

Claims

1. A computer-implemented method, comprising:
 - obtaining a first script (404) associated with a blockchain transaction, the first script (404) comprising:
 - a first set of commands; and
 - one or more cryptographic hash values (418, 414);
 - generating a second script (402) comprising:
 - a second set of commands;
 - one or more subsets of a plurality of elements (412, 416), wherein the plurality of elements collectively form a verification key (212) and the one or more subsets collectively include each element of verification key (212);
 - the first script (404); and
 - an identifier (406) associated with a computer system generating the second script; and
 - generating an attestation that the computer system has access to the verification key (212) based at least in part on executing the first set of commands and the second set of commands in connection to determine that the one or more cryptographic hash values match the one or more subsets of the verification key (212).
2. The computer-implemented method according to claim 1, wherein an element of the plurality of elements (412, 416) is a point on an elliptic curve.
3. The computer-implemented method according to any preceding claim, wherein the first set of commands and the second set of command collectively comprise instructions to determine whether a first cryptographic hash value of the one or more cryptographic hash values matches a hash output based at least in part on a subset of the one or more subsets of the verification key (212).
4. The computer-implemented method according to claims 3, wherein the hash output is generated using at least a SHA-256 and a RIPEMD-160 cryptographic hash algorithm.

5. The computer-implemented method according to any preceding claim, wherein obtaining the first script (404) comprises:
 - identifying the one or more subsets of the verification key (212); and
 - calculating, for each subset of the one or more subsets of the verification key (212), a corresponding cryptographic hash value, wherein the one or more cryptographic hash values comprises each corresponding cryptographic hash value.
6. The computer-implemented method according to any preceding claim, further comprising, contingent upon verifying the generated attestation, transferring control of digital assets encumbered by the transaction to the computer system, and preferably further comprising obtaining the first script from a second computer system, wherein the second computer system contributed at least part of the digital assets.
7. The computer-implemented method according to any preceding claim, wherein the transaction is a P2SH transaction.
8. The computer-implemented method according to any preceding claim, wherein at least one of the one or more subsets of the verification key (212) is greater or equal to 512 bytes in size and less than or equal to 520 bytes in size.
9. The computer-implemented method according to any preceding claim, wherein:
 - the first script (404) is greater than or equal to 58 bytes in size and less than or equal to 104 bytes in size; and
 - the second script (402) is greater than or equal to 1628 bytes in size and less than or equal to 1650 bytes in size.
10. The computer-implemented method according to any preceding claim, wherein the transaction is a standard transaction in accordance with a blockchain protocol.
11. The computer-implemented method according to any preceding claim, wherein each element of the verification key (212) is in exactly one of the subsets.

12. The computer-implemented method according to any preceding claim, wherein the one or more subsets (412, 416) is one subset, the one subset comprising the verification key (212).
13. The computer-implemented method according to any preceding claim, wherein:
 - the first script further comprises a public key associated with the computer system;
 - the identifier associated with the computer system is a digital signature generated using a private key corresponding to the public key associated with the computer system; and
 - the attestation that the computer system has access to the verification (212) key is further based at least in part on the digital signature and the public key.
14. A system, comprising:
 - a processor; and
 - memory including executable instructions that, as a result of being executed by the processor, causes the system to perform the computer-implemented method according to any preceding claim.
15. A non-transitory computer-readable storage medium having stored thereon executable instructions that, as a result of being executed by a processor of a computer system, cause the computer system to at least perform the computer-implemented method according to any of claims 1 to 13.