

CLAIMS

What is claimed is:

1. A method for storing merchant authentication data in a blockchain of a blockchain network, the blockchain network including a plurality of verification nodes and a plurality of usage nodes, the plurality of verification nodes corresponding to various organizations issuing various types of authentication data, respectively, and the method being performed on a first verification node of the plurality of verification nodes, including:

obtaining authentication data of a merchant, the authentication data being issued by an organization corresponding to the first verification node; and

broadcasting the authentication data and a digital signature of the first verification node to other verification nodes of the plurality of verification nodes in the blockchain network, so that the authentication data is verified based on a consensus mechanism and stored in the blockchain network in response to that verification of the authentication data succeeds, wherein the verification comprises verifying the digital signature of the first verification node, wherein the verification is performed by using a smart contract deployed in the blockchain network, wherein the smart contract is jointly signed by the plurality of verification nodes, and wherein the signed smart contract comprises a plurality of clauses each corresponding to a specific verification action.-

2. The method according to claim 1, wherein the authentication data includes one or more of image data or text data.

3. The method according to claim 1, wherein the authentication data is stored in the blockchain network in association with a merchant identifier of the merchant in response to that verification of the authentication data succeeds.

4. The method according to claim 1, wherein the authentication data is stored in the blockchain network in association with a node identifier of the first verification node in response to that the verification of the authentication data succeeds.

~~5. The method according to claim 1, wherein the verification is performed by using a smart contract deployed in the blockchain network, and the smart contract is jointly signed by the plurality of verification nodes.~~

5 ~~65.~~ The method according to claim 1, wherein the verification includes verifying image data with respect to one or more of: a size of the image data, a resolution of the image data, content legality of the image data, content validity of the image data, or whether the image data has been modified.

10 ~~76.~~ The method according to claim 1, wherein the verification includes verifying text data with respect to one or more of: a format or content validity of the text data.

~~8. The method according to claim 1, wherein the broadcasting the authentication data to the other verification nodes of the plurality of verification nodes in the blockchain network includes: broadcasting the authentication data and a digital signature of the first verification node to the other verification nodes of the plurality of verification nodes in the blockchain network, the verification including verifying the digital signature.~~

15

20 ~~97.~~ A method for obtaining merchant authentication data from a blockchain of a blockchain network, the blockchain network including a plurality of verification nodes and a plurality of usage nodes, the plurality of verification nodes corresponding to various organizations issuing various types of authentication data, respectively, and the method being performed on a first usage node of the plurality of usage nodes, including:

25

obtaining all blocks in the blockchain network, the blocks storing respective authentication data of a plurality of merchants, wherein the blocks of the blockchain are stored according to any of claims 1 to 6, and the plurality of merchants including a first merchant; and

30 retrieving at least one piece of authentication data of the first merchant from the blocks.

~~108.~~ The method according to claim ~~97,~~ wherein the retrieving the at least one piece of authentication data of the first merchant from the blocks includes:

establishing an index of the plurality of merchants for the blocks, and retrieving the at least one piece of authentication data of the first merchant based on the index.

119. The method according to claim 97, wherein the retrieving the at least one
5 piece of authentication data of the first merchant from the blocks includes:
establishing a database of the authentication data for the blocks, and retrieving the at
least one piece of authentication data of the first merchant based on the database, the
database including an association relationship between the plurality of merchants and
the authentication data.

10

1210. The method according to claim 119, wherein the database further includes
an association relationship between the authentication data and a node identifier of a
verification node corresponding to an organization issuing the authentication data, and
the retrieving the at least one piece of authentication data of the first merchant from
15 the blocks includes: retrieving, from the blocks, the at least one piece of
authentication data of the first merchant and a node identifier of a verification node
corresponding to an organization issuing each of the at least one piece of
authentication data; and screening the at least one piece of authentication data based
on the node identifier of the verification node corresponding to the organization
20 issuing each of the at least one piece of authentication data.

1311. The method according to claim 119, wherein the database further includes
an association relationship between the authentication data and a timestamp of a block
at which the authentication data is located, and the retrieving the at least one piece of
25 authentication data of the first merchant from the blocks includes: retrieving, from the
blocks, the at least one piece of authentication data of the first merchant and a
timestamp corresponding to each of the at least one piece of authentication data; and
screening the at least one piece of authentication data based on the timestamp
corresponding to each of the at least one piece of authentication data.

30

1412. An apparatus for storing merchant authentication data in a blockchain of a
blockchain network, the blockchain network including a plurality of verification
nodes and a plurality of usage nodes, the plurality of verification nodes corresponding
to various organizations issuing various types of authentication data, respectively, and

the apparatus being implemented on a first verification node of the plurality of verification nodes, including:

an acquisition unit, configured to obtain authentication data of a merchant, the authentication data being issued by an organization corresponding to the first verification node; and

a broadcast unit, configured to broadcast the authentication data and a digital signature of the first verification node to other verification nodes of the plurality of verification nodes in the blockchain network, so that the authentication data is verified based on a consensus mechanism and stored in the blockchain network in response to that the verification of the authentication data succeeds, wherein the verification comprises verifying the digital signature of the first verification node, wherein the verification is performed by using a smart contract deployed in the blockchain network, wherein the smart contract is jointly signed by the plurality of verification nodes, and wherein the signed smart contract comprises a plurality of clauses each corresponding to a specific verification action.

~~15~~13. The apparatus according to claim ~~14~~12, wherein the authentication data includes one or more of image data or text data.

~~16~~14. The apparatus according to claim ~~14~~12, wherein the authentication data is stored in the blockchain network in association with a merchant identifier of the merchant in response to that the verification of the authentication data succeeds.

~~17~~15. The apparatus according to claim ~~14~~12, wherein the authentication data is stored in the blockchain network in association with a node identifier of the first verification node in response to that the verification of the authentication data succeeds.

~~18~~16. The apparatus according to claim ~~14~~12, wherein the verification is performed by using a smart contract deployed in the blockchain network, and the smart contract is jointly signed by the plurality of verification nodes.

~~19~~17. The apparatus according to claim ~~14~~12, wherein the verification includes verifying image data with respect to one or more of: a size of the image data, a resolution of the image data, content legality of the image data, content validity of the image data, or whether the image data has been modified.

5

~~20~~18. The apparatus according to claim ~~14~~12, wherein the verification includes verifying text data with respect to one or more of: a format or content validity of the text data.

10 ~~21~~19. The apparatus according to claim ~~14~~12, wherein the broadcast unit is further configured to broadcast the authentication data and a digital signature of the first verification node to other verification nodes of the plurality of verification nodes in the blockchain network, the verification including verifying the digital signature.

15 ~~22. An apparatus for obtaining merchant authentication data from a blockchain of a blockchain network, the blockchain network including a plurality of verification nodes and a plurality of usage nodes, the plurality of verification nodes corresponding to various organizations issuing various types of authentication data, respectively, and the apparatus being implemented on a first usage node of the plurality of usage nodes, including:~~

20

~~an acquisition unit, configured to obtain all blocks in the blockchain network, the blocks storing respective authentication data of a plurality of merchants, and the plurality of merchants including a first merchant; and~~

~~a retrieving unit, configured to retrieve at least one piece of authentication data of the first merchant from the blocks.~~

25

~~23. The apparatus according to claim 22, wherein the retrieving unit includes: an index establishment subunit, configured to establish an index of the plurality of merchants for the blocks; and a first retrieving subunit, configured to retrieve the at least one piece of authentication data of the first merchant based on the index.~~

30

~~24. The apparatus according to claim 22, wherein the retrieving unit includes: a database establishment subunit, configured to establish a database of the authentication data for the blocks, the database including an association relationship~~

~~between the plurality of merchants and the authentication data; and a second retrieving subunit, configured to retrieve the at least one piece of authentication data of the first merchant based on the database.~~

5 ~~25. The apparatus according to claim 24, wherein the database further includes an association relationship between the authentication data and a node identifier of a verification node corresponding to an organization issuing the authentication data, and the retrieving unit further includes a third retrieving subunit, configured to retrieve, from the blocks, the at least one piece of authentication data of the first merchant and~~
10 ~~a node identifier of a verification node corresponding to an organization issuing each of the at least one piece of authentication data; and a first screening subunit, configured to screen the at least one piece of authentication data based on the node identifier of the verification node corresponding to the organization issuing each of the at least one piece of authentication data.~~

15 ~~26. The apparatus according to claim 24, wherein the database further includes an association relationship between the authentication data and a timestamp of a block at which the authentication data is located, and the retrieving unit further includes a fourth retrieving subunit, configured to retrieve, from the blocks, the at least one piece~~
20 ~~of authentication data of the first merchant and a timestamp corresponding to each of the at least one piece of authentication data; and a second screening subunit, configured to screen the at least one piece of authentication data based on the timestamp corresponding to each of the at least one piece of authentication data.~~

25 ~~27~~20. A computing device, comprising a memory and a processor, the memory storing executable code, and the processor executing the executable code to implement the method according to any one of claims 1 to ~~13~~11.