RISKS AND OPPORTUNITIES OF BLOCKCHAIN BASED ON E-VOTING SYSTEMS

YOUSIF ABUIDRIS, ABDELRHMAN HASSAN, ABDALLA HADABI, ISSAMELDEEN ELFADUL

School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: yousif_cs@std.uestc.edu.cn

Abstract:

Elections are one of a democratic society's primary pillars, but the Internet's emerging influence is continually challenging the voting process. Recently, E-voting based-Blockchain has already taken place in some countries. However, there are vulnerabilities issues around the E-voting system based-blockchain. This paper aims to highlight some of the risks and opportunities of the e-voting systems based blockchain. As well, we believe that this study can bring a valuable contribution as it illustrates some of the risks and opportunities of e-voting systems based-blockchain. That to offer users and developers a broad view of the potential risks and opportunities associated with the adoption of blockchain in the e-voting system.

Keywords:

Blockchain; Vulnerabilities; E-voting system; Risks.

1. Introduction

Blockchain is a challenging to secure the e-voting systems, given the complexity created by the synergy of individuals, procedures, equipment, technology, policies, and legislation that influence the outcome of a single, individual act and vote. Because online system uses equipment that crossed international borders, it is possible to launch an attack from anywhere in the world. As researchers in the blockchain-based applications [1], we believe in several industries in the transformative potential of blockchain systems. Blockchains, such as Bitcoin blockchain and other cryptocurrencies, can do much more than allowing strangers to send money to each other without fear of fraud or manipulation [2]. The blockchain technology also created new ways for people to invest in projects that have drawn billions of dollars, and one day they can store documents that make education certificates, land ownership, and casting a vote more open and more difficult to forge. Data and information attached to a blockchain cannot be removed or changed because multiple copies are maintained on computers held by different individuals or organizations and may be distributed throughout countries. Strict controls can be imposed on the contents of a blockchain, preventing the entrance of unauthorized information. Blockchain networks are designed to be transparent, sometimes readable by any computer device joined the system from anywhere in the world. However, as a researchers who have studied blockchain-based voting, we believe that while blockchains can help with certain specific security issues, but that's not the story's end. Blockchain security risks [3] do exist, and if blockchain holds its commitment to change the way in which data is stored and acted on, it must be acknowledged and mitigated, which might make things worse. In the worst-case scenario, it could put the democracy community at risk of tampering in casting ballot or buying vote.

This paper highlights some of the risks and opportunities of blockchain-based e-voting while blockchain-inherent security features make distributed ledger technology (DLT) resistant to attack, not immune. Towards the end of the paper, in Table.1 we provided a taxonomy of risks and opportunities for Blockchain-based e-voting systems.

The rest of the paper is organized according to the following: In section. 2, for the scope of the blockchain applications, we discuss and evaluate the e-voting systems related work. Section. 3, presents the vulnerabilities of Blockchain-based e-voting systems in the context of risks and opportunities. Finally, in Section. 4, we conclude this paper.

2. Related work

In this section, we present several systems of e-voting that claim to provide Blockchain-based e-voting.

Follow My Vote is an organization of an e-voting system that follows a restricted number of security assets [4]. It includes a phase of authentication that ensures the eligibility of the voter. It allows voters to locate their votes and use their unique voter ID to check that they are both present and correct. Nevertheless, some security properties

do not meet this e-voting system. Indeed, to ensure voter confidentiality, it requires a trusted authority to hide the correspondence between the real identity of the voters and their voting key. If this authority is corrupted, there will be no more anonymous voting. This authority can also change votes as it has passphrases for all voters, thus compromising the integrity of elections. This system does not verify the confidentiality of votes because there is no encryption of votes cast. The ability to change votes, coupled with the ability to track the election in real-time, violates the property of fairness.

Singh and Chatterjee proposed a model for the university campus election to maintain an e-voting system based on blockchain (SecEVS) [5]. During the phase of security analysis, the proposed method was validated. The system security scheme proposed is based on Merkle root hash. This system maintained a transmitted data privacy, voter confidentiality, and uniqueness, in which there are no duplication cases during the voting stage. However, this proposed system has limitations in some security features like the anonymity, auditability, universal verifiability, consistency, coercion, which that make this proposed system not robust at all.

Wang and Sun proposed a scheme to secure the large-scale e-voting systems based on a blockchain [6]. Using homomorphic ElGamal encryption and one-time ring signature technique to ensure and preserve the privacy of the e-voting system. However, the main disadvantage of this system not support robustness and does not maintain coercion resistance.

Z. Wenbin et al., proposed an e-voting protocol based on blockchain preserves end-to-end privacy and maintains detectability, and correctability against fraud without a third party committed [7]. This protocol implementation respecting the Hyperledger structure proves the validity and practical applicability. Nevertheless, the main disadvantages of this protocol do not provide consistency, fairness, individual verifiability, universal verifiability, and coercion resistance.

As we can see from the above-mentioned existing works, the lack of concrete system designs in their technical documents makes it difficult to determine whether or not their systems accomplish the correct properties what stated.

3. The vulnerabilities of Blockchain-based E-voting

There are some vulnerabilities with the current method of casting votes and keeping votes secure using blockchain. In this section, we will highlight some of these vulnerabilities. Fig.1 Shows some vulnerabilities of blockchain-based e-voting.

3.1. The vulnerabilities of the endpoint

One of the vulnerabilities of the DLT most likely comes from outside the blockchain. Nevertheless, these problems are impacting on the security of blockchain technology as a whole, dubbed "endpoint vulnerabilities," and they must, therefore, be tackled. Endpoints are the spaces where electors and blockchains meet. Endpoints are mostly the machines used by users and businesses to access services based on blockchain. If the democratic institutions, companies, or cryptocurrencies are providers of such services, the use of a blockchain starts with the input of information into a computer and ends with the output of information from a computer. The data on the chain is most vulnerable during the process of accessing the blockchain. The reason is the credentials needed to access a shared distributed ledger and how the security vulnerabilities could expose these credentials at the endpoints [8]. While there are restrictions on the blockchain, this is more of a user constraint as we shall see.

3.1.1. The Security of the public and private key

Access to the blockchain wants both a private and a public key. Keys are enigmatic strings of enough length characters to render the chances of genuinely unimaginable guessing them. Because it is virtually impossible to access data within a blockchain without the proper combination of public and private keys, it reflects the power and weakness of blockchain technology. No attacker will ever be able to access data without the right keys. Notwithstanding, everything the attacker wants is the right keys to access information and do what they want to do with it. Since attackers know there is no use in trying to estimate the keys of anyone, they are concentrating on stealing them. Hence, the best chance to get keys is to attack the weakest point in the entire system, personal computer, or mobile device. Researchers have found repeatedly that different manufacturers ' voting terminals are vulnerable to attack [9]. If the unit itself is not protected against interference, it becomes pointless to use blockchain technology, even if the intentions are good.

The highly effective two points to keep attackers away from stealing the blockchain keys are:

- Run regular scans for anti-malware.
- The blockchain keys should not ever store in a text file, Word Document, or another folder in which the unauthorized person can read them easily.

Just as it needs a common-sense approach to keeping all the rest of information secure from attackers and keep the blockchain keys from leaving the computer or mobile device

by taking a few simple steps.

3.2. Untested in full scale (Scalability)

Another unknown is the scaling up of a blockchain-based e-voting to cater for what could be processing hundreds of millions of votes. Scalability is one of the critical security concerns of the blockchain. The architecture of distributed ledger technology is fundamentally scalable. Blockchain would scale up whenever any change happened. Once Bitcoin hit a price of nearly $20,000 in December 2017[10], the number of people trying to buy and sell the cryptocurrency made transactions much slower. If this happens with voting, it will cause problems because there is a need for election results within hours. It would be incredibly hard to scale. On bitcoin transactions, there is a statistic that can only handle seven seconds. If we do that in an election, we might be able to vote if we have thousands of people, not millions. However, if we are talking about millions of votes, take the 35 million votes cast in the Brexit referendum, like example [11]; if we could only verify those at seven seconds, it would take fifty-five days to get everything worked out. One field where blockchain can boost elections is transparency, not only because the ledgers can be easily accessed, but also because the technology-providing start-ups can release open-source code that demonstrates how the system works and can be trusted.

Recently, researchers proposed a solution to this type of critical security concern is based sharding-style [12], which breaks the barrier of low transaction rate and block generation speed.

3.3. Anonymity and verification

One of the primary voting conditions is being anonymous, with outsiders unable to access information on how someone voted. However, to get citizens to cast a vote, they need to be eligible, and there needs to be some way to verify that. It is a challenge to balance these two requirements. Once it is on the blockchain, we want the person to see that is their vote, but we do not want anyone else to see what is going on, because it does not help to make sure the voting is reasonable.

Nevertheless, countries are pressing along with an attempt to introduce blockchain voting; one of them is Brazil [13], which uses the Ethereum blockchain to store election data. It is a huge task to collect and validate the information of around 145 million registered voters. Therefore, to conduct an utterly blockchain-based e-voting, different issues need to be overcome.

Verifying voter identity from various angles is always a challenge; some works [14] have tried the biometric solutions, such as facial comparison, fingerprint, Iris and retinal scan but this can be biased and easily gamed or stolen. However, we think that one way to protect the stolen biometrics data is by using a complex algorithms that are hard to crack. It can be hashed using any hashing algorithm instead of saving the biometric information as binary data and then stored as a reference string. The sample model should be converted to a hash value during the validation and identification process and then compared with the reference value.

3.4. Vote-buying (Coercion)

Another way e-voting based-blockchain might aggravate existing voting issues is by increasing the possibility of buying votes [15]. In large-scale elections, buying votes is happily rare, in part because the secret ballot makes it very difficult to verify a bought vote and because severe criminal penalties exist. Placing votes on blockchains removes the voting booth's confidentiality. Encryption does not help, and Software can mathematically prove to a buyer of votes that the device of a voter encrypted a candidate's name. However, outsiders who may try to influence the votes of people are very difficult to prosecute. Many voting companies claim that their systems only recognize voters by random numerical identifiers publicly, so they are not subject to Coercion or harassment. Nevertheless, voting identities in many of these systems can be connected to accounts in cryptocurrency systems where an elector might obtain a bribe, probably without disclosing who was charged, how much or by whom. In pursuing to use blockchains as a protective element, new threats can be introduced into the crucial mechanics of democracy.

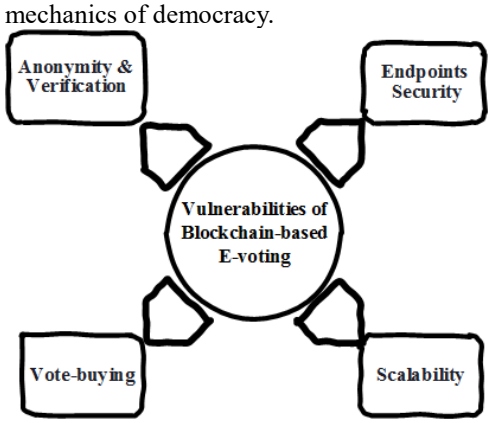

Fig.1 the vulnerabilities of e-voting systems based on blockchain

As we can see in Table.1, a taxonomy of risks and opportunities for the e-voting system using blockchain

technology has been discussed in terms of some vulnerabilities which require more improvement in future.

Table 1 taxonomy of risks and opportunities of blockchain-based e-voting systems

Risk	Reason	Solution Opportunity
End-point	Personal user security. Losing private security key. New malware and key-loggers	Trusted Execution Environment
Untested in full scale (Scalability)	Consensus , Data Size, Response Time, Cost	Sharding-style, Lightning Network.
Anonymity and Verification	Identity management techniques.	Encrypted Biometric solution
Vote-buying (Coercion)	A higher power influences or pressures other to vote in one direction.	Hard to achieve

4. Conclusions

Shortly, e-voting based-blockchain technology is likely to continue to evolve. The benefits include improved efficiencies, lower costs, increased transparency, and an unchangeable record of all voting transactions. However, there are risks and threats associated with benefits. This paper highlights these risks and opportunities of e-voting systems based blockchain. Finally, it is essential to recognize that technology based on e-voting blockchain is still in its infancy. Hence blockchain is likely to take years to morph into its most effective form.

References

[1] V. Dhillon, D. Metcalf, and M. Hooper, Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You. Springer, 2017.

[2] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] Y.-S. Chung and J.-S. Cha, "The Security Risk and Countermeasures of Blockchain based Virtual Currency Trading," The Journal of Korea Institute of Information, Electronics, and Communication Technology, vol. 11, no. 1, pp. 100-106, 2018.

[4] followmyvote. (2016). Introducing a secure and Transparent online voting solution for modern age: FOLLOW MY VOTE. Available: https://followmyvote.com/

[5] A. Singh and K. Chatterjee, "SecEVS : Secure Electronic Voting System Using Blockchain Technology," in 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 28-29 Sept. 2018, Piscataway, NJ, USA, 2018, pp. 863-7: IEEE.

[6] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu, "Large-scale Election Based On Blockchain," Procedia Computer Science, vol. 129, pp. 234-237, 2018/01/01/ 2018.

[7] Z. Wenbin et al., "A privacy-preserving voting protocol on blockchain," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2-7 July 2018, Los Alamitos, CA, USA, 2018, pp. 401-8: IEEE Computer Society.

[8] F. Caron, "Blockchain: Identifying risk on the road to distributed ledgers," ISACA Journal, vol. 5, 2017.

[9] R. Osgood, "The future of democracy: Blockchain voting," COMP116: Information Security, pp. 1-21, 2016.

[10] M. CAMPBELL - VERDUYN and M. Goguen, "Blockchains, trust and action nets: extending the pathologies of financial globalization," Global Networks, vol. 19, no. 3, pp. 308-328, 2019.

[11] H. D. Clarke, M. Goodwin, and P. Whiteley, "Why Britain voted for Brexit: an individual-level analysis of the 2016 referendum vote," Parliamentary Affairs, vol. 70, no. 3, pp. 439-464, 2017.

[12] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in 2019 International Conference on Management of Data, SIGMOD 2019, June 30, 2019 - July 5, 2019, Amsterdam, Netherlands, 2019, pp. 123-140: Association for Computing Machinery.

[13] T. Fujiwara, "Voting technology, political responsiveness, and infant health: Evidence from Brazil," Econometrica, vol. 83, no. 2, pp. 423-464, 2015.

[14] Voatz, "Voatz: A Secure Vote in Every Hand," white paper, 2019.

[15] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability," International Journal of Information Security, pp. 1-19, 2019.