

ABSTRACT

The invention relates to computer-based, electronic ledgers, and in particular distributed ledgers known as “blockchains”. The invention is suited for use with the Bitcoin blockchain and associated protocol, but is not limited in this regard and can be deployed using other blockchain platforms. The invention provides a novel and advantageous technique for executing a micropayment channel in which the number of transactions (TXs) that need to be submitted to the blockchain can be greatly reduced. An initial transaction (Tx) can be replaced by one or more subsequent transactions which another party can hold onto until a selected transaction is completed (signed) and submitted to the network. In one embodiment, the invention provides a computer-implemented method for performing an exchange via a blockchain, comprising the step of submitting a funding transaction to the blockchain network, wherein the funding transaction i) comprises a tokenised contract relating to an asset to be transferred from a second user to a first user; and ii) is signed by the first user. It also comprises the step of sending, from the first user to the second user, one or more subsequent transactions wherein each said subsequent transaction spends an output of the funding transaction and is signed by the first user. It includes the step of submitting one of the subsequent transactions to the blockchain network, the submitted transaction having been signed by the second user.

20

(Fig. 2)