

CLAIMS

What is claimed is:

1. A data processing method, comprising:

obtaining user service data sent by a trusted institution in response to a data request of a data owner;

detecting whether an end-user device of the data owner is provided with trusted hardware to obtain a detection result;

storing the user service data in trusted hardware having a use permission on a target server when the detection result indicates that the end-user device of the data owner is not provided with the trusted hardware;

storing the user service data in at least one of the trusted hardware on the end-user device and the trusted hardware having the use permission on the target server when the detection result indicates that the end-user device of the data owner is provided with the trusted hardware;

obtaining (202) data use authorization information sent by a data requester;

verifying (204) the data use authorization information;

sending (206) data authorized to be accessed by the data use authorization information to the data requester if the verification is successful, the data being stored in the trusted hardware, and the data being data obtained from athe trusted institution; and

storing (208) a data sending record for the data in a blockchain network.

2. The method according to claim 1, wherein before the obtaining data use authorization information sent by a data requester, the method further comprises:

obtaining a use authorization instruction of a data owner for target data, the use authorization instruction being used to indicate that a specified data requester is allowed to obtain the target data stored in the trusted hardware; and

generating target data use authorization information in response to the use authorization instruction; and

the verifying the data use authorization information specifically comprises:

comparing the data use authorization information with the target data use authorization information, the verification being successful if the data use authorization information and the target data use authorization information are consistent.

3. The method according to claim 2, wherein the generating target data use authorization information in response to the use authorization instruction specifically comprises:

generating, in response to the use authorization instruction, the target data use authorization information by using the trusted hardware; and

the comparing the data use authorization information with the target data use authorization information specifically comprises:

comparing the data use authorization information with the target data use authorization information by using the trusted hardware.

~~4. The method according to claim 1, wherein before the obtaining data use authorization information sent by a data requester, the method further comprises:~~

~~obtaining user service data sent by the trusted institution in response to a data request of a data owner; and~~

~~storing the user service data in the trusted hardware.~~

~~45.~~ The method according to claim ~~14~~, wherein after the storing the user service data in the trusted hardware, the method further comprises:

obtaining registered account information of the data owner at a target mailbox application; and

sending the user service data to a registered account indicated by the registered account information.

~~6. The method according to claim 4, wherein before the storing the user service data in the trusted hardware, the method further comprises:~~

~~detecting whether an end-user device of the data owner is provided with trusted hardware to obtain a detection result; and~~

~~the storing the user service data in the trusted hardware specifically comprises:~~

~~storing the user service data in trusted hardware having a use permission on a target server when the detection result indicates that the end-user device of the data owner is not provided with trusted hardware; and~~

~~storing the user service data in at least one of the trusted hardware on the end-user device and the trusted hardware having the use permission on the target server when the detection result indicates that the end-user device of the data owner is provided with trusted hardware.~~

~~57.~~ The method according to claim ~~41~~, wherein after the storing the user service data in the trusted hardware, the method further comprises:

deleting the user service data in the trusted hardware in response to a deletion instruction of the data owner for the user service data.

~~86~~. The method according to claim ~~41~~, wherein a TEE is deployed in the trusted hardware, and the TEE is isolated from an operating system of the trusted hardware; and
the storing the user service data in the trusted hardware specifically comprises:
storing the user service data in the TEE in the trusted hardware.

~~97~~. The method according to claim 1, wherein the sending data authorized to be accessed by the data use authorization information to the data requester specifically comprises:
sending data authorized to be accessed by the data use authorization information to the data requester through a blockchain network.

~~108~~. The method according to claim 1, wherein the sending data authorized to be accessed by the data use authorization information to the data requester specifically comprises:
sending data authorized to be accessed by the data use authorization information and a data signature of the trusted institution for the data to the data requester.

~~119~~. The method according to claim 1, wherein after the storing a data sending record for the data in a blockchain network, the method further comprises:
obtaining a data sending record related to the data owner of the data from the blockchain network, the data sending record related to the data owner of the data comprising a data sending record of the data held by the data owner; and
performing statistics on the data sending record related to the data owner of the data to obtain a statistical result.

~~12. A data processing apparatus, comprising:
a first acquisition module, configured to obtain data use authorization information sent by a data requester;
a verification module, configured to verify the data use authorization information;
a first sending module, configured to send data authorized to be accessed by the data use authorization information to the data requester if the verification is successful, the data being stored in trusted hardware, and the data being data obtained from a trusted institution; and~~

~~a second sending module, configured to store a data sending record for the data in a blockchain network.~~

~~13. The apparatus according to claim 12, further comprising:~~

~~a second acquisition module, configured to obtain a use authorization instruction of a data owner for target data, the use authorization instruction being used to indicate that a specified data requester is allowed to obtain the target data stored in the trusted hardware; and~~

~~a use authorization information generation module, configured to generate target data use authorization information in response to the use authorization instruction; and~~

~~the verification module is specifically configured to compare the data use authorization information with the target data use authorization information, the verification being successful if the data use authorization information and the target data use authorization information are consistent.~~

~~14. The apparatus according to claim 13, wherein the use authorization information generation module is specifically configured to:~~

~~generate, in response to the use authorization instruction, the target data use authorization information by using the trusted hardware; and~~

~~the verification module is specifically configured to:~~

~~compare the data use authorization information with the target data use authorization information by using the trusted hardware.~~

~~15. The apparatus according to claim 12, further comprising:~~

~~a third acquisition module, configured to obtain user service data sent by the trusted institution in response to a data request of a data owner; and~~

~~a storage module, configured to store the user service data in the trusted hardware.~~

~~16. The apparatus according to claim 15, further comprising:~~

~~a fourth acquisition module, configured to obtain registered account information of the data owner at a target mailbox application; and~~

~~a third sending module, configured to send the user service data to a registered account indicated by the registered account information.~~

~~17. The apparatus according to claim 15, further comprising:~~

~~a detection module, configured to detect whether an end user device of the data owner is provided with trusted hardware to obtain a detection result; and~~

~~the storage module is specifically configured to:~~

~~storing the user service data in trusted hardware having a use permission on a target server when the detection result indicates that the end-user device of the data owner is not provided with trusted hardware; and~~

~~store the user service data in at least one of the trusted hardware on the end-user device and the trusted hardware having the use permission on the target server when the detection result indicates that the end-user device of the data owner is provided with trusted hardware.~~

~~18. The apparatus according to claim 15, further comprising:~~

~~a deletion module, configured to delete the user service data in the trusted hardware in response to a deletion instruction of the data owner for the user service data.~~

~~19. The apparatus according to claim 15, wherein a TEE is deployed in the trusted hardware, and the TEE is isolated from an operating system of the trusted hardware; and~~

~~the storage module is specifically configured to store the user service data in the TEE in the trusted hardware.~~

~~20. The apparatus according to claim 12, wherein the first sending module is specifically configured to:~~

~~send data authorized to be accessed by the data use authorization information to the data requester through a blockchain network.~~

~~21. The apparatus according to claim 12, further comprising:~~

~~a fifth acquisition module, configured to obtain a data sending record related to the data owner of the data from the blockchain network, the data sending record related to the data owner of the data comprising a data sending record of the data held by the data owner; and~~

~~a statistics module, configured to perform statistics on the data sending record related to the data owner of the data to obtain a statistical result.~~

~~22~~10. A data processing device, comprising:

at least one processor; and

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

~~the memory stores instructions executable 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:~~

~~obtain data use authorization information sent by a data requester;~~

~~verify the data use authorization information;~~

~~send data authorized to be accessed by the data use authorization information to the data requester if the verification is successful, the data being stored in trusted hardware, and the data being data obtained from a trusted institution; and~~

~~store a data sending record for the data in a blockchain network.~~ the device is configured

to perform a method according to any one of the preceding claims.