CLAIMS

What is claimed is:

1. A matching method based on trusted asset data, comprising:

obtaining asset description information of a first entity, the asset description information being obtained by analyzing trusted asset data of the first entity, and the trusted asset data being stored on a trusted device;

obtaining service information of each second entity;

determining target service information matched with the first entity based on the asset description information and the service information of each second entity, wherein, in the determining, the trusted asset data of the first entity is not out of domain of the trusted device, the determining is performed using the asset description information rather than the trusted asset data; and

sending the target service information to the first entity.

2. The method according to claim 1, wherein the determining target service information matched with the first entity based on the asset description information and the service information of each second entity specifically comprises:

analyzing the asset description information of the first entity to obtain a data feature corresponding to the asset description information; and

matching the service information of each second entity based on the data feature to obtain target service information matched with the first entity.

3. The method according to claim 1, before the obtaining asset description information of a first entity, further comprising:

obtaining trusted asset data published by the first entity in a blockchain network; and

analyzing the trusted asset data to obtain asset description information of the first entity.

4. The method according to claim 1, wherein the obtaining asset description information of a first entity specifically comprises:

obtaining asset description information published by the first entity in a blockchain network.

5. The method according to claim 3 or 4, wherein the asset description information is stored in a decentralized identifiers document corresponding to the first entity.

6. The method according to claim 1, after the determining target service information matched with the first entity based on the asset description information and the service information of each second entity, further comprising:

determining one or more second entities supporting the target service information; and

sending the service information of the first entity to the one or more second entities supporting the target service information.

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

receiving a first service request sent by an end-user device of the first entity;

determining a service type requested by the first service request;

determining target service information matched with the service type from the service information of each second entity based on the service type; and

sending the target service information to the first entity, the target service information at least comprising an entity information list of each entity of the target service information.

8. The method according to claim 7, after the sending the target service information to the first entity, further comprising:

determining a target entity selected by the first entity from the entity information list; and

sending the trusted asset data of the target entity to the first entity.

9. The method according to claim 8, after the determining a target entity selected by the first entity from the entity information list, further comprising:

obtaining a second service request sent by the first entity;

receiving asset description information returned by the target entity and needed to be provided by the first entity;

obtaining asset description information provided by the first entity; and

sending the asset description information provided by the first entity to the target entity for verification.

10. The method according to claim 9, after the sending the asset description information provided by the first entity to the target entity for verification, further comprising:

sending a verifiable claim returned by the target entity to the first entity after the asset description information is approved, the verifiable claim being used to authorize the first entity to obtain the trusted asset data of the target entity.

11. The method according to claim 9, after the sending the asset description information provided by the first entity to the target entity for verification, further comprising:

sending the trusted asset data of the target entity to the first entity after the asset description information is approved; and

deleting the trusted asset data stored in a device of the target entity after the trusted asset data is sent to the first entity.

12. A matching apparatus based on trusted asset data, comprising:

an asset description information acquisition module, configured to obtain asset description information of a first entity, the asset description information being obtained by analyzing trusted asset data of the first entity, and the trusted asset data being stored on a trusted device;

a service information acquisition module, configured to obtain service information of each second entity;

a target service information matching module, configured to determine target service information matched with the first entity based on the asset description information and the service information of each second entity, wherein, in the determine, the trusted asset data of the first entity is not out of domain of the trusted device, the determine is performed using the asset description information rather than the trusted asset data; and

an information sending module, configured to send the target service information to the first entity.

13. The apparatus according to claim 12, wherein the target service information matching module specifically comprises:

a data feature extraction unit, configured to analyze the asset description information of the first entity to obtain a data feature corresponding to the asset description information; and

a matching unit, configured to match the service information of each second entity based on the data feature to obtain target service information matched with the first entity.

14. The apparatus according to claim 12, wherein the apparatus further comprises:

a trusted asset data acquisition module, configured to obtain trusted asset data published by the first entity in a blockchain network; and

an analysis module, configured to analyze the trusted asset data to obtain asset

description information of the first entity.

15. The apparatus according to claim 12, wherein the apparatus further comprises:

a second entity determination module, configured to determine one or more second entities supporting the target service information; and

a service information sending module, configured to send the service information of the first entity to the one or more second entities supporting the target service information.

16. The apparatus according to claim 12, wherein the apparatus is further configured to:

receive a first service request sent by an end-user device of the first entity;

determine a service type requested by the first service request;

determine target service information matched with the service type from the service information of each second entity based on the service type; and

send the target service information to the first entity, the target service information at least comprising an entity information list of each entity of the target service information.

17. The apparatus according to claim 16, wherein the apparatus further comprises:

a target entity selection module, configured to determine a target entity selected by the first entity from the entity information list; and

a sending module, configured to send the trusted asset data of the target entity to the first entity.

18. The apparatus according to claim 17, wherein the apparatus further comprises:

a second service request acquisition module, configured to obtain a second service request sent by the first entity;

an asset description information determination module, configured to receive asset description information returned by the target entity and needed to be provided by the first entity;

an asset description information receiving module, configured to obtain asset description information provided by the first entity; and

a verification module, configured to send the asset description information provided by the first entity to the target entity for verification.

19. The apparatus according to claim 18, wherein the apparatus further comprises:

a verifiable claim sending module, configured to send a verifiable claim returned by the target entity to the first entity after the asset description information is approved,

the verifiable claim being used to authorize the first entity to obtain the trusted asset data of the target entity.

20. The apparatus according to claim 18, wherein the apparatus further comprises:

a trusted asset data sending module, configured to send the trusted asset data of the target entity to the first entity after the asset description information is approved; and

a trusted asset data deletion module, configured to delete the trusted asset data stored in a device of the target entity after the trusted asset data is sent to the first entity.

21. A matching device based on trusted asset data, comprising:

at least one processor; and

a memory communicably coupled to the at least one processor, wherein

the memory stores instructions executable by the at least one processor, and the instructions are executed by the at least one processor so that the at least one processor can:

obtain asset description information of a first entity, the asset description information being obtained by analyzing trusted asset data of the first entity, and the trusted asset data being stored on a trusted device;

obtain service information of each second entity;

determine target service information matched with the first entity based on the asset description information and the service information of each second entity, wherein, in the determine, the trusted asset data of the first entity is not out of domain of the trusted device, the determine is performed using the asset description information rather than the trusted asset data; and

send the target service information to the first entity.

22. A computer-readable medium, wherein computer-readable instructions are stored on the computer-readable medium, and the computer-readable instructions can be executed by a processor to implement the matching method based on trusted asset data according to any one of claims 1 to 11.