A Survey of Blockchain Based on E-voting Systems

YOUSIF ABUIDRIS
School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu, china
yousif_cs@std.uestc.edu.cn

RAJESH KUMAR
School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu, china
rajakumarlohano@gmail.com

WANG WENYONG
School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu, china
wangwy@uestc.edu.cn

ABSTRACT
Blockchain technology as a decentralized and distributed public ledger in a P2P network has recently gained much attention. In this technology, a linked block structure is applied, and a trusted consensus mechanism is established to synchronize data modifications, making it possible to develop a tamper-proof digital platform for data storage and sharing. We think that blockchain could be used in various interactive online systems, such as the Internet of Things, supply chain systems, voting systems, etc. The scope of this survey is to shed light on some recent contributions of the security and privacy issues associated with e-voting based on blockchain. At the end of this paper, we provided a comparison for the security and privacy requirements of the existing e-voting systems based on blockchain.

CCS Concepts
• General and reference → Surveys and overviews• Security and privacy → Security requirements.

Keywords
Blockchain; E-voting system; privacy; security

1. INTRODICATION
Electronic voting or E-voting, which uses automated systems to help to cast and counting the votes in the polling process, Recently, for the past a few years, it has been the subject of active research in cryptography. To assure voter anonymity, minimizing the cost of running polling, while ensuring the polling integrity and end-to-verification by carrying out the security and privacy issues with compliance the requirements [1–3] . In the present era, when considering implementing an electronic voting system, the security issues of e-voting systems are always the biggest concern. There can be no suspicion about the ability of the system to secure data and defend against potential attacks with such massive decisions at stake. One way to potentially solve security issues is through Blockchain technology [4–6]. Blockchain technology comes from the fundamental architecture of the bitcoin cryptocurrency [7, 8]. It is a distributed database form in which recordss take the shape of transactions; a block is a collection of these transactions. In these circumstances, we believe that Blockchain also falls because this technology self-cryptographic validation structure among transactions and can be employed for authenticating, authorizing, and auditing device produced data. Moreover, because of the blockchain's decentralized nature, which will lead to the achievement of the transparency principle. Also, blockchain eliminates the need for the third party trust and has no single point of failure. Furthermore, blockchain is immutable, meaning that any proposed (new block) to the ledger must reference the previous version of the ledger, which will lead to the creation of an immutable chain from which the blockchain gets its name and prevents the integrity of the previous entries from being tampered. Therefore, a safe and robust e-voting system can be developed with the use of blockchain. Fig.1, show the e-voting system stages based on blockchain technology. The paper aims to familiarize newly interested scientists. Besides, updating the readers with some prior understanding of Blockchain, including the latest security and privacy issues in the e-voting systems based on blockchain . This study approach will present a survey of the state-of-the-art papers in which the Blockchain is used to provide the e-voting schemes with some level of privacy and security.

ICBTA 2019, December 9–11, 2019, Xi'an, China

ACM ISBN 978-1-4503-7743-0/19/12…$15.00
DOI: https://doi.org/10.1145/3376044.3376060

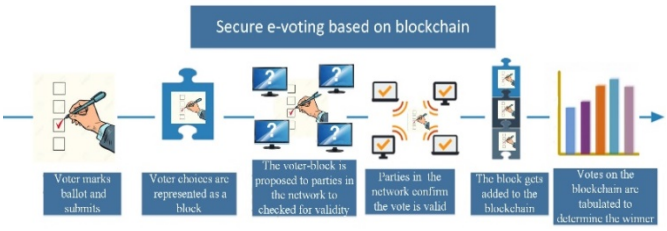

Figure 1. E-voting system stages based on blockchain technology.

2. OVERVIEWS
2.1 E-voting Essential Issues
The major challenge of e-voting is to expand and develop the constitutional democracy and reinforce procedures going for the strengthening inhabitants [9].

The modern human advancement, achieved by the Information Society, ought to consent to the standards and estimations of majority rule government. The presentation of an e-voting framework ought to adjust to this standard, since casting a ballot is one of the capacities "e-residents" may wish to see performed on the web. In this regard, a wonder, which ought to be thought about is the digital divide. Severe many security gaps are surrounding e-voting that should be dealt with before something like this can turn into a completely confided in all actuality

anywhere. Any election has certain phases, and each of them carries hazards, and few elections do not include stakeholders with a vested interest in the outcome, irrespective of whether it is a local election or a large-scale national election with widespread global ramifications, and the motive is to go around the law to achieve their goal. Notwithstanding the kinds of challenges that have been mentioned before, you can include stuff like spoofing votes and voters, denial of service attacks, voting phishing sites, fraud, redirecting or intercepting votes, attacks on data centers, and basic use error. Therefore, It is time for government agencies and security experts to come together to proactively create policies and security standards that can be followed and implemented because we will continue to have a severe security issue until that occurs.

2.2 Benefits of Blockchain-based E-voting

1) Security: Blockchain offers a refreshed framework for voters that could fix the issues of security breaches, fraud, and corruption.

2) Transparency: It is a crucial necessity for a democratic society with considering the blockchain anonymous and decentralized nature; votes can be easily pursued, checked, and associated by a wide range of sources while keeping up voter privacy.

3) Auditability: When data is stored, it gives a changeless record that fills in as a steady auditable trail to the populace

2.3 Challenges Faced Blockchain-Based E-Voting Systems

1) Scalability: Blockchain works well for a few numbers of users. However, when using it for large-scale elections, the number of users will increase over the network and lead to a higher cost and time consuming for the transaction.

2) Immatureness: In 2016, the not-for-profit Democracy Earth organization utilized a blockchain to give Colombian exiles a voice in the peace referendum that was led to endorse the consent to end the contention between the Colombian government and FARC guerillas. According to the organization, the underlying challenge of using blockchain innovations is still in its early days.

3) Acceptableness: Even though blockchain is excellent at giving security and accuracy, citizen's confidence and trust are vital elements for Blockchain-based E-voting success. Blockchain's complexity may prevent standard citizens from the worthiness of Blockchain-based E-voting.

4) Coercion: Although there are numerous methodologies tended to the issue of coercion-resistance, but still (vote-buying, and voter coercion) is highly scalable in the e-voting environment.

3. THE COMPANIES OF E-VOTING SYSTEMS BASED ON BLOCKCHAIN

The following companies and organizations are enhancing the e-voting field: some of them are well-established, but most of them have been created over the past five years. They all have a common desire to bring democracy to the power of the blockchain network.

3.1 Follow My Vote

It is an organization proposed a secure online voting platform based-blockchain with the capacity to audit the ballot box and see the elections progress in real-time. This platform using a webcam and user ID, the voter can remotely and safely sign in and vote in favor of his ideal candidate then he can use his identifier to quite literally open the ballot box, locate his vote, and check that it is both existing and right [10].

3.2 Agora

It is an organization that proposed a digital voting platform using blockchain. It was founded in 2015 and deployed partially in March 2018 during the presidential election of Sierra Leone. In this system, votes are recorded to various layers of blockchains promptly, guaranteeing that the result has not tampered. The ballot data is completely auditable by any third party, including the voters themselves, while keeping up voter privacy [11].

3.3 Voatz

This company established a phone-based voting system for public elections using blockchain. Electors verify their characters on the application by snapping a photo of themselves and their ID and giving distinguishing biometric proof as to either a unique mark like the fingerprint or retinal scan [12].

3.4 Polyas

This company was established in 1996. The company used the blockchain technology to offers an e-voting system for public and private sectors. Polyas was certified as safe enough for the e-voting systems by the German Federal Office for Information Security in 2016.To perform e-voting systems, many big companies across Germany use Polyas. Polyas now has customers across North American and European nations [13].

3.5 Luxoft

It is a global IT service provider created a blockchain-based solution e-Vote for municipal elections in Switzerland. The first time this system was used in June 2038 by city of Zug in Switzerland [14].

3.6 Polys

It affords a secure mobile online voting based-blockchain. Electors get customized codes employing email and use them to cast a ballot either online or at a public polling station. the details can found in a whitepaper [15].

4. LITERATURE SURVEY

Over the past few years, several articles have been released to discuss the security and privacy issues related to e-voting systems based on blockchain. Table.1 shows the Comparison of the security and privacy requirement for the different references. Table.2 Reflect the cons and pros for the protocols which proposed in various references.

1) The authors in [16], proposed a voting protocol based on Quantum Blockchain. This protocol provides essential security requirements such as anonymous, binding, nonreusable, verifiable, eligible, fair and self-tallying. Besides this Quantum Blockchain, they used other quantum techniques such as:

- Quantum Secure Communication (QSC).
- Quantum Bit commitment (QBC).
- Quantum Key Distribution (QKD).

2) The authors in [17], proposed bearable new e-voting protocol that used blockchain as a transparent ballot box. This protocol has been intended to:

- Abide by the underlying of e-voting properties.
- Allow a degree of decentralization.
- Provide for the elector to modify/update their vote within the allowable voting phase.

Furthermore, the author reveals some pros and cons of blockchain-based systems.

3) The author's in [18], designed a secure online e-voting protocol based blockchain named Verify-Your- Vote (VYV). This protocol guarantees the following features:

- Eligibility: Just the acceptable elector can vote.
- Fairness: No essential results that could affect other elector's choices are made available.
- Vote privacy: privately keep the votes; this can likewise be demonstrated as an unlinkability between the elector and his ballot.
- Receipt-freeness: The elector cannot create a certificate that enables him to back to the third party to inform he voted for a particular candidate. That is to stop vote-selling.
- Verifiability: Each elector can verify whether his/her vote has been counted rightly.
- Robustness: The protocol can allow a set numberof offending electors.

4) The authors in [19], proposed likewise an e-voting protocol based on the blockchain without a trusted third party, which affords a safe and adaptable voting technique. The protocol provides Public Verifiability, Individual Verifiability, Dependability, Consistency, Auditability, Anonymity and Transparency.

5) The authors in [20], proposed voting protocol preserves end-to-end privacy based-blockchain and maintains detectability and correctability against defrauding without a third party committed. The protocol implementation respecting the hyperledger structure proves the validity and practical applicability.

6) The authors in [21] proposed a scheme to secure electronic voting based on blockchain for the largescale voting using homomorphic ElGamal encryption, and they used the technique of one-time ring signature to guarantee and protect the anonymity of the voting scheme in the blockchain.

7) The author's in [22], proposed techniques to employ blockchain to enhance the security issues for e-voting as following:

- He designed a synchronized model of voting records based on DLT to avoid fraud in the ballot.
- He designed a user credential model based on ECC cryptography to manage the cost of verification and non-repudiation.
- He designed a withdrawal model that enables electors to replace their votes before a preset deadline.
- The verification of the system scheme has been proved and designed on Linux platforms in the P2P network.

8) The authors in [23], proposed e-voting system based on the Prˆet `a Voter e-voting method. The system designed to support special requirements such as privacy, eligibility, convenience, receipt-freeness, and verifiability. The rest of the author contribution arranged as follow:

- The system intends to accomplish secure digital voting without jeopardizing its usability.
- The system is designed using a web-based interface to help users dealing fingerprinting to prevent double voting.
- The security concerns of the votes are based on the blockchain using cryptographic hashes to secure end-to-end verification.

9) The authors in [24] proposed a methodology of combining the secret sharing scheme and homomorphic encryption with the blockchain to build up decentralized e-voting framework without a trusted third party. Moreover, the framework provides a transparent voting manner while preserving the anonymity of the voter's identity. The author's during the billing phase, preserve the data transmission privacy and verify the ballots.

Table 1. A comparison of the security and privacy for e-voting systems based blockchain in different references.

References											
Security Requirements	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]
Eligibility	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anonymity	✓	x	x	✓	✓	✓	✓	✓	✓	✓	x
Fairness	✓	✓	✓	x	✓	✓	✓	✓	✓	✓	✓
Auditability	x	x	✓	✓	✓	✓	x	x	✓	✓	x
Individual verifiability	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	✓
Universal verifiability	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	x
Vote-Privacy	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
Consistency	x	x	✓	✓	x	✓	✓	x	✓	✓	x
Receipt-freeness	x	x	✓	x	x	✓	✓	✓	x	x	x
Coercion resistance	x	✓	x	x	x	x	x	x	x	x	x
Robustness	x	x	✓	x	x	x	x	x	x	x	x
References											
Security Requirements	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]
Eligibility	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anonymity	✓	x	x	✓	✓	✓	✓	✓	✓	✓	x
Fairness	✓	✓	✓	x	✓	✓	✓	✓	✓	✓	✓
Auditability	x	x	✓	✓	✓	✓	x	x	✓	✓	x

Individual verifiability	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	✓
Universal verifiability	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	x
Vote-Privacy	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓
Consistency	x	x	✓	✓	x	✓	✓	x	✓	✓	x
Receipt-freeness	x	x	✓	x	x	✓	✓	✓	x	x	x
Coercion resistance	x	✓	x	x	x	x	x	x	x	x	x
Robustness	x	x	✓	x	x	x	x	x	x	x	x

Table 2. The pros and cons of the different references.

References	Protocol	Pros	Cons
[16]	Based on Quantum Blockchain.	anonymous, binding, non-reusable, verifiable, eligible, fair and self-tallying	The main disadvantage of it does not provide auditability consistency
[17]	Used blockchain as a transparent ballot box.	Abide by the underlying of e-voting properties. Allow a degree of decentralization. Provide for the elector to modify/update their vote within the allowable voting phase.	It does not provide privacy, consistency and auditability.
[18]	Design blockchain-based protocol named Verify-Your-Vote (VYV).	Eligibility , Fairness, Vote privacy, Receipt-freeness, Verifiability	This protocol not support the anonymity.
[19]	Design the blockchain-based protocol without a trusted third party.	Public Verifiability ,Dependability , Dependability, Consistency, Auditability, Transparency, Anonymity.	The robustness and fairness is the limitations.
[20]	Proposed protocol preserves end-to-end privacy.	Detectability, correct ability.	It does not provide consistency and fairness.
[21]	Proposed blockchain based protocol using homomorphic ElGamal encryption.	It guarantee and protect the anonymity of the voting scheme.	The main disadvantage not support robustness.
[22]	Designed a synchronized model. Designed a user credential model. Designed a withdrawal model.	Achieves the essential security and privacy requirements of e-voting process.	Countermeasures attacks is problem.
[23]	Used Prêt à Voter e-voting method.	Secure digital voting without jeopardizing cryptographic hashes to secure end-to-end verification.	It allowed multiple votes to one user.
[24]	Combining the secret sharing scheme and homomorphic encryption.	It provide preserving the anonymity of the voter's identity.	The fairness is the main problem in this scheme.
[25]	Design smart contract using the ethereum wallets and the Solidity language.	Design Android a pplication for the voting system.	The main disadvantage not support robustness and not support the receipt-freeness feature.
[26]	The proposed system security scheme is based on Merkle root hash.	Transmitted data privacy, Voter confidentiality. No duplication cases during the voting.	The robustness and anonymity is the limitations.

10) The author's in [25], implemented and tested a sample of secure e-voting application on a smaller scale as a smart contract using the ethereum wallets and the Solidity language. Further, an Android platform has been appropriated to enable voting for people who do not have an ethereum wallet.

11) The authors in [26], proposed a model to secure the e-voting system based blockchain (SecEVS) for the university campus election. The proposed method was validated during the security analysis phase. The proposed system security scheme is based on Merkle root hash. Further, the system maintained the following:

- Transmitted data privacy.
- Voter confidentiality.
- The uniqueness of the ballot which that there are no duplication cases during the voting.

5. DISCUSSION AND FUTURE WORK

A successful e-voting system requires several key features to balance out. Security and privacy issues are undoubtedly one of the most critical factors because we want to avoid being able to manipulate the outcomes by any adversaries or self-interested parties and maintain the election integrity. We believed that blockchain had improved some of the security and privacy aspects. However, there is still room for improvement. We want to make sure the counted votes are authentic as well. Otherwise the outcome will not be fair and democratic. The other properties need to be included in e-voting systems based blockchain are:

1) **Anonymity:** In e-voting systems, the need for anonymity is complicated because, in all aspects, we don't want anonymity. To stop people from voting multiple times and committing certain types of fraud, they need to be able to verify who is voting. However, we want the votes themselves to be anonymous. It can lead to bullying or coercion if the government, opposition party, or anyone else can find out who a person voted for. This would jeopardize voting credibility.

2) Accessibility: Accessibility must be taken into account by all voters. It would be nice to encourage everyone to vote and make the process easier to vote from their own location. At the same time, we don't want an overly technical system that makes voting impossible for some segments of the population.

3) Scalability: Blockchain scalability still in its early days. So the time to put a transaction in the block and the time to reach the consensus still needs an improvement.

4) Speed: It is best if in a relatively short period of time we will obtain the results. If it took a long time to determine the count of

the final vote, people's will at the time of the results that differ greatly from what it was when the votes were cast.

We believe that this study can bring a valuable contribution as it illustrates the issues in e-voting systems based on blockchain. In doing so, we provide a better understanding of the e-voting issues and address opportunities and challenges in this scenario for implementing blockchain technology. In addition, the study's external validity should be improved, which should be discussed in future research activities. Accordingly, we would also like to encourage researchers to make their effect on blockchain research taking into account a wide variety of factors, including underlying cryptography and its ecosystem limitations.

6. CONCLUSIONS

Blockchain has recently drawn remarkable attention in decentralized application systems because of its decentralized nature and safety function. It provides an entirely different way to store, distribute, and update data and will play a vital role in the future interactive internet system. This paper has presented and compared the recent researcher's contributions to security and privacy issues for the existing e-voting mechanisms based-blockchain. However, the developing need for security and privacy protections may be a barrier to emerging the real blockchain applications.

7. ACKNOWLEDGMENTS

This work was supported by Sichuan Department of Science and Technology, Blockchain-based IoT Tracing Integrated Platform, Project Number: 218GZ0218.

8. REFERENCES

[1] P. Akritidis, Y. Chatzikian, M. Dramitinos,E.Michalopoulos, D. Tsigos, and N. Ventouras, "The votesecure secure internet voting system," in International Conference on Trust Management, vol. 3477. Springer, 2005, pp. 420 – 423.

[2] G. Beroggi, "Secure and easy internet voting," Computer, vol. 41, no. 2, pp. 52 – 6, 2008.

[3] L. Weinstein, "Risks of internet voting," Communications of the ACM, vol. 43, no. 6, pp. 128–128, 2000.

[4] M. Di Pierro, "What is the blockchain?" Computing in Science &Engineering, vol. 19, no. 5, pp. 92–95, 2017.

[5] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, "Decentralized applications: The blockchain-empowered software system," IEEE Access, vol. 6, pp. 53 019–53 033, 2018.

[6] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," Security and Communication Networks, vol. 2018, 2018.

[7] B. Howley, "Blockchain, ledger legerdemain, and the public library [bitcoin cryptocurrency]," Information Today, vol. 33, no. 9, pp. 14 – 15, 2016/11/.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin. org/bitcoin. pdf.

[9] S. Alonso, J. Keane, and W. Merkel, The future of representative democracy. Cambridge University Press, 2011.

[10] Follow my vote, "Introducing a secure and transparent online voting solution for modern age: Follow my vote." https://followmyvote.com/, accessed: 2019-08-1.

[11] Agora, "Bringing our voting systems into the 21st century," 2017, white paper.

[12] A. KENNEY, "Denver will allow smartphone voting for thousands of people (but probably not you)." A vailable:www.denverpost.com/2019/03/07/voting-smartphoneblockchain- denver/, 2019.

[13] POLYAS, "Online voting with polyas." https://www.polyas.com/, accessed: 2019-07-28.

[14] luxoft, "Luxoft's e-voting platform enables first consultative vote based on blockchain in switzerland." https://www.luxoft.com/pr/luxoftsevoting- platform-enables-first-consultative-vote-based-on-blockchainin- switzerland/, accessed: 2019-07-28.

[15] Polys, "online voting systems." https://polys.me/assets/docs/Polys whitepaper.pdf, accessed: 2019-08-1.

[16] X. Sun, Q. Wang, P. Kulicki, and M. Sopek, "A simple voting protocol on quantum blockchain," International Journal of Theoretical Physics, vol. 58, no. 1, pp. 275–281, 2019.

[17] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "Evoting with blockchain: an e-voting protocol with decentralisation and voter privacy," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018, pp. 1561– 1567.

[18] M. Chaieb, S. Yousfi, P. Lafourcade, and R. Robbana, "Verify-your-vote: A verifiable blockchain-based online voting protocol," in European, Mediterranean, and Middle Eastern Conference on Information Systems. Springer, 2018, pp. 16–30.

[19] Y. Liu and Q. Wang, "An e-voting protocol based on blockchain." IACR Cryptology ePrint Archive, vol. 2017, p. 1043, 2017.

[20] W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, and S. Huang, "A privacy-preserving voting protocol on blockchain," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018, pp. 401–408.

[21] 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.

[22] H. Yi, "Securing e-voting based on blockchain in p2p network," EURASIP Journal on Wireless Communications and Networking, vol. 2019, no. 1, p. 137, 2019.

[23] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," International Journal of Electronic Government Research (IJEGR), vol. 14, no. 1, pp. 53–62, 2018.

[24] J.-H. Hsiao, R. Tso, C.-M. Chen, and M.-E. Wu, "Decentralized e-voting systems based on the blockchain technology," in Advances in Computer Science and Ubiquitous Computing. Springer, 2017, pp. 305–309.

[25] E. Yavuz, A. K. Koc, U. C. C¸ abuk, and G. Dalkılıc¸, "Towards secure evoting using ethereum blockchain," in 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018, pp. 1–7.

[26] A. Singh and K. Chatterjee, “Secevs: Secure electronic voting system using blockchain technology,” in 2018 International Conference on Computing, Power and Communication Technologies (GUCON). IEEE, 2018, pp. 863–867.