

BLOCKCHAIN-BASED EXCHANGE WITH TOKENISATION

ABSTRACT

The invention provides a secure method for exchanging entities via a blockchain. The invention incorporates tokenisation techniques, and also techniques for embedding metadata in a redeem script of a blockchain transaction. Embodiment(s) provide a computer implemented method of performing an exchange of entities, the method comprising: receiving, from a first user over a communications network, a first invitation to perform the exchange, the first invitation comprising a first set of metadata associated with the invitation, wherein the first set of metadata comprises an indication of entities to be exchanged and a first set of conditions for the exchange; generating a first script, the first script comprising: the first set of metadata, a first user public key (P1A) associated with the first user, wherein the first user public key (P1A) is a cryptographic pair with a first user private key (V1A), and a first third-party public key (P1T) associated with a first third-party, wherein the first third-party public key (P1T) is a cryptographic pair with a first third-party private key (V1T); hashing the first script to generate a first script hash; publishing the first script and the first script hash on a distributed hash table (DHT) distributed across a first network; and broadcasting, on a second network, a first invitation transaction for inclusion on a peer-to-peer (P2P) distributed ledger, the first invitation transaction comprising an indication of a first quantity of a cryptocurrency to be transferred and the first script hash.

Fig. 1