A Survey On Security Of Electronic Voting Data Using Blockchain Technology

Pooja Patil and Prof. A.G. Phakatkar, Department of Computer Engineering, PICT, Pune, India

Abstract: Elections are the most important event in any democratic country and conducting them safe and transparent is a challenging job for the agencies. This is because most of the electoral agencies are nowadays dealing with a huge number of voters and voting booths in remote locations. So the challenge to protect the vote after the voting process becomes more tedious and financial burden to the country. To secure this data in the most efficient and trusted manner various technologies are used. One of the trending techniques used in a distributed environment to secure data is blockchain. Blocks in blockchain have body and header. In most of the trivial systems, the body of the block contains plain transactions that is threat to the system. So this paper puts its efforts to investigate the pros and cons of the past research work to understand them in detail. This understanding will lead to a conclusion on providing greater security for the election data with less complexity.

Keywords: Blockchain, Election data, Data Security, Network Security, Hash Keys.

1 INTRODUCTION

Blockchain as a framework has been around for a long time. It was first introduced by a group of researchers in the early 1990s. It is defined as a chain of blocks that contain information. Every new data added is in the form of a block and is connected to the previous block thereby forming a very secure chain of data that is tamper-proof[13]. At the time of its release, it was envisioned as a system that could form a digital form of a notary, as the blockchain would timestamp the digital documents and prevent any backdating, perfect for its application as a notary. The time blockchain was introduced it was not well received and researchers did not take interest to find its uses, thus it quickly slipped into obscurity. Until then it was treated as a novelty with a specialized purpose of a notary and there were better security options that emerged around that time such as encryption and cryptography[4]. Thus blockchain lost all relevance and was largely untouched and unexplored until its recent application. It was launched back into the limelight when an individual from japan named Satoshi Nakamoto launched Bitcoin[5]. It is a digital currency based on the blockchain, utilizing the security it offers to build a distributed ledger system to track transactions that take place. The tamper-proof nature of the blockchain is perfect as it makes the system resilient and builds trust in the user. Blockchain works on one principle that once a data is recorded, it cannot be changed. It consists of 3 central components in a single block that guarantees its security, namely, the data, hash of the data and hash of the previous block[12]. The data stored with respect to the bitcoin is the transactional data, such as the id of the sender and the receiver, the number of coins transferred, etc. The hash is like a fingerprint of the data and can be used to identify the data in the block and is unique for every block. The hash of the previous block forms a chain connecting the blocks together in a chain-like structure. Figure 1 shows a simple blockchain structure which consist of header of that block, body and hash of previous block.

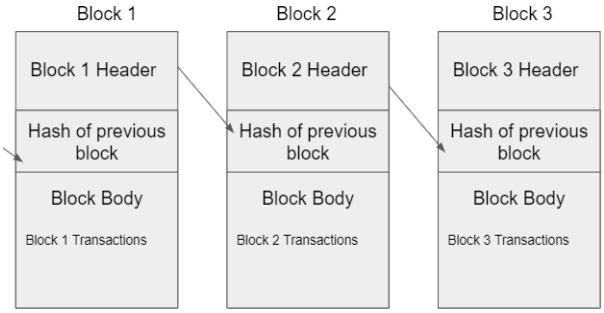

Figure 1. *Blockchain Illustration*

The hash of the previous block is the main point of security, as the hash of the previous block cannot be changed. If any of the blocks or the data inside them have tampered, it would change the hash of that particular block. This would result in all the subsequent blocks being corrupted as the hash of the tampered block is saved in the next block and hence would not be able to point to the block anymore. This makes the blockchain extremely secure and tamper-proof and it can be used for various applications where security is most important such as medical records, creating a digital notary or collecting taxes, etc[4]. As it is distributed, the computational complexity is very less. There has been active research in the field of electronic voting[2]. Majority of the voting is generally achieved through physical votes or using voting machines. The physical efforts involved in this process from registration of voter to results are large. Elections conducted on paper makes use of a lot of resources and contribute to the degradation of forests, causing climate deterioration[1]. EVM's machine needs to be transported from one place to another and there is possibility of manipulation during the transportation. The machine can get damaged due to which they need to be discarded. Thus voters have lost faith in these machines due to its inefficient behavior and there needs to be greater security to protect data. The overall research came to an end and thus we definitely need upliftment in the current voting process. As most of the world is going digital it is imperative to consider an e-voting and maintain a polling booth. It will eventually reduce the use of paper and other items that would adversely affect the environment. The security, on the other hand, will be top-notch due to the

application of the blockchain framework that is proven to highly tamper proof and accurate addition to the voting paradigm. In this paper, section 2 is dedicated to the literature review of past work and Section 3 concludes this paper.

2 LITERATURE REVIEW

X. Yang et al. say that election is the most important aspect of any democratic country and there are many techniques to secure votes. But when conducted on ballot paper causes a lot of paper wastage leading to an adverse impact on the environment [1]. Therefore, moving to the online elections decreases security, thus, to bolster security the researchers propose a verifiable ranked-choice online voting system based on homomorphic encryption. The main disadvantage of this technique is increased computational complexity. Fridrik P. et al. states that due to the rising populations there is an increase in the amount of paper used by the election commission. The authors present an innovative technique for conducting elections online with the help of blockchain technology for providing unparalleled security[2]. The major drawback of this technique is the increased time complexity. A. Qureshi et al.[3] proposed a system that will increase the convenience of the users. They developed an innovative secure and verifiable Electronic polling system. The system is highly secure but the major drawback in this paper is that it cannot be evaluated on its performance due to lack of extensive testing. B. Shahzad et al. introduce the concept of blockchain, as it is one of the most secure frameworks out there that can detect any kind of tampering done to the data. This concept is highly useful in applications where utmost security is needed for a fair and transparent execution, such as voting [4]. The main drawback of this technique is that it has not been implemented extensively to monitor its performance. A. Singh et al. state that due to the large advancements in the field of electronics and digital systems, the procedure of voting should no longer be just done in offline fashion as it is highly resource-consuming and a great inconvenience for the citizens. Therefore, the researchers in this study have proposed a system that stores results in the form of bitcoins at various locations[5]. The proposed methodology has been demonstrated to be highly efficient and secure. One drawback of this technique is that it takes a very long time for the generation of the results securely. E. Belanger et al. explain that there have been multiple lapses in trust between the people and their government. It is highly evident in most nations by the technique they perform their elections. The study in this paper focuses on reducing the political trust of the people in Canada. The distrust stems from the actions of the election commission that have come under scrutiny. All of this can be eliminated by the help of an innovative voting system based online with very little chance of tampering and using multinomial logit[6]. R. Cullen et al. [7] assess the security of the government websites of New Zealand, for their reliability and ease of use. The assessment was based upon the people's perception of the government and the effectivity of a government website in providing convenience to the average citizen of New Zealand. This is done by documenting people's experiences through a feedback form. The users who are the citizens of New Zealand were asked to vote on their experience of using one of the government websites and their responses have been collected for a consensus. The authors indicate that there have to be paramount changes made as the drawbacks of the services are highly obvious. S. Wolchok et al. conducts an extensive evaluation of the EVM's or the Electronic Voting Machine that have been deployed by the Government of India. As the primary mode of the election has been utilizing these machines across the country. The authors evaluated the machines as there was speculation of the machines being tampered with to produce false results. The authors have evaluated and confirmed that the machine is indeed highly tamper-proof and secure, they also suggested to move to a much more convenient and accountable system such as a blockchain-based approach for a highly accurate and reliable system [8]. Rong Wang et al. proposed a privacy-aware PKI system based on permissions BCs [9]. The system consists of registration BC (RBC), certificate BC (CBC) and user. The RBC node is responsible for user identification, encrypting user identity information and storing authenticated user data after encryption. The CBC node is responsible for user legality authentication, and then certificates with authentication information and service information to users and stores anonymous digital certificates, and stores anonymous digital certificate data. The Concurrent Byzantine Fault Tolerance (CBFT) algorithm is adopted in each BC to ensure the consistency and difficult modification of information between the nodes, and to ensure the consistency of the BC itself.Junjun Lou et al. proposed an NDN key authentication and control scheme based on blockchain generation, that is to install each site as blockchain node, imparting public key hash garage, verification (public key hash is published in the blockchain and is queried via the proxy gateways) and revocation provider. This scheme is based on the permission blockchain so it is fairly scalable [10]. The proposed method of a more flat hierarchy reduces the number of signatures and authentication keys. The way to save hash is used to update signature, and the manner of query and evaluation to hash is used to perform signature and the manner of query and evaluation to hash is used to perform a signature verification, This brings much less computation value than public-key cryptography. The major drawback of the proposed technique is slow key signing and verification. Ali Kaan Koc et al. present a system of secure e-voting using blockchain. The blockchain with the clever contracts emerges as an excellent candidate to apply in tendencies of more secure, less expensive, more comfy, extra transparent, and simpler-to-use e-voting systems. Ethereum and its network are one of the most appropriate ones, due to its consistency, large use, and provision of smart contracts logic. An e-voting technique ought to be comfy, as it needs to no longer allow duplicated votes and be completely transparent, even as protecting the privacy of the attendees. The authors implemented and examined a pattern e-voting application as a clever contract for the Ethereum network [11].Rifa Hanifatunnisa et al.[12] proposed a database recording system on e-voting using blockchain technology. However, in this e-voting system blockchain permission is used. Before the election begins each node generates a private key and public key. This method aims to maintain data integrity, and thus manipulation does not occur during elections. Silvia Bartolucci et al. introduced the SHARVOT protocol that uses the blockchain method to announce and build an election and determine a prevailing candidate with the aid of accumulating voters'

ballots in an unchangeable, storage-efficient and unremarkable manner [13]. In SHARVOT protocol, transactions I/O shuffling and voting encryption methods are implemented to assure the de-linking of the users from their vote submission, even as conveniently built transactions make sure a permanent and immutable record of the ballot on the blockchain.

3 CONCLUSION

In this paper, different implementation techniques of E-voting are studied. This is the fact that most of the government bodies use e-voting or ballot voting. The process has low efficiency and creates a lot of waste utilizing a large amount of paper, hurting the environment. The EVM used does not guarantee that the system is secure or manipulation can't be done after voting. We came forward to encryption techniques such as AES and DES run multiple passes so the computationl time increases. RSA and El Gamal techniques take large number of bits to store data. Hashing technique like MD5, the hashed output for same input is always same i.e hash collision. RIPEMD is quite slow in computation. Thus different implementations of E-voting enabled us to achieve an effective methodology based on blockchain and an encryption technique. Encryption will make sure that data at rest is protected and the blockchain will protect the system from hacks and threats.

REFERENCES

[1] X. Yang et al, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption", IEEE Access, 2018.
[2] Fridrik P. et al, "Blockchain-Based E-Voting System", IEEE 11th International Conference on Cloud Computing, 2018.
[3] A. Qureshi et al, "SeVEP: Secure and VerifiableElectronic Polling System", IEEE Access, 2019.
[4] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology", IEEE Access, 2019.
[5] A. Singh and K. Chatterjee, "SecEVS: Secure Electronic Voting System Using Blockchain Technology", International Conference on Computing, Power and Communication Technologies (GUCON), 2018.
[6] E. Belanger and R. Nadeau, "Political trust and the vote in multiparty elections: The Canadian Case", European Journal of Political Research, 2005.
[7] R. Cullen and C. Houghton, "Democracy Online: An Assessment of new Zealand Government Web Sites", Government Information Quarterly, Volume 17, Number 3, 2000.
[8] S. Wolchok et al, "Security Analysis of India's Electronic Voting Machines", Proceedings of the 17th ACM conference on Computer and communications security, 2010.
[9] Rong Wang, Wei-Tek Tsai, EnyanDeng, Juan He, Can Liu and Qi Li, "A Privacy-Aware PKI System Based on Permissioned Blockchains", 9th International Conference on Software Engineering and Service Science (ICSESS), IEEE, 2018.
[10] Junjun Lou, Qichao Zhang, Zhuyun Qi and Kai Lei, "A Blockchain-based key Management Scheme for Named Data Networking", IEEE International Conference on Hot Information-Centric Networking (HotICN 2018), IEEE, 2018.
[11] Ali Kaan Koc, Emre Yavuz, Umut Can Çabuk and Gökhan Dalkılıc, "Towards Secure E-Voting Using Ethereum Blokchain", ResearchGate, IEEE, March 2018.
[12] Rifa Hanifatunnisa and Budi Rahardjo, "Blockchain-Based E-Voting Recording System Design", 11th International Conference on Telecommunication Systems Services and Applications (TSSA), IEEE, 2017.
[13] Silvia Bartolucci, Pauline Bernat and Daniel Joseph, "SHARVOT: secret SHARe-based VOTing on the blockchain", arXiv.org,n, 13 March 2018.

****