E-Voting with Blockchain: An E-Voting Protocol  
with Decentralisation and Voter Privacy

Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis  
ISG-SCC, Royal Holloway, University of London, Egham, United Kingdom  
Email: *f*Freya.SheerHardwick.2016, Apostolos.Gioulis.2015*g*@live.rhul.ac.uk, *f*r.n.akram, k.markantonakis*g*@rhul.ac.uk

Brief Description of the Topic

Technology has significantly impacted social life, with the internet providing easy access to resources and services. Blockchain technology, a keystone of cryptocurrencies, is a game changer in many technologies and services due to its immutability property and decentralized architecture. One potential application of blockchain is in e-voting schemes, providing a decentralized architecture for open, fair, and independently verifiable voting. This paper proposes a new e-voting protocol that uses blockchain as a transparent ballot box, adhering to fundamental e-voting properties and offering decentralisation. The paper highlights the pros and cons of using blockchain for this proposal, providing a roadmap for blockchain technology to support complex applications.

Modern democracies rely on voting, including traditional ballet-based and e-voting, to combat voter apathy, particularly among younger tech-savvy generations[1]. Robust e-voting schemes require transparency, accuracy, suitability, system integrity, and authority distribution.

Blockchain technology, a distributed network of interconnected nodes, allows users to remain anonymous and has the potential to make e-voting more acceptable and reliable. Its distributed ledger contains the full history of transactions, and no single authority controls the network.[2]

The proposed e-voting protocol uses a blockchain-based system to allow voters to change their minds and cancel votes. It uses a transparent ballot box as a network of equals, with each voter acting as a node. A Central Authority verifies eligibility using application-dependent methods. Ballots are digital representations of physical ballots, sealed if not revealed. The protocol has three phases: initialisation, preparation, voting, and counting. The protocol ensures eligibility, privacy, fairness, and verification of election results, with a blind signature scheme preventing party identification. Centralisation and fraud prevention are key concerns.

Conclusions of the Paper

The article evaluates the potential of blockchain technology in e-voting to address the lack of enthusiasm among young tech-savvy people. It suggests an e-voting mechanism and provides performance metrics. The article also covers the difficulties encountered by the blockchain platform in implementing complicated applications such as e-voting. It proposes two potential future directions for improving the underlying blockchain technology for e-voting and other related applications.

Critical Opinion of the Paper

This paper Proposes a new e-voting protocol using blockchain for a transparent ballot box, adhering to e-voting principles, offering decentralisation, and allowing voter updatement within permissible voting periods. I mean the paper Presents a detailed protocol or system architecture that leverages blockchain technology to ensure security, transparency, and accuracy in electronic voting. for implementation, they used Ethereum blockchain API and used GAS for expenses. Blockchain applications maximize profits by determining transactions worth above computational cost, preventing mining overtaken by mining nodes. But Ethical concerns arise when charging voters for voting rights.

It shows the importance of decentralization in an e-voting system and trust in electronic voting systems.in conclusion, e-voting mechanisms, including blockchain-based schemes like BitCongress, Follow My Vote, and Tivi, offer promising solutions for secure and efficient voting processes.It can improve security of voting system.

1. 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>
2. 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

Citation /Reference: Use **APA** format

Hardwick, F. S., ApostolosGioulis, R. N. A., & Markantonakis, K. (2018). E-Voting with Blockchain: An E-Voting Protocolwith Decentralisation and Voter Privacy.‏