CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:

generating, a description of target data, wherein the target data is stored in a trusted device of a data owner;

publishing, as a published description, the description of the target data without publishing the target data stored in the trusted device of the data owner;

in response to the published description, receiving a data acquisition request from a data requestor for the target data wherein the data acquisition request is configured to retrieve the target data based on a first resource;

sending the data acquisition request to the data owner;

receiving first confirmation information from the data owner;

identifying the target data from the trusted device based on the first confirmation information; and

sending the target data to the data requestor, wherein the trusted device is a pluggable device and is bound to a hardware device it first connects to, and wherein the trusted device comprises a trusted execution environment (TEE) isolated from an operating system, and the pluggable device is configured to allow data to be added and removed, but unallowable to be modified.

2. The computer-implemented method according to claim 1, wherein that the target data is obtained by the trusted device from a terminal device of the data owner through an interface provided by the TEE.

3. The computer-implemented method according to claim 1, comprising:

receiving second confirmation information from the data requestor after sending the data acquisition request, wherein the second confirmation information indicates that the data requestor has received the target data; and

deleting the target data from the trusted device.

4. The computer-implemented method according to claim 1, comprising:

obtaining third confirmation information from the data requestor, wherein the third confirmation information indicates that the data requestor has received the target data;

storing a mapping relationship between the target data and the data requestor in a blockchain of a blockchain network; and

updating, based on the mapping relationship, a usage record of the target data, wherein the usage record comprises a number of users who retrieves the target data.

5. The computer-implemented method according to claim 4, comprising:

sending the mapping relationship between the target data and the data requestor to the trusted device for storage; and

sending the usage record of the target data to the trusted device to be stored by the trusted device.

6. The computer-implemented method according to claim 1, further comprising:

determining that fourth confirmation information from the data requestor is received, wherein the fourth confirmation information indicates that the data requestor has received the target data; and

in response to determining that the fourth confirmation information is received, sending the first resource to the data owner.

7. The computer-implemented method according to claim 1, comprising:

sending a private key of the data owner to the data requestor; and

encrypting the target data by using a public key of the data owner corresponding to the private key before sending the target data to the data requestor.

8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

generating, a description of target data, wherein the target data is stored in a trusted device of a data owner;

publishing, as a published description, the description of the target data without publishing the target data stored in the trusted device of the data owner;

in response to the published description, receiving a data acquisition request from a data requestor for the target data wherein the data acquisition request is configured to retrieve the target data based on a first resource;

sending the data acquisition request to the data owner;

receiving first confirmation information from the data owner;

identifying the target data from the trusted device based on the first confirmation information; and

sending the target data to the data requestor, wherein the trusted device is a pluggable device and is bound to a hardware device it first connects to, and wherein the trusted device comprises a trusted execution environment (TEE) isolated from an operating system, and the pluggable device is configured to allow data to be added and removed, but unallowable to be modified.

9. The non-transitory, computer-readable medium according to claim 8, wherein that the target data is obtained by the trusted device from a terminal device of the data owner through an interface provided by the TEE.

10. The non-transitory, computer-readable medium according to claim 8, comprising:

receiving second confirmation information from the data requestor after sending the data acquisition request, wherein the second confirmation information indicates that the data requestor has received the target data; and

deleting the target data from the trusted device.

11. The non-transitory, computer-readable medium according to claim 8, comprising:

obtaining third confirmation information from the data requestor, wherein the third confirmation information indicates that the data requestor has received the target data;

storing a mapping relationship between the target data and the data requestor in a blockchain of a blockchain network; and

updating a usage record of the target data, wherein the usage record comprises a number of users who retrieves the target data.

12. The non-transitory, computer-readable medium according to claim 11, comprising:

sending the mapping relationship between the target data and the data requestor to the trusted device for storage; and

sending the usage record of the target data to the trusted device to be stored by the trusted device.

13. The non-transitory, computer-readable medium according to claim 8, further comprising:

determining that fourth confirmation information from the data requestor is received, wherein the fourth confirmation information indicates that the data requestor has received the target data; and

in response to determining that the fourth confirmation information is received, sending the first resource to the data owner.

14. The non-transitory, computer-readable medium according to claim 8, comprising:

sending a private key of the data owner to the data requestor; and

encrypting the target data by using a public key of the data owner corresponding to the private key before sending the target data to the data requestor.

15. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

generating, a description of target data, wherein the target data is stored in a trusted device of a data owner;

publishing, as a published description, the description of the target data without publishing the target data stored in the trusted device of the data owner;

in response to the published description, receiving a data acquisition request from a data requestor for the target data wherein the data acquisition request is configured to retrieve the target data based on a first resource;

sending the data acquisition request to the data owner;

receiving first confirmation information from the data owner;

identifying the target data from the trusted device based on the first confirmation information; and

sending the target data to the data requestor, wherein the trusted device is a pluggable device and is bound to a hardware device it first connects to, and wherein the trusted device comprises a trusted execution environment (TEE) isolated from an operating system, and the pluggable device is configured to allow data to be added and removed, but unallowable to be modified.

16. The computer-implemented system according to claim 15, wherein that the target data is obtained by the trusted device from a terminal device of the data owner through an interface provided by the TEE.

17. The computer-implemented system according to claim 15, comprising:

receiving second confirmation information from the data requestor after sending the data acquisition request, wherein the second confirmation information indicates that the data requestor has received the target data; and

deleting the target data from the trusted device.