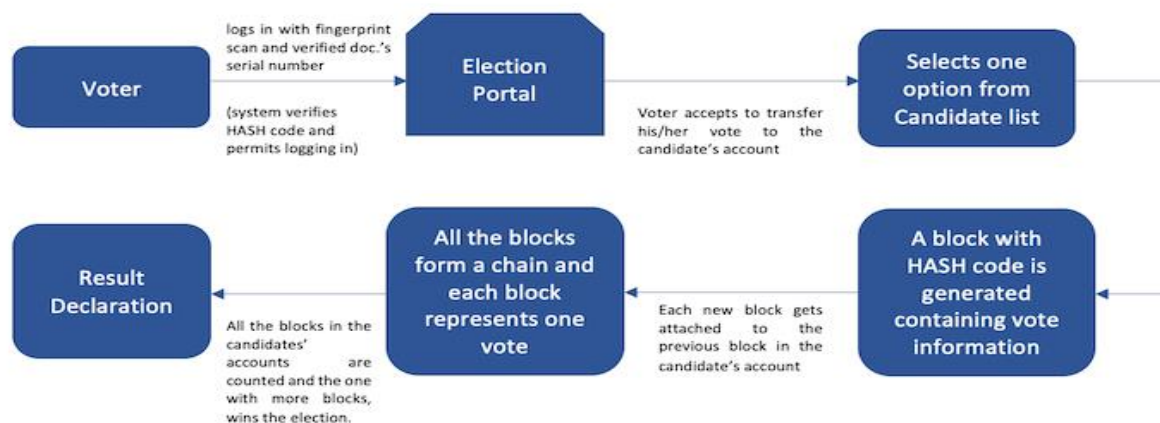
Benefits of Blockchain in e-Voting

Accessible- A registered voter can exercise his/her voting rights from any part of the country without the need to visit the polling booth in a specific province of residence.
This feature will benefit all the working professionals who are not able to vote just because they stay at their place of job and can't travel all the way to their home-town on a particular date for voting. This is one reason India loses millions of potential votes in every election and blockchain is set to overcome this problem.

Secure- As discussed above, as blockchain technology uses hash technique to encrypt data, it is almost impossible to tamper the votes as any change or removal of any block will change the hash and the misconduct will come to notice. This technology also ensures voter anonymity and integrity. The question of booth capturing and identity theft also do not arise, thanks to the biometric authentication.

Transparent- Blockchain Technology will leave no room for any allegations of foul play or vote tampering as the system will be transparent

Expeditious- The e-voting system will be very fast, seamless and un-complicated which will let any common man use it without any difficulties. All the steps of voter registration, voting and result declaration will be very prompt and on-time.

Less effort on part of Election Commission- The election commission needs to provide a lot of security in the areas where elections are on-going to avoid any distress situations as tension is always running high during this time. There have been a lot of incidents of blackmailing voters, stealing their identity to vote and also large-scale fights between groups at the polling booths which sometimes lead to booth capturing. By using blockchain technology, these miss-happenings can be avoided all together.

Challenges and limitations

Research & Development Costs- The R&D of any new technology consumes lot of time, effort and investment and blockchain technology being relatively new will require more efforts to grow to a fully functional state.

Implementation on large scale- The implementation this technology on such a large

scale will be challenging specially for a country like India where the total number of eligible voters come close to a billion.

Outreach- A large section of the country is still oblivious to the technological advancements and has no access to Internet or smart phones whatsoever. In such a scenario, completely transforming the voting system is a big challenge for the government as first the people need to be made aware of technology and taught how to use it securely before implementing a voting system which is solely based on it.

Sustaining the platform for a huge population- Even if all these challenges are met and finally the blockchain based voting system is implemented, sustaining the platform on such a huge network in itself will be a big challenge. As any breach of security would make the entire system incompetent to solve the purpose it was built for.

Conclusion

Blockchain's capability at solving real world problems and it's underlying potential to become the next big thing are well-known. In the coming years, block chain will be used just as Internet is used now, which no one would have even imagined in the early 1990's. The future global economy will move towards one of distributed property and trust where anyone with an access to internet can get involved in blockchain based transactions and third-party trust organisations may no longer be necessary. The next technological revolution is here. Now, it is up-to us to capitalize on this potential to our advantage and customize it to meet our requirements and solve the many problems with the benefits it has to offer.

References:

Adida, B.; 'Helios (2008). Web-based open-audit voting, in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335{348.

Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). Star-vote: A secure, transparent, auditable, and reliable voting system, in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.

Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008) Scantegrity: End-to-end voter-veri_able optical- scan voting, IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.

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.

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

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

P. Noizat, "Blockchain Electronic Vote," in handbook of digital Currency, Paris, Elsevier Inc., 2015, pp. 453-461.

G. Schryen, "Security Aspects of Internet Voting," in IEEE, Hawaii, 2004.

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]

IJSER