

CLAIMS

What is claimed is:

1. An information sharing method, comprising:
receiving (310), by a sales agency, user basic data of a user, and sending a user
5 ID of the user to a financial institution;
sending (320), by the financial institution, a data sharing request to the sales
agency by using a privacy computing unit, wherein the data sharing request comprises
the user ID corresponding to user basic data that is expected to be shared;
obtaining (330), by the privacy computing unit from the sales agency, encrypted
10 user basic data corresponding to the user ID, and decrypting the encrypted user basic
data, so as to perform matching on the decrypted user basic data to obtain a matching
result; and 76778SG
sending (340), by the privacy computing unit, the matching result to the
financial institution,
15 wherein a first smart contract is deployed in the privacy computing unit, and the
first smart contract is used to receive an invoking request sent by the financial
institution, and in response to the invoking request, send the data sharing request to the
sales agency, and
wherein the obtaining, by the privacy computing unit from the sales agency, the
20 encrypted user basic data corresponding to the user ID, and decrypting the encrypted
user basic data comprises:
receiving, by the privacy computing unit, a transaction that is initiated by the
sales agency and that invokes a second smart contract deployed at the privacy
computing unit, wherein parameters in the transaction comprise the user ID and the
25 encrypted user basic data corresponding to the user ID; and
decrypting, by the privacy computing unit, the encrypted user basic data.
2. The method according to claim 1, wherein the user ID comprises:
an account registered by the user at the sales agency; or
30 an account allocated by a system of the sales agency to the user when the user
initiates a purchase operation at the sales agency.
3. The method according to claim 2, wherein the user ID comprises:

a digest value obtained through hash calculation on one or more pieces of information of the user.

4. The method according to claim 3, wherein the user ID comprises:

5 a digest value obtained through salting hash calculation on one or more pieces of information of the user.

5. The method according to claim 1, wherein the user ID in the data sharing request is encrypted; and/or

10 wherein the data sharing request comprises a signature of the financial institution;

and/or

before the sending, by the financial institution, a data sharing request to the sales agency, further comprising:

15 verifying, by the financial institution, an identity of the sales agency.

6. The method according to claim 1, wherein the sending, by the financial institution, the data sharing request to the sales agency by using the privacy computing unit comprises:

20 sending, by the financial institution, the data sharing request to the sales agency by using the privacy computing unit on a blockchain.

7. The method according to claim 1, wherein the sending, by the financial institution, the data sharing request to the sales agency by using the privacy computing unit comprises:

25 sending, by the financial institution, the data sharing request to the sales agency by using a privacy computing unit off a blockchain.

8. The method according to claim 6, wherein the sending, by the financial institution, the data sharing request to the sales agency by using the privacy computing unit comprises:

30

sending, by the financial institution, the data sharing request to the privacy computing unit by initiating a transaction for invoking the first smart contract, and then sending, by the privacy computing unit, the data sharing request to the sales agency.

5 9. The method according to claim 6,
 wherein the data sharing request is signed by the privacy computing unit, and the sales agency verifies the signature by using a public key of the privacy computing unit; or

 the data sharing request is signed by the first smart contract, and the sales agency
10 verifies the signature by using a public key of the first smart contract.

10. The method according to claim 1,

 wherein the performing, by the privacy computing unit, matching on the decrypted user basic data comprises:

15 executing, by the privacy computing unit, the second smart contract to perform matching on the decrypted user basic data.

11. The method according to claim 1 or 10, before the obtaining, by the privacy computing unit from the sales agency, the encrypted user basic data corresponding to the user ID, further comprising:

20 proving, by the privacy computing unit, an identity of the privacy computing unit to the sales agency.

12. The method according to claim 1, wherein the method further comprises:

25 sending, by the privacy computing unit, a proof of the matching result to a blockchain,

 wherein the proof of the matching result comprises a verifiable claim signed by the privacy computing unit,

 wherein the sending, by the privacy computing unit, the matching result to the
30 financial institution comprises:

 sending, by the privacy computing unit, the verifiable claim signed by the privacy computing unit to the financial institution; and

after the sending, by the privacy computing unit, a proof of the matching result to the financial institution, the method further comprises:

verifying, by a regulatory organization, a signature of the verifiable claim at the financial institution by using a public key of the privacy computing unit.

5

13. An information sharing system, comprising: a sales agency; a financial institution; and a privacy computing unit, wherein the information sharing system is configured to perform a method according to any one of claims 1 to 12.

10 14. An information sharing method performed by a privacy computing unit, the method comprising:

obtaining, by the privacy computing unit from a sales agency, encrypted user basic data corresponding to a user ID, and decrypting the encrypted user basic data, so as to perform matching on the decrypted user basic data to obtain a matching result;

15 and

sending, by the privacy computing unit, the matching result to a financial institution,

wherein a first smart contract is deployed in the privacy computing unit, and the first smart contract is used to receive an invoking request sent by the financial institution, and in response to the invoking request, send the data sharing request to the sales agency, and

20

wherein the obtaining, by the privacy computing unit from the sales agency, the encrypted user basic data corresponding to the user ID, and decrypting the encrypted user basic data comprises:

25

receiving, by the privacy computing unit, a transaction that is initiated by the sales agency and that invokes a second smart contract deployed at the privacy computing unit, wherein parameters in the transaction comprise the user ID and the encrypted user basic data corresponding to the user ID; and

decrypting, by the privacy computing unit, the encrypted user basic data.

30

15. A privacy computing unit configured to perform the method of claim 14.