in the blockchain network. The research found that when consensus processing is being performed on service data, the duration of the consensus processing is lengthened as more blockchain nodes participate in the consensus processing. Consequently, the efficiency of the consensus processing performed on the service data is reduced.

SUMMARY

[0005] In view of this, implementations of the present application provide a blockchain consensus method and device to alleviate the problem of low consensus processing efficiency in the existing technology.

[0006] The following technical solutions are adopted in the implementations of the present application.

[0007] An implementation of the present application provides a blockchain consensus method, including the following: obtaining, by a blockchain node, service data to be performed a consensus procedure on, and determining a service type of the service data; selecting, by the blockchain node from a consensus network based on the service type, at least one consensus node that provides a consensus service; and sending, by the blockchain node, the service data to the selected consensus node so that the selected consensus node performs consensus processing on the service data.

[0007a] According to an embodiment of the present application, there is provided a blockchain consensus method including the following: obtaining, by a blockchain node of a blockchain network, service data on which to perform consensus processing, the service data comprising data generated with a request of a service, the blockchain network comprising a plurality of blockchain nodes; classifying, by the blockchain node, the service data based on a service function and a service content of the service, wherein the service function comprises a function to be performed using the service data and the service content defines an item processed by the service function; determining, by the blockchain node, a service type of the service data based on classifying the service data and based on a vulnerability of the service data, wherein the vulnerability of the service data indicates whether the service data is vulnerable or invulnerable to an attack; determining, by the blockchain node, a consensus policy based on a predetermined mapping relationship between the consensus policy and the service type, wherein the consensus policy comprises a

method of performing consensus processing on the service data; identifying, by the blockchain node, based on the consensus policy, a consensus algorithm that comprises a respective set of operating principles defining a consensus service for the service type; identifying, by the blockchain node, based on the consensus algorithm, a minimum number of consensus nodes to perform a round of consensus processing, wherein the minimum number of consensus nodes comprises a percentage of all available consensus nodes within the blockchain network required by the consensus algorithm to process the service data; selecting, by the blockchain node from a consensus network based on the consensus policy, the minimum number of consensus nodes that provides the consensus service corresponding to the service type; sending, by the blockchain node, the service data to the minimum number of consensus nodes; and performing, by the minimum number of consensus nodes, the consensus service on the service data. Further embodiments of the present application also provide a non-transitory, computer-readable medium storing instructions executable by a computer system to perform operations in accordance with the above method, as well as a computer-implemented system including one or more computers and one or more memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing instructions when executed by the one or more computers to perform operations in accordance with the above method.

[0008] An implementation of the present application further provides a blockchain consensus device, including an acquisition unit, a selection unit, and a sending unit, where the acquisition unit obtains service data to be performed a consensus procedure on, and determines a service type of the service data; the selection unit selects, from a consensus network based on the service type, at least one consensus node that provides a consensus service; and the sending unit sends the service data to the selected consensus node so that the selected consensus node performs consensus processing on the service data.

[0009] An implementation of the present application further provides a blockchain consensus device, including a memory and at least one processor, where the memory stores a program, and the at least one processor is configured to perform the following steps: obtaining service data to be performed a consensus procedure on, and determining a service type of the service data; selecting, from a consensus network based on the service type, at least one consensus node that provides a

CLAIMS

What is claimed is:

1. A blockchain consensus method, comprising:

obtaining, by a blockchain node of a blockchain network, service data on which to perform consensus processing, the service data comprising data generated with a request of a service, the blockchain network comprising a plurality of blockchain nodes;

classifying, by the blockchain node, the service data based on a service function and a service content of the service, wherein the service function comprises a function to be performed using the service data and the service content defines an item processed by the service function;

determining, by the blockchain node, a service type of the service data based on classifying the service data and based on a vulnerability of the service data, wherein the vulnerability of the service data indicates whether the service data is vulnerable or invulnerable to an attack;

determining, by the blockchain node, a consensus policy based on a predetermined mapping relationship between the consensus policy and the service type, wherein the consensus policy comprises a method of performing consensus processing on the service data;

identifying, by the blockchain node, based on the consensus policy, a consensus algorithm that comprises a respective set of operating principles defining a consensus service for the service type;

identifying, by the blockchain node, based on the consensus algorithm, a minimum number of consensus nodes to perform a round of consensus processing, wherein the minimum number of consensus nodes comprises a percentage of all available consensus nodes within the blockchain network required by the consensus algorithm to process the service data;

selecting, by the blockchain node from a consensus network based on the consensus policy, the minimum number of consensus nodes that provides the consensus service corresponding to the service type;

sending, by the blockchain node, the service data to the minimum number of consensus nodes; and

performing, by the minimum number of consensus nodes, the consensus service on the service data.

2. The blockchain consensus method according to claim 1, wherein the minimum number of consensus nodes that provides the consensus service comprises a portion of the available consensus nodes within the blockchain network that is smaller than all of the available consensus nodes within the blockchain network for the service data that is invulnerable to the attack.

3. The blockchain consensus method according to claim 1, wherein selecting, by the blockchain node from the consensus network based on the consensus algorithm, the minimum number of consensus nodes that provides the consensus service comprises:

determining, by the blockchain node based on the consensus algorithm, a quantity of consensus nodes to participate in the consensus processing of the service data, wherein the quantity of consensus nodes satisfies a predetermined quantity of the consensus algorithm; and

selecting, by the blockchain node, the quantity of consensus nodes from the consensus network.

4. The blockchain consensus method according to claim 3, wherein selecting, by the blockchain node, the quantity of consensus nodes from the consensus network comprises:

randomly selecting, by the blockchain node, the quantity of consensus nodes from the consensus network; or

selecting, by the blockchain node, the quantity of consensus nodes from the consensus network based on a load of consensus nodes in the consensus network.

5. The blockchain consensus method according to claim 1, wherein the consensus algorithm comprises a Proof of Work algorithm, a Proof of Stake algorithm, a Delegated Proof of Stake algorithm, a Practical Byzantine Fault Tolerance algorithm, or a Delegated Byzantine Fault Tolerance algorithm.

6. The blockchain consensus method according to claim 1, wherein, before sending, by the blockchain node, the service data to the minimum number of consensus nodes, the method further comprises:

broadcasting, by the blockchain node, the minimum number of consensus nodes to other blockchain nodes so that the other blockchain nodes vote on whether to agree that the minimum number of consensus nodes provides the consensus service; and

wherein sending, by the blockchain node, the service data to the minimum number of consensus nodes comprises:

sending, by the blockchain node, the service data to the minimum number of consensus nodes in response to receiving consensus reaching messages sent by the other blockchain nodes.

7. The blockchain consensus method according to claim 6, further comprising:

in response to receiving a consensus result sent by the minimum number of consensus nodes for the service data, and in response to determining a need to globally share the consensus result, sending, by the blockchain node, the consensus result to a consensus node that does not participate in the consensus processing in the consensus network, and storing the consensus result for the service data to a blockchain.

8. The blockchain consensus method according to claim 6, further comprising:

in response to receiving a consensus result sent by the minimum number of consensus nodes for the service data, determining whether the consensus result for the service data is assigned to global sharing; and

in response to determining that the consensus result for the service data is not assigned to global sharing, storing, by the blockchain node, the consensus result to a blockchain in response to determining a need to not globally share the consensus result.

9. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system comprising one or more processors to perform operations comprising:

obtaining, by a blockchain node of a blockchain network, service data on which to perform consensus processing, the service data comprising data generated with a request of a service, the blockchain network comprising a plurality of blockchain nodes;

classifying, by the blockchain node, the service data based on a service function

and a service content of the service, wherein the service function comprises a function to be performed using the service data and the service content defines an item processed by the service function;

determining, by the blockchain node, a service type of the service data based on classifying the service data and based on a vulnerability of the service data, wherein the vulnerability of the service data indicates whether the service data is vulnerable or invulnerable to an attack;

determining, by the blockchain node, a consensus policy based on a predetermined mapping relationship between the consensus policy and the service type, wherein the consensus policy comprises a method of performing consensus processing on the service data;

identifying, by the blockchain node, based on the consensus policy, a consensus algorithm that comprises a respective set of operating principles defining a consensus service for the service type;

identifying, by the blockchain node, based on the consensus algorithm, a minimum number of consensus nodes to perform a round of consensus processing, wherein the minimum number of consensus nodes comprises a percentage of all available consensus nodes within the blockchain network required by the consensus algorithm to process the service data;

selecting, by the blockchain node from a consensus network based on the consensus policy, the minimum number of consensus nodes that provides the consensus service corresponding to the service type;

sending, by the blockchain node, the service data to the minimum number of consensus nodes; and

performing, by the minimum number of consensus nodes, the consensus service on the service data.

10. The non-transitory, computer-readable medium according to claim 9, wherein the minimum number of consensus nodes that provides the consensus service comprises a portion of the available consensus nodes within the blockchain network that is smaller than all of the available consensus nodes within the blockchain network for the service data that is invulnerable to the attack.

11. The non-transitory, computer-readable medium according to claim 9, wherein

selecting the minimum number of consensus nodes that provides the consensus service comprises:

determining, based on the consensus algorithm, a quantity of consensus nodes that are to participate in the consensus processing of the service data, wherein the quantity of consensus nodes satisfies a predetermined quantity of the consensus algorithm; and

selecting the quantity of consensus nodes from the consensus network.

12. The non-transitory, computer-readable medium according to claim 11, wherein selecting the quantity of consensus nodes from the consensus network comprises:

randomly selecting the quantity of consensus nodes from the consensus network; or

selecting the quantity of consensus nodes from the consensus network based on a load of consensus nodes in the consensus network.

13. The non-transitory, computer-readable medium according to claim 9, wherein the consensus algorithm comprises a Proof of Work algorithm, a Proof of Stake algorithm, a Delegated Proof of Stake algorithm, a Practical Byzantine Fault Tolerance algorithm, or a Delegated Byzantine Fault Tolerance algorithm.

14. The non-transitory, computer-readable medium according to claim 9, the operations further comprising:

broadcasting the minimum number of consensus nodes to other blockchain nodes before the service data is sent to the minimum number of consensus nodes, so that the other blockchain nodes vote on whether to agree that the minimum number of consensus nodes provides the consensus service; and

wherein sending the service data to the selected minimum number of consensus nodes comprises:

sending the service data to the minimum number of consensus nodes in response to receiving consensus reaching messages sent by the other blockchain nodes.

15. The non-transitory, computer-readable medium according to claim 14, the operations further comprising:

in response to determining that a consensus result sent by the minimum number of consensus nodes for the service data is received, and in response to determining a need to globally share the consensus result, sending the consensus result for the service data to a consensus node that does not participate in the consensus processing in the consensus network, and storing the consensus result for the service data to a blockchain.

16. The non-transitory, computer-readable medium according to claim 14, the operations further comprising:

in response to determining that a consensus result sent by the minimum number of consensus nodes for the service data is received, storing the consensus result for the service data to a blockchain in response to determining a need to not globally share the consensus result.

17. A computer-implemented system comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

obtaining, by a blockchain node of a blockchain network, service data on which to perform consensus processing, the service data comprising data generated with a request of a service, the blockchain network comprising a plurality of blockchain nodes;

classifying, by the blockchain node, the service data based on a service function and a service content of the service, wherein the service function comprises a function to be performed using the service data and the service content defines an item processed by the service function;

determining, by the blockchain node, a service type of the service data based on classifying the service data and based on a vulnerability of the service data, wherein the vulnerability of the service data indicates whether the service data is vulnerable or invulnerable to an attack;

determining, by the blockchain node, a consensus policy based on a predetermined mapping relationship between the consensus policy and the service

type, wherein the consensus policy comprises a method of performing consensus processing on the service data;

identifying, by the blockchain node, based on the consensus policy, a consensus algorithm that comprises a respective set of operating principles defining a consensus service for the service type;

identifying, by the blockchain node, based on the consensus algorithm, a minimum number of consensus nodes to perform a round of consensus processing, wherein the minimum number of consensus nodes comprises a percentage of all available consensus nodes within the blockchain network required by the consensus algorithm to process the service data;

selecting, by the blockchain node from a consensus network based on the consensus policy, the minimum number of consensus nodes that provides the consensus service corresponding to the service type;

sending, by the blockchain node, the service data to the minimum number of consensus nodes; and

performing, by the minimum number of consensus nodes, the consensus service on the service data.