

WHAT IS CLAIMED IS:

1. A blockchain-based digital identity management method performed by a digital identity management device, the method comprising:

5 first storing identity identification information of a subscription request in a first block of a blockchain in response to the subscription request from a service request device and obtaining a block hash value of the first block as a result of the first storing;

second storing the block hash value of the first block and data of authentication information of the subscription request in a second block of the blockchain and obtaining a
10 block hash value of the second block as a result of the second storing;

inserting the block hash value of the second block into a digital identity data structure as a result of processing the subscription request;

receiving a digital identity authentication request comprising a biometric identifier from a user terminal connected to a second service server of a second service provider;

15 generating a hash value of the biometric identifier included in the digital identity authentication request;

if the block storing the generated hash value of the biometric identifier is found, obtaining identity identification information from a block indicated by a block hash value matched and stored with the generated hash value of the biometric identifier in the found
20 block; and

transmitting at least part of the obtained identity identification information to the second service server,

wherein the identity identification information is stored in the first block and is not stored in the second block, and

25 the data of authentication information is not in the first block and is stored in the second block.

2. The method of claim 1, wherein the data of the authentication information of the subscription request is a hash value of the authentication information of the
30 subscription request.

3. The method of claim 1, wherein the authentication information of the subscription request is a biometric identifier for identifying a user who made the subscription request.

5 4. The method of claim 3, wherein the data of the authentication information of the subscription request is a hash value of the authentication information of the subscription request, the method further comprising:

searching for a block storing the generated hash value of the biometric identifier, in the blockchain; and

10 transmitting the response to the digital identity authentication request based on the searching for the block.

5. The method of claim 4, wherein the searching for the block comprises searching for the block storing the generated hash value of the biometric identifier among
15 blocks indicated by block hash values included in the digital identity data structure.

6. The method of claim 4, wherein the service request device is a first service server of a first service provider that is different from the second service provider, and the blockchain is stored, in a distributed manner, in blockchain nodes, the blockchain nodes
20 including a computing device managed by the first service provider and a computing device managed by the second service provider.

7. The method of claim 3, wherein the digital identity management device is a first service server of a first service provider, the service request device is a user terminal
25 connected to the first service server, the data of the authentication information of the subscription request is a hash value of the authentication information of the subscription request, the method further comprising:

receiving a digital identity authentication request comprising the biometric identifier from the user terminal by using a second service server of a second service
30 provider that is different from the first service provider;

generating a hash value of the biometric identifier included in the digital identity authentication request by using the second service server;

searching for a block storing the generated hash value of the biometric identifier, in the blockchain by using the second service server; and

transmitting a response to the digital identity authentication request to the user terminal based on the searching for the block,

5 wherein the blockchain is stored, in a distributed manner, in blockchain nodes, the blockchain nodes including a computing device managed by the first service provider and a computing device managed by the second service provider.

8. The method of claim 1, wherein the inserting of the block hash value of the second block into the digital identity data structure comprises:

10 inserting only the block hash value of the second block into the digital identity data structure without inserting the block hash value of the first block into the digital identity data structure; and

 deleting the block hash value of the first block.

15

9. The method of claim 8, wherein the inserting of only the block hash value of the second block into the digital identity data structure without inserting the block hash value of the first block into the digital identity data structure comprises:

20 inserting only the block hash value of the second block into the digital identity data structure without inserting both the identity identification information of the subscription request and the block hash value of the first block into the digital identity data structure; and

 deleting the identity identification information of the subscription request.

25 10. A digital identify management device comprising:

 a processor;

 a memory which stores instructions to be executed on the processor; and

 a storage which stores a digital identity data structure,

 wherein the instructions comprise:

30 an operation of performing a first process for storing identity identification information of a subscription request in a first block of a blockchain in response to

the subscription request from a service request device and obtaining a block hash value of the first block as a result of performing the first process;

an operation of performing a second process for storing the block hash value of the first block and data of authentication information of the subscription request in a second block of the blockchain and obtaining a block hash value of the second block as a result of performing the second process;

an operation of inserting the block hash value of the second block into a digital identity data structure as a result of processing the subscription request;

an operation of receiving a digital identity authentication request comprising a biometric identifier from a user terminal connected to a second service server of a second service provider;

an operation of generating a hash value of the biometric identifier included in the digital identity authentication request;

if the block storing the generated hash value of the biometric identifier is found, an operation of obtaining identity identification information from a block indicated by a block hash value matched and stored with the generated hash value of the biometric identifier in the found block; and

an operation of transmitting at least part of the obtained identity identification information to the second service server,

wherein the identity identification information is stored in the first block and is not stored in the second block, and

the data of authentication information is not in the first block and is stored in the second block.

11. The digital identity management device of claim 10, wherein the data of the authentication information of the subscription request is a hash value of the authentication information of the subscription request.

12. The digital identity management device of claim 10, wherein the authentication information of the subscription request is a biometric identifier for identifying a user who made the subscription request.

13. The digital identity management device of claim 12, wherein the data of the authentication information of the subscription request is a hash value of the authentication information of the subscription request, the instructions further comprising:

5 an operation of performing a third process for searching for a block, which stores the generated hash value of the biometric identifier, in the blockchain by using the digital identity management device; and

an operation of transmitting the response to the digital identity authentication request based on the result of performing the third process by using the digital identity management device.

10

14. The digital identity management device of claim 13, wherein the operation of performing the third process comprises an operation of performing a process of searching for the block storing the generating hash value of the biometric identifier among blocks indicated by block hash values included in the digital identity data structure.

15

15. The digital identity management device of claim 13, wherein the service request device is a first service server of a first service provider that is different from the second service provider, and the blockchain is stored, in a distributed manner, in blockchain nodes, the blockchain nodes comprising a computing device managed by the first service provider and a computing device managed by the second service provider.

20

16. The digital identity management device of claim 12, wherein the digital identity management device is a first service server of a first service provider, wherein the service request device is a user terminal connected to the first service server, the data of the authentication information of the subscription request is a hash value of the authentication information of the subscription request, the instructions further comprising;

25

an operation of receiving a digital identity authentication request comprising the biometric identifier from the user terminal by using a second service server of a second service provider that is different from the first service provider;

30

an operation of generating a hash value of the biometric identifier included in the digital identity authentication request by using the second service server;

an operation of performing a third process for searching for a block, which stores the generated hash value of the biometric identifier, in the blockchain by using the second service server; and

an operation of transmitting a response to the digital identity authentication request to the user terminal based on the result of performing the third process,

wherein the blockchain is stored, in a distributed manner, in blockchain nodes, the blockchain nodes comprising a computing device managed by the first service provider and a computing device managed by the second service provider.

10 17. The digital identity management device of claim 10, wherein the operation of inserting the block hash value of the second block into the digital identity data structure as a result of processing the subscription request comprises:

an operation of inserting only the block hash value of the second block into the digital identity data structure without inserting both the identity identification information of the subscription request and the block hash value of the first block into the digital identity data structure;

an operation of deleting the identity identification information of the subscription request; and

an operation of deleting the block hash value of the first block.

20

18. A non-transitory recording medium storing a computer program implemented as computer-readable code, wherein the computer program comprises instructions, the instructions comprising:

an operation of performing a first process for storing identity identification information of a subscription request in a first block of a blockchain and then obtaining a block hash value of the first block as a result of performing the first process;

an operation of performing a second process for storing the block hash value of the first block and data of authentication information of the subscription request in a second block of the blockchain and then obtaining a block hash value of the second block as a result of performing the second process;

an operation of inserting the block hash value of the second block into a digital identity data structure as a result of processing the subscription request;

an operation of receiving a digital identity authentication request comprising a biometric identifier from a user terminal connected to a second service server of a second service provider;

5 an operation of generating a hash value of the biometric identifier included in the digital identity authentication request;

 if the block storing the generated hash value of the biometric identifier is found, an operation of obtaining identity identification information from a block indicated by a block hash value matched and stored with the generated hash value of the biometric identifier in the found block; and

10 an operation of transmitting at least part of the obtained identity identification information to the second service server,

 wherein the identity identification information is stored in the first block and is not stored in the second block, and

15 the data of authentication information is not in the first block and is stored in the second block.