Abstract

COMPUTER-IMPLEMENTED SYSTEMS AND METHODS FOR CONTROLLING OR ENFORCING PERFORMANCE OF TRANSFERS CONDUCTED OVER A BLOCKCHAIN

The invention provides methods and systems by which an agreed set of conditions governing transfers on a blockchain (e.g. the Bitcoin blockchain) can be generated and enforced. Advantageously, the conditions can be used to specify and influence the behaviour of another party who will be receiving the asset, by enforcing their fulfilment of an agreed set of rules. In one embodiment, a computer-implemented method comprises the step of providing, to a recipient, a representation of at least one rule (*r*) relating to a transfer to be conducted over a blockchain network. It also comprises the step of receiving, from a sender: a redeem script (*R*) which comprises the representation (*r*); and a script address comprising a hash (*HR*) of the redeem script (*R*). It also comprises the step of generating a hash (*H*) of the redeem script (*R*) and comparing it with the script address. If the hash (*H*) matches the script address, the sender can use the script address in a locking script associated with an output of a blockchain transaction (TX_0) safe in the knowledge that the rules (r) will be enforced in order to unlock the asset.

Figure 1