Abstract

The invention relates to distributed ledger technologies such as consensus-based blockchains. A blockchain transaction may include digital resources that are encumbered by a locking script that encodes a set of conditions that must be fulfilled before the encumbered resources may be used (e.g., transferring ownership/control of encumbered resources). A worker (e.g., a computer system) performs one or more computations to generate a proof, which is encoded as part of an unlocking script. A verification algorithm may utilize the proof, a verification key, and additional data such as a cryptographic material associated with the worker (e.g., a digital signature) to verify that digital assets of the transaction should be transferred. As a result of the validation of this transaction, any third party is able to check the contract was executed corrected rather than re-executing the contract, thus saving computational power.

Figure 6.