Abstract

Digital payment systems are an evolving field in present day with the recent enhancements in seamless digital currencies. Thus, despite the benefits of cryptocurrency based digital payments systems, their adoption and diffusion within general payment platform domain are significantly hindered. The blockchain architecture is widely recognized as a promising mechanism to support the management of cryptocurrency related transactions. However, ensuring the security of digital payment transactions is a challenging task due to various security threats and existing prevention mechanisms that are either computationally expensive or domain dependent. Among many, Double Spending is identified as a key security vulnerability.

The purpose of this study is to investigate the means of addressing the said security issue by proposing a feasible transaction verification methodology; targeting a common payment platform that integrates different vendor based digital currencies together. The currency miners and the user applications are identified as the core components that cooperate with transactions. Accordingly, a scenario based transaction verification model is designed by
considering transaction patterns among miners and user applications. The bitcoin-similar concept of ‘trust network’ is adopted in verifying transactions via building a trusted network among currency miners in the payment platform using digital signatures along with SHA-256 hashing and RSA algorithm. In strengthening the verification level, an approach of acknowledgments is defined associated with a minimum required level of probability. Furthermore, a time constraint is set depending on the peer-to-peer network conditions for a particular transaction to get completed with proper verification.

References


**Index Terms**

Computer Science | Information Systems

**Keywords**

Cryptocurrency, Blockchain Architecture, Peer-to-Peer, Online Transactions, Digital Payment, Double Spending Attack