Paillier Cryptosystem Based ChainNode for Secure Electronic Voting

Authors: Umar, B. U., Olaniyi, O. M., Olajide, D. O., & Dogo, E. M.

Abstract: Blockchain is a distributed and decentralized ledger of transactions that are linked together cryptographically leading to immutability and tamper-resistance, thereby ensuring the integrity of data. Due to the ability of blockchain to guarantee the integrity of data, it has found widerange adoption in electronic voting (e-voting) systems in recent years, this is in a bid to prevent manipulation of votes. However, due to the distributed nature of the blockchain, opportunities arise for privacy intrusion of the data being secured. The translation of this privacy flaw in blockchain to e-voting systems is the possibility of violation of the privacy of the electorates. Consequently, in a bid to achieve integrity and privacy of votes in e-voting, this study presents the use of an open-source blockchain system, coupled with a privacy-oriented cryptosystem known as the Paillier cryptosystem, towards addressing the privacy concerns of the blockchain. The performance of the system was evaluated and a transaction throughput of 1424 tps was obtained for ten thousand simulated ballot transactions. Further evaluation was carried out on the system, by increasing the number of system transactions. This showed that themining time of the blockchain increased by an average factor of 0.18 s for every thousand increases in the number of transactions. Also, the response time of the system to a range of user actions was evaluated over an increasing number of voters. Results obtained showed that the response time of the system for vote casting operations increased by an average of 0.33min per thousand voters while for vote tallying there was an increase in response time by an average of 0.848 min per thousand voters. The scientific value of this study is the development of an integrity and privacy-preserving e-voting system consisting of an open-source nodechain coupled with a privacy oriented cryptosystem known as the Paillier cryptosystem following the security requirements of e-voting systems. The proposed system addresses the issue of integrity in e-voting while still maintaining the privacy of the electorates.

Keywords: e-voting, blockchain, homomorphic encryption, proof-of-work, ballot

url: doi: 10.3389/fbloc.2022.927013