

ABSTRACT

A secure peer-to-peer network is implemented with computing devices over unsecure network connections. Each computing device can include or be coupled to a proof of origin hardware. The proof of origin hardware can be validated by publicly available data, such as a trusted server. In addition, the proof of origin hardware can facilitate cryptographic key generation to facilitate encryption of communications at the computing devices, to secure such communications over the unsecure network connections. The proof of origin hardware can include hardware acceleration circuitry to provide network services, such as cryptocurrency transactions, blockchain validation computations, and even blockchain services integrating smart contracts, token exchange, survey services leveraging proof of origin data, distributed data backup, distributed computing, among others.

[Fig. 7]