CLAIMS:

1. A computer-implemented control system for controlling a device, the system comprising:

a device configured for communication with a network and having an IP address and a public-private key cryptographic key pair associated with the device;

a software-implemented control component arranged to monitor the state of a blockchain network and/or transmit blockchain Transactions to the blockchain network; wherein the control component is arranged to access the set of instructions from a stored location which is separate to the device; and

a set of instructions arranged for execution by the control component to control the functionality of the device; wherein the set of instructions is stored in a Distributed Hash Table (DHT) and accessed for download and installation by the control component from the DHT, and the location of the DHT is indicated or provided using metadata provided within a blockchain transaction.

2. A system according to claim 1 wherein the control component is arranged to receive an input signal from an input source, and wherein the input source is:

a further device; and/or

a computer-based resource or agent.

3. A system according to claim 1 or 2 wherein the set of instructions is accessed by the control component using a look-up key which is related to a cryptographic key pair.

4. A system according to any preceding claim wherein the control component is provided on or in the device.

5. A system according to any preceding claim wherein the control component is provided in an off-device location and arranged for wireless communication with the device.

6. A system according to any preceding claim wherein the control component is arranged to:

Perform cryptographic calculations;
Access its associated private/public key pair;
have an associated Bitcoin or other blockchain-related address;
operate the device via an API;
perform secret sharing protocol operations.

7. A system according to any preceding claim wherein the control component is arranged to influence or control the activities of the device based upon detection of a valid blockchain transaction.

8. A computer-implemented control method for controlling a device, the method comprising the steps:
providing a device configured for wireless communication with a network and having an IP address and a public-private key cryptographic key pair associated with the device;
providing a software-implemented control component arranged to monitor the state of a blockchain network and/or transmit blockchain Transactions to the blockchain network;
providing a set of instructions arranged for execution by the control component to control the functionality of the device;
wherein:
i) the control component is arranged to access the set of instructions from a stored location which is separate to the device;
ii) the set of instructions is stored in a Distributed Hash Table (DHT) and accessed for download and installation by the control component from the DHT; and
iii) the location of the DHT is indicated or provided using metadata provided within a blockchain transaction.

9. A method according to claim 8 wherein the control component is arranged to receive an input signal from an input source, and wherein the input source is:
a further device; and/or
a computer-based resource or agent.

10. A method according to claim 9 wherein the set of instructions is accessed by the control component using a look-up key which is related to a cryptographic key pair.

11. A method according to any of claims 8 to 10, wherein the control component is provided on or in the device.

12. A method according to claims 18 to 11 wherein the control component is provided in an off-device location and arranged for wireless communication with the device.

13. A method according to any of claims 8 to 12, wherein the control component is arranged to:
Perform cryptographic calculations;
Access its associated private/public key pair;
have an associated Bitcoin or other blockchain-related address;
operate the device via an API;
perform secret sharing protocol operations

14. A method according to any of claims 8 to 13, wherein the control component is arranged to influence or control the activities of the device based upon detection of a valid blockchain transaction.

CLAIMS:

1. A computer-implemented control system for controlling a device, the system comprising:
   a device configured for communication with a network and having an IP address and a public-private key cryptographic key pair associated with the device;
   a software-implemented control component arranged to monitor the state of a blockchain network and/or transmit blockchain transactions to the blockchain network; wherein the control component is arranged to access a set of instructions from a repository which is separate to the device; and
   a set of instructions arranged for execution by the control component to control the functionality of the device; wherein:
      the set of instructions is stored in the repository which is separate to the device and accessed for download and installation by the control component from the repository, and
      the location of the repository is indicated or provided using metadata provided within a blockchain transaction.

2. A system according to claim 1 wherein the control component is arranged to receive an input signal from an input source, and wherein the input source is:
   a further device; and/or
   a computer-based resource or agent.

3. A system according to claim 1 or 2 wherein:
   i) the repository is a Distributed Hash Table (DHT);
   ii) the set of instructions is retrieved from an operating system for coordinating, controlling and/or influencing the activities of the device; and/or
   iii) the device is an IOT device.

4. A system according to claim 1, 2 or 3 wherein the set of instructions is accessed by the control component using a look-up key which is related to a cryptographic key pair.

5. A system according to any preceding claim wherein the control component is provided on or in the device; or in an off-device location and arranged for wireless communication with the device.

6. A system according to any preceding claim wherein the control component is arranged to:
   perform cryptographic calculations;
   access its associated private/public key pair;
   have an associated Bitcoin or other blockchain-related address;
   operate the device via an API;
   perform secret sharing protocol operations.

7. A system according to any preceding claim wherein the control component is arranged to influence or control the activities of the device based upon detection of a valid blockchain transaction.

8. A computer-implemented control method for controlling a device, the method comprising the steps:
   providing a device configured for wireless communication with a network and having an IP address and a public-private key cryptographic key pair associated with the device;
   providing a software-implemented control component arranged to monitor the state of a blockchain network and/or transmit blockchain transactions to the blockchain network;
   providing a set of instructions arranged for execution by the control component to control the functionality of the device;
   wherein:
   i) the control component is arranged to access the set of instructions from a repository which is separate to the device;
   ii) the set of instructions is stored in the repository which is separate to the device and accessed for download and installation by the control component from the repository; and

iii) the location of the repository is indicated or provided using metadata provided within a blockchain transaction.

9. A method according to claim 8 wherein:
i) the repository is a Distributed Hash Table (DHT);
ii) the set of instructions is retrieved from an operating system for coordinating, controlling and/or influencing the activities of the device; and/or
iii) the device is an IOT device.

10. A method according to claim 8 or 9 wherein the control component is arranged to receive an input signal from an input source, and wherein the input source is:
a further device; and/or
a computer-based resource or agent.

11. A method according to claims 8 to 10 wherein the set of instructions is accessed by the control component using a look-up key which is related to a cryptographic key pair.

12. A method according to any of claims 8 to 11, wherein the control component is provided on or in the device.

13. A method according to claims 8 to 12 wherein the control component is provided in an off-device location and arranged for wireless communication with the device.

14. A method according to any of claims 8 to 13, wherein the control component is arranged to:
perform cryptographic calculations;
access its associated private/public key pair;
have an associated Bitcoin or other blockchain-related address;
operate the device via an API;
perform secret sharing protocol operations.

15. A method according to any of claims 8 to 14, wherein the control component is arranged to influence or control the activities of the device based upon detection of a valid blockchain transaction.