Blockchain Technology for Secure Electronic Voting

Anita Thakur
Student
Department of computer science
Himachal Pradesh University
Shimla, India

A.J. Singh
Professor
Department of Computer Science
Himachal Pradesh University
Shimla, India

ABSTRACT
In a democracy, citizens of the country choose their favourite candidate by voting who represents them, therefore it is important for the elections to be reliable. Voting could be paper-based, E-voting, or I-voting. Lack of security and transparency could jeopardize the whole election process. Voters must be assured that their vote has been counted and counted correctly. Anyone having direct physical access to a voting machine and with malicious motives can lead to the vote manipulation. Blockchain (decentralized ledger technology) provides tremendous transparency and security to the voting system. It does not store the data in a central database instead all the node participating in the block chain can have access to the data. Apart from the decentralization blockchain also provides many assets to the E-voting, including anonymity, confidentiality, verifiability, and robustness, etc. Blockchain technology fulfills all the essential and desirable security requirements of the E-voting that have mentioned in this study. This study proposes blockchain-based secure E-voting that is fair, secure, and trustworthy.

General Terms
Blockchain, Electronic Voting.

Keywords
Electronic Voting, Blockchain, Smart contract, Decentralization

1. INTRODUCTION
Electing the right government is very important in a modern democracy because it determines the fate of the nation and civilization. A blemished electoral system could be a major concern for democracy. Even the world's largest democracies like India, Japan, and the USA still suffers from an imperfect electoral system. Polling booth capturing, voter intimidation, and machine hijacking are the major problems in the current voting system [1]. Voting can be stated as a process of expressing or signifying choice. The citizens of the country express their opinion, approval and rejection of government policies and decisions as by casting a ballot. To cast a ballot various voting method are used including paper-based method, machine method, online method, postal method and open ballot methods.

In paper-based voting, votes are cast and counted by hand. Thomas Bronack [2] presented a white paper entitled "the problem with the paper-based voting system" pointed out that paper-based voting is too easy for corruption to occur, resulting in the people's voice not being heard clearly, or drowned out entirely by fraud. On the other hand, electronic voting involves the voting done through electronic means, i.e. via the use of hardware and software. Over the years, many countries have been using the electronic voting machine in the election. It provides better productivity than paper-based voting. It is environmental-friendly and saves the cost of printing the papers.

Figure1: Electronic voting and counting around the world [3]

According to the recent research [3] there are 31 countries that have used or studied the EVM. Some of the countries have discontinued the use of EVM. 20 countries are using the electronic voting machine and pilots are on in 6 countries. The electronic voting machine has various security concerns, especially anyone with direct physical access to the voting machine can manipulate the machine. Any compromise with EVM security can jeopardize the entire election process resulting in voters losing their trust in voting. Enter the Blockchain.

2. BLOCKCHAIN
With the invention of Bitcoin in 2008, the world has been introduced to a new emerging technology named Blockchain. It is a peer-to-peer, distributed ledger that is cryptographically-secure, immutable and updateable only via consensus [4]. Blockchain technology is a developing technology that provides a decentralized network without a single point of failure. When a block is added into the Blockchain it is nearly impossible to delete the block or change the block since the attacker has to change the previous blocks too. This kind of malicious act requires a lot of computation power, i.e. upgraded hardware & software and power supply.

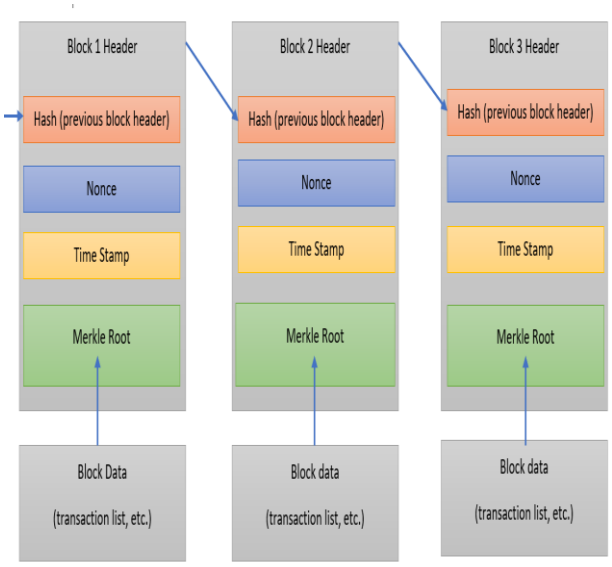

Figure 2: Structure of Blockchain

In order to connect the one block to another block the hash value of the previous block is inserted in the next block as shown in Figure2 and then its hash value is calculated [5]. In Blockchain every "new block" is connected to the previous block using cryptography to form a secure and immutable chain. The first block in the Blockchain is acknowledged as genesis block.

HASH: It is input to the block hash which includes data and meta data about block.

NONCE: It is a random number used in cryptographic communication only for once.

TIMESTAMP: It specifies the time when the block was created.

MERKLE ROOT: It is the hash of all the hashes of all the transactions that are part of a block in a Blockchain network.

Blockchain technology plays an important role in E-voting. Blockchain builds a trust less trust by not trusting anyone. There is no central authority to verify transactions in the Blockchain as the entire Blockchain network verifies every single transaction. In other words, Blockchain has the property of verifiability. It provides individual verifiability and universal verifiability which means that every voter who casts the vote can audit the outcome of the votes.

Blockchain uses the cryptographic function, consensus algorithm, and protocols to make the voting secure and tamper-proof. Building an E-voting is a very crucial task when it comes to voter privacy and anonymity. Once the voter cast his/her vote, it cannot be traced back to the voter. No one in the network could know who voted for whom. On the other hand, voter can observe the voting result in the real time.

2.1 Benefits of Blockchain in Electronic voting

Blockchain has capability to fulfill the requirements of secure E-voting. Blockchain has numerous benefits and like all other technology it has its own limitations too[6] [7]. Herein some of the major benefits are discussed with the slight change in expression.

Decentralization: In Blockchain, there is no central authority to validate the transaction between the parties. All the data is spread across the entire network, instead of one central place. The consensus mechanism validates all the transactions.

Transparency: In Blockchain the users are notified about the completion of the transaction. Transparency guarantees that the code in Blockchain cannot be modified by anyone unless they do not consume the majority of computational power in Blockchain network. It also restricts the piece of information according to the participant.

Fraud control: In Blockchain all the piece of information is copied in all the node of the network. This makes the Blockchain immune to attacks such as manipulation and deletion of the data. Any node in the network is allowed to audit the Blockchain. Attacker cannot alter all the data without detection.

Reduced cost: In Blockchain there is no trusted third party to monitor the transactions so it is not essential to pay intermediaries. It also reduces the cost of validating and conducting the transaction.

Immutability: It is the ability of Blockchain to remain unchanged, permanent and indelible. Once the block of records enters the Blockchain it cannot be tampered with. The blocks are linked to each other using the hash. So, if any changes happen in one block, it would change its subsequent blocks.

Availability: It is the ability of the Blockchain to make the data available to the user in the Blockchain since the data is replicated across the network. The voting system will always be available to the voter and candidates as long as the Blockchain network has sufficient node to achieve consensus to validate the vote. If any node leaves the network data still remains accessible to all the users.

Security: Data in the Blockchain is highly secured. Cryptographic hash function, consensus mechanism and protocols provide the network integrity. Data is copied in the entire network and hacking it all is likely not possible.

User privacy / Anonymity: The identity of the user remains anonymous to the network. People are free to make transactions without revealing their personal information to the nodes in the network. The identity of the user is encrypted in the Blockchain. Every voter is identified by his public key so no one can associate the voter with a vote, i.e. no one can know who voted for whom.

Reliability: In a Blockchain network data is stored at almost all the places in the network instead of one central place. Consensus mechanisms make sure that only the valid transaction can make it to the Blockchain and all the miners agree on the block of records.

Authenticity: All the transactions are cryptographically secured. In E-voting, the administrator or the election committee authenticates the validity of the voter and also verifies that if the voter is an authorized voter or not.

Integrity: Integrity ensures that the data is secured from unauthorized access and alteration. Integrity allows the stored vote to be tamper-resistant i.e. vote cannot be polluted. Blockchain property of verifiability ensures the data integrity and any user can verify if their transaction has been added or not.

Verifiability: Blockchain ensures the universal verifiability and the individual verifiability. Every node in the network can ensure that the number of votes cast and counted are the same.

3. LITERATURE REVIEW

Speaking of electronic voting, Estonia is the first country to use the E-voting. In the 2005 election, Estonia used the remote internet voting for local elections. Since Estonian public held the positive attitude toward the E-voting it encouraged the voters to vote who only vote sometimes [8].

Electronic voting suffers from reliability, transparency, and security flaws. Blockchain technology provides the security requirements to the E-voting. In 2008, Satoshi Nakamoto introduced the term Blockchain. Satoshi Nakamoto presented a peer-to-peer digital payment system [9] that does not rely on the trusted central authority. It provided the solution to the double spending problem. Since then Blockchain is gaining the popularity in various field of study and electronic voting is one them.

P. McCorry, S. F. Shahandashti and F. Hao [5] provided the first implementation of a decentralised and self-tallying internet voting protocol with maximum voter privacy using the Blockchain, called Open Vote Network (OVN). Open Vote Network is written as a smart contract for Ethereum and is suitable for boardroom elections. OVN is a self-tallying protocol, and each voter is in control of the privacy of their own vote such that it can only be breached by a full collusion involving all other voters.

R. Hanifatunnisa and B. Rahardjo [10] discussed the recording of voting results using Blockchain technology. Blockchain reduces the problem related to data manipulation in E-voting.

F. Þ. Hjálmarsson and G. K. Hreiðarsson [11] evaluated the application Blockchain to develop an electronic voting system. The paper gathers the requirement for developing electronic-voting system and identifies the limitation of using Blockchain as a service for building a voting system. The paper also evaluates the popular Blockchain platforms that provide Blockchain as a service. The authors proposed a voting system where multiple institutions and individuals are enrolled in the same role and these participants are election administrator, voters, district nodes and Bootnodes. This system improves security and minimizes the cost of conducting elections nationwide.

According to Nir Kshetri and Jeffrey Voas [12] Blockchain-enabled voting could increase the voter access and minimize the voter fraud. To cast a ballot, eligible voter will use computer or smartphone. BEV takes tamper proof personal IDs and an encrypted key. Votes are registered in public ledger that established the permanent and immutable records. Blockchain makes it difficult for the bad actor to perform any malicious activity in the Blockchain. Blockchain also ensures that no vote has been removed or replaced by the hacker.

Ahmed Ben Ayed [13] provided a design for E-voting that is based on Blockchain technology and could be used for nationwide election. It will motivate the voters to vote and also increase the trust of the voter in government.

A. K. Koç, E. Yavuz, U. C. Çabuk and G. Dalkihç [14] implemented an E-voting application using Ethereum wallet and solidity language. They have also tested the application as a smart contract. Ethereum Blockchain is used to record the ballet after the completion of election.

4. IMPLEMENTATION/DISCUSSION

A Blockchain is an increasing list of blocks that are linked together using a cryptographic hash technique. In this study Ethereum Blockchain network has been used. Ethereum is an open source, decentralized, and distributed public ledger that stores the votes. Vitalik Buterin in 2013 [15] first proposed the Ethereum which is a distributed computing platform based on public Blockchain having Turing-Complete scripting language.

Ethereum is the worlds' programmable Blockchain [16], since it is programmable so unlike other Blockchains Ethereum allows the participants to create their own new application. Smart contract and cryptographic rules in Ethereum allow the participant to build their own rules of ownership or operation of any complexity [17]. This is because the Ethereum virtual machine has the ability to execute a code of random complexity.

Solidity Programming language is used to write the smart contract. An NPM module called solc is used to compile the contract and also the smart contract is saved with the extension ".sol". Once the code is successfully compiled it generates the Bytecode which will be deployed to the Blockchain. Voting.sol in e-voting application code is a smart contract that act as a virtual ballot. Migration.sol is a secondary smart contract file that maintains the migration pattern, i.e. it maintains track which migration script to run next. In this research implementation, various dependencies are used such as Nodejs, Node package manager, solidity, Metamask, and Ganache. Web application is written in the HTML/CSS and JavaScript.

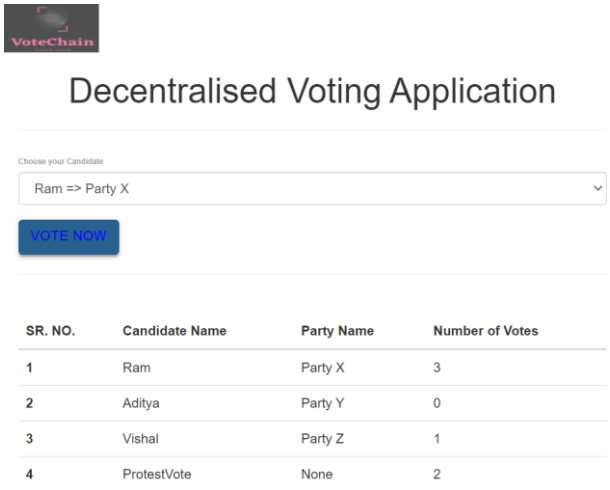

Figure 3: Screenshot of E-voting application based on blockchain showing the candidates information and number of votes candidates have

This application provides an interface to the voters to interact with the Blockchain. After successfully logging into the E-voting web application, a list of candidates in the election is shown to the voters with id, name, the party they belong to, and many more details. The voter chooses his/her favorite candidate and casts a vote. To cast a vote, voters must be logged in to the Metamask which is a deterministic Ethereum wallet.

Metamask is used to access the Ethereum Blockchain. It is a browser extension that works as a bridge between Ethereum blockchain and browser.

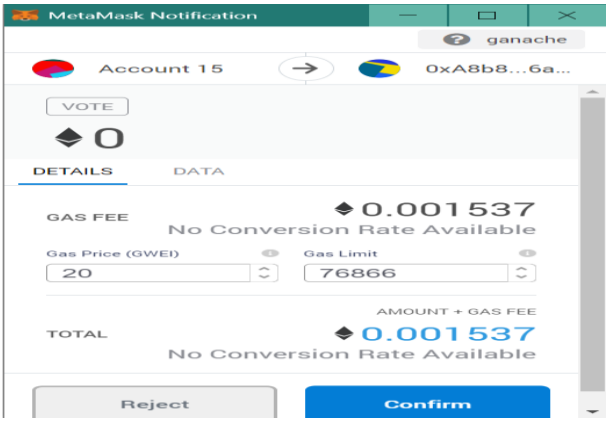

Figure 4: A Metamask notification for a transaction and asks permission for the voter to reject or confirm the transaction

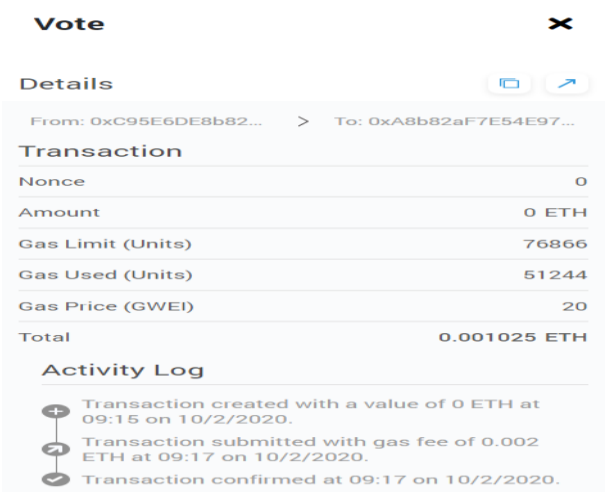

Figure 5: Transaction detail of a vote activity indicating the nonce, amount, gas limit, gas used and gas price of a particular transaction

Metamask holds the keys for Ethereum cryptocurrency only. This Ethereum wallet holds Ether (cryptocurrency) which will be used to cast a vote. Votes are then recorded on the local Blockchain. The voting results are shown in real-time so that the voter can see the voting outcome and also verify if his/her vote is counted. In an E-voting system, protection of the voters' identity is the main concern. This application provides the privacy/anonymity to the voter. The identity of the voter remains unknown and anonymous to the network. The voter casts his/her vote using an Ethereum account instead of his/her personal identity. Every voter is identified by its public key which cannot be traced back to the voter. Votes recorded to the Blockchain are free from unauthorized access and alteration. It provides the integrity to the votes. All the votes are spread across the network and cannot be tempered. This application also provides protection from hacking unless the hacker does not own an enormous amount of computational power hardware and software. A single voter is not allowed to vote more than once using the same account.

5. CONCLUSION

The election is a foundation of a democratic pillar. People express their approval or disapproval in the form of a vote. It is very important for the election to be secure and trusted since people put their trust in the election, in the hope to make their ideal candidate win. Blockchain is a distributed public ledger that makes voting secure from any malicious activity. Blockchain properties like immutability make manipulation impossible. In this research, authors have proposed a Blockchain-based E-voting system that ensures privacy, integrity, non-repudiation, and anonymity. The objective of the study is to acquire knowledge about Blockchain to develop a secure E-voting system. A secure and trusted voting system encourages the voter to vote. This E-voting application could be improved further to gain more security and transparency.

6. REFERENCES

[1] G. Srivastava, A. D. Dwivedi and R. Singh, "Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology," *In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT*, pp. 508-513.

[2] T. Bronack, "The problems with a paper-based voting system". In: White Paper (2010).

[3] Electronic voting and counting around the world. Available at: *https://www.ndi.org/E-voting-guide/electronic-voting-and-counting-around-the-world* Accessed on(August 25, 2020

[4] I. Bashir, Mastering Blockchain Distributed ledgers, decentralization and smart contracts explained, (2017).

[5] P. McCorry, S. F. Shahandashti and F. Hao, " A Smart Contract for Boardroom Voting with Maximum Voter Privacy," *available at: http://eprints.whiterose.ac.uk/117996/1/e_voting_over_Ethereum.pdf*

[6] Y. Abuidris, R. Kumar and W. Wenyong, "A Survey of Blockchain Based on E-voting Systems" *in proceeding of 2019 2nd International Conference on Blockchain Technology and Applications ICBTA 2019, December 9–11, 2019, Xi'an, China*, pp. 99-104, 2019.

[7] S. Ølnesa, J. Ubachtb and M. Janssenb, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Information Quarterly*,34, pp. 355-364, October 2017.

[8] Ü. Madise and T. Martens, "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world.," *Electronic voting*, 2nd international workshop, Bregenz, Austria, (2006) August 2-4.

[9] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Www.bitcoin.org, 2008.

[10] R. Hanifatunnisa and B. Rahardjo, "Blockchain Based E-voting Recording System Design," *in proceedings of 11th International Conference on Telecommunication Systems Services and Application (TSSA)*, 2017.

[11] F. Þ. Hjálmarsson and G. K. Hreiðarsson, "Blockchain-Based E-voting System," *in proceedings of 11th International Conference on Cloud Computing (CLOUD)*, 2018.

[12] Nir Kshetri and Jeffrey Voas, "Blockchain-Enabled E-voting", *in IEEE software* 35(4), pp.95-99

[13] Ahmed Ben Ayed, "A Conceptual Secure Blockchain-Based Electronic Voting System*", in International Journal of Network Security & Its Applications (IJNSA)* Vol.9, No.3, MAY 2017

[14] A. K. Koç, E. Yavuz, U. C. Çabuk and G. Dalkihç, "Towards Secure E-voting Using Ethereum Blockchain," *6th International Symposium on Digital Forensic and Security (ISDFS)*, March. 2018.

[15] V. Buterin, "A Next Generation Smart Contract and Decentralized Application Platform," Available at: *https://fermatslibrary.com/s/Ethereum-a-nextgeneration-smart-contract-and-decentralized-application-platform#emailnewsletter*

[16] *https://Ethereum.org/what-is-Ethereum/* (accessed on August 26, 2020) .

[17] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014