

CLAIMS:

1. A computer-implemented method of verifying ownership of a computer software after installation and prior to execution of the computer software using a distributed hash table and a peer-to-peer distributed ledger, the method comprising:

determining a second user public key (PU2) associated with a second user (U2) from a transaction record stored on the peer-to-peer distributed ledger;

determining a second public key (P2) associated with the second user (U2) from an entry stored on the distributed hash table;

comparing the second user public key (PU2) and the second public key (P2); and

verifying the ownership of the computer software based on the comparing of the second user public key (PU2) and the second public key (P2).

2. The method of claim 1, wherein comparing the second user public key (PU2) and the second public key (P2) comprises determining whether the second user public key (PU2) and the second public key (P2) match.

3. The method of claim 1 or 2, wherein the computer software comprises a header and a body.

4. The method of claim 3, wherein the header comprises a hash value of the body of the computer software.

5. The method of claims 3 or 4, wherein the header further comprises a hash value (H2) of a data associated with the computer software or a licence.

6. The method of claims 3, 4 or 5, wherein the body of the computer software comprises an executable of the computer software.

7. The method of claim 5, wherein before determining the second user public key (PU2), the method comprises installing the executable of the computer software on a processing device associated with the second user (U2).
8. The method of claim 7, wherein before installing the executable of the computer software, the method comprises encrypting the executable of the computer software.
9. The method of claim 8, wherein encrypting the executable of the computer software comprises:
- determining a generator value (GV);
 - determining a second user second public key (P2U2) based on the second user public key (PU2) and the generator value (GV), wherein the second user second public key (P2U2) forms a cryptographic pair with a second user second private key (V2U2);
 - determining a first user second public key (P2U1) based on a first user public key (PU1) and the generator value (GV), wherein the first user second public key (P2U1) forms a cryptographic pair with a first user second private key (V2U1);
 - determining a common secret (CS) based on the second user second public key (P2U2) and the first user second private key (V2U1); and
 - encrypting the executable of the computer software with the common secret (CS) to generate an encrypted executable of the computer software.
10. The method of claim 9, wherein the encrypted executable of the computer software is decrypted before installing the executable of the computer software by:
- determining the common secret (CS) based on the first user second public key (P2U1) and the second user second private key (V2U2); and
 - decrypting the executable of the computer software with the common secret (CS) to generate a decrypted executable of the computer software.

11. The method of claim 10, further comprising executing instructions of the decrypted executable of the computer software on the processing device associated with the second user (U2) after verifying the ownership of the computer software.

12. The method of claim 11, wherein before executing instructions the method further comprises:

determining an activation key (AK) from the second user (U2); and

executing instructions of the decrypted executable of the computer software based on the activation key (AK) on the processing device associated with the second user (U2).

13. The method of any of claims 8 to 12, wherein before encrypting the executable of the computer software, the method further comprises:

determining a data (D1) associated with the computer software;

determining a first hash value (H1) of the computer software;

determining a second hash value (H2) based on the data (D1) and the computer software;

sending, over a communications network, the data (D1), the first hash value (H1) and the second hash value (H2) to an entry for storage in the distributed hash table, wherein the second hash value (H2) is a key of a key-value pair and the data (D1) and the first hash value (H1) are a value in the key-value pair; and

determining the metadata (M) comprising the second hash value (H2) for storage on the peer-to-peer distributed ledger.

14. A computer software program comprising machine-readable instructions to cause a processing device to implement the method of any one of the preceding claims.

15. A computer system for verifying ownership of a computer software after installation and prior to execution using a distributed hash table and a peer-to-peer distributed ledger, the

system comprising a processing device associated with a node on a peer-to-peer network of nodes, configured to:

determine a second user public key (PU2) associated with a second user (U2) from a transaction record stored on the peer-to-peer distributed ledger;

determine a second public key (P2) associated with the second user (U2) from an entry stored on the distributed hash table;

compare the second user public key (PU2) and the second public key (P2); and

verify the ownership of the computer software based on the compare of the second user public key (PU2) and the second public key (P2).