

## 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, ~~the~~  
10 encrypted 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

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.~~  
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.~~  
information of the user.

5

4.- \_\_\_\_ The method according to claim 3, wherein the user ID comprises:  
a digest value obtained through salting hash calculation on one or more pieces  
of information of the user.

10 5. ~~The method according to claim 1, wherein the sending a user ID of the user to  
a financial institution comprises:~~

~~encrypting and sending, by the sales agency, the user ID to the financial  
institution.~~

15 ~~6. The method according to claim 1, before the sending a user ID of the user to a  
financial institution, further comprising:~~

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

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

20 ~~8. The method according to claim 1, wherein the data sharing request comprises  
a signature of the financial institution-;~~

~~9. The method according to claim 1, and/or~~

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

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

25 ~~10.~~

~~6. The method according to claim 1, wherein the sending, by the financial  
institution, a data sharing request to the sales agency comprises:~~

~~directly sending, by the financial institution, the data sharing request to the sales  
agency; or~~

30 ~~sending, by the financial institution, the data sharing request to the sales agency  
by using a privacy computing unit.~~

~~11. The method according to claim 10~~, wherein the sending, by the financial institution, the data sharing request to the sales agency by using athe privacy computing unit comprises:

5        sending, by the financial institution, the data sharing request to the sales agency by using athe privacy computing unit on a blockchain; ~~or,~~

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:

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

~~12.~~

8. The method according to claim ~~40~~6, wherein the sending, by the financial institution, the data sharing request to the sales agency by using athe privacy computing unit comprises:

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

20        ~~13. The method according to claim 10, 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.~~

9. The method according to claim 6,

25

~~14. The method according to claim 13~~, 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

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

~~15. The method according to claim 1, wherein the obtaining, by a 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:~~

~~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~~

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

~~16~~

10. The method according to claim ~~15~~, 1,

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

10 executing, by the privacy computing unit, the second smart contract to perform

~~matching on the decrypted user basic data~~

matching on the decrypted user basic data.~~17~~

11. The method according to claim 1 or ~~15~~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:

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

~~18.~~

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

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

~~19. The method according to claim 18,~~ wherein the proof of the matching result comprises a verifiable claim signed by the privacy computing unit~~;~~

25 ~~20. The method according to claim 19,~~ wherein the sending, by the privacy computing unit, the matching result to the financial institution comprises:

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

30 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 ~~blockchain~~financial institution by using a public key of the privacy computing unit.

~~21.~~

13. ~~\_\_\_\_\_~~ An information sharing ~~method~~system, comprising:  
receiving, by a ~~first~~sales agency; a ~~financial~~ institution, ~~first data~~; and sending a  
user ID corresponding to the first data to a second institution;  
sending, by the second institution, a data sharing request to the first institution a privacy  
5 computing unit, wherein the information sharing system is configured to perform a  
method according to any one of claims 1 to 12.

~~14. data~~ \_\_\_\_\_ An information sharing request comprises the user ID corresponding to  
the first data that is expected to be shared;  
10 ~~obtaining, method performed~~ by a privacy computing unit ~~from~~, the ~~first~~  
~~institution, method comprising:~~

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

sending, by the privacy computing unit, the processing matching result to ~~the~~  
~~second~~a financial institution.

~~22. The method according to claim 21, wherein the user ID comprises:~~  
an account of a user corresponding to the first data that is registered at the first  
20 ~~institution; or~~

an account allocated to a user corresponding to the first data by a system of the  
first institution when the user initiates a purchase operation at the first institution.

~~23. The method according to claim 22, wherein the user ID comprises:~~  
a digest value obtained through hash calculation on one or more pieces of  
25 ~~information in the first data.~~

~~24. The method according to claim 23, wherein the user ID comprises:~~  
a digest value obtained through salting hash calculation on one or more pieces of  
information in the first data.

~~25. The method according to claim 21, wherein the sending a user ID~~  
30 ~~corresponding to the first data to a second institution comprises:~~  
encrypting and sending, by the first institution, the user ID corresponding to the  
first data to the second institution.

26. The method according to claim 21, before the sending a user ID corresponding to the first data to a second institution, further comprising:  
verifying, by the first institution, an identity of the second institution.
27. The method according to claim 21, wherein the user ID in the data sharing request is encrypted.
28. The method according to claim 21, wherein the data sharing request comprises a signature of the second institution.
29. The method according to claim 21, before the sending, by the second institution, a data sharing request to the first institution, further comprising:  
verifying, by the second institution, an identity of the first institution.
30. The method according to claim 21, wherein the sending, by the second institution, a data sharing request to the first institution comprises:  
directly sending, by the second institution, the data sharing request to the first institution; or  
sending, by the second institution, the data sharing request to the first institution by using a privacy computing unit.
31. The method according to claim 30, wherein the sending, by the second institution, the data sharing request to the first institution by using a privacy computing unit comprises:  
sending, by the second institution, the data sharing request to the first institution by using a privacy computing unit on a blockchain; or  
sending, by the second institution, the data sharing request to the first institution by using a privacy computing unit off a blockchain.
32. The method according to claim 30, wherein the sending, by the second institution, the data sharing request to the first institution by using a privacy computing unit comprises:  
sending, by the second institution, the data sharing request to the privacy computing unit by initiating a transaction for invoking a contract, and then sending, by the privacy computing unit, the data sharing request to the first institution.
33. The method according to claim 30, 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 ~~second~~financial institution, and in response to the invoking request, send the data sharing request to the ~~first institution~~sales agency, and

~~34. The method according to claim 33, wherein the data sharing request is signed<sup>obtaining</sup>, by the privacy computing unit, and the first institution 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 first  
5 institution verifies the signature by using a public key of the first smart contract.~~

~~35. The method according to claim 21, wherein the obtaining, by a privacy computing unit from the first institutions<sup>sales agency</sup>, the encrypted first<sup>user basic</sup> data corresponding to the user ID, and decrypting the encrypted first<sup>user basic</sup> data comprises:~~

~~10 receiving, by the privacy computing unit, a transaction that is initiated by the first institutions<sup>sales agency</sup> 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 first<sup>user basic</sup> data corresponding to the user ID; and~~

~~decrypting, by the privacy computing unit, the encrypted first<sup>data</sup>  
15 corresponding to the user ID<sup>basic data</sup>.~~

~~15. 36. The method according to claim 35, wherein the processing the decrypted first data comprises:~~

~~executing, by the<sup>A</sup> privacy computing unit, the second smart contract to process  
20 the decrypted first data.~~

~~37. The method according to claim 21 or 35, before the obtaining, by a privacy computing unit from the first institution, the encrypted first data corresponding to the user ID, further comprising:~~

~~proving, by the privacy computing unit, an identity of the privacy computing unit  
25 to the first institution.~~

~~38. The method according to claim 21, wherein the method further comprises:  
sending, by the privacy computing unit, a proof of the processing result to a  
blockchain.~~

~~39. The method according to claim 38, wherein the proof of the processing result  
30 comprises a verifiable claim signed by the privacy computing unit.~~

~~40. The method according to claim 39, wherein the sending, by the privacy computing unit, the processing result to the second institution specifically comprises:~~

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

~~after the sending, by the privacy computing unit, a proof of the processing result to the second institution, the method further comprises:~~

5       ~~verifying, by a third institution, a signature of the verifiable claim at the second institution by using a public key of the privacy computing unit.~~

~~41. An information sharing system, comprising:~~

~~a sales agency, configured to: receive basic data of a user, and send a user ID of the user to a financial institution;~~

10       ~~the financial institution, configured to send a data sharing request to the sales agency, wherein the data sharing request comprises the user ID corresponding to user basic data that is expected to be shared;~~

~~a privacy computing unit, configured to: obtain, from the sales agency, the encrypted user basic data corresponding to the user ID, and decrypt the encrypted user basic data,~~

15       ~~so as to perform matching on the decrypted user basic data to obtain a matching result; and further configured to send the matching result to the financial institution~~the method of claim 14.

~~42. The system according to claim 41, wherein the user ID comprises:~~

~~an account registered by the user at the sales agency; or~~

20       ~~an account allocated by a system of the sales agency to the user when the user initiates a purchase operation at the sales agency.~~

~~43. The system according to claim 42, wherein the user ID comprises:~~

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

25       ~~44. The system according to claim 43, wherein the user ID comprises:~~

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

~~45. The system according to claim 41, wherein the sending a user ID of the user to a financial institution comprises:~~

30       ~~encrypting and sending, by the sales agency, the user ID to the financial institution.~~

~~46. The system according to claim 41, before the sending a user ID of the user to a financial institution, further comprising:~~

- ~~verifying, by the sales agency, an identity of the financial institution.~~
- ~~47. The system according to claim 41, wherein the user ID in the data sharing request is encrypted.~~
- ~~48. The system according to claim 41, wherein the data sharing request~~  
5 ~~comprises a signature of the financial institution.~~
- ~~49. The system according to claim 41, before the sending a data sharing request to the sales agency, further comprising:~~
- ~~verifying, by the financial institution, an identity of the sales agency.~~
- ~~50. The system according to claim 41, wherein the sending a data sharing request~~  
10 ~~to the sales agency comprises:~~
- ~~directly sending, by the financial institution, the data sharing request to the sales agency; or~~
- ~~sending, by the financial institution, the data sharing request to the sales agency by using a privacy computing unit.~~
- 15 ~~51. The system according to claim 50, wherein the sending, by the financial institution, the data sharing request to the sales agency by using a privacy computing unit comprises:~~
- ~~sending, by the financial institution, the data sharing request to the sales agency by using a privacy computing unit on a blockchain; or~~
- 20 ~~sending, by the financial institution, the data sharing request to the sales agency by using a privacy computing unit off a blockchain.~~
- ~~52. The system according to claim 50, wherein the sending, by the financial institution, the data sharing request to the sales agency by using a privacy computing unit comprises:~~
- 25 ~~sending, by the financial institution, the data sharing request to the privacy computing unit by initiating a transaction for invoking a contract, and then sending, by the privacy computing unit, the data sharing request to the sales agency.~~
- ~~53. The system according to claim 50, wherein a first smart contract is deployed in the privacy computing unit, and the first smart contract is used to receive an~~  
30 ~~invoking request sent by the financial institution, and in response to the invoking request, send the data sharing request to the sales agency.~~

54. The system according to claim 53, 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
- 5 the data sharing request is signed by the first smart contract, and the sales agency verifies the signature by using a public key of the first smart contract.
55. The system according to claim 41, wherein the obtaining, from the sales agency, the encrypted user basic data corresponding to the user ID and decrypting the user basic data comprises:
- 10 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.
56. The system according to claim 55, wherein the performing matching on the
- 15 decrypted user basic data comprises:
- executing, by the privacy computing unit, the second smart contract to perform matching on the decrypted user basic data.
57. The system according to claim 41 or 55, before the obtaining, from the sales agency, the encrypted user basic data corresponding to the user ID, further
- 20 comprising:
- proving, by the privacy computing unit, an identity of the privacy computing unit to the sales agency.
58. The system according to claim 41, wherein the privacy computing unit is further configured to send a proof of the matching result to a blockchain.
- 25 59. The system according to claim 58, wherein the proof of the matching result comprises a verifiable claim signed by the privacy computing unit.
60. The system according to claim 59, wherein the privacy computing unit is configured to send the verifiable claim signed by the privacy computing unit to the financial institution; and
- 30 the system further comprises a regulatory organization, configured to verify a signature of the verifiable claim at the financial institution using a public key of the privacy computing unit.
61. An information sharing system, comprising:

~~a first institution, configured to: receive first data, and sending a user ID corresponding to the first data to a second institution;~~

~~the second institution, configured to send a data sharing request to the first institution, wherein the data sharing request comprises the user ID corresponding to the first data that is expected to be shared;~~

~~a privacy computing unit, configured to: obtain, from the first institution, the encrypted first data corresponding to the user ID, and decrypt the encrypted first data, so as to process the decrypted first data to obtain a processing result; and further configured to send the processing result to the second institution.~~

~~62. The system according to claim 61, wherein the user ID comprises:~~

~~an account of a user corresponding to the first data that is registered at the first institution; or~~

~~an account allocated to a user corresponding to the first data by a system of the first institution when the user initiates a purchase operation at the first institution.~~

~~63. The system according to claim 62, wherein the user ID comprises:~~

~~a digest value obtained through hash calculation on one or more pieces of information in the first data.~~

~~64. The system according to claim 63, wherein the user ID comprises:~~

~~a digest value obtained through salting hash calculation on one or more pieces of information in the first data.~~

~~65. The system according to claim 61, wherein the sending a user ID corresponding to the first data to a second institution comprises:~~

~~encrypting and sending, by the first institution, the user ID corresponding to the first data to the second institution.~~

~~66. The system according to claim 61, before the sending a user ID corresponding to the first data to a second institution, further comprising:~~

~~verifying, by the first institution, an identity of the second institution.~~

~~67. The system according to claim 61, wherein the user ID in the data sharing request is encrypted.~~

~~68. The system according to claim 61, wherein the data sharing request comprises a signature of the second institution.~~

~~69. The system according to claim 61, before the sending a data sharing request to the first institution, further comprising:~~

~~verifying, by the second institution, an identity of the first institution.~~

~~70. The system according to claim 61, wherein the sending a data sharing request to the first institution comprises:~~

~~directly sending, by the second institution, the data sharing request to the first~~  
5 ~~institution; or~~

~~sending, by the second institution, the data sharing request to the first institution by using a privacy computing unit.~~

~~71. The system according to claim 70, wherein the sending, by the second institution, the data sharing request to the first institution by using a privacy~~  
10 ~~computing unit comprises:~~

~~sending, by the second institution, the data sharing request to the first institution by using a privacy computing unit on a blockchain; or~~

~~sending, by the second institution, the data sharing request to the first institution by using a privacy computing unit off a blockchain.~~

~~72. The system according to claim 70, wherein the sending, by the second institution, the data sharing request to the first institution by using a privacy~~  
15 ~~computing unit comprises:~~

~~sending, by the second institution, the data sharing request to the privacy computing unit by initiating a transaction for invoking a contract, and then sending,~~  
20 ~~by the privacy computing unit, the data sharing request to the first institution.~~

~~73. The system according to claim 70, 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 second institution, and in response to the invoking request, send the data sharing request to the first institution.~~

~~74. The system according to claim 73, wherein the data sharing request is signed by the privacy computing unit, and the first institution 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 first institution verifies the signature by using a public key of the first smart contract.~~

~~75. The system according to claim 61, wherein the obtaining, from the first institution, the encrypted first data corresponding to the user ID, and decrypting the encrypted first data comprises:~~

30

receiving, by the privacy computing unit, a transaction that is initiated by the first institution 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 first data corresponding to the user ID; and

5        decrypting, by the privacy computing unit, the encrypted first data corresponding to the user ID.

76. The system according to claim 75, wherein the processing the decrypted first data comprises:

10        executing, by the privacy computing unit, the second smart contract to process the decrypted first data.

77. The system according to claim 61 or 75, before the obtaining, from the first institution, the encrypted first data corresponding to the user ID, further comprising:

      proving, by the privacy computing unit, an identity of the privacy computing unit to the first institution.

15        78. The system according to claim 61, wherein the privacy computing unit is further configured to send a proof of the processing result to a blockchain.

79. The system according to claim 78, wherein the proof of the processing result comprises a verifiable claim signed by the privacy computing unit.

20        80. The system according to claim 79, wherein the privacy computing unit is configured to send the verifiable claim signed by the privacy computing unit to the second institution; and

      the system further comprises a third institution, configured to verify a signature of the verifiable claim at the second institution using a public key of the privacy computing unit.

25