What is claimed is:

1. An Internet of Things (IoT) device for implementing trust IoT services based on a block chain, the IoT device being configured with a pair of IoT device public key (P_{IoT}) and IoT device private key (K_{IoT}), the IoT device comprising:

a memory and a processor, the memory being stored with machine executable instructions that, when executed by the processor, cause the IoT device to perform operations including:

receiving an authentication request from a user device, the user device being configured with a pair of user public key (P_u) and user private key (K_u), and the authentication request including a hash value of user data of the user device, first encrypted information obtained based on the IoT device public key (P_{IoT}) and a user random number (R_u) and second encrypted information obtained based on the user private key (K_u), the user random number (R_u) and the hash value;

authenticating, based on the IoT device private key (K_{IoT}) and the authentication request, the user device to obtain the user public key (P_u);

determining whether the user public key (P_u) exists in a list of access permitted user devices of the IoT device; and

in response to determining that the user public key (P_u) exists in the list of access permitted user devices of the IoT device, determining that authentication of the user device succeeds.

2. The IoT device according to claim 1, wherein authenticating, based on the IoT device private key (K_{IoT}) and the authentication request, the user device to obtain the user public key (P_u) further comprises:

calculating, based on the IoT device private key (K_{IoT}) and the first encrypted information, the user random number (R_u);

calculating, based on the user random number (R_u) and the second encrypted information, a user signature of the user device, wherein the user signature is obtained by encrypting the hash value using the user private key (K_u); and

determining the user public key (P_u) based on the user signature and the hash value using an elliptic curve cryptography.

3. The IoT device of claim 2, wherein calculating, based on the IoT device private key (K_{IoT}) and the first encrypted information, the user random number (R_u) comprises: calculating the user random number (R_u) according to the following equation:

$R_u=K^{-1}_{IoT}(P_{IoT}(R_u))$,

where $P_{IoT}(R_u)$ represents the first encrypted information, and K^{-1}_{IoT} represents a decryption operation using the IoT device private key (K_{IoT}); and

wherein calculating, based on the user random number (R_u) and the second encrypted information, a user signature of the user device comprises: calculating the user signature according to the following equation:

$K_u(H)=R^{-1}_u(R_u(K_u(H)))$,

where $K_u(H)$ represents the user signature, H represents the hash value of the user data, $R_u(K_u(H))$ represents the second encrypted information, and R^{-1}_u represents a decryption operation using the user random number (R_u).

4. The IoT device of claim 3, wherein determining whether the user public key (P_u) exists in a list of access permitted user devices of the IoT device comprises:

sending the user public key (P_u) to a provider of the IoT device, the provider saving a list of access permitted user devices for each IoT device that belongs to the provider; and

receiving, from the provider, a search result indicating whether the user public key (P_u) exists in the list of access permitted user devices of the IoT device.

5. The IoT device of claim 3, wherein determining whether the user public key (P_u) exists in a list of access permitted user devices of the IoT device comprises:

determining whether the user public key (P_u) exists in the list of access permitted user devices saved by the IoT device.

6. A method for implementing trust Internet of Things (IoT) services based on a block chain, the method being performed by an IoT device configured with a pair of IoT device public key (P_{IoT}) and IoT device private key (K_{IoT}), the method comprising:

receiving an authentication request from a user device, the user device being

configured with a pair of user public key (P_u) and user private key (K_u), and the authentication request including a hash value of user data of the user device, first encrypted information obtained based on the IoT device public key (P_{IoT}) and a user random number (R_u) and second encrypted information obtained based on the user private key (K_u), the user random number ($R_{u)}$ and the hash value;

authenticating, based on the IoT device private key (K_{IoT}) and the authentication request, the user device to obtain the user public key (P_u);

determining whether the user public key (P_u) exists in a list of access permitted user devices of the IoT device; and

in response to determining that the user public key (P_u) exists in the list of access permitted user devices of the IoT device, determining that authentication of the user device succeeds.

7. The method according to claim 6, wherein authenticating, based on the IoT device private key (K_{IoT}) and the authentication request, the user device, to obtain the user public key (P_u) further comprises:

calculating, based on the IoT device private key (K_{IoT}) and the first encrypted information, the user random number (R_u);

calculating, based on the user random number (R_u) and the second encrypted information, a user signature of the user device, wherein the user signature is obtained by encrypting the hash value using the user private key (K_u); and

determining, based on the user signature and the hash value using an elliptic curve cryptography, the user public key (P_u).

8. The method of claim 7, wherein calculating, based on the IoT device private key (K_{IoT}) and the first encrypted information, the user random number (R_u) comprises: calculating the user random number (R_u) according to the following equation:

$R_u=K^{-1}{}_{IoT}(P_{IoT}(R_u))$,

where $P_{IoT}(R_u)$ represents the first encrypted information, and $K^{-1}{}_{IoT}$ represents a decryption operation using the IoT device private key (K_{IoT}); and

wherein calculating, based on the user random number (R_u) and the second encrypted information, a user signature of the user device comprises: calculating

the user signature according to the following equation:

$K_u(H)=R^{-1}{}_u(R_u(K_u(H)))$,

where $K_u(H)$ represents the user signature, H represents the hash value of the user data, $R_u(K_u(H))$ represents the second encrypted information, and $R^{-1}{}_u$ represents a decryption operation using the user random number (R_u).

9. The method of claim 8, wherein determining whether the user public key (P_u) exists in a list of access permitted user devices of the IoT device comprises:

sending the user public key (P_u) to a provider of the IoT device, the provider saving a list of access permitted user devices for each IoT device that belongs to the provider; and

receiving, from the provider, a search result indicating whether the user public key (P_u) exists in the list of access permitted user devices of the IoT device.

10. The method of claim 8, wherein determining whether the user public key (P_u) exists in a list of access permitted user devices of the IoT device comprises:

determine whether the user public key (P_u) exists in the list of access permitted user devices saved by the IoT device.

11. A nonvolatile computer readable storage medium for implementing trusted Internet of Things (IoT) services based on a block chain comprising machine executable instructions that, when executed by a machine, are adapted to cause the machine to implement the method as any of claims 6-10.

12. A user device for implementing trust Internet of Things (IoT) services based on a block chain, the user device being configured with a pair of user public key (P_u) and user private key (K_u), the user device comprising:

a memory and a processor, the memory being stored with machine executable instructions that, when executed by the processor, cause the user device to perform operations including:

performing a hash operation on user data of the user device to generate a hash value of the user data;

obtaining, based on the IoT device public key (P_{IoT}) of the IoT device

and a user random number (R_u), first encrypted information;

obtaining, based on the user private key (K_u), the user random number (R_u) and the hash value, second encrypted information; and

sending an authentication request to the IoT device, the authentication request including the hash value of the user data, the first encrypted information, and the second encrypted information.

13. The user device of claim 12, wherein obtaining, based on the IoT device public key (P_{IoT}) of the IoT device and a user random number (R_u), first encrypted information comprises: encrypting the user random number (R_u) by using the IoT device public key (P_{IoT}) to generate the first encrypted information ($P_{IoT}(R_u)$); and

wherein obtaining based on the user private key (K_u), the user random number (R_u), and the hash value, second encrypted information comprises: encrypting the hash value by using the user private key (K_u) to generate a user signature ($K_u(H)$) of the user device, wherein H represents the hash value; and encrypting the user signature by using the random number to generate the second encrypted information ($R_u(K_u(H))$).

14. A method for implementing trust Internet of Things (IoT) services based on a block chain, the method being performed by a user device configured with a pair of user public key (P_u) and user private key (K_u), the method comprising:

performing a hash operation on user data of the user device to generate a hash value of the user data;

obtaining, based on an IoT device public key (P_{IoT}) of an IoT device and a user random number (R_u), first encrypted information;

obtaining, based on the user private key (K_u), the user random number (R_u), and the hash value, second encrypted information; and

sending an authentication request to the IoT device, the authentication request including the hash value of the user data, the first encrypted information, and the second encrypted information.

15. The method of claim 14, wherein obtaining, based on the IoT device public key (P_{IoT}) of the IoT device and a user random number (R_u), first encrypted

information comprises: encrypting the user random number (R_u) by using the IoT device public key (P_{IoT}) to generate the first encrypted information ($P_{IoT}(R_u)$); and

wherein obtaining, based on the user private key (K_u), the user random number (R_u) and the hash value, second encrypted information comprises: encrypting the hash value by using the user private key (K_u) to generate a user signature ($K_u(H)$) of the user device, wherein H represents the hash value; and encrypting the user signature by using the random number to generate the second encrypted information ($R_u(K_u(H))$).

16. A nonvolatile computer readable storage medium for implementing trust Internet of Things (IoT) services based on a block chain comprising machine executable instructions that, when executed by a machine, are adapted to cause the machine to implement the method as any of claims 14-15.

17. An application server for implementing trust Internet of Things (IoT) services based on a block chain, comprising:

a memory and a processor, the memory being stored with machine executable instructions that, when executed by the processor, cause the application server to perform operations including:

determining a uniform device identifier specification for a plurality of IoT devices, wherein the plurality of IoT devices are provided by at least one provider;

determining a unique identifier for each IoT device of the plurality of IoT devices, the unique identifier conforming to the uniform device identifier specification and the unique identifier being a public key in a pair of public key and private key of the IoT device; and

registering the unique identifier of the IoT device with a block chain platform.

18. The application server of claim 17, wherein determining a unique identifier for each IoT device of the plurality of IoT devices comprises:

sending the uniform device identifier specification to the plurality of IoT devices; and

receiving, from each IoT device of the plurality of IoT devices, the unique identifier generated by the IoT device that conforms to the uniform device identifier specification, wherein the private key of the IoT device is generated by the IoT device and is merely stored in the IoT device in an unreadable manner.

19. The application server of claim 17, wherein determining a unique identifier for each IoT device of the plurality of IoT devices comprises:

sending the uniform device identifier specification to the at least one provider; and

receiving, from the at least one provider, the unique identifier generated by the provider for a corresponding IoT device of the plurality of IoT devices that conforms to the uniform device identifier specification, wherein the private key of the IoT device is generated by the provider and is merely stored in the IoT device in an unreadable manner.

20. The application server of claim 17, wherein determining a unique identifier for each IoT device of the plurality of IoT devices comprises:

generating the public key and the private key for each IoT device of the plurality of IoT devices, wherein the public key conforms to the uniform device identifier specification;

sending the public key and the private key to the IoT device to store the private key in the IoT device in an unreadable manner and taking the public key as the unique identifier of the IoT device; and

destroying the generated private key of the IoT device.

21. The application server of claim 17, wherein the operations further include:

receiving, from each IoT device of the plurality of IoT devices, index information of the IoT device; and

registering the index information of the IoT device with the block chain platform.

22. The application server of claim 21, wherein the index information includes a location of the IoT device.

23. The application server of claim 17, wherein the operations further include:

determining a uniform device data specification for the plurality of IoT devices;

receiving raw data from each IoT device of the plurality of IoT devices, the raw data being in a format specific to a provider of the IoT device;

converting the raw data into device data that conforms to the uniform device data specification; and

storing the device data on the block chain platform.

24. The application server of claim 23, wherein the raw data includes raw history data and the device data includes device history data, and wherein the operations further include:

in response to a request from a user device for the device history data of the IoT device, obtaining, from the block chain platform, the device history data; and

sending the device history data to the user device.

25. The application server of claim 23, wherein the raw data includes raw real-time data and the device data includes device real-time data, and wherein the operations further include:

receiving a request from a user device for the real-time data of the IoT device before receiving the raw data from the IoT device;

requesting the IoT device for the raw real-time data of the IoT device; and

sending the device real-time data to the user device after converting the raw real-time data into the device real-time data that conforms to the uniform device data specification.

26. A method for implementing trust Internet of Things (IoT) services based on a block chain, comprising:

determining a uniform device identifier specification for a plurality of IoT devices, wherein the plurality of IoT devices are provided by at least one provider;

determining a unique identifier for each IoT device of the plurality of IoT devices, the unique identifier conforming to the uniform device identifier

specification and the unique identifier being a public key in a pair of public key and private key of the IoT device; and

registering the unique identifier of the IoT device with a block chain platform.

27. The method of claim 26, wherein determining a unique identifier for each IoT device of the plurality of IoT devices comprises:

sending the uniform device identifier specification to the plurality of IoT devices; and

receiving, from each IoT device of the plurality of IoT devices, the unique identifier generated by the IoT device that conforms to the uniform device identifier specification, wherein the private key of the IoT device is generated by the IoT device and is merely stored in the IoT device in an unreadable manner.

28. The method of claim 26, wherein determining a unique identifier for each IoT device of the plurality of IoT devices comprises:

sending the uniform device identifier specification to the at least one provider; and

receiving, from the at least one provider, the unique identifier generated by the provider for a corresponding IoT device of the plurality of IoT devices that conforms to the uniform device identifier specification, wherein the private key of the IoT device is generated by the provider and is merely stored in the IoT device in an unreadable manner.

29. The method of claim 26, wherein determining a unique identifier for each IoT device of the plurality of IoT devices comprises:

generating the public key and the private key for each IoT device of the plurality of IoT devices, wherein the public key conforms to the uniform device identifier specification;

sending the public key and the private key to the IoT device to store the private key in the IoT device in an unreadable manner and use the public key as the unique identifier of the IoT device; and

destroying the generated private key of the IoT device.

30. The method of claim 26, further comprising:

receiving, from each IoT device of the plurality of IoT devices, index information of the IoT device; and

registering the index information of the IoT device with the block chain platform.

31. The method of claim 30, wherein the index information includes a location of the IoT device.

32. The method of claim 26, further comprising:

determining a uniform device data specification for the plurality of IoT devices;

receiving raw data from each IoT device of the plurality of IoT devices, the raw data being in a format specific to a provider of the IoT device;

converting the raw data into device data that conforms to the uniform device data specification; and

storing the device data on the block chain platform.

33. The method of claim 32, wherein the raw data includes raw history data and the device data includes device history data, and wherein the method further comprises:

in response to a request from a user device for the device history data of the IoT device, obtaining, from the block chain platform, the device history data; and

sending the device history data to the user device.

34. The method of claim 32, wherein the raw data includes raw real-time data and the device data includes device real-time data, and wherein the method further comprises:

receiving a request from a user device for the real-time data of the IoT device before receiving the raw data from the IoT device;

requesting the IoT device for the raw real-time data of the IoT device; and

sending the device real-time data to the user device after converting the raw real-time data into the device real-time data that conforms to the uniform device

data specification.

35. A nonvolatile computer readable storage medium for implementing trust Internet of Things (IoT) services based on a block chain, comprising machine executable instructions that, when executed by a machine, are adapted to cause the machine to implement the method as any of claims 26-34.