WHAT IS CLAIMED IS:

1. A method for processing an ethereum-based falsified transaction, wherein the method is performed by a computer comprising a processor and a memory storing a program to be executed by the processor, and the method comprises:

sending, by the processor, a falsified transaction to a preset node in an ethereum network, such that the preset node broadcasts a block including the falsified transaction to all nodes in the ethereum network; and

determining, by the processor, whether the falsified transaction successfully attacks the ethereum network based on information on a chain maintained by the node in the ethereum network.

2. The method according to claim 1, wherein the determining whether the falsified transaction successfully attacks the ethereum network based on information on a chain maintained by the node in the ethereum network comprises:

sending, by the processor, requests for acquiring block information to the preset node and a non-set node in the ethereum network respectively, the requests for acquiring block information being configured for acquiring a last piece of block information on the chain maintained by the node;

receiving, by the processor, a first piece of block information returned by the preset node and a second piece of block information returned by the non-set node, and comparing header information of the first piece of block information with header information of the second piece of block information to determine whether the header information of the first piece of block information is identical to the header information of the second piece of block information;

determining, by the processor, the falsified transaction

successfully attacking the ethereum network, when the header information of the first piece of block information is identical to the header information of the second piece of block information; and

determining, by the processor, the falsified transaction failing to attack the ethereum network, when the header information of the first piece of block information is different from the header information of the second piece of block information.

3. The method according to claim 1, wherein the determining whether the falsified transaction successfully attacks the ethereum network based on information on a chain maintained by the node in the ethereum network comprises:

sending, by the processor, a transaction information request to the non-set node in the ethereum network, the transaction information request comprising an identifier of the falsified transaction;

receiving, by the processor, a response message returned by the non-set node, and viewing whether the response message includes information of the falsified transaction;

determining, by the processor, the falsified transaction successfully attacking the ethereum network, when the response message includes the information of the falsified transaction; and

determining, by the processor, the falsified transaction failing to attack the ethereum network, when the response message does not include the information of the falsified transaction.

4. A method for processing an ethereum-based falsified transaction, wherein the method is performed by a computer comprising a processor and a memory storing a program to be

executed by the processor, and the method comprises:

receiving, by the processor, a falsified transaction, and packing the falsified transaction into a block to obtain a block including the falsified transaction; and

broadcasting, by the processor, the obtained block to all nodes in an ethereum network where a present node broadcasting the obtained block is located, to determine whether the falsified transaction successfully attacks the ethereum network based on information on a chain maintained by the node in the ethereum network.

5. The method according to claim 4, wherein after the receiving a falsified transaction, the method further comprises:

broadcasting, by the processor, the falsified transaction to a preset node in the ethereum network.

6. The method according to claim 4, wherein after the broadcasting the obtained block to all nodes in an ethereum network where a present node broadcasting the obtained block is located, the method further comprises:

receiving, by the processor, a block broadcasted to the present node, and acquiring transaction information in the received block;

determining, by the processor, whether the transaction information in the received block is included in the transaction information on the chain maintained by the present node;

discarding, by the processor, the received block when the transaction information in the received block is included in the transaction information on the chain maintained by the present node;

acquiring, by the processor, header signature in the received block when the transaction information in the

received block is not included in the transaction information on the chain maintained by the present node;

determining, by the processor, whether a node identifier in the header signature is included in a preset node identifier; and

incorporating, by the processor, the received block onto the chain maintained by the present node, when the node identifier in the header signature is included in the preset node identifier.

7. An apparatus for processing an ethereum-based falsified transaction, the apparatus comprising:

a sending unit configured to send a falsified transaction to a preset node in an ethereum network, such that the preset node broadcasts a block including the falsified transaction to all nodes in the ethereum network; and

a processing unit configured to determine whether the falsified transaction successfully attacks the ethereum network based on information on a chain maintained by the node in the ethereum network.

8. The apparatus according to claim 7, wherein

the sending unit is further configured to send requests for acquiring block information to the preset node and a non-set node in the ethereum network respectively, the requests for acquiring block information being configured for acquiring a last piece of block information on the chain maintained by the node;

the apparatus further comprises: a receiving unit configured to receive a first piece of block information returned by the preset node and a second piece of block information returned by the non-set node; and

the processing unit is further configured to compare

header information of the first piece of block information with header information of the second piece of block information to determine whether the header information of the first piece of block information is identical to the header information of the second piece of block information;

determine the falsified transaction successfully attacking the ethereum network, when the header information of the first piece of block information is identical to the header information of the second piece of block information; and

determine the falsified transaction failing to attack the ethereum network, when the header information of the first piece of block information is different from the header information of the second piece of block information.

9. The apparatus according to claim 7, wherein

the sending unit is further configured to send a transaction information request to the non-set node in the ethereum network, the transaction information request comprising an identifier of the falsified transaction;

the apparatus further comprises: a receiving unit configured to receive a response message returned by the non-set node; and

the processing unit is further configured to view whether the response message includes information of the falsified transaction;

determine the falsified transaction successfully attacking the ethereum network, when the response message includes the information of the falsified transaction; and

determine the falsified transaction failing to attack the ethereum network, when the response message does not include the information of the falsified transaction.

10. An apparatus for processing an ethereum-based falsified transaction, comprising:

a receiving unit configured to receive a falsified transaction;

a processing unit configured to pack the falsified transaction into a block to obtain a block including the falsified transaction; and

a sending unit configured to broadcast the obtained block to all nodes in an ethereum network where a present node broadcasting the obtained block is located, to determine whether the falsified transaction successfully attacks the ethereum network based on information on a chain maintained by the node in the ethereum network.

11. The apparatus according to claim 10, wherein the sending unit is further configured to broadcast the falsified transaction to a preset node in the ethereum network.

12. The apparatus according to claim 10, wherein

the receiving unit is further configured to receive a block broadcasted to the present node, and acquire transaction information in the received block; and

the processing unit is further configured to determine whether the transaction information in the block is included in the transaction information on the chain maintained by the present node; discard the received block when the transaction information in the received block is included in the transaction information on the chain maintained by the present node; acquire header signature in the received block when the transaction information in the received block is not included in the transaction information on the chain maintained by the present node; determine whether a node identifier in the header signature is included in a preset node identifier; and

incorporate the received block onto the chain maintained by the present node, when the node identifier in the header signature is present in the preset node identifier.

13. A storage medium, storing an instruction, the instruction, when executed by a computer, causing the computer to execute at least one of the method for processing an ethereum-based falsified transaction according to claim 1, or the method for processing an ethereum-based falsified transaction according to claim 6.