

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 or by secure storage of valid proof of origin data, or other modality. Once validated on the peer-to-peer network, peer nodes can provide or can receive network services, such as blockchain services, cryptocurrency transaction services, smart contract-enabled services, token exchange, survey services leveraging proof of origin data, distributed data backup services, distributed computing services, among others.

[Fig. 5]