

Keychain

Blockchain-based Public Key Infrastructure

Author: Jonathan Hope

1 Abstract

We present a new method for providing public key infrastructure services using blockchain technology. The described method provides a basis for application-level end-to-end encryption and allows one or more parties to securely exchange messages, data, and documents over networks of various security levels.

Keychain differs from Bitcoin in that new transactions created by an end user have a single output to an address that was also newly created by the same user. The user which controlled the private keys of the previous transaction also control the private keys of the new transaction. Such transactions carry a different payload, however control is maintained by the same user thus creating a link between the different payloads. Participants use this aspect to deduce that the new payload represents a replacement of the older and that both came from the same end user. Given this, participants may trust that off-chain messages that are encrypted or signed by the new public key come from the same source as the previous public key, and this forms the basis of a communication pattern where authentication outside the blockchain is anchored by transactions in the blockchain.

Applications include finance, trade, Internet of Things, insurance, real estate, and peer-to-peer communication, among others.