CLAIMS

1. A method for blockchain-based access control of Software Defined Perimeter (SDP), comprising:

transmitting, by an SDP connection accepting host, to-be-verified information to a blockchain system node, the to-be-verified information comprising host information and a supported connection policy of the SDP connection accepting host, so that the to-be-verified information will be verified by the blockchain system node, and be recorded into a blockchain ledger after the verification is successful;

receiving, by the SDP connection accepting host, a connection request transmitted by an SDP connection initiating host, the connection request comprising signature information made by the blockchain system node for the SDP connection accepting host in a list of SDP connection accepting hosts; and

verifying, by the SDP connection accepting host, the signature information according to the supported connection policy when the SDP connection accepting host is in the list of SDP connection accepting hosts, and transmitting, by the SDP connection accepting host, a request response to the SDP connection initiating host after the verification is successful,

wherein the supported connection policy comprises a blockchain node verification or endorsement policy, the signature information made by the blockchain system node for the SDP connection accepting host in the list of SDP connection accepting hosts comprises signatures made by one or more blockchain system nodes, the one or more blockchain system nodes are determined according to the blockchain node verification or endorsement policy, and verifying, by the SDP connection accepting host, the signature information according to the supported connection policy comprises:

verifying, by the SDP connection accepting host, whether the signature information is generated by the one or more blockchain system nodes determined according to the blockchain node verification or endorsement policy.

2. The method for blockchain-based access control of SDP of claim 1, wherein the host information of the SDP connection accepting host comprises at least one of: an Internet Protocol (IP) address, a port, or protocol information; and the supported connection policy further comprises at least one of: a login identity (ID), an IP address or a geographic location of an access user.

3. The method for blockchain-based access control of SDP of claim 1, wherein the to-be-verified information further comprises a signature of the SDP connection accepting host for the host information and the supported connection policy.

4. A method for blockchain-based access control of Software Defined Perimeter (SDP), comprising:

receiving, by a blockchain system node, to-be-verified information transmitted by an SDP connection accepting host, the to-be-verified information comprising host information and a supported connection policy of the SDP connection accepting host, wherein the supported connection policy comprises a blockchain node verification or endorsement policy;

verifying, by the blockchain system node, the to-be-verified information and recording the information into a blockchain ledger after the verification is successful;

receiving, by the blockchain system node, an identity authentication request submitted by an SDP connection initiating host; and

verifying, by the blockchain system node, the identity authentication request, searching in a blockchain, by the blockchain system node, for a list of SDP connection accepting hosts accessible to the SDP connection initiating host after the verification is successful, and returning, by the blockchain system node, the list of SDP connection accepting hosts with signature information to the SDP connection initiating host, wherein the signature information made by the blockchain system node for an SDP connection accepting host in the list of SDP connection accepting hosts comprises signatures made by one or more blockchain system nodes, and the one or more blockchain system nodes are determined according to the blockchain node verification or endorsement policy.

5. The method for blockchain-based access control of SDP of claim 4, wherein the to-be-verified information further comprises a signature of the SDP connection accepting host for the host information and the supported connection policy.

6. The method for blockchain-based access control of SDP of claim 4, wherein when the SDP connection initiating host signs a timestamp with its own private key in the identity authentication request, verifying, by the blockchain system node, the identity authentication request comprises:

verifying, by the blockchain system node, the signature and timestamp submitted by the SDP connection initiating host.

7. The method for blockchain-based access control of SDP of claim 4, wherein when the identity authentication request comprises a Key Derivation Function (KDF) or encrypted information of the KDF with a public key of an authentication node A1, verifying, by the blockchain system node, the identity authentication request comprises:

verifying, by the blockchain system node, whether the KDF is correct.

8. The method for blockchain-based access control of SDP of claim 4, wherein when the identity authentication request comprises a token or encrypted information of the token with a public key of an authentication node A2, verifying, by the blockchain system node, the identity authentication request comprises:

verifying, by the blockchain system node, whether the token is correct.

9. A method for blockchain-based access control of Software Defined Perimeter (SDP), comprising:

transmitting, by an SDP connection initiating host, an identity authentication request to a blockchain system node;

receiving, by the SDP connection initiating host, a list of SDP connection accepting hosts accessible to the SDP connection initiating host with signature information transmitted by the blockchain system node;

transmitting, by the SDP connection initiating host, a connection request to an SDP connection accepting host in the list of SDP connection accepting hosts, the connection request comprising the signature information made by the blockchain system node for the SDP connection accepting host in the list of SDP connection accepting hosts, wherein the signature information made by the blockchain system node for the SDP connection accepting host in the list of SDP connection accepting hosts comprises signatures made by one or more blockchain system nodes, and the one or more blockchain system nodes are determined according to a blockchain node verification or endorsement policy of the SDP connection accepting host; and

receiving, by the SDP connection initiating host, a request response transmitted by the SDP connection accepting host.

10. The method for blockchain-based access control of SDP of claim 9, wherein the SDP connection initiating host signs a timestamp with its own private key in the identity authentication request.

11. The method for blockchain-based access control of SDP of claim 9, wherein when the SDP connection initiating host and an authentication node A1 share a user name and secret information, the identity authentication request comprises a KDF or encrypted information of the KDF with a public key of the authentication node A1.

12. The method for blockchain-based access control of SDP of claim 9, wherein when the SDP connection initiating host has a token provided by an authentication node A2, the identity authentication request comprises the token or encrypted information of the token with a public

key of the authentication node A2.

13. A system for blockchain-based access control of Software Defined Perimeter (SDP), comprising:

a first information verification module, configured to transmit to-be-verified information to a blockchain system node, the to-be-verified information comprising host information and a supported connection policy of an SDP connection accepting host, so that the to-be-verified information will be verified by the blockchain system node, and be recorded into a blockchain ledger after the verification is successful;

a first connection request module, configured to receive a connection request transmitted by an SDP connection initiating host, the connection request comprising signature information made by the blockchain system node for the SDP connection accepting host in a list of SDP connection accepting hosts; and

a first request response module, configured to verify the signature information according to the supported connection policy when the SDP connection accepting host is in the list of SDP connection accepting hosts, and transmit a request response to the SDP connection initiating host after the verification is successful,

wherein the supported connection policy comprises a blockchain node verification or endorsement policy, the signature information made by the blockchain system node for the SDP connection accepting host in the list of SDP connection accepting hosts comprises signatures made by one or more blockchain system nodes, the one or more blockchain system nodes are determined according to the blockchain node verification or endorsement policy, and the first request response module is specifically configured to:

verify whether the signature information is generated by the one or more blockchain system nodes determined according to the blockchain node verification or endorsement policy.

14. A system for blockchain-based access control of Software Defined Perimeter (SDP), comprising:

a second information verification module, configured to: receive to-be-verified information transmitted by an SDP connection accepting host, the to-be-verified information comprising host information and a supported connection policy of the SDP connection accepting host, and the supported connection policy comprising a blockchain node verification or endorsement policy; and verify the to-be-verified information and record the information into a blockchain ledger after the verification is successful;

a first identity authentication request module, configured to receive an identity authentication request submitted by an SDP connection initiating host; and

a verification feedback module, configured to: verify the identity authentication request; search, in a blockchain, for a list of SDP connection accepting hosts accessible to the SDP connection initiating host after the verification is successful; and return the list of SDP connection accepting hosts with signature information to the SDP connection initiating host, wherein the signature information made by a blockchain system node for an SDP connection accepting host in the list of SDP connection accepting hosts comprises signatures made by one or more blockchain system nodes, and the one or more blockchain system nodes are determined according to the blockchain node verification or endorsement policy.

15. A system for blockchain-based access control of Software Defined Perimeter (SDP), comprising:

a second identity authentication request module, configured to transmit an identity authentication request to a blockchain system node, and receive a list of SDP connection accepting hosts accessible to an SDP connection initiating host with signature information transmitted by the blockchain system node;

a second connection request module, configured to transmit a connection request to an SDP connection accepting host in the list of SDP connection accepting hosts, the connection request comprising the signature information made by the blockchain system node for the SDP connection accepting host in the list of SDP connection accepting hosts, wherein the signature information made by the blockchain system node for the SDP connection accepting host in the list of SDP connection accepting hosts comprises signatures made by one or more blockchain system nodes, and the one or more blockchain system nodes are determined according to a

blockchain node verification or endorsement policy of the SDP connection accepting host; and

a second request response module, configured to receive a request response transmitted by the SDP connection accepting host.

16. A Software Defined Perimeter (SDP) connection accepting host, comprising a processor and a memory having stored thereon a program executable on the processor, wherein the processor is configured to implement steps of the method for blockchain-based access control of SDP of any one of claims 1 to 3 when the program is executed by the processor.

17. A blockchain system node, comprising a processor and a memory having stored thereon a program executable on the processor, wherein the processor is configured to implement steps of the method for blockchain-based access control of SDP of any one of claims 4 to 8 when the program is executed by the processor.

18. A Software Defined Perimeter (SDP) connection initiating host, comprising a processor and a memory having stored thereon a program executable on the processor, wherein the processor is configured to implement steps of the method for blockchain-based access control of SDP of any one of claims 9 to 12 when the program is executed by the processor.