CLAIMS

What is claimed is:

1. A trusted hardware-based data management method, comprising:

obtaining, by trusted hardware, data description information to be published, wherein the data description information is used to describe target data of a data owner that can be provided by a trusted institution, and the trusted hardware has a binding relationship with a decentralized identifier of the data owner, wherein the trusted hardware stores a private key of the data owner, and wherein a public key corresponding to the private key is stored in a decentralized identifier document of the data owner;

requesting the trusted institution to verify whether the trusted institution stores user service data needed for generating the target data;

receiving a verification result fed back by the trusted institution, wherein the trusted institution determines an identity of the data owner based on the decentralized identifier of the data owner and performs signature verification on the data description information signed by using the public key corresponding to the private key stored in the decentralized identifier document of the data owner; and

publishing the data description information if the verification result indicates that the trusted institution stores the user service data needed for generating the target data,

wherein the obtaining, comprises:

obtaining, by the trusted hardware, the user service data of the data owner from the trusted institution by using an interface predefined in code in a trusted execution environment;

processing the user service data by using a target trusted application comprised in the trusted hardware, to obtain the target data; and

generating the data description information to be published for the target data;

wherein the target trusted application is comprised in the trusted execution environment of the trusted hardware, and the trusted execution environment is isolated from an operating system of the trusted hardware.

2. The method according to claim 1, before the obtaining data description information to be published, further comprising:

obtaining identity identifier information of the data owner;

obtaining hardware identifier information of the trusted hardware;

generating a decentralized identifier binding request based on the identity identifier information and the hardware identifier information, wherein the decentralized identifier binding request is used to request to establish a mapping relationship between the decentralized identifier of the data owner and the trusted hardware; and

sending the decentralized identifier binding request to a decentralized identity server.

3. The method according to claim 1, wherein the obtaining, by trusted hardware, data description information to be published specifically comprises:

identifying, by the trusted hardware, a selection operation performed by the data owner on a program identifier of a target trusted application displayed in a target application interface, wherein the selection operation is used to indicate to process the user service data of the data owner in the trusted institution by using the target trusted application to obtain the target data, and the target trusted application is deployed in a trusted application environment of a target server; and

generating the data description information to be published for the target data based on the selection operation.

4. The method according to claim 3, after the publishing the data description information, further comprising:

storing information about a mapping relationship between the target trusted application and the target data in the decentralized identifier document of the data owner.

5. The method according to claim 3, after the publishing the data description information, further comprising:

obtaining an acquisition request generated by a data user for the target data based on the data description information;

sending a request for generating the target data to the target server carrying the target trusted application in response to the acquisition request; and

receiving a processing result fed back by the target server.

6. The method according to claim 5, wherein before the sending a request for generating the target data to the target server carrying the target trusted application, the method further comprises:

obtaining a usage authorization instruction of a usage authorization approver of the target data for the acquisition request;

generating usage authorization information based on the usage authorization instruction; and

digitally signing the usage authorization information by using the private key, to obtain digitally signed usage authorization information; and

the sending a request for generating the target data to the target server carrying the target trusted application specifically comprises:

sending the digitally signed usage authorization information to the target server carrying the target trusted application.

7. The method according to claim 1,

wherein after the publishing the data description information, the method further comprises:

obtaining an acquisition request generated by a data user for the target data based on the data description information;

digitally signing the target data stored in the trusted hardware by using the private key in response to the acquisition request, to obtain digitally signed data; and

sending the digitally signed data to the data user.

8. The method according to claim 7, before the sending the digitally signed data to the data user, further comprising:

obtaining a usage authorization instruction of a usage authorization approver of the target data for the acquisition request.

9. The method according to claim 6 or 8, before the publishing the data description information, further comprising:

obtaining usage authorization approval process information specified by the data owner for the target data; and

establishing a mapping relationship between the usage authorization approval process information and the data description information.

10. The method according to claim 5 or 7, wherein the publishing the data description information specifically comprises:

publishing the data description information to a data transmission application; and

the obtaining an acquisition request generated by a data user for the target data based on the data description information specifically comprises:

obtaining the acquisition request of the data user for the target data, wherein the acquisition request is generated based on the data description information obtained from the data transmission application.

11. A data acquisition method, comprising:

obtaining data description information published by a data owner, wherein the data description information is used to describe target data of the data owner that can be provided by a trusted institution;

generating an acquisition request for the target data based on the data description information;

sending the acquisition request to trusted hardware of the data owner, wherein the trusted hardware has a binding relationship with a decentralized identifier of the data owner, wherein the trusted hardware stores a private key of the data owner, and wherein a public key corresponding to the private key is stored in a decentralized identifier document of the data owner;

receiving the target data digitally signed by using the private key and fed back by the trusted hardware, wherein the target data is obtained by processing user service data of the data owner that is stored in the trusted institution by using a target trusted application comprised in the trusted hardware;

obtaining the public key from the decentralized identifier document of the data owner; and

performing signature verification on the digitally signed target data by using the public key, wherein the target trusted application is comprised in a trusted execution environment of the trusted hardware, and the trusted execution environment is isolated from an operating system of the trusted hardware.

12. A device, comprising:

at least one processor; and

a memory communicably coupled to the at least one processor, wherein the device is configured to perform a method according to any one of the preceding claims.