CLAIMS

What is claimed is:

1. A method for backtracking a service behavior, applied to an identity management system, comprising:

receiving an authorization request sent by a service device, wherein the authorization request is sent based on a service processing request sent by a client device, and the authorization request comprises behavior data of an operational behavior of a first user in the client device corresponding to a service to be processed, authorization information on an operation permission for the behavior data granted by the first user to the service device, first digital identity information of the first user, and second digital identity information of the service device;

if it is determined that the authorization information satisfies a predetermined authorization condition, generating a first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information, wherein the first verifiable claim represents that the service device is granted the operation permission; and

saving the first verifiable claim to a blockchain, such that a supervision organization, when granted an access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain, wherein the authorization request further comprises: first identification information of service data of the service to be processed;

the generating a first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information comprises:

generating first ciphertext data of the behavior data based on a predetermined encryption method; and

generating the first verifiable claim based on the first identification information, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information, wherein after the saving the first verifiable claim to a blockchain, the method further comprising:

receiving a permission sharing request sent by the service device, wherein the permission sharing request is sent based on a query request sent by the supervision

organization, and the permission sharing request comprises the first identification information associated with the behavior data to be queried; and

performing permission sharing processing based on the permission sharing request to grant the supervision organization the access permission for the behavior data associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data, wherein the permission sharing request further comprises: third digital identity information of the supervision organization;

the performing permission sharing processing based on the permission sharing request comprises:

obtaining the associated first verifiable claim from the blockchain based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the blockchain, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the blockchain based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a blockchain comprises:

encrypting the first key based on the public key corresponding to the obtained

second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the blockchain.

2. The method according to claim 1, wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

encrypting the behavior data based on a public key corresponding to the obtained second digital identity information to obtain the first ciphertext data;

the generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information comprises:

decrypting the first ciphertext data in the first verifiable claim based on a private key corresponding to the obtained second digital identity information to obtain the behavior data; and

encrypting the obtained behavior data based on the public key corresponding to the obtained third digital identity information to obtain the second ciphertext data.

3. The method according to claim 1, wherein the generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information comprises:

obtaining the third ciphertext data associatively saved with the first verifiable claim from the blockchain;

decrypting the third ciphertext data based on the private key corresponding to the obtained second digital identity information to obtain the first key; and

encrypting the obtained first key based on the public key corresponding to the obtained third digital identity information to obtain the second ciphertext data;

the associatively saving the second ciphertext data and the third digital identity information to the blockchain comprises:

associatively saving the first identification information, the second ciphertext data, and the third digital identity information to the blockchain;

the sending the second ciphertext data to the supervision organization comprises:

sending the first ciphertext data and the second ciphertext data to the supervision organization.

4. The method according to claim 1, after the saving the first verifiable claim to a blockchain, further comprising:

generating permission sharing record information based on the first identification

information and the third digital identity information of the predetermined supervision organization, and saving the permission sharing record information to the blockchain;

receiving a query request sent by the supervision organization, wherein the query request comprises the third digital identity information and the first identification information of the service data to be queried;

if it is determined that the associated permission sharing record information is identified from the blockchain based on the third digital identity information and the first identification information in the query request, obtaining the associated first verifiable claim from the blockchain based on the first identification information; and

decrypting the first ciphertext data in the obtained first verifiable claim to obtain the behavior data, and sending the obtained behavior data to the supervision organization.

5. The method according to any one of claims 1 to 4, further comprising:

receiving a message subscription request sent by the supervision organization;

performing message subscription processing based on the message subscription request, and sending message subscription success information to the supervision organization; and

if it is determined that the first verifiable claim is successfully saved to the blockchain, sending push information to the supervision organization, such that the supervision organization, when granted the access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain.

6. The method according to claim 1, wherein the authorization request comprises: a hash value of the behavior data and a storage address of the behavior data;

the generating a first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information comprises:

generating the first verifiable claim based on the hash value, the storage address, the authorization information, the first digital identity information, and the second digital identity information, such that the supervision organization, when granted the access permission of the first verifiable claim, obtains the behavior data from a corresponding storage area based on the storage address comprised in the first verifiable claim in the blockchain, and backtracks the operational behavior of the first user corresponding to the service to be processed based on the obtained behavior data and

the hash value comprised in the first verifiable claim.

7. The method according to claim 1, wherein the determining that the authorization information satisfies a predetermined authorization condition comprises:

obtaining verification information to be verified of the first user, and determining that the authorization information satisfies the predetermined authorization condition if the verification information passes verification; or

the authorization request further comprises first signature data, the first signature data being data obtained by signing specified data with a private key corresponding to the first digital identity information of the first user;

the determining that the authorization information satisfies a predetermined authorization condition comprises:

obtaining a public key corresponding to the first digital identity information; and

verifying the first signature data based on the obtained public key, and determining that the authorization information satisfies the predetermined authorization condition if the verification succeeds.

8. The method according to claim 1, before the receiving an authorization request sent by the service device, further comprising:

receiving an application request for digital identity information sent by the service device, wherein the application request comprises user information of the first user;

generating the first digital identity information of the first user based on the application request; and

associatively saving the first digital identity information and the user information, and sending the first digital identity information to the service device, such that the service device sends the first digital identity information to the client device.

9. The method according to claim 1, wherein the behavior data comprises one or more of video data, image data, and text data.

10. A method for backtracking a service behavior, applied to a service device, comprising:

receiving a service processing request sent by a client device, wherein the service processing request comprises behavior data of an operational behavior of a first user in the client device corresponding to a service to be processed;

performing corresponding service processing based on the service processing request, and obtaining authorization information on an operation permission for the behavior data granted by the first user to the service device; and

sending an authorization request to an identity management system based on the authorization information, the behavior data, obtained first digital identity information of the first user, and second digital identity information of the service device, such that the identity management system saves a first verifiable claim generated based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information to a blockchain, and a supervision organization, when granted an access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain, wherein the first verifiable claim is used to prove that the service device is granted the operation permission,

wherein the authorization request further comprises: first identification information of service data of the service to be processed;

wherein the first verifiable claim is generated by generating first ciphertext data of the behavior data based on a predetermined encryption method, and generating the first verifiable claim based on the first identification information, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information,

wherein after the identity management system saves the first verifiable claim to the blockchain, the method further comprising:

receiving a permission sharing request sent by the service device, wherein the permission sharing request is sent based on a query request sent by the supervision organization, and the permission sharing request comprises the first identification information associated with the behavior data to be queried; and

performing permission sharing processing based on the permission sharing request to grant the supervision organization the access permission for the behavior data associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data;

wherein the permission sharing request further comprises: third digital identity information of the supervision organization;

the performing permission sharing processing based on the permission sharing request comprises:

obtaining the associated first verifiable claim from the blockchain based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the blockchain, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the blockchain based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a blockchain comprises:

encrypting the first key based on the public key corresponding to the obtained second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the blockchain.

11. The method according to claim 10, after receiving a service processing request sent by a client device, further comprising:

performing hash processing on the behavior data based on a predetermined algorithm to obtain a hash value of the behavior data; and

saving the behavior data to a designated storage area;

the sending an authorization request to an identity management system based on the authorization information, the behavior data, obtained first digital identity information of the first user, and second digital identity information of the service device comprises:

sending the authorization request to the identity management system based on the

authorization information, the hash value, a storage address of the behavior data, the first digital identity information, and the second digital identity information.

12. The method according to claim 10, after receiving a service processing request sent by a client device, further comprising:

determining first identification information of service data of the service to be processed,

wherein the sending an authorization request to an identity management system based on the authorization information, the behavior data, obtained first digital identity information of the first user, and second digital identity information of the service device comprises:

sending the authorization request to the identity management system based on the first identification information, the authorization information, the behavior data, the first digital identity information, and the second digital identity information, such that the identity management system generates the first verifiable claim based on the first identification information, the authorization information, the behavior data, the first digital identity information, and the second digital identity information;

after the sending an authorization request to an identity management system based on the authorization information, the behavior data, obtained first digital identity information of the first user, and second digital identity information of the service device, the method further comprises:

receiving a query request sent by the supervision organization, wherein the query request comprises third digital identity information of the supervision organization and the first identification information associated with the behavior data to be queried;

sending a permission sharing request to the identity management system based on the third digital identity information and the first identification information, such that the identity management system performs permission sharing processing to grant the supervision organization the access permission for the behavior data associated with the first identification information, and the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data; and

receiving permission sharing result information sent by the identity management system.

13. The method according to claim 10, before the sending an authorization request to an identity management system based on the authorization information, the behavior

data, obtained first digital identity information of the first user, and second digital identity information of the service device, further comprising:

if it is determined that the service processing request does not comprise the first digital identity information of the first user, obtaining user information of the first user;

sending an application request for digital identity information to the identity management system based on the obtained identity information of the first user, such that the identity management system generates the first digital identity information of the first user, and associatively saves the first digital identity information with the user information; and

receiving the first digital identity information sent by the identity management system, and sending the first digital identity information to the client device.

14. The method according to claim 10, wherein the behavior data comprises one or more of video data, image data, and text data.

15. A system for backtracking a service behavior, comprising an application layer subsystem, a backtracking layer subsystem, and a storage layer subsystem, wherein:

the application layer subsystem is configured to obtain behavior data of an operational behavior of a first user in the application layer subsystem corresponding to a service to be processed, and send a service processing request to the backtracking layer subsystem based on the behavior data;

the backtracking layer subsystem is configured to perform corresponding service processing based on the service processing request, and obtain authorization information on an operation permission for the behavior data granted by the first user to the backtracking layer subsystem; if it is determined that the authorization information satisfies a predetermined authorization condition, generate a first verifiable claim based on the behavior data, the authorization information, first digital identity information of the first user, and second digital identity information of the backtracking layer subsystem; and send the first verifiable claim to the storage layer subsystem, wherein the first verifiable claim represents that a service device is granted the operation permission; and

the storage layer subsystem is configured to store the first verifiable claim, such that a supervision organization, when granted an access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the storage layer subsystem,

wherein the backtracking layer subsystem is configured to generate first ciphertext

data of the behavior data based on a predetermined encryption method, and generate the first verifiable claim based on first identification information of service data of the service to be processed comprised in the authorization request, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information.

wherein the backtracking layer subsystem comprises a first permission processing module, and the first permission processing module is configured to receive a query request sent by the supervision organization, wherein the query request comprises the first identification information associated with the behavior data to be queried; and perform permission sharing processing based on the query request to grant the supervision organization the access permission for the behavior data associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data;

wherein the query request further comprises: third digital identity information of the supervision organization;

wherein the permission sharing processing based on the query request comprises:

obtaining the associated first verifiable claim from the storage layer subsystem based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the storage layer subsystem, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the storage layer subsystem based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a

predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a storage layer subsystem comprises:

encrypting the first key based on the public key corresponding to the obtained second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the storage layer subsystem.

16. The system according to claim 15, further comprising an application extension management subsystem, the application extension management subsystem distributing a plug-in to the application layer subsystem, such that the application layer subsystem is installed with the plug-in to obtain the behavior data of the first user based on the plug-in.

17. The system according to claim 15, wherein the application layer subsystem comprises a client device deployed in an end-user device of the first user, and the client device obtains the behavior data of the operational behavior of the first user in the client device corresponding to the service to be processed, and sends a service processing request to the backtracking layer subsystem based on the behavior data.

18. The system according to claim 15, wherein the backtracking layer subsystem comprises a service device and an identity management system;

the service device is configured to perform corresponding service processing based on the service processing request, obtain authorization information on an operation permission for the behavior data granted by the first user to the backtracking layer subsystem, and send the authorization request to the identity management system based on the authorization information, the behavior data, the first digital identity information, and the second digital identity information; and

the identity management system is configured to, if it is determined that the authorization information comprised in the authorization request satisfies a predetermined authorization condition, generate the first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information, and send the first verifiable claim to the storage layer subsystem.

19. An apparatus for backtracking a service behavior, applied to an identity

management system, comprising:

a receiving module, configured to receive an authorization request sent by a service device, wherein the authorization request is sent based on a service processing request sent by a client device, and the authorization request comprises behavior data of an operational behavior of a first user in the client device corresponding to a service to be processed, authorization information on an operation permission for the behavior data granted by the first user to the service device, first digital identity information of the first user, and second digital identity information of the service device;

a generation module, configured to, if it is determined that the authorization information satisfies a predetermined authorization condition, generate a first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information, wherein the first verifiable claim represents that the service device is granted the operation permission; and

a saving module, configured to save the first verifiable claim to a blockchain, such that a supervision organization, when granted an access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain,

wherein the authorization request further comprises: first identification information of service data of the service to be processed;

wherein the generation module is configured to generate first ciphertext data of the behavior data based on a predetermined encryption method; and generate the first verifiable claim based on the first identification information, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information,

wherein the receiving module is configured to receive a permission sharing request sent by the service device, wherein the permission sharing request is sent based on a query request sent by the supervision organization, and the permission sharing request comprises the first identification information associated with the behavior data to be queried;

wherein the apparatus further comprises a first permission processing module configured to perform permission sharing processing based on the permission sharing request to grant the supervision organization the access permission for the behavior data associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the

service to be processed based on the behavior data,

wherein the permission sharing request further comprises: third digital identity information of the supervision organization;

the permission sharing processing based on the permission sharing request comprises:

obtaining the associated first verifiable claim from the blockchain based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the blockchain, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the blockchain based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a blockchain comprises:

encrypting the first key based on the public key corresponding to the obtained second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the blockchain.

20. An apparatus for backtracking a service behavior, applied to a service device, comprising:

a receiving module, configured to receive a service processing request sent by a

client device, wherein the service processing request comprises behavior data of an operational behavior of a first user in the client device corresponding to a service to be processed;

a processing module, configured to perform corresponding service processing based on the service processing request, and obtain authorization information on an operation permission for the behavior data granted by the first user to the service device; and

a sending module, configured to send an authorization request to an identity management system based on the authorization information, the behavior data, obtained first digital identity information of the first user, and second digital identity information of the service device, such that the identity management system saves a first verifiable claim generated based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information to a blockchain, and a supervision organization, when granted an access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain, wherein the first verifiable claim is used to prove that the service device is granted the operation permission,

wherein the authorization request further comprises: first identification information of service data of the service to be processed

wherein the processing module is configured to generate first ciphertext data of the behavior data based on a predetermined encryption method, and generate the first verifiable claim based on the first identification information, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information,

wherein the processing module comprises a first permission processing module, and the first permission processing module is configured to receive a query request sent by the supervision organization, and the permission sharing request comprises the first identification information associated with the behavior data to be queried; and perform permission sharing processing based on the permission sharing request to grant the supervision organization the access permission for the behavior data associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data;

wherein the query request further comprises: third digital identity information of the supervision organization;

the performing permission sharing processing based on the query request comprises:

obtaining the associated first verifiable claim from the blockchain based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the blockchain, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the blockchain based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a blockchain comprises:

encrypting the first key based on the public key corresponding to the obtained second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the blockchain.

21. A system for backtracking a service behavior, comprising:

a client device, configured to obtain behavior data of an operational behavior of a first user in the client device corresponding to a service to be processed, and send a service processing request to a service device based on the behavior data;

the service device, configured to receive the service processing request sent by the client device, perform corresponding service processing based on the service processing request, obtain authorization information on an operation permission of the data granted by the first user to the service device, and send an authorization request to the identity management system based on the authorization information, the behavior data, obtained first digital identity information of the first user, and second digital identity information of the service device;

the identity management system, configured to receive the authorization request sent by the service device, generate a first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information if it is determined that the authorization information satisfies a predetermined authorization condition, and save the first verifiable claim to a blockchain, wherein the first verifiable claim represents that the service device is granted the operation permission;

a supervision organization, configured to, if determined to be granted an access permission of the first verifiable claim, backtrack the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain; and

the blockchain, configured to save the first verifiable claim,

wherein the authorization request further comprises: first identification information of service data of the service to be processed;

wherein the first verifiable claim is generated by generating first ciphertext data of the behavior data based on a predetermined encryption method, and generating the first verifiable claim based on the first identification information, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information,

wherein after the identity management system saves the first verifiable claim to the blockchain, the identity management system:

receives a permission sharing request sent by the service device, wherein the permission sharing request is sent based on a query request sent by the supervision organization, and the permission sharing request comprises the first identification information associated with the behavior data to be queried; and

performs permission sharing processing based on the permission sharing request to grant the supervision organization the access permission for the behavior data

associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data, wherein the permission sharing request further comprises: third digital identity information of the supervision organization;

the performing permission sharing processing based on the permission sharing request comprises:

obtaining the associated first verifiable claim from the blockchain based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the blockchain, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the blockchain based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a blockchain comprises:

encrypting the first key based on the public key corresponding to the obtained second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the blockchain.

22. A device for backtracking a service behavior, comprising:

a processor; and

a memory arranged to store computer-executable instructions that, when executed, cause the processor to:

receive an authorization request sent by a service device, wherein the authorization request is sent based on a service processing request sent by a client device, and the authorization request comprises behavior data of an operational behavior of a first user in the client device corresponding to a service to be processed, authorization information on an operation permission for the behavior data granted by the first user to the service device, first digital identity information of the first user, and second digital identity information of the service device;

if it is determined that the authorization information satisfies a predetermined authorization condition, generate a first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information, wherein the first verifiable claim represents that the service device is granted the operation permission; and

save the first verifiable claim to a blockchain, such that a supervision organization, when granted an access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain,

wherein the authorization request further comprises: first identification information of service data of the service to be processed;

the generating a first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information comprises:

generating first ciphertext data of the behavior data based on a predetermined encryption method; and

generating the first verifiable claim based on the first identification information, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information,

wherein after the saving the first verifiable claim to a blockchain, the instructions, that when executed, further cause the processor to:

receive a permission sharing request sent by the service device, wherein the permission sharing request is sent based on a query request sent by the supervision organization, and the permission sharing request comprises the first identification

information associated with the behavior data to be queried; and

perform permission sharing processing based on the permission sharing request to grant the supervision organization the access permission for the behavior data associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data, wherein the permission sharing request further comprises: third digital identity information of the supervision organization;

the performing permission sharing processing based on the permission sharing request comprises:

obtaining the associated first verifiable claim from the blockchain based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the blockchain, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the blockchain based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a blockchain comprises:

encrypting the first key based on the public key corresponding to the obtained second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the blockchain.

23. A device for backtracking a service behavior, comprising:

a processor; and

a memory arranged to store computer-executable instructions that, when executed, cause the processor to:

receive a service processing request sent by a client device, wherein the service processing request comprises behavior data of an operational behavior of a first user in the client device corresponding to a service to be processed;

perform corresponding service processing based on the service processing request, and obtain authorization information on an operation permission for the behavior data granted by the first user to the service device; and

send an authorization request to an identity management system based on the authorization information, the behavior data, obtained first digital identity information of the first user, and second digital identity information of the service device, such that the identity management system saves a first verifiable claim generated based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information to a blockchain, and a supervision organization, when granted an access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain, wherein the first verifiable claim is used to prove that the service device is granted the operation permission,

wherein the authorization request further comprises: first identification information of service data of the service to be processed;

wherein the first verifiable claim is generated by generating first ciphertext data of the behavior data based on a predetermined encryption method, and generating the first verifiable claim based on the first identification information, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information,

wherein after the identity management system saves the first verifiable claim to the blockchain, the instructions, that when executed, further cause the processor to:

receive a permission sharing request sent by the service device, wherein the permission sharing request is sent based on a query request sent by the supervision organization, and the permission sharing request comprises the first identification

information associated with the behavior data to be queried; and

perform permission sharing processing based on the permission sharing request to grant the supervision organization the access permission for the behavior data associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data;

wherein the permission sharing request further comprises: third digital identity information of the supervision organization;

the performing permission sharing processing based on the permission sharing request comprises:

obtaining the associated first verifiable claim from the blockchain based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the blockchain, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the blockchain based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a blockchain comprises:

encrypting the first key based on the public key corresponding to the obtained second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the blockchain.

24. A storage medium for storing computer-executable instructions that, when executed by a processor, implement the following process:

receiving an authorization request sent by a service device, wherein the authorization request is sent based on a service processing request sent by a client device, and the authorization request comprises behavior data of an operational behavior of a first user in the client device corresponding to a service to be processed, authorization information on an operation permission for the behavior data granted by the first user to the service device, first digital identity information of the first user, and second digital identity information of the service device;

if it is determined that the authorization information satisfies a predetermined authorization condition, generating a first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information, wherein the first verifiable claim represents that the service device is granted the operation permission; and

saving the first verifiable claim to a blockchain, such that a supervision organization, when granted an access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain,

wherein the authorization request further comprises: first identification information of service data of the service to be processed;

the generating a first verifiable claim based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information comprises:

generating first ciphertext data of the behavior data based on a predetermined encryption method; and

generating the first verifiable claim based on the first identification information, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information, wherein after the saving the first verifiable claim to a blockchain, the process further comprising:

receiving a permission sharing request sent by the service device, wherein the permission sharing request is sent based on a query request sent by the supervision organization, and the permission sharing request comprises the first identification

information associated with the behavior data to be queried; and

performing permission sharing processing based on the permission sharing request to grant the supervision organization the access permission for the behavior data associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data, wherein the permission sharing request further comprises: third digital identity information of the supervision organization;

the performing permission sharing processing based on the permission sharing request comprises:

obtaining the associated first verifiable claim from the blockchain based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the blockchain, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the blockchain based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a blockchain comprises:

encrypting the first key based on the public key corresponding to the obtained second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the blockchain.

25. A storage medium for storing computer-executable instructions that, when executed, implement the following process:

receiving a service processing request sent by a client device, wherein the service processing request comprises behavior data of an operational behavior of a first user in the client device corresponding to a service to be processed;

performing corresponding service processing based on the service processing request, and obtaining authorization information on an operation permission for the behavior data granted by the first user to a service device; and

sending an authorization request to an identity management system based on the authorization information, the behavior data, obtained first digital identity information of the first user, and second digital identity information of the service device, such that the identity management system saves a first verifiable claim generated based on the behavior data, the authorization information, the first digital identity information, and the second digital identity information to a blockchain, and a supervision organization, when granted an access permission of the first verifiable claim, backtracks the operational behavior of the first user corresponding to the service to be processed based on the first verifiable claim in the blockchain, wherein the first verifiable claim is used to prove that the service device is granted the operation permission,

wherein the authorization request further comprises: first identification information of service data of the service to be processed

wherein the first verifiable claim is generated by generating first ciphertext data of the behavior data based on a predetermined encryption method, and generating the first verifiable claim based on the first identification information, the first ciphertext data, the authorization information, the first digital identity information, and the second digital identity information,

wherein after the identity management system saves the first verifiable claim to the blockchain, the process further comprising:

receiving a permission sharing request sent by the service device, wherein the permission sharing request is sent based on a query request sent by the supervision organization, and the permission sharing request comprises the first identification information associated with the behavior data to be queried; and

performing permission sharing processing based on the permission sharing request

to grant the supervision organization the access permission for the behavior data associated with the first identification information, such that the supervision organization backtracks the operational behavior of the first user corresponding to the service to be processed based on the behavior data;

wherein the permission sharing request further comprises: third digital identity information of the supervision organization;

the performing permission sharing processing based on the permission sharing request comprises:

obtaining the associated first verifiable claim from the blockchain based on the first identification information;

generating second ciphertext data based on the obtained first verifiable claim and a public key corresponding to the third digital identity information; and

associatively saving the second ciphertext data and the third digital identity information to the blockchain, and sending permission sharing success information to the service device, such that the service device sends query acknowledgment information to the supervision organization, and the supervision organization obtains the associated second ciphertext data from the blockchain based on the third digital identity information, and performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data; or,

sending the second ciphertext data to the supervision organization such that the supervision organization performs decryption based on the second ciphertext data and a private key corresponding to the third digital identity information to obtain the behavior data, and sending permission sharing success information to the service device,

wherein the generating first ciphertext data of the behavior data based on a predetermined encryption method comprises:

determining a first key of the service device;

encrypting the behavior data based on the first key to obtain the first ciphertext data;

the saving the first verifiable claim to a blockchain comprises:

encrypting the first key based on the public key corresponding to the obtained second digital identity information to obtain third ciphertext data; and

associatively saving the third ciphertext data and the first verifiable claim to the blockchain.