CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:

identifying a data use request of a data requestor, wherein the data use request comprises a data type of target data;

identifying authorization information of a data owner;

generating a data authorization use claim based on the authorization information, wherein the data authorization use claim indicates that the data owner authorizes the data requestor to use data;

sending the data authorization use claim to a trusted application (TAPP) in a proxy service provider device, wherein the TAPP corresponds to the data type of the target data;

obtaining initial data collected by the TAPP from a data acquisition address in the data authorization use claim, wherein the TAPP is executed in a trusted execution environment (TEE) and is configured to collect the initial data;

verifying the initial data to obtain the target data that is successfully verified, wherein the target data comprises a data validity claim indicating a validity of the target data; and

sending the target data to the data requestor.

2. The computer-implemented method according to claim 1, wherein the initial data is encrypted data encrypted by using a public key corresponding to the TAPP.

3. The computer-implemented method according to claim 2, further comprising:

decrypting the target data by using a private key corresponding to the TAPP after sending the target data to the data requestor.

4. The computer-implemented method according to claim 1, wherein the data authorization use claim at least comprises: an approval record of the initial data and a data acquisition address of the initial data;

the data validity claim at least comprises: a storage address of the initial data, a data type of the initial data, a validity period of the initial data, and a data collection method of the initial data; and

the authorization information at least comprises a specified use range of the initial data.

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

before identifying the data use request, obtaining a data directory issued by the data owner in a blockchain network, wherein the data directory comprises data authorized to be disclosed by the data owner.

6. The computer-implemented method according to claim 1, wherein identifying authorization information of the data owner comprises:

sending an authorization request notification to the data owner based on the data use request, wherein the authorization request notification comprises a uniform resource locator (URL) address;

determining an operation behavior of the data owner in a web page corresponding to the URL address; and

obtaining the authorization information of the data owner in response to determining that the operation behavior indicates that the data owner agrees to the data use request of the data requestor.

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

obtaining a first verification result of the TAPP for the data authorization use claim, wherein the first verification result indicates that the data authorization use claim is valid, wherein the data authorization use claim indicates that an approval record of the data use request is valid, and

wherein obtaining the initial data collected by the TAPP from the data acquisition address in the data authorization use claim comprises:

sending a data acquisition request to the data owner; and

receiving the initial data from the data owner.

8. The computer-implemented method according to claim 7, wherein the data acquisition request comprises an identifier of the TAPP, the computer-implemented method further comprises:

receiving a second verification result of the data owner for the identifier of the TAPP, wherein the second verification result indicates that the identifier of the TAPP is consistent with an identifier specified by the data requestor for the TAPP, and wherein

the initial data from the data owner is received in response to the second verification result.

9. The computer-implemented method according to claim 1, wherein the initial data is encrypted by using a public key of the data owner when the data requestor does not specify a TAPP, the computer-implemented method further comprises:

decrypting the initial data by using a private key of the data owner, wherein the private key is included in the data authorization use claim.

10. A trusted data transmission apparatus, comprising:

a data use request acquisition module, configured to identify a data use request of a data requestor, wherein the data use request comprises a data type of target data;

an authorization information acquisition module, configured to identify authorization information of a data owner;

a data authorization use claim generation module, configured to generate a data authorization use claim based on the authorization information, wherein the data authorization use claim indicates that the data owner authorizes the data requestor to use data;

an initial data acquisition module, configured to send the data authorization use claim to a trusted application (TAPP) in a proxy service provider device, wherein the TAPP corresponds to the data type of the target data, and obtain initial data collected by the TAPP from a data acquisition address in the data authorization use claim, wherein the TAPP is executed in a trusted execution environment (TEE) and is configured to collect the initial data;

a target data acquisition module, configured to verify the initial data to obtain target data that is successfully verified, wherein the target data comprises a data validity claim and an initial data, and the data validity claim is used for indicating a validity of the target data; and

a target data transmission module, configured to send the target data to the data requestor.

11. The apparatus according to claim 10,

wherein the initial data is encrypted data encrypted by using a public key corresponding to the TAPP.

12. The apparatus according to claim 11, further comprising:

a first decryption module, configured to decrypt the target data by using a private key corresponding to the TAPP after the target data is sent to the data requestor.

13. The apparatus according to claim 10, further comprising:

a data directory acquisition module, configured to, before identifying the data use request, obtain a data directory issued by the data owner in a blockchain network, wherein the data directory comprises data authorized to be disclosed by the data owner.

14. The apparatus according to claim 10, wherein the authorization information acquisition module specifically comprises:

an authorization request notification sending unit, configured to send an authorization request notification to the data owner based on the data use request, wherein the authorization request notification comprises a URL address;

an operation behavior acquisition unit, configured to determine an operation behavior of the data owner in a web page corresponding to the URL address; and

an authorization information acquisition unit, configured to obtain the authorization information of the data owner in response to determining that the operation behavior indicates that the data owner agrees to the data use request of the data requestor.

15. The apparatus according to claim 10, further comprising:

a first verification module, configured to obtain a first verification result of the TAPP for the data authorization use claim, wherein the first verification result indicates that the data authorization use claim is valid, wherein the data authorization use claim indicates that an approval record of the data use request is valid;

wherein the initial data acquisition module is configured to:

send a data acquisition request to the data owner when the first verification result indicates that the data authorization use claim is valid; and

receive, from the data owner, the initial data.

16. The apparatus according to claim 15, wherein the data acquisition request comprises an identifier of the TAPP, the apparatus further comprising:

a second verification module, configured to receive a second verification result of the data owner for the identifier of the TAPP, wherein the second verification result indicates that the identifier of the TAPP is consistent with an identifier specified by the data requestor for the TAPP, and

wherein the initial data acquisition module is configured to receive the initial data

from the data owner in response to the second verification result.

17. The apparatus according to claim 10, wherein the initial data is encrypted by using a public key of the data owner when the data requestor does not specify a TAPP.

18. The apparatus according to claim 17, further comprising:

a third decryption module, configured to decrypt the initial data in the target data by using a private key of the data owner, wherein the private key is included in the data authorization use claim.

19. The apparatus according to claim 10, wherein the data authorization use claim at least comprises: an approval record of the initial data and a data acquisition address of the initial data;

the data validity claim at least comprises: a storage address of the initial data, a data type of the initial data, a validity period of the initial data, and a data collection method of the initial data; and

the authorization information at least comprises a specified use range of the initial data.

20. A trusted data transmission device, comprising:

at least one processor; and

a memory communicatively connected to the at least one processor, wherein

the memory stores instructions that can be executed by the at least one processor, and the instructions are executed by the at least one processor, such that the at least one processor can:

identify a data use request of a data requestor, wherein the data use request comprises a data type of target data;

identify authorization information of a data owner;

generate a data authorization use claim based on the authorization information, wherein the data authorization use claim indicates that the data owner authorizes the data requestor to use data;

send the data authorization use claim to a trusted application (TAPP) in a proxy service provider device, wherein the TAPP corresponds to the data type of the target data;

obtain initial data collected by the TAPP from a data acquisition address in the data authorization use claim, wherein the TAPP is executed in a trusted execution

environment (TEE) and is configured to collect the initial data;

verify the initial data to obtain the target data that is successfully verified, wherein the target data comprises a data validity claim indicating a validity of the target data; and

send the target data to the data requestor.

21. A non-transitory, computer-readable storage medium that stores computer readable instructions; wherein the computer readable instructions can be executed by a processor to implement the trusted data transmission method according to any one of claims 1 to 9.