I/We Claim:

1. A method of managing user identity authentication data, comprising:

authenticating, at a management device, a query request from a query requester for original identity data of a user to be queried, the query request including at least a key for encrypting the original identity data to be queried;

in response to the query request being successfully authenticated, sending authorization information for the query request to the query requester;

determining, based on mapping information associated with the original identity data stored by one or more of a plurality of authentication devices, at least one of the plurality of authentication devices to query for the original identity data; and

in response to receiving signature information corresponding to the query request from the user to be queried, transmitting the signature information and a key to the at least one authentication device, wherein the signature information indicates the user to be queried approves the request and was generated by a terminal device of the user to be queried based on the authorization information, the authorization information having been received at the terminal device of the user to be queried from the query requester.

2. The method according to claim 1, where sending the authorization information comprises:

determining whether the query request is successfully authenticated based on confirming whether the query requester is legitimate and whether the at least one authentication device that has stored the original identity data to be queried is present; and

in response to determining that the query request is successfully authenticated, sending the authorization information to the query requester, the authorization information comprising a temporary session token.

3. The method according to claim 1, wherein the step of determining the at least one authentication device from the plurality of authentication devices comprises:

determining, based on the query request and the mapping information, the at least one authentication device that is storing the original identity data to be queried, the query request further comprising an associated account identifier of the user to be queried, and the mapping information being associated with a flag of an authentication result of the original identity

data from a prior authentication of the original identity data by the authentication device that is storing the original identity data to be queried.

4. The method according to claim 1, further comprising:

obtaining feedback data from the user to be queried, the feedback data being generated by the user to be queried based on the authorization information received from the query requester; and

in response to confirming that the feedback data matches the authorization information, sending to the user to be queried an authorization confirmation request, the authorization confirmation request being used for requesting the user to be queried to reply with the signature information to confirm authorization.

5. The method according to claim 1, wherein the signature information indicates at least the query requester, the user to be queried, and the original identity data to be queried.

6. The method according to claim 1, further comprising:

obtaining, from the at least one authentication device that stores the original identity data to be queried, the original identity data to be queried and a hash value of the original identity data to be queried, the original identity data to be queried and the hash value of the original identity data to be queried being encrypted by the key, the hash value of the original identity data to be queried being obtained from a blockchain platform, and the key being a public key of the query requester; and

sending the encrypted original identity data to be queried and the encrypted hash value of the original identity data to be queried to the query requester, the hash value of the original identity data to be queried being used to authenticate the original identity data to be queried.

7. A method of managing user identity authentication data, comprising:

at an authentication device, transmitting mapping information to a user identity authentication data management device, the mapping information being associated with original identity data stored by the authentication device;

obtaining, from the management device, signature information and a key, the signature information providing authorization to release the original identity data to be queried ;

in response to confirming that the signature information is successfully authenticated, encrypting, with the key, the original identity data to be queried and a hash value of the original identity data to be queried, the hash value of the original identity data to be queried being obtained from a blockchain platform; and

sending the encrypted original identity data to be queried and the encrypted hash value of the original identity data to be queried to the management device or a query requester, the hash value of the original identity data to be queried being used to authenticate the original identity data to be queried.

8. The method according to claim 7, further comprising:

applying to the management device for an account for the authentication device;

deploying a smart contract for transmitting identity authentication result data to the blockchain platform by using a private key of the authentication device; and

synchronizing the mapping information and a domain name to the management device, the domain name being associated with the associated account of the authentication device.

9. The method according to claim 7, further comprising:

in response to confirming that the original identity data of the user is successfully authenticated, generating identity authentication result data, the identity authentication result data including at least one of an associated account identifier of the user to be queried, an authentication result, and a hash value of the original identity data, the associated account identifier of the user being associated with the authentication device; and

transmitting the identity authentication result data to the blockchain platform with a smart contract deployed via a private key.

10. The method according to claim 9, wherein the authentication result comprises at least one of the following: an associated account identifier of the user, an associated account identifier of an associated user that is associated with the user, a status of the associated account of the user, and an identity type of the user, the identity type being selected from a group consisting of an individual, an organization, a device, and a smart contract.

11. The method according to claim 9, wherein the authentication result comprises multiple binary flags, each binary flag indicating whether a corresponding one of the original identity data comprising a plurality of items was successfully authenticated; and

wherein the original identity data comprises at least one aspect of image data and text data.

12. The method according to claim 11, wherein the mapping information includes a data dictionary rule for describing the meaning of each of the flags.

13. The method according to claim 11, wherein the hash value of the original identity data is generated by hashing items in the original identity data corresponding to the flags indicating that the authentication of the corresponding items was successful.

14. The method according to claim 7, further comprising:

obtaining, based on the signature information, the original identity data to be queried and the hash value of the original identity data to be queried, the signature information indicating at least the query requester, the user to be queried, and the original identity data to be queried.

15. The method according to claim 7, further comprising:

in response to confirming that the signature information was not successfully authenticated or not stored by the authentication device, sending error information regarding the original identity data to be queried.

16. The method according to claim 7, wherein the authentication device is at least one authentication device that stores the original identity data to be queried, the at least one authentication device being determined by the management device based on the query request of the query requester and the mapping information, the query request comprising an associated account identifier of the user to be queried, and the mapping information being associated with a flag of an authentication result of the original identity data stored by the corresponding authentication device.

17. A management device for user identity authentication data, the device comprising:

a memory configured to store one or more programs; and

a processing unit coupled to the memory and configured to execute said one or more programs to cause the management device to perform the method according to any of claims 1-6.

18. An authentication device for user identity authentication data, the device comprising:

a memory configured to store one or more programs; and

a processing unit coupled to the memory and configured to execute said one or more programs to cause the authentication device to perform the method according to any of claims 7-16.

19. A non-transitory computer readable storage medium having machine executable instructions stored thereon, the machine executable instructions, when executed, causing a machine to perform steps of the method according to any of claims 1-16.

20. A computer program product being tangibly stored on a non-transient computer readable medium and comprising machine executable instruction, the machine executable instructions, when being executed, causing a machine to perform steps of the method according to any of claims 1-16.