

Claims

1. A computer-implemented method for controlling one or more devices of a first network, wherein the first network comprises a set of bridging nodes and a set of devices controllable by one or more of the set of bridging nodes, each bridging node also being a node of a blockchain network, and each device having a respective device identifier; the method being performed by a first one of the bridging nodes and comprising:
generating a first blockchain transaction, wherein the first blockchain transaction comprises a first input comprising a signature linked to a first public key of the first node, and a first output comprising command data, wherein the command data comprises a respective identifier of a first one of the devices controlled by a second one of the bridging nodes, and a command message for controlling the first device.
2. The method of claim 1, wherein the first blockchain transaction comprises a second output locked to a first public key of the second node.
3. The method of claim 1 or claim 2, comprising transmitting the first blockchain transaction to the second node.
4. The method of claim 2, wherein the blockchain comprises a previous blockchain transaction, the previous transaction comprising: a first input comprising a signature linked to a first public key of a third one of the bridging nodes; a first output comprising command data, wherein the command data comprises the respective identifier of the first device, and a command message for controlling the first device; and a second output locked to at least the first public key of the first node and a first public key of a fourth one of the bridging nodes, and wherein the first input of the first blockchain transaction comprises a signature linked to the first public key of the fourth node.
5. The method of claim 4, comprising, transmitting the first blockchain transaction to the blockchain network for inclusion in the blockchain.

6. The method of any of claims 1 to 5, wherein the command message is configured to cause the second node to transmit a control instruction to the first device, wherein the control instruction is based on the command message.
7. The method of any of claims 1 to 6, wherein the command data is encrypted, or otherwise encoded, command data.
8. The method of claim 7, wherein the command data is encrypted using a first encryption key generated based on a second public key of the first node and a second public key of the second node.
9. The method of claim 8, wherein the set of bridging nodes comprises a master node, and wherein the first output of the first blockchain transaction comprises encryption data, the encryption data comprising the first encryption key encrypted using a second encryption key generated based on a third public key of the first node and a first public key of the master node.
10. The method of any of claims 1 to 9, wherein the first network comprises a master layer comprising a master node, one or more intermediary layers each comprising a plurality of intermediary nodes, and a device layer comprises the one or more devices; and wherein the first node is the master node.
11. The method of claim 10, wherein the master node has a main master private key, and wherein the method comprises:
 - obtaining a seed private key;
 - generating a set of joint private keys based on the seed private key; and
 - transmitting the set of joint private keys to the plurality of intermediary nodes.
12. The method of claim 11, comprising:
 - generating a set of secondary master private keys, wherein each private key in the set of secondary master private keys is generated by adding the main master private key to each private key in the set of joint private keys, and wherein each public key of the first

node that is linked to a signature is generated based on a respective private key from the set of secondary master private keys.

13. The method of claim 11 or claim 12, wherein the main master private key corresponds to a main master public key certified by the master node.

14. The method of claim 1, wherein the first blockchain transaction comprises a second output locked to at least a public key of third node and a public key of a fourth node.

15. The method of any of claims 1 to 9 or claim 14, wherein the first network comprises a master layer comprising a master node, one or more intermediary layers each comprising a plurality of intermediary nodes, and a device layer comprises the one or more devices; and wherein the first node is an intermediary node.

16. The method of claim 15, wherein the first node has a main private key, and wherein the method comprises:

obtaining a set of joint private keys;

generating a set of secondary private keys by adding the main private key to each private key in the set of joint private keys, wherein each public key of the first node that is linked to a signature is generated based on a respective private key from the set of secondary private keys.

17. The method of claim 16, wherein the main private key corresponds to a main public key certified by the master node.

18. The method of any of claims 1 to 17, wherein the command data further comprises one or more of the following:

a protocol identifier;

a software version number;

a data type indicator;

a device certificate location for the first device;

a current status for the first device; and

a previous status for the first device.

19. A computer-implemented method for controlling one or more devices of a first network, wherein the first network comprises a plurality of bridging nodes and a set of devices controllable by one or more of the set of bridging nodes, each bridging node also being a node of a blockchain network, and each device having a respective device identifier; the method being performed by a second one of the bridging nodes and comprising:

obtaining a first blockchain transaction, wherein the first blockchain transaction comprises a first input comprising a signature linked to a first public key of a first one of the bridging nodes, and a first output comprising command data, wherein the command data comprises a respective identifier of a first one of the devices controlled by the second node, and a command message for controlling the first device; and

transmitting a command to the first device, wherein the command is based on the command message.

20. The method of claim 19, wherein said transmitting is conditional on the signature being a valid signature.

21. The method of claim 19 or claim 20, wherein the command is transmitted to the first device via an off-chain connection.

22. The method of any of claims 19 to 21, comprising:

updating the first blockchain transaction by including a second input comprising a signature linked to a first public key of the second node; and

causing the updated first blockchain transaction to be transmitted to the blockchain network for inclusion in the blockchain.

23. The method of claim 22, wherein said causing comprises transmitting the updated first blockchain transaction to the blockchain network.

24. The method of claim 22 or claim 23, comprising:

receiving a command completion message from the first device; and

said updating is conditional on receipt of the command completion message.

25. The method of any of claims 22 to 24, wherein said updating comprises including a second output locked to a second public key of the second node.
26. The method of any of claims 19 to 25, wherein said obtaining comprises receiving the first blockchain transaction from the first node.
27. The method of any of claims 19 to 26, wherein said obtaining comprises obtaining the first blockchain transaction from the blockchain.
28. The method of any of claims 19 to 27, wherein the command data is encrypted using a first encryption key generated based on a second public key of the first node and a second public key of the second node, and wherein the method comprises decrypting the command data using the first encryption key.
29. The method of any of claims 19 to 28, wherein the first network comprises a master layer comprising a master node, one or more intermediary layers each comprising a plurality of intermediary nodes, and a device layer comprises the one or more devices; and wherein the second node is an intermediary node.
30. The method of claim 29, wherein the second node has a main private key, and wherein the method comprises:
- obtaining a set of joint private keys; and
 - generating a set of secondary private keys by adding the main private key to each private key in the set of joint private key.
31. The method of claim 29 when dependent on claim 22, wherein the first public key of the second node is a public key having a corresponding secondary private key.
32. Computer equipment comprising:
- memory comprising one or more memory units; and

processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of claims 1 to 18.

33. A computer program embodied on computer-readable storage and configured so as, when run on computer equipment of claim 32, to perform the method of any of claims 1 to 18.

34. Computer equipment comprising:
memory comprising one or more memory units; and
processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of claims 19 to 31.

35. A computer program embodied on computer-readable storage and configured so as, when run on computer equipment of claim 34, to perform the method of any of claims 19 to 31.

36. A first transaction for inclusion within a blockchain, the first transaction comprising:
a first input comprising a signature linked to a public key of a first node; and
a first output comprising command data, wherein the command data comprises a respective identifier of a device controlled by a second node and a command message for controlling the device.

37. An updated first transaction for inclusion within a blockchain, the update first transaction comprising:
a first input comprising a signature linked to a first public key of a first node;
a second input comprising a signature linked to a first public key of a second node;
a first output comprising command data, wherein the command data comprises a respective identifier of a first device controlled by the second node and a command message for controlling the first device; and
a second output locked to the first public key of the second node.

38. A command-request transaction for inclusion within a blockchain, the command-request transaction comprising:
- a first input comprising a signature linked to a public key of a first node;
 - a first output comprising command data, wherein the command data comprises a respective identifier of a device controlled by a second node and a command message for controlling the device; and
 - a second output locked to at least a public key of a third node and a public key of a fourth node.
39. A command-approval transaction for inclusion within a blockchain, the command-approval transaction comprising:
- a first input comprising a signature linked to a public key of a third node and a signature linked to a public key of a fourth node, wherein the first input references the second output of the command-request transaction of claim 37;
 - a first output comprising command data, wherein the command data comprises a respective identifier of a device controlled by a second node and a command message for controlling the device; and
 - a second output locked to a public key of the second node.
40. A computer-readable storage medium having stored thereon the first transaction claim 36.
41. A computer-readable storage medium having stored thereon the updated first transaction claim 37.
42. A computer-readable storage medium having stored thereon the command-request transaction of claim 38.
43. A computer-readable storage medium having stored thereon the command-approval transaction of claim 39.