National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Survey on E-Voting Protocol with Decentralisation and Voter Privacy

Prof. Pushpanjali C H, Prof. Anuradha K N
Seshadripuram Degree College Tumkur, Karnataka, India

ABSTRACT

Technology has positive impacts on many aspects of our social life. Designing a 24 hour globally connected architecture enables ease of access to a variety of resources and services. Furthermore, technology like the Internet has been a fertile ground for innovation and creativity. One such disruptive innovation is blockchain – a keystone of cryptocurrencies. The blockchain technology is presented as a game changer for many of the existing and emerging technologies/services. With its immutability property and decentralised architecture, it is taking centre stage in many services as an equalisation factor to the current parity between consumers and large corporations/governments. One potential application of the blockchain is in e-voting schemes. The objective of such a scheme would be to provide a decentralised architecture to run and support a voting scheme that is open, fair, and independently verifiable. In this paper, we propose a potential new e-voting protocol that utilises the blockchain as a transparent ballot box. The protocol has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralisation and allow for the voter to change/update their vote (within the permissible voting period). This paper highlights the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts. Concluding the paper is a potential roadmap for blockchain technology to be able to support complex applications.

Keywords : E-Voting, Decentralisation, Voter Privacy, Equalisation

I. INTRODUCTION

Voting, whether traditional ballet based or electronic voting (e-voting), is what modern democracies are built upon. In recent years voter apathy has been increasing, especially among the younger computer/tech savvy generation [1]. E-voting is pushed as a potential solution to attract young voters [2, 3]. For a robust e-voting scheme, a number of functional and security requirements are specified [4]–[6] including transparency, accuracy, auditability, system and data integrity, secrecy/privacy, availability, and distribution of authority. Blockchain technology is supported by a distributed network consisting of a large number of interconnected nodes. Each of these nodes have their own copy of the distributed ledger that contains the full history of all transactions the network has processed. There is no single authority that controls the network. If the majority of the nodes agree, they accept a transaction. This network allows users to remain anonymous. A basic analysis of the blockchain technology (including smart contracts) suggests that it is a suitable basis for e-voting and, moreover, it could have the potential to make e-voting more acceptable and reliable. There are number of papers that have explored this idea [7]–[9] including now this one.

Obvious advantages of e-voting using blockchains includes:

i) greater transparency due to open and distributed ledgers,
ii) inherent anonymity ,
iii) security and reliability (especially against Denial of Service Attacks)
iv) immutability (strong integrity for the voting scheme and individual votes).

Existing works explore how blockchains can be used to improve the evoting schemes or provide some strong guarantees of the above listed requirements. However, these papers do not discuss the implementation challenges and limitations of the blockchain (and smart contract) technologies at their current state to fully support a large scale voting scheme. In this paper we explore both the possibilities of an e-voting scheme, along with the challenges and limitation of the blockchain technology in the e-voting context. A. Contribution of the Paper Contributions of the paper can be summed up as below:
1) The paper proposes an e-voting scheme based on blockchain technology that meets the fundamental e-voting properties whilst, at the same time, provides a degree of decentralisation and places as much control of the process in the hands of the voters as was deemed possible.
2) Discussion on the implementation challenges and underlying platform's (blockchain and smart contracts) limitation to support the e-voting proposal.

II. PROPOSED PROTOCOL

The motivation behind the proposed e-voting protocol, is to have a blockchain based scheme that meets the above stated goals. In addition to those properties the protocol must allow for a voter to change one's mind and cancel one's vote, replacing it with another. As a secondary goal, it has been actively pursued to provide the maximum degree of decentralisation and to create a protocol which the voters control as a network of peers. After careful consideration, however, it was decided that a certain degree of centralisation is necessary to reach the primary goal. This is because when using the blockchain, one is unable to store secret information in the public ledger without the use of external oracles that maintain such information. So if the identity of the voters is to remain secret, whilst at the same time permitting only eligible voters to participate in the elections, a Central Authority needs to be introduced that acts as a trusted third party.

The proposed voting protocol utilises the blockchain to store the cast ballots, therefore in this context the blockchain acts as a transparent ballot box. The main reason for using the blockchain in an e-voting protocol is to take advantage of the fact that it enables a group of people to maintain a public database, that is owned, updated, and maintained by every user, but controlled by no one. Since the protocol is based on the blockchain, it will be realised as a network of peers. Each voter will be a peer i.e. a node in a network of equals. Every voter will be responsible for making sure that fraudulent votes are rejected, hence that consensus is maintained according to the election rules. The blockchain also has the additional advantage of being increasingly well-known and well-trusted to operate as intended, as evidenced by the sheer size of the cryptocurrency market.

III. CONCLUSION

E-voting, as discussed in the paper, is a potential solution to the lack of interest in voting amongst the young tech savvy population. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on blockchain technology. This paper explores the potential of the blockchain technology and its usefulness in the e-voting scheme. The paper proposes an e-voting scheme, which is then implemented. The implementation and related performance measurements are given in the paper along with the challenges presented by the blockchain platform to develop a complex application like e-voting. The paper

highlights some shortcomings and presents two potential paths forward to improve the underlying platform (blockchain technology) to support e-voting and other similar applications. Blockchain technology has a lot of promise; however, in its current state it might not reach its full potential. There needs to be concerted effort in the core blockchain technology research to improve is features and support for complex applications that can execute within the blockchain network.

IV. REFERENCES

[1]. L. C. Schaupp and L. Carter, "E-voting: from apathy to adoption," Journal of Enterprise Information Management, vol. 18, no. 5, pp. 586–601, 2005.

[2]. W. D. Eggers, Government 2.0: Using technology to improve education, cut red tape, reduce gridlock, and enhance democracy. Rowman & Littlefield, 2007.

[3]. T. M. Harrison, T. A. Pardo, and M. Cook, "Creating open government ecosystems: A research and development agenda," Future Internet, vol. 4, no. 4, pp. 900–928, 2012.

[4]. K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie, "A review of contemporary e-voting: Requirements, technology, systems and usability," Data Science and Pattern Recognition, vol. 1, no. 1, pp. 31–47, 2017.

[5]. D. A. Gritzalis, "Principles and requirements for a secure e-voting system," Computers & Security, vol. 21, no. 6, pp. 539–556, 2002.

[6]. R. Anane, R. Freeland, and G. Theodoropoulos, "E-voting requirements and implementation," in The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382–392.

[7]. T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 574–575. Online]. Available: http://doi.acm.org/10.1145/3085228.3085263

8A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.

[8]. P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.

[9]. BitCongress. Control the world from your phone. Online]. Available: http://www.bitcongress.org/BitCongress Whitepaper.pdf

[10]. FollowMyVote.com, Tech. Rep., 2017. Online]. Available: https: //followmyvote.com 12"Tivi

Cite this Article

Prof. Pushpanjali C H, Prof. Anuradha K N, "Survey on E-Voting Protocol with Decentralisation and Voter Privacy", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. , September-October 2019.

Journal URL : http://ijsrcseit.com/CSEIT194736