BLOCK PROCESSING METHODS, NODE AND SYSTEM

[0001] This application claims priority to Chinese Patent Application No. 201910345985.4, entitled "BLOCK PROCESSING METHODS, NODE AND SYSTEM" filed on April 26, 2019, which is incorporated by reference in its entirety.

FIELD OF THE TECHNOLOGY

[0002] The present disclosure relates to the field of computer technologies, and in particular, to a block processing method, a node, and a system.

BACKGROUND OF THE DISCLOSURE

[0003] A user may initiate a transaction through a client, and all transaction information recorded during the transaction is packaged into a block for storage. With the continuous transactions, blocks are linked to each other to form a blockchain, which is also referred to as a ledger. The blockchain is an open network ledger, and may include a plurality of blocks. The blockchain may be formed in a plurality of forms, such as a public chain, a private chain, and an alliance chain. The public chain may include a Bitcoin series, an Ethereum series, or the like.

[0004] Currently, a block generation method for the public chain may specifically include the following procedure.

[0005] After a new transaction arrives at a node (for example, a node 1) in the blockchain, the node 1 first verifies whether the transaction is valid, then puts a valid transaction in a local transaction pool, and broadcasts transaction information to other nodes in the blockchain.

[0006] After a new block generation cycle arrives, the node 1 obtains a transaction list from the transaction pool, then packages the transaction list as a candidate block, and after adding a signature to the candidate bloc, broadcasts the candidate block through the blockchain.

[0007] All nodes in the blockchain perform consensus on the received candidate block, and save the candidate block after a consensus is reached successfully. After that, the transaction in the candidate block is executed by the node 1.

[0008] In a case that the foregoing block generation method is applied to the public chain, security of underlying data of the blockchain can be ensured. However, in the alliance chain and the private chain, verification of security factors can be achieved in a plurality of layers, and is not limited to underlying data of the blockchain. In a case that the foregoing block generation method is applied to the alliance chain or the private chain, the time required for block generation is too long, resulting in accumulation because transactions cannot be processed in time. Consequently, a congestion of the blockchain is caused.

SUMMARY

[0009] Embodiments of the present disclosure provide a block processing method, a node, and a system, to improve the speed of block generation and the performance of transaction processing.

[0010] The embodiments of the present disclosure provide the following solutions:

[0011] According to an aspect, an embodiments of the present disclosure provides a block processing method, the method being executed by a first node in a blockchain, the blockchain further including a second node, the first node being a leader node, the second node being a follower node, and the method including:

packaging, by the first node, first transaction information in a transaction queue of the first node into a candidate block, and broadcasting the candidate block through the blockchain;

performing, by the first node, verification on the first transaction information in the candidate block to generate a first verification result, and executing a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result;

broadcasting, by the first node, a first node processing result through the blockchain, the first node processing result including the first verification result and the first transaction execution result;

receiving, by the first node, a second node processing result broadcast by the second node through the blockchain, the second node processing result including: a second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and a second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block; and

performing, by the first node, consensus on the candidate block according to the first node processing result and the second node processing result, saving, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and saving the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0012] According to an aspect, an embodiment of the present disclosure provides a block processing method, the method being executed by a second node in a blockchain, the blockchain further including a first node, the first node being a leader node, the second node being a follower node, and the method including:

receiving, by the second node, a candidate block broadcast by the first node through the blockchain, and obtaining first transaction information from the candidate block;

performing, by the second node, verification on the first transaction information in the candidate block to generate a second verification result, and executing a transaction indicated by the first transaction information in the candidate block to generate a second transaction execution result;

broadcasting, by the second node, a second node processing result through the blockchain, the second node processing result including the second verification result and the second transaction execution result; and

saving, by the second node, the candidate block in a case that the first transaction information is verified successfully, and saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0013] According to an aspect, an embodiments of the present disclosure provides a block processing method, the method being executed by a first node in a blockchain, the blockchain further including a second node, the first node being a leader node, the second node being a follower node, and the method including:

putting, by the first node in response to at least one client transmitting transaction information to the blockchain, the transaction information transmitted by the client into a transaction queue of the first node;

checking, by the first node, whether the transaction queue meets a preset block generation condition;

packaging, by the first node in response to the transaction queue meeting the block generation condition, first transaction information in the transaction queue of the first node into a

candidate block, adding a signature to the candidate block, and broadcasting the candidate block through the blockchain;

performing, by the first node, verification on the first transaction information in the candidate block to generate a first verification result, and executing a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result;

adding, by the first node, a signature to a first node processing result, and then broadcasting the first node processing result through the blockchain, the first node processing result including: the first verification result and the first transaction execution result;

receiving, by the first node, a second node processing result broadcast by the second node through the blockchain, the second node processing result including: a second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and a second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block; and

performing, by the first node according to the first node processing result and the second node processing result, consensus on the candidate block by using a distributed consensus algorithm, then saving, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and saving the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0014] According to an aspect, an embodiment of the present disclosure provides a block processing method, the method being executed by a second node in a blockchain, the blockchain further including a first node, the first node being a leader node, the second node being a follower node, and the method including:

receiving, by the second node, a candidate block broadcast by the first node through the blockchain, and obtaining first transaction information from the candidate block;

performing, by the second node, verification on the first transaction information in the candidate block to generate a second verification result, and executing a transaction indicated by the first transaction information in the candidate block to generate a second transaction execution result;

adding, by the second node, a signature to a second node processing result, and broadcasting the second node processing result through the blockchain, the second node processing result including the second verification result and the second transaction execution result; and

saving, by the second node, the candidate block in a case that the first transaction information is verified successfully, and saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0015] According to an aspect, an embodiment of the present disclosure further provides a blockchain node, the blockchain node being a first node in a blockchain, the blockchain further including a second node, the first node being a leader node, the second node being a follower node, and the first node including: a processing module and a transceiver module,

the processing module being configured to package first transaction information in a transaction queue of the first node into a candidate block;

the transceiver module being configured to broadcast the candidate block through the blockchain;

the processing module being further configured to perform verification on the first transaction information in the candidate block to generate a first verification result, and execute a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result;

the transceiver module being further configured to broadcast a first node processing result through the blockchain, the first node processing result including the first verification result and the first transaction execution result;

the transceiver module being further configured to receive a second node processing result broadcast by the second node through the blockchain, the second node processing result including: a second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and a second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block; and

the processing module being further configured to perform consensus on the candidate block according to the first node processing result and the second node processing result, and save, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and save the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0016] According to an aspect, this embodiment of the present disclosure further provide a blockchain node, the blockchain node being a second node in a blockchain, the blockchain further

including a first node, the first node being a leader node, the second node being a follower node, and the second node including: a processing module and a transceiver module,

the transceiver module being configured to receive a candidate block broadcast by the first node through the blockchain;

the processing module being configured to obtain first transaction information from the candidate block;

the processing module being further configured to perform verification on the first transaction information in the candidate block to generate a second verification result, and execute a transaction indicated by the first transaction information in the candidate block to generate a second transaction execution result;

the transceiver module being further configured to broadcast a second node processing result through the blockchain, the second node processing result including the second verification result and the second transaction execution result; and

the processing module being further configured to save the candidate block in a case that the first transaction information is verified successfully, and save the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0017] According to an aspect, an embodiment of the present disclosure further provides a blockchain node, the blockchain node being a first node in a blockchain, the blockchain further including a second node, the first node being a leader node, the second node being a follower node, and the first node including: a processing module and a transceiver module,

the processing module being configured to put, in response to at least one client transmitting transaction information to the blockchain, the transaction information transmitted by the client into a transaction queue of the first node;

the processing module being configured to check whether the transaction queue meets a preset block generation condition;

the transceiver module being configured to package, in response to the transaction queue meeting the block generation condition, first transaction information in a transaction queue of the first node into a candidate block, add a signature to the candidate block, and broadcast the candidate block through the blockchain;

the processing module being configured to perform verification on the first transaction information in the candidate block to generate a first verification result, and execute a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result;

the transceiver module being configured to add a signature to a first node processing result, and then broadcast the first node processing result through the blockchain, the first node processing result including the first verification result and the first transaction execution result;

the transceiver module being configured to receive a second node processing result broadcast by the second node through the blockchain, the second node processing result including: a second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and a second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block; and

the processing module being configured to perform, according to the first node processing result and the second node processing result, consensus on the candidate block by using a distributed consensus algorithm, and then save the candidate block in a case that a consensus on the candidate block is reached successfully, and save the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0018] According to an aspect, this embodiment of the present disclosure further provide a blockchain node, the blockchain node being a second node in a blockchain, the blockchain further including a first node, the first node being a leader node, the second node being a follower node, and the second node including: a processing module and a transceiver module,

the transceiver module being configured to receive a candidate block broadcast by the first node through the blockchain, and obtain first transaction information from the candidate block;

the processing module being configured to perform verification on the first transaction information in the candidate block to generate a second verification result, and execute a transaction indicated by the first transaction information in the candidate block to generate a second transaction execution result;

the transceiver module being configured to add a signature a second node processing result, and then broadcast the second node processing result through the blockchain, the second

node processing result including the second verification result and the second transaction execution result; and

the processing module being configured to save the candidate block in a case that the first transaction information is verified successfully, and save the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0019] According to an aspect, an embodiment of the present disclosure provides a blockchain node, the blockchain node being a first node in a blockchain, the first node including: a processor and a memory, the memory being configured to store instructions; and the processor being configured to execute the instructions in the memory, causing the first node to perform the block processing method on a first node side.

[0020] According to an aspect, this embodiment of the present disclosure provides a blockchain node, the blockchain node being a second node in a blockchain, the second node including: a processor and a memory, the memory being configured to store instructions; and the processor being configured to execute the instructions in the memory, causing the second node to perform the block processing method on second node side.

[0021] According to an aspect, an embodiment of the present disclosure provides a block processing system, the block processing system including: a first node and a second node,

the first node being configured to perform the above block processing method on a first node side; and

the second node being configured to perform the above block processing method on a second node side.

[0022] According to an aspect, an embodiment of the present disclosure provides a computer-readable storage medium, the computer-readable storage medium storing instructions, when run on a computer, causing the computer to perform the method according to the foregoing aspects.

[0023] According to an aspect, an embodiment of the present disclosure provides a computer program product, when run on a computer, causing the computer to perform the foregoing method.

[0024] In the embodiments of the present disclosure, in a case that a first node is a leader node, and a second node is a follower node, the first node packages first transaction information in a transaction queue of the first node into a candidate block, and broadcasts the candidate block

through the blockchain. Then the first node performs verification on the first transaction information in the candidate block to generate a first verification result, and executes a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result. The first node broadcasts a first node processing result through the blockchain, the first node processing result including the first verification result and the first transaction execution result. The first node receives a second node processing result broadcast by the second node through the blockchain. The first node performs consensus on the candidate block according to the first node processing result and the second node processing result. Then the first node saves the candidate block in a case that a consensus on the candidate block is reached successfully, and saves the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully. In the embodiments of the present disclosure, the first node serves as the leader node. The first node may cache to-be-processed transaction information by using the transaction queue, and package the transaction information in the transaction queue into the candidate block, so that the candidate block can be broadcast, and the follower node in the blockchain can perform transaction verification and transaction execution. After broadcasting the candidate block, the first node can perform the transaction verification and transaction execution. Then the first node can broadcast the first node processing result. The first node performs consensus on the candidate block according to a processing result of each node in the blockchain, and saves the block when a consensus is reached successfully. In the embodiments of the present disclosure, the order of steps of block generation is changed, so that all nodes in the blockchain can perform transaction verification and transaction execution, and therefore, the speed of block generation and the performance of transaction processing can be improved.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] To describe the technical solutions of embodiments of the present disclosure more clearly, the following briefly describes the accompanying drawings required for describing the embodiments. Apparently, the accompanying drawings in the following description show only some embodiments of the present disclosure, and a person of ordinary skill in the art may still derive other accompanying drawings according to these accompanying drawings without creative efforts.

[0026] FIG. 1 is a schematic diagram of a blockchain system according to an embodiment of the present disclosure.

[0027] FIG. 2 is a schematic structural diagram of a block according to an embodiment of the present disclosure.

[0028] FIG. 3 is a schematic structural diagram of composition of a block processing system according to an embodiment of the present disclosure.

[0029] FIG. 4 is a schematic flowchart of interaction between a leader node and a follower node according to an embodiment of the present disclosure.

[0030] FIG. 5 is a schematic block flowchart of a block processing method performed by a leader node according to an embodiment of the present disclosure.

[0031] FIG. 6 is a schematic block flowchart of a block processing method performed by a follower node according to an embodiment of the present disclosure.

[0032] FIG. 7 is a schematic diagram of an application scenario of a block generation procedure according to an embodiment of the present disclosure.

[0033] FIG. 8 is a schematic diagram of a Raft data submission procedure according to an embodiment of the present disclosure.

[0034] FIG. 9 is a schematic diagram of a BFT-Raft data submission procedure according to an embodiment of the present disclosure.

[0035] FIG. 10 is a schematic structural diagram of composition of a first node according to an embodiment of the present disclosure.

[0036] FIG. 11 is a schematic structural diagram of composition of a second node according to an embodiment of the present disclosure.

[0037] FIG. 12 is a schematic structural diagram of composition of a server applying a block processing method according to an embodiment of the present disclosure.

DESCRIPTION OF EMBODIMENTS

[0038] Embodiments of the present disclosure provide a block processing method, a node, and a system, to improve the speed of block generation and the performance of transaction processing.

[0039] To make the objectives, features, and advantages of the embodiments of the present disclosure clearer and more comprehensible, the following clearly and completely describes the technical solutions in the embodiments of the present disclosure with reference to the

accompanying drawings in the embodiments of the present disclosure. Apparently, the embodiments described are merely some rather than all of the embodiments of the present disclosure. All other embodiments obtained by a person skilled in the art based on the embodiments of the present disclosure shall fall within the protection scope of the present disclosure.

[0040] In the specification, claims, and accompanying drawings of the embodiments of the present disclosure, the terms "include", "contain", and any other variants are intended to cover a non-exclusive inclusion. Therefore, a process, method, system, product, or device that includes a series of units is not necessarily limited to those units, but may include other units not specified expressly, or inherent to such units of the process, method, product, or device.

[0041] First, a blockchain system used in the embodiments of the present disclosure is briefly introduced.

[0042] Blockchain system is a data sharing system, that is, a system used for sharing data between nodes. FIG. 1 is a schematic diagram of a blockchain system 100 according to an embodiment of the present disclosure. The blockchain system 100 may include a plurality of nodes 110 (also referred to as "blockchain nodes"). Each node 110, in normal operation, may receive input information, and maintain shared data in the blockchain system 100 based on the received input information. To ensure information exchange in the blockchain system 100, the nodes 110 in the blockchain system 100 may have direct or indirect information connections, and the nodes 110 may perform information transmission through the information connections. For example, when any node in the blockchain system 100 receives the input information, other nodes in the blockchain system 100 obtain the input information according to a consensus algorithm, and store the input information as data in shared data, to make data stored on all nodes in the blockchain system 100 consistent.

[0043] The nodes 110 in the blockchain system 100 all have corresponding node identifiers, and the nodes 110 in the blockchain system 100 all may store node identifiers of other nodes in the blockchain system 100, in order to subsequently broadcast a generated block to the other nodes in the blockchain system according to the node identifiers of the other nodes. Each node may maintain a node identifier list as shown in the following table, which stores node names and node identifiers correspondingly in the node identifier list. A node identifier may be an Internet Protocol (IP) address and any other type of information capable of identifying the node. IP addresses in Table 1 are only used as an example for description.

Table 1

Node name	Node identifier
Node 1	117.114.151.174
Node 2	117.116.189.145
…	…
Node N	119.123.789.258

[0044] The nodes 101 in the blockchain system 100 store an identical blockchain. The blockchain includes a plurality of blocks. Referring to FIG. 2, a blockchain 200 includes a plurality of blocks 201. An initial block includes a block header and a block body. The block header stores an input information eigenvalue, a version number, a timestamp, and a difficulty value, and the block body stores input information. A next block to the initial block uses the initial block as a parent block, and also includes a block header and a block body. The block header stores an input information eigenvalue of a current block, a block header eigenvalue of the parent block, a version number, a timestamp, and a difficulty value. In this way, block data stored in each block in the blockchain is associated with block data stored in the parent block, thereby ensuring the security of the input information in the blocks.

[0045] FIG. 2 is an optional schematic diagram of a block structure according to an embodiment of the present disclosure. Referring to FIG. 2, in generating the blocks 201 in the blockchain 200, when receiving input information, a node where the blockchain is located performs verification on the input information, and then stores the input information in a memory pool, and updates a hash tree that is used for recording the input information. Subsequently, an update timestamp is updated to a time at which the input information is received, and different nonces are tried to calculate the eigenvalue a plurality of times, so that the calculated eigenvalue can meet the following formula:

$$\mathrm{SHA256}\left(\mathrm{SHA256}\left(\mathrm{version}+\mathrm{prev_hash}+\mathrm{merkle_root}+\mathrm{ntime}+\mathrm{nbits}+\mathrm{x}\right)\right)<\mathrm{TARGET}$$

where SHA256 is an eigenvalue algorithm used for calculating the eigenvalue; version (version number) is version information of a relevant block protocol in the blockchain; prev_hash is the block header eigenvalue of the parent block of the current block; merkle_root is the eigenvalue of the input information; ntime is the update time at which the timestamp is updated; nbits is the current difficulty, which has a fixed value within a period of time and is determined

again after a fixed period of time expires; x is a nonce; and TARGET is an eigenvalue threshold, which may be determined according to nbits.

[0046] In this way, when the nonce that meets the foregoing formula is calculated, information can be correspondingly stored, so that the block header and the block body are generated to obtain a current block. Subsequently, the node where the blockchain is located transmits, according to node identifiers of other nodes in the blockchain system, a newly generated block separately to the other nodes in the blockchain system where the node is located. The other nodes perform verification on the newly generated block, and after completing the verification, add the newly generated block to the blockchain that the other nodes store.

[0047] The block processing method provided in the embodiments of the present disclosure may be applied to the block processing system, and the block processing system is a part of the blockchain. As shown in FIG. 3, the block processing system may include at least two blockchain nodes. For example, a first node and a second node may be included. The first node is a leader node, and the second node is a follower node. The first node and the second node may communicate with each other, for example, through a wireless network or a wired network. Specifically, in the block processing system, the leader node and the follower node may be determined through a node role selection. For example, the Raft algorithm is run among all the nodes of the blockchain to elect a leader node and a follower node. There is only one leader node in the blockchain, but there may be one or more follower nodes in the blockchain. The Raft algorithm is a distributed consensus algorithm ensuring that a plurality of nodes achieve a consensus in state. In normal operation, a node either plays a leader role or plays a follower role, the follower role following a state of the leader role. The algorithm used for the node role selection in the embodiments of the present disclosure is not limited to the Raft algorithm. For example, a byzantine fault tolerance (BFT) like algorithm, such as a practical byzantine fault tolerance (PBFT) algorithm, may alternatively be used for the node role selection, which is not limited herein.

[0048] First, an interaction procedure between the leader node and the follower node in the block processing system in the embodiments of the present disclosure is described by using an example. Referring to FIG. 4, the block processing method provided in one of the embodiments of the present disclosure may include the following steps.

[0049] 201. In a case that a first node is a leader node, and a second node is a follower node, the first node packages first transaction information in a transaction queue of the first node into a candidate block, and broadcasts the candidate block through a blockchain.

[0050] In this embodiment of the present disclosure, one leader node and at least one follower node may be determined through the node role selection in the blockchain. For example, the first node is the leader node, and the second node is the follower node. When the first node is elected as the leader node, the first node can manage a transaction queue, where the transaction queue is used for storing transaction information transmitted by a client. There may be one or more pieces of transaction information stored in the transaction queue, and the transaction information may also be referred to as a transaction.

[0051] For example, the first node packages the first transaction information in the transaction queue of the first node into the candidate block, where the candidate block is a block to be written to a blockchain ledger. When the first transaction information is packaged into the candidate block, the first node may broadcast the candidate block through the blockchain. When the first node broadcasts the candidate block, all nodes in the blockchain (including the follower node and the leader node) may receive the candidate block. It is not limited that, in this embodiment of the present disclosure, before broadcasting, the first node may add a signature to the candidate block or the first transaction information to prevent the information that is broadcast from being tampered with.

[0052] 211. The second node receives the candidate block broadcast by the first node through the blockchain, and obtains the first transaction information from the candidate block.

[0053] In this embodiment of the present disclosure, when the first node broadcasts the candidate block through the blockchain, the second node in the blockchain may receive the candidate block broadcast by the first node through the blockchain. It is not limited that, another follower node in the blockchain may also receive the candidate block. For example, a third node in the blockchain may also receive the candidate block transmitted by the first node. In the following embodiments, an example in which the second node processes the candidate block and the transaction information is described. For procedures of another follower node in the blockchain, one can refer to the execution procedure of the second node, which is not limited herein.

[0054] After the second node obtains the candidate block from the first node, the second node may obtain, from the candidate block, the first transaction information that is packaged into the candidate block by the first node.

[0055] 212. The second node performs verification on the first transaction information in the candidate block to generate a second verification result, and executes a transaction indicated by the first transaction information in the candidate block to generate a second transaction execution result.

[0056] In this embodiment of the present disclosure, after the second node obtains the first transaction information from the candidate block, the second node may perform verification on the first transaction information, and may also perform a transaction execution operation on the first transaction information. The verification performed by the second node on the first transaction information may also be referred to as validity verification. The validity verification may include at least one of the following verification processes of performing verification on a transaction data format and parameters, verifying whether there are duplicate transactions in a transaction list, verifying whether an input of the transaction is valid and whether double-spending occurs, verifying whether a signature of the transaction is correct, and verifying whether an input amount of the transaction is greater than or equal to an output amount. The execution of the transaction indicated by the first transaction information by the second node may generate the second transaction execution result. There may be a plurality of scenarios for executing the transaction, which are not limited herein.

[0057] 202. The first node performs verification on the first transaction information in the candidate block to generate a first verification result, and executes a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result.

[0058] In this embodiment of the present disclosure, after the first node obtains the first transaction information from the candidate block, the first node may perform verification on the first transaction information, and may also perform a transaction execution operation on the first transaction information. The verification performed by the first node on the first transaction information may also be referred to as validity verification. The validity verification may include at least one of the following verification processes of performing verification on a transaction data format and parameters, verifying whether there are duplicate transactions in a transaction list, verifying whether an input of the transaction is valid and whether double-spending occurs, verifying whether a signature of the transaction is correct, and verifying whether an input amount of the transaction is greater than or equal to an output amount. The execution of the transaction indicated by the first transaction information by the first node may generate the first transaction execution result. There may be a plurality of scenarios for executing the transaction, which are not limited herein.

[0059] 203. The first node broadcasts a first node processing result through the blockchain, the first node processing result including: the first verification result and the first transaction execution result.

[0060] In this embodiment of the present disclosure, after the first node completes the transaction verification and the transaction execution, the first node may generate the first node processing result including the first verification result and the first transaction execution result. The first node broadcasts the first node processing result through the blockchain, and all nodes (including the follower node and the leader node) in the blockchain may receive the first node processing result.

[0061] 213. The second node broadcasts a second node processing result through the blockchain, the second node processing result including the second verification result and the second transaction execution result.

[0062] In this embodiment of the present disclosure, after the second node completes the transaction verification and the transaction execution, the second node may generate the second node processing result including the second verification result and the second transaction execution result. The second node broadcasts the second node processing result through the blockchain, and all nodes (including the follower node and the leader node) in the blockchain may receive the second node processing result.

[0063] In the foregoing embodiments, the step 202 to step 203 and step 211 to step 213 may be performed in a different order. FIG. 2 only shows a feasible implementation, but is not intended to limit the embodiments of the present disclosure.

[0064] 204. The first node receives a second node processing result broadcast by the second node through the blockchain, the second node processing result including: the second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and the second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block.

[0065] In this embodiment of the present disclosure, the second node broadcasts the second node processing result through the blockchain, and the first node in the blockchain may receive the second node processing result broadcast by the second node through the blockchain.

[0066] 205. The first node performs consensus on the candidate block according to the first node processing result and the second node processing result, and then the first node saves the candidate block in a case that a consensus on the candidate block is reached successfully, and saves the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0067] In this embodiment of the present disclosure, the first node receives, through step 204, the second node processing result broadcast by the second node, and the first node may perform consensus on the candidate block according to the first node processing result and the second node processing result. For example, the first node may use the distributed consensus algorithm to perform consensus. The distributed consensus algorithm may be a Raft algorithm. In addition, the distributed consensus algorithm in this embodiment of the present disclosure may alternatively be a BFT-Raft algorithm, which is a Raft algorithm that is compatible with BFT. The BFT is used for handling an unexpected failure of a node caused by a hardware error, a network failure, and a malicious attack from a network node.

[0068] In this embodiment of the present disclosure, the first node performs consensus on the candidate block, and then the first node saves the candidate block in a case that a consensus on the candidate block is reached successfully, thereby completing the block generation of the candidate block. The first node may also save the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully, so that the first transaction execution result corresponding to the first transaction information can be found through querying in the subsequent processing procedure.

[0069] In some embodiments of the present disclosure, the process that the first node saves the candidate block in a case that a consensus on the candidate block is reached successfully in step 205 includes that, in a case that a consensus on the candidate block is reached successfully, the first node saves header information of the candidate block and the first transaction information that is successfully verified.

[0070] The first transaction information is packaged in the candidate block. After the first node performs consensus on the candidate block, the first node may, in a case that a consensus on the candidate block is reached successfully, specifically save the header information of the candidate block and save the first transaction information that is successfully verified. The header information of the candidate block, in terms of a data format of the candidate block, for example, may include a hash value of a previous block, a root of Merkle tree, a root of state, a receipt root, a signature of node, a nonce, and the like. The header information of the candidate block may be specifically determined according to an application scenario, which is not limited herein.

[0071] 214. The second node saves the candidate block in a case that the first transaction information is verified successfully, and saves the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0072] In this embodiment of the present disclosure, after the second node broadcasts the second node processing result through the blockchain, the second node may determine whether to save the candidate block according to whether the first transaction information is verified successfully. When the first transaction information is verified successfully, the second node saves the candidate block, thereby completing the block generation of the candidate block. The second node may further save the second transaction execution result in the case that the transaction indicated by the first transaction information is executed successfully, so that the second transaction execution result corresponding to the first transaction information can be found through querying in the subsequent processing procedure.

[0073] It may be learned from the descriptions of the embodiments of the present disclosure in the foregoing embodiments that, in a case that a first node is a leader node, and a second node is a follower node, the first node packages first transaction information in a transaction queue of the first node into a candidate block, and broadcasts the candidate block through a blockchain. Then the first node performs verification on the first transaction information in the candidate block to generate a first verification result, and executes a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result. The first node broadcasts a first node processing result through the blockchain, the first node processing result including the first verification result and the first transaction execution result. The first node receives a second node processing result broadcast by the second node through the blockchain. The first node performs consensus on the candidate block according to the first node processing result and the second node processing result, and then the first node saves the candidate block in a case that a consensus on the candidate block is reached successfully, and saves the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully. In the embodiments of the present disclosure, the first node serves as the leader node. The first node may cache to-be-processed transaction information by using the transaction queue, and package the transaction information in the transaction queue into the candidate block, so that the candidate block can be broadcast, and the follower node in the blockchain can perform transaction verification and transaction execution. After broadcasting the candidate block, the first node can perform the following processing: transaction verification and transaction execution. Then the first node can broadcast the first node processing result. The first node performs consensus on the candidate block according to a processing result of each node in the blockchain, and saves the block when a consensus is reached successfully. In the embodiments of the present disclosure, the order of steps of block generation is changed, so that all nodes in the

blockchain can perform transaction verification and transaction execution, and therefore, the speed of block generation and the performance of transaction processing can be improved.

[0074] The block processing method provided in this embodiment of the present disclosure is described from a perspective of a first node. Referring to FIG. 5, the block processing method provided in this embodiment of the present disclosure mainly includes the following steps.

[0075] 301. In a case that a first node is a leader node, and a second node is a follower node, the first node receives transaction information transmitted by at least one client to a blockchain.

[0076] It is not limited that, in some embodiments of the present disclosure, step 301 may alternatively be replaced with the following step: receiving, by the first node, transaction information obtained by the second node from at least one client.

[0077] In this embodiment of the present disclosure, after obtaining the transaction information of the user, the at least one client may transmit the transaction information to the blockchain. For example, the transaction information may be transmitted to the first node or the second node in the blockchain, which may be specifically determined according to an application scenario. If the client directly transmits the transaction information to the first node, the first node receives the transaction information transmitted by the at least one client to the blockchain. If the client directly transmits the transaction information to the second node, after the second node serving as the follower node receives the transaction information of the client, the second node transmits the transaction information to the first node, and the first node may receive the transaction information obtained by the second node from the at least one client.

[0078] 302. The first node puts the transaction information of the at least one client into a transaction queue.

[0079] In this embodiment of the present disclosure, the first node maintains the transaction queue. After the first node obtains the transaction information of the at least one client, the first node puts the transaction information of the at least one client into the transaction queue.

[0080] 303. The first node checks whether the transaction queue meets a preset block generation condition.

[0081] In this embodiment of the present disclosure, the first node may pre-configure a block generation condition for the transaction queue, to check whether the transaction queue meets the preset block generation condition when new transaction information is stored in the transaction queue. The block generation condition is an execution condition for determining whether to perform a block generation process. In a case that the transaction queue meets the block generation

condition, the first node executes the block generation process, and in a case that the transaction queue does not meet the block generation condition, the first node does not execute the block generation process, and continues determining whether the block generation condition is met. The block generation procedure is executed when the block generation condition is met.

[0082] In some embodiments of the present disclosure, the step 303that the first node checks whether the transaction queue meets a preset block generation condition includes: checking, by the first node, whether a quantity of pieces of transaction information stored in the transaction queue exceeds a first threshold, determining, in a case that the quantity of pieces of transaction information exceeds the first threshold, that the transaction queue meets the block generation condition, and determining, in a case that the quantity of pieces of transaction information does not exceed the first threshold, that the transaction queue does not meet the block generation condition.

[0083] The first node counts a quantity of pieces of the transaction information stored in the transaction queue. The quantity of pieces of transaction information indicates the size of the transaction queue. The first node checks whether the quantity of pieces of the transaction information meets a preset first threshold. The first threshold is a block generation threshold. For example, the first threshold may be 1000. The first node determines that the transaction queue meets the block generation condition in a case that the quantity of pieces of transaction information included in the transaction queue reaches 1000, and determines that the transaction queue does not meet the block generation condition in a case that the quantity of pieces of transaction information included in the transaction queue does not reach 1000.

[0084] In some embodiments of the present disclosure, the step 303 that the first node checks whether the transaction queue meets a preset block generation condition includes: checking, by the first node, whether a volume of data stored in the transaction queue exceeds a second threshold, determining, in a case that the volume of data exceeds the second threshold, that the transaction queue meets the block generation condition, and determining, in a case that the volume of data does not exceed the second threshold, that the transaction queue does not meet the block generation condition.

[0085] The first node counts a volume of data stored in the transaction queue. The volume of data indicates a storage space capacity occupied by the transaction queue. The first node checks whether the volume of data meets a preset second threshold. The second threshold is a block generation threshold. For example, the second threshold may be 1M. The first node determines that the transaction queue meets the block generation condition in a case that the volume of data stored in the transaction queue reaches 1M, and determines that the transaction queue does not meet the

block generation condition in a case that the volume of data stored in the transaction queue does not reach 1M.

[0086] In some embodiments of the present disclosure, the step 303 that the first node checks whether the transaction queue meets a preset block generation condition includes: checking, by the first node, whether a time difference between a previous time of generating a block for the transaction queue and a current time exceeds a block generation time threshold, determining, in a case that the time difference exceeds the block generation time threshold, that the transaction queue meets the block generation condition, and determining, in a case that the time difference does not exceed the block generation time threshold, that the transaction queue does not meet the block generation condition.

[0087] The first node may count a quantity of times of block generation of the transaction queue, record a block generation time each time a block of the transaction queue is generated, calculate a time difference between a previous block generation time and a current time in real time, check whether the time difference exceeds a block generation time threshold, determine that the transaction queue meets the block generation condition in a case that the time difference exceeds the block generation time threshold, and determine that the transaction queue does not meet the block generation condition in a case that the time difference does not exceed the block generation time threshold. For example, the block generation time threshold may be 5 seconds.

[0088] 304. The first node packages first transaction information in the transaction queue of the first node into a candidate block, and broadcasts the candidate block through the blockchain, in a case that the transaction queue meets the block generation condition.

[0089] In this embodiment of the present disclosure, the first node packages the first transaction information in the transaction queue of the first node into the candidate block in response to detecting that the transaction queue meets the block generation condition, and broadcasts the candidate block, so that all the nodes in the blockchain may receive the candidate block.

[0090] 305. The first node performs verification on the first transaction information in the candidate block to generate a first verification result, and executes a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result.

[0091] 306. The first node broadcasts a first node processing result through the blockchain, the first node processing result including the first verification result and the first transaction execution result.

[0092] 307. The first node receives a second node processing result broadcast by the second node through the blockchain, the second node processing result including: second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block.

[0093] 308. The first node performs consensus on the candidate block according to the first node processing result and the second node processing result, and then the first node saves the candidate block in a case that a consensus on the candidate block is reached successfully, and saves the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0094] In this embodiment of the present disclosure, the procedure of step 304 to step 308 is similar to the procedure of step 202 to step 205, and details are not described herein again.

[0095] In some embodiments of the present disclosure, when the first node performs any one of step 304 to step 308, the block generation processing method provided in this embodiments of the present disclosure may further include the following steps:

packaging, by the first node, second transaction information in the transaction queue into the candidate block while packaging the first transaction information into the candidate block, and broadcasting the candidate block through the blockchain;

performing, by the first node, verification on the second transaction information in the candidate block to generate a third verification result, and executing a transaction indicated by the second transaction information in the candidate block to generate a third transaction execution result;

broadcasting, by the first node, a third node processing result through the blockchain, the third node processing result including the third verification result and the third transaction execution result;

receiving, by the first node, a fourth node processing result broadcast by the second node through the blockchain, the fourth node processing result including: a fourth verification result generated by the second node by performing verification on the second transaction information in the candidate block, and a fourth transaction execution result generated by the second node by executing the transaction indicated by the second transaction information in the candidate block; and

performing, by the first node, consensus on the candidate block according to the third node processing result and the fourth node processing result, then saving, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and saving the third transaction execution result in a case that the transaction indicated by the second transaction information is executed successfully.

[0096] The transaction queue of the first node stores the first transaction information and the second transaction information. When performing any procedure of packaging, verification, execution, consensus, and saving on the first transaction information, the first node may further perform a procedure of packaging, verification, execution, consensus or saving, on the second transaction information at the same time. Therefore, during the block generation procedure in this embodiment of the present disclosure, a block concurrency verification algorithm is used for concurrently performing verification on blocks that are independent of each other, thereby further improving the efficiency of the block generation.

[0097] It may be learned from the descriptions of the embodiments of the present disclosure that, the first node serves as the leader node. The first node may cache to-be-processed transaction information by using the transaction queue, and package the transaction information in the transaction queue into the candidate block, so that the candidate block can be broadcast, and the follower node in the blockchain can perform transaction verification and transaction execution. After broadcasting the candidate block, the first node can perform the transaction verification and transaction execution. Then the first node can broadcast the first node processing result. The first node performs consensus on the candidate block according to a processing result of each node in the blockchain, and saves the block when a consensus is reached successfully. In the embodiments of the present disclosure, the order of steps of block generation is changed, so that all nodes in the blockchain can perform transaction verification and transaction execution, and therefore, the speed of block generation and the performance of transaction processing can be improved.

[0098] The block processing method provided in the embodiments of the present disclosure is described from a perspective of the second node. Referring to FIG. 6, the block processing method provided in this embodiment of the present disclosure mainly includes the following steps.

[0099] 401. In a case that a first node is a leader node, and a second node is a follower node, the second node receives a candidate block broadcast by the first node through a blockchain, and obtains first transaction information from the candidate block.

[0100] 402. The second node performs verification on the first transaction information in the candidate block to generate a second verification result, and executes a transaction indicated by

the first transaction information in the candidate block to generate a second transaction execution result.

[0101] 403. The second node broadcasts a second node processing result through the blockchain, the second node processing result including the second verification result and the second transaction execution result.

[0102] In this embodiment of the present disclosure, the procedure of step 401 to step 403 is similar to the procedure of step 211 to step 213 in the embodiment of FIG. 4, and details are not described herein again.

[0103] 404. The second node receives a first node processing result broadcast by the first node through the blockchain, the first node processing result including: a first verification result generated by the first node by performing verification on the first transaction information in the candidate block, and a first transaction execution result generated by the first node by executing the transaction indicated by the first transaction information in the candidate block.

[0104] In some embodiments of the present disclosure, in addition to the leader node (that is, the first node) in the blockchain, the follower node in the blockchain may also perform consensus. For example, the second node receives, through step 404, the first node processing result broadcast by the first node, and the second node may perform consensus on the candidate block according to the first node processing result and the second node processing result. For example, the second node may use a distributed consensus algorithm to perform consensus. The distributed consensus algorithm may be a Raft algorithm. In addition, the distributed consensus algorithm in this embodiment of the present disclosure may alternatively be a BFT-Raft algorithm.

[0105] 405. The second node performs consensus on the candidate block according to the first node processing result and the second node processing result, and triggers, in a case that a consensus on the candidate block is reached successfully, to perform the following step: saving, by the second node, the candidate block in a case that the first transaction information is verified successfully, and saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0106] In this embodiment of the present disclosure, the second node may perform consensus on the candidate block. In a case that a consensus on the candidate block is reached successfully, the second node saves the candidate block in a case that the first transaction information is verified successfully, and saves the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully. In the

blockchain, in a case that the first node may be malicious, the second node broadcasts the second node processing result, so that all the nodes in the blockchain receive the processing results of other nodes. Each node determines whether to store the data according to the received processing results from the other nodes, instead of relying on a notification from the first node, thereby ensuring the correct execution of the transaction indicated by the first transaction information.

[0107] In some embodiments of the present disclosure, after the second node broadcasts the second node processing result through the blockchain in step 403, , the following steps may be performed instead of step 404 to step 405:

receiving, by the second node, a notification message transmitted by the first node in a case that a consensus on the candidate block is reached successfully on the first node; and

triggering, by the second node, according to the notification message, to perform the following step: saving, by the second node, the candidate block in a case that the first transaction information is verified successfully, and saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0108] The first node may perform consensus on the candidate block. In a case that a consensus on the candidate block is reached successfully, the first node broadcasts the notification message, and the second node in the blockchain may receive the notification message and determine, according to the notification message, that a consensus is reached successfully. Then the second node saves the candidate block in a case that the first transaction information is verified successfully, and saves the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0109] In some embodiments of the present disclosure, when the first node performs any one of step 304 to step 308, the block generation processing method provided in this embodiments of the present disclosure may further include the following steps:

receiving, by the second node, the candidate block broadcast by the first node through the blockchain, and obtaining the second transaction information from the candidate block;

performing, by the second node, verification on the second transaction information in the candidate block to generate a fourth verification result, and executing a transaction indicated by the second transaction information in the candidate block to generate a fourth transaction execution result;

broadcasting, by the second node, a fourth node processing result through the blockchain, the fourth node processing result including the fourth verification result and the fourth transaction execution result; and

saving, by the second node, the candidate block in a case that the second transaction information is verified successfully, and saving the fourth transaction execution result in a case that the transaction indicated by the second transaction information is executed successfully.

[0110] The transaction queue of the first node stores the first transaction information and the second transaction information. When performing any procedure of packaging, verification, execution, consensus, and saving on the first transaction information, the first node may further perform a procedure, such as packaging, verification, execution, consensus, or saving, on the second transaction information at the same time. In a case that the second node receives the broadcast of the first node, the second node may also verify and execute a transaction indicated by the second transaction information. Therefore, during the block generation procedure in this embodiment of the present disclosure, a block concurrency verification algorithm is used for concurrently performing verification on blocks that are not dependent on each other, thereby further improving the efficiency of the block generation.

[0111] It may be learned from the descriptions of the embodiments of the present disclosure that, in the embodiments of the present disclosure, the first node serves as the leader node. The first node may cache to-be-processed transaction information by using the transaction queue, and package the transaction information in the transaction queue into the candidate block, so that the candidate block can be broadcast, and the second node can perform transaction verification and transaction execution. Then the second node can broadcast the second node processing result, so that the first node performs consensus on the candidate block according to a processing result of each node in the blockchain, and saves the block when a consensus is reached successfully. In the embodiments of the present disclosure, the order of steps of block generation is changed, so that all nodes in the blockchain can perform transaction verification and transaction execution, and therefore, the speed of block generation and the performance of transaction processing can be improved.

[0112] For better understanding and implementation of the foregoing solutions of this embodiment of the present disclosure, the following makes a detailed description by using a specific application scenario as an example.

[0113] This embodiment of the present disclosure provides a novel block generation solution. An example in which a first node is a leader node and a second node is a follower node is

used. In this embodiment of the present disclosure, an unverified series of transactions may be packaged into a candidate block, and broadcast by the leader node to the follower node by using the BFT-Raft algorithm. The leader node and the follower node, serving as consensus nodes, may verify and execute the transactions in a verification process on the candidate block, and mark a transaction with a verification or execution result as a success or a failure. Finally, all the consensus nodes perform consensus on the verification results of the candidate block. After a consensus is reached successfully, all the nodes save the candidate block, save a transaction marked as a success in the candidate block, and remove a failed transaction.

[0114] FIG. 7 is a schematic diagram of an application scenario of a block generation procedure according to an embodiment of the present disclosure. The following procedure is mainly included.

[0115] S101. A leader node and a follower node are elected from a blockchain network based on a Raft algorithm.

[0116] A node role selection is first performed. The Raft algorithm is run on all the nodes of the blockchain network to elect the leader node and the follower node, where there is only one leader node in the blockchain.

[0117] S102. A user transmits a transaction to the blockchain, and the leader node receives the transaction and directly puts the transaction into a transaction queue.

[0118] The user may transmit the transaction to the blockchain network by using a terminal. For the transaction that is transmitted to the leader node, the leader node directly puts the transaction into the transaction queue. Alternatively, for the transaction that is transmitted to the follower node, the follower node forwards the transaction to the leader node, and then the leader node puts the transaction that is received from the follower node into the transaction queue.

[0119] S103. The leader node checks whether transactions in the transaction queue meets a block generation requirement.

[0120] S104. In a case that the block generation requirement is met, the leader node packages the transactions in the transaction queue into a candidate block, adds a signature to the candidate block, and broadcasts the candidate block to the follower node.

[0121] The leader node checks whether the transaction queue meets the block generation requirement. For example, the leader node detects whether a quantity of transactions or a volume of data of transactions stored in the transaction queue meets the block generation requirement. If the block generation requirement is met, the transactions in the transaction queue are packaged into the

candidate block, a signature is added to the candidate block, and the candidate block is broadcast. If the block generation requirement is not met, the leader node checks whether a block generation time arrives. If the block generation time arrives, the leader node packages the transactions in the transaction queue into the candidate block, adds a signature to the candidate block, and broadcasts the candidate block.

[0122] S105. A consensus node in the blockchain network performs verification on the candidate block, including performing verification on a transaction list in the candidate block.

[0123] S106. The consensus node adds a signature to a candidate block verification result and broadcasts the candidate block verification result.

[0124] The leader node and the follower node, serving as consensus nodes, perform verification on the candidate block. During the verification procedure, the leader node and the follower node perform validity verification on the transaction list in the candidate block, mark a transaction as a valid transaction or an invalid transaction, execute the transaction, generate a transaction execution result, and cache a valid transaction execution result.

[0125] S107. The consensus node in the blockchain network performs BFT determining on the results, and saves the candidate block and a valid transaction after a consensus is reached.

[0126] The leader node and the follower node each add a signature to respective verification results and execution results thereof in the foregoing step S106, and broadcast the signed results. Then consensus is performed on the received node-signed result by using the BFT algorithm. The node-signed result includes: the verification result and the transaction execution result.

[0127] After a consensus on the node-signed result is reached successfully by the leader node and the follower node, the nodes save header information of the candidate block, save the valid transaction in the candidate block, and save the transaction execution result cached in the candidate block. Saving the valid transaction in the candidate block refers to saving original transaction data transmitted by the user (that is, the transaction execution result is not included herein), and saving the transaction execution results refers to saving a state of a transaction execution result.

[0128] The header information of the candidate block, in term of a data format of the block, includes a hash value of a previous block, a root of Merkle tree, a root of state, a receipt root, a signature of node, and a nonce.

[0129] FIG. 8 is a schematic diagram of a Raft data submission procedure according to an embodiment of the present disclosure. In FIG. 8, L represents a leader node, and F represents a follower node. The following procedure is mainly included.

[0130] Step 1. A client submits data v=3 to the leader node.

[0131] Step 2.1. A leader node copies the data v=3 and transmits the data v=3 to follower nodes.

[0132] Step 3.1. A follower node confirms to the leader node that the data v=3 is received.

[0133] Step 3.2. A follower node confirms to the leader node that the data v=3 is received.

[0134] Step 4.1. The leader node confirms to the client that the data v=3 is received.

[0135] Step 4.2. The leader node submits the data v=3 to the follower nodes.

[0136] In the foregoing procedure, a fault tolerance technology of the Raft algorithm is based on a leader node. After receiving the data of the leader node, the follower nodes cache the data, and return results to the leader node. The leader node receives the results from the follower nodes for fault tolerance determining. In a case that a proportion of nodes from which the same result is received is greater than 50%, the data is considered to be successful, and then the leader node instructs the follower nodes to save the state of data.

[0137] FIG. 9 is a schematic diagram of a BFT-Raft data submission procedure according to an embodiment of the present disclosure. The following procedure is mainly included.

[0138] A client 1 generates a transaction 1 and transmits the transaction 1 to a leader node. A client 2 generates a transaction 2 and transmits the transaction 2 to a follower node 1. The follower node 1 further transmits the transaction 2 to the leader node. After the leader node generates a block, the block is broadcast to three follower nodes. The three follower nodes transmit a broadcast response to a blockchain. The leader node and the three follower nodes submit the block and perform consensus. After a consensus is reached successfully, the leader node and the three follower nodes transmit submission success messages to the client 1 and the client 2.

[0139] In the blockchain, the fault tolerance technology shown in the embodiment of FIG. 8 cannot deal with a situation where the leader node is malicious, and therefore, the BFT technology is added in the present disclosure. The foregoing follower nodes broadcast the result, so that all the nodes in the blockchain network receive signed results of other nodes. Each node determines, according to the received node-signed results instead of relying on a notification from the leader node, whether the data can be submitted and saved.

[0140] In this embodiment of the present disclosure, in step S101 to step S107, a block concurrency verification technology may be further used. That is, there are a plurality of transactions in a block, and in a block generation procedure, a block concurrency verification algorithm is used for concurrently performing verification on blocks that are not dependent on each other.

[0141] The foregoing solutions provided in this embodiment of the present disclosure can improve the speed of block generation and the performance of transaction processing in an alliance chain or a private chain.

[0142] The foregoing method embodiments are expressed as a series of action combinations for the purpose of brief description, but a person skilled in the art is to learn that because some steps may be performed in other sequences or simultaneously according to the embodiments of the present disclosure, the embodiments of the present disclosure are not limited to a described action sequence. In addition, a person skilled in the art is to also learn that the embodiments described in this specification are all preferred embodiments; and therefore, an action and a module involved may not be necessary in the embodiments of the present disclosure.

[0143] For the convenience of a better implementation of the foregoing solutions of the embodiments of the present disclosure, the following further provides related apparatuses configured to implement the foregoing solutions.

[0144] Referring to FIG. 10, this embodiment of the present disclosure provides a first node 800 in a blockchain. The blockchain further includes a second node. The first node is a leader node, and the second node is a follower node. The first node 800 includes a processing module 801 and a transceiver module 802.

[0145] The processing module is configured to package first transaction information in a transaction queue of the first node into a candidate block.

[0146] The transceiver module is configured to broadcast the candidate block through the blockchain.

[0147] The processing module is further configured to perform verification on the first transaction information in the candidate block to generate a first verification result, and execute a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result.

[0148] The transceiver module is further configured to broadcast a first node processing result through the blockchain, the first node processing result including: the first verification result and the first transaction execution result.

[0149] The transceiver module is further configured to receive a second node processing result broadcast by the second node through the blockchain, the second node processing result including: a second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and a second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block.

[0150] The processing module is further configured to perform consensus on the candidate block according to the first node processing result and the second node processing result, and then save, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and save the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0151] In some embodiments of the present disclosure, before the transceiver module packages the first transaction information in the transaction queue of the first node into the candidate block, the processing module is further configured to check whether the transaction queue meets a preset block generation condition; and trigger, in a case that the transaction queue meets the block generation condition, to perform the step of packaging the first transaction information in the transaction queue of the first node into the candidate block.

[0152] In some embodiments of the present disclosure, the processing module is further configured to check whether a quantity of pieces of transaction information stored in the transaction queue exceeds a first threshold, determine, in a case that the quantity of pieces of transaction information exceeds the first threshold, that the transaction queue meets the block generation condition, and determine, in a case that the quantity of pieces of transaction information does not exceed the first threshold, that the transaction queue does not meet the block generation condition.

[0153] In some embodiments of the present disclosure, the processing module is further configured to check whether a volume of data stored in the transaction queue exceeds a second threshold, determine in a case that the volume of data exceeds the second threshold, that the transaction queue meets the block generation condition, and determine, in a case that the volume of data does not exceed the second threshold, that the transaction queue does not meet the block generation condition.

[0154] In some embodiments of the present disclosure, the processing module is further configured to check whether a time difference between a previous time of generating a block for the transaction queue and a current time exceeds a block generation time threshold, determine, in a case that the time difference exceeds the block generation time threshold, that the transaction queue meets the block generation condition, and determine, in a case that the time difference does not exceed the block generation time threshold, that the transaction queue does not meet the block generation condition.

[0155] In some embodiments of the present disclosure, the transceiver module is further configured to receive transaction information transmitted by at least one client to the blockchain. Alternatively, the first node receives transaction information obtained by the second node from at least one client.

[0156] The processing module is further configured to put the transaction information of the at least one client into the transaction queue.

[0157] In some embodiments of the present disclosure, the processing module is further configured to package second transaction information in the transaction queue into the candidate block while packaging the first transaction information into the candidate block.

[0158] The transceiver module is further configured to broadcast the candidate block through the blockchain.

[0159] The processing module is further configured to perform verification on the second transaction information in the candidate block to generate a third verification result, and execute a transaction indicated by the second transaction information in the candidate block to generate a third transaction execution result.

[0160] The transceiver module is further configured to broadcast a third node processing result through the blockchain, the third node processing result including: the third verification result and the third transaction execution result.

[0161] The transceiver module is further configured to receive a fourth node processing result broadcast by the second node through the blockchain, the fourth node processing result including: a fourth verification result generated by the second node by performing verification on the second transaction information in the candidate block, and a fourth transaction execution result generated by the second node by executing the transaction indicated by the second transaction information in the candidate block.

[0162] The processing module is further configured to perform consensus on the candidate block according to the third node processing result and the fourth node processing result, and then save, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and save the third transaction execution result in a case that the transaction indicated by the second transaction information is executed successfully.

[0163] In some embodiments of the present disclosure, the processing module is further configured to, in a case that a consensus on the candidate block is reached successfully, save header information of the candidate block and the first transaction information that is successfully verified.

[0164] It may be learned from the descriptions of the embodiments of the present disclosure that, in a case that a first node is a leader node, and a second node is a follower node, the first node packages first transaction information in a transaction queue of the first node into a candidate block, and broadcasts the candidate block through a blockchain. Then the first node performs verification on the first transaction information in the candidate block to generate a first verification result, and executes a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result. The first node broadcasts a first node processing result through the blockchain, the first node processing result including: the first verification result and the first transaction execution result. The first node receives a second node processing result broadcast by the second node through the blockchain. The first node performs consensus on the candidate block according to the first node processing result and the second node processing result, and then the first node saves the candidate block in a case that a consensus on the candidate block is reached successfully, and saves the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully. In the embodiments of the present disclosure, the first node serves as the leader node. The first node may cache to-be-processed transaction information by using the transaction queue, and package the transaction information in the transaction queue into the candidate block, so that the candidate block can be broadcast, and the follower node in the blockchain can perform transaction verification and transaction execution. After broadcasting the candidate block, the first node can perform the transaction verification and transaction execution. Then the first node can broadcast the first node processing result. The first node performs consensus on the candidate block according to a processing result of each node in the blockchain, and saves the block when a consensus is reached successfully. In the embodiments of the present disclosure, the order of steps of block generation is changed, so that all nodes in the blockchain can perform transaction verification and transaction execution, and therefore, the speed of block generation and the performance of transaction processing can be improved.

[0165] Referring to FIG. 11, this embodiment of the present disclosure provides a second node 900 in a blockchain. The blockchain further includes a first node. The first node is a leader node, and the second node is a follower node. The second node 900 includes a processing module 901 and a transceiver module 902.

[0166] The transceiver module is configured to receive a candidate block broadcast by the first node through the blockchain.

[0167] The processing module is configured to obtain first transaction information from the candidate block.

[0168] The processing module is further configured to perform verification on the first transaction information in the candidate block to generate a second verification result, and execute a transaction indicated by the first transaction information in the candidate block to generate a second transaction execution result.

[0169] The transceiver module is further configured to broadcast a second node processing result through the blockchain, the second node processing result including: the second verification result and the second transaction execution result.

[0170] The processing module is further configured to save the candidate block in a case that the first transaction information is verified successfully, and save the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0171] In some embodiments of the present disclosure, after broadcasting the second node processing result through the blockchain, the transceiver module receives a first node processing result broadcast by the first node through the blockchain, the first node processing result including: a first verification result generated by the first node by performing verification on the first transaction information in the candidate block, and a first transaction execution result generated by the first node by executing the transaction indicated by the first transaction information in the candidate block.

[0172] The processing module is further configured to perform consensus on the candidate block according to the first node processing result and the second node processing result, and trigger, in a case that a consensus on the candidate block is reached successfully, to perform the step of saving the candidate block in a case that the first transaction information is verified successfully, and saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0173] In some embodiments of the present disclosure, after broadcasting the second node processing result through the blockchain, the transceiver module receives a notification message transmitted by the first node in a case that a consensus on the candidate block is reached successfully on the first node.

[0174] The processing module is further configured to trigger, according to the notification message, to perform the step of saving the candidate block in a case that the first transaction information is verified successfully, and saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0175] In some embodiments of the present disclosure, the transceiver module is further configured to receive the candidate block broadcast by the first node through the blockchain, and obtain second transaction information obtained from the candidate block.

[0176] The processing module is further configured to perform verification on the second transaction information in the candidate block to generate a fourth verification result, and execute a transaction indicated by the second transaction information in the candidate block to generate a fourth transaction execution result.

[0177] The transceiver module is further configured to broadcast a fourth node processing result through the blockchain, the fourth node processing result including: the fourth verification result and the fourth transaction execution result.

[0178] The processing module is further configured to save the candidate block in a case that the second transaction information is verified successfully, and save the fourth transaction execution result in a case that the transaction indicated by the second transaction information is executed successfully.

[0179] It may be learned from the descriptions of the embodiments of the present disclosure that, in the embodiments of the present disclosure, the first node serves as the leader node. The first node may cache to-be-processed transaction information by using the transaction queue, and package the transaction information in the transaction queue into the candidate block, so that the candidate block can be broadcast, and the second node can perform transaction verification and transaction execution. Then the second node can broadcast the second node processing result, so that the first node performs consensus on the candidate block according to a processing result of each node in the blockchain, and saves the block when a consensus is reached successfully. In the embodiments of the present disclosure, the order of steps of block generation is changed, so that all nodes in the blockchain can perform transaction verification and transaction execution, and

therefore, the speed of block generation and the performance of transaction processing can be improved.

[0180] In an exemplary embodiment, referring to FIG. 10, this embodiment of the present disclosure provides a first node 800 in another blockchain. The blockchain further includes a second node. The first node is a leader node, and the second node is a follower node. The first node 800 including: a processing module 801 and a transceiver module 802.

[0181] The processing module is configured to put, in response to at least one client transmitting transaction information to the blockchain, the transaction information transmitted by the client into a transaction queue of the first node.

[0182] The processing module is further configured to check whether the transaction queue meets a preset block generation condition.

[0183] The transceiver module is configured to package, in response to the transaction queue meeting the block generation condition, first transaction information in the transaction queue of the first node into a candidate block, add a signature to the candidate block, and broadcast the candidate block through the blockchain.

[0184] The processing module is further configured to perform verification on the first transaction information in the candidate block to generate a first verification result, and execute a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result.

[0185] The transceiver module is further configured to add a signature to a first node processing result, and then broadcast the first node processing result through the blockchain, the first node processing result including: the first verification result and the first transaction execution result.

[0186] The transceiver module is further configured to receive a second node processing result broadcast by the second node through the blockchain, the second node processing result including: a second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and a second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block.

[0187] The processing module is further configured to perform, according to the first node processing result and the second node processing result, consensus on the candidate block by using a distributed consensus algorithm, and then save the candidate block in a case that a consensus on

the candidate block is reached successfully, and save the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0188] In some embodiments of the present disclosure, the transceiver module is further configured to package second transaction information in the transaction queue into the candidate block while packaging the first transaction information into the candidate block, add a signature to the candidate block, and then broadcast the candidate block through the blockchain.

[0189] The processing module is further configured to perform verification on the second transaction information in the candidate block to generate a third verification result, and execute a transaction indicated by the second transaction information in the candidate block to generate a third transaction execution result.

[0190] The transceiver module is further configured to add a signature to a third node processing result, and then broadcast the third node processing result through the blockchain, the third node processing result including: the third verification result and the third transaction execution result.

[0191] The processing module is further configured to receive a fourth node processing result broadcast by the second node through the blockchain, the fourth node processing result including: a fourth verification result generated by the second node by performing verification on the second transaction information in the candidate block, and a fourth transaction execution result generated by the second node by executing the transaction indicated by the second transaction information in the candidate block.

[0192] The processing module is further configured to perform, by the first node, consensus on the candidate block according to the third node processing result and the fourth node processing result, and then save the candidate block in a case that a consensus on the candidate block is reached successfully, and save the third transaction execution result in a case that the transaction indicated by the second transaction information is executed successfully.

[0193] In some embodiments of the present disclosure, the processing module is further configured to, in a case that a consensus on the candidate block is reached successfully, save header information of the candidate block and save first transaction information that is verified successfully, the header information of the candidate block including: a hash value of a previous block of the candidate block, a root of Merkle tree, a root of state, a receipt root, a signature of node, and a nonce.

[0194] It may be learned from the descriptions of the embodiments of the present disclosure in the foregoing embodiments that, in the embodiments of the present disclosure, the first node serves as the leader node. The first node may cache to-be-processed transaction information by using the transaction queue, and package the transaction information in the transaction queue into the candidate block, so that the candidate block can be broadcast, and the follower node in the blockchain can perform transaction verification and transaction execution. After broadcasting the candidate block, the first node can perform the transaction verification and transaction execution. Then the first node can broadcast the first node processing result. The first node performs consensus on the candidate block according to a processing result of each node in the blockchain, and saves the block when a consensus is reached successfully. In the embodiments of the present disclosure, the order of steps of block generation is changed, so that all nodes in the blockchain can perform transaction verification and transaction execution, and therefore, the speed of block generation and the performance of transaction processing can be improved.

[0195] In an exemplary embodiment, referring to FIG. 11, this embodiment of the present disclosure provides a second node 900 in another blockchain. The blockchain further includes a first node. The first node is a leader node, and the second node is a follower node. The second node 900 includes a processing module 901 and a transceiver module 902.

[0196] The transceiver module is configured to receive a candidate block broadcast by the first node through the blockchain, and obtain first transaction information from the candidate block.

[0197] The processing module is configured to perform verification on the first transaction information in the candidate block to generate a second verification result, and execute a transaction indicated by the first transaction information in the candidate block to generate a second transaction execution result.

[0198] The transceiver module is configured to add a signature a second node processing result, and then broadcast the second node processing result through the blockchain, the second node processing result including: the second verification result and the second transaction execution result.

[0199] The processing module is configured to save the candidate block in a case that the first transaction information is verified successfully, and save the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

[0200] It may be learned from the descriptions of the embodiments of the present disclosure that, in the embodiments of the present disclosure, the first node serves as the leader node. The first node may cache to-be-processed transaction information by using the transaction queue, and package the transaction information in the transaction queue into the candidate block, so that the candidate block can be broadcast, and the second node can perform transaction verification and transaction execution. Then the second node can broadcast the second node processing result, so that the first node performs consensus on the candidate block according to a processing result of each node in the blockchain, and saves the block when a consensus is reached successfully. In the embodiments of the present disclosure, the order of steps of block generation is changed, so that all nodes in the blockchain can perform transaction verification and transaction execution, and therefore, the speed of block generation and the performance of transaction processing can be improved.

[0201] FIG. 12 is a schematic structural diagram of a server according to an embodiment of the present disclosure. The server may be specifically the first node in the foregoing blockchain to implement the block processing method on a first node side, or may be the second node in the blockchain to implement the block processing method on a second node side. The server 1100 may greatly vary in configurations or performances, and may include one or more central processing units (CPUs) 1122 (for example, one or more processors), a memory 1132, and one or more storage media 1130 (for example, one or more mass storage devices) for storing application programs 1142 or data 1144. The memory 1132 and the storage medium 1130 may be transient or persistent storages. The program stored in the storage medium 1130 may include one or more modules (not shown), and each module may include a series of instructions and operations for the server. Further, the CPU 1122 may communicate with the storage medium 1130, and perform, on the server 1100, the series of instructions and operations in the storage medium 1130.

[0202] The server 1100 may further include one or more power supplies 1126, one or more wired or wireless network interfaces 1150, one or more input/output interfaces 1158, and/or one or more operating systems 1141, such as the Windows Server™, Mac OS X™, Unix™, Linux™, or FreeBSD™.

[0203] Steps of the block processing method performed by the first node in the foregoing embodiment may be based on the server structure shown in FIG. 12. Similarly, steps of the block processing method performed by the second node in the foregoing embodiment may be based on the server structure shown in FIG. 12.

[0204] In addition, the described apparatus embodiment is merely exemplary. The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, may be located in one position, or may be distributed on multiple network units. Some or all of the modules may be selected according to actual needs to achieve the objectives of the solutions of the embodiments. In addition, in the accompanying drawings of the apparatus embodiments provided by the embodiments of the present disclosure, connection relationships between modules indicate that the modules have communication connections with each other, which may be specifically implemented as one or more communication buses or signal cables. A person of ordinary skill in the art may understand and implement the embodiments without creative efforts.

[0205] Based on the description of the foregoing implementations, a person skilled in the art may clearly understand that the embodiments of the present disclosure may be implemented by software with necessary universal hardware, or by dedicated hardware, including a dedicated integrated circuit, a dedicated CPU, a dedicated memory, a dedicated component, and the like. Generally, any functions that can be performed by a computer program can be easily implemented by using corresponding hardware. Moreover, a specific hardware structure used to achieve the same function may be of various forms, for example, in a form of an analog circuit, a digital circuit, or a dedicated circuit. However, for the embodiments of the present disclosure, software program implementation is a better implementation in most cases. Based on such an understanding, the essential technical solutions of the embodiments of the present disclosure or the part contributing to the existing technology may be implemented in a form of a software product. The software product is stored in a readable storage medium, such as a floppy disk, a USB flash drive, a removable hard disk, a read-only memory (ROM), a random access memory (RAM), a magnetic disk, or an optical disc of a computer, and includes several instructions for instructing a computer device (which may be a personal computer, a server, a network device, or the like) to perform the methods described in the embodiments of the present disclosure.

[0206] In an exemplary embodiment, a computer program product is further provided, when executed on a first node, the computer program product being configured to implement the block processing method on the first node side; and when executed on a second node, the computer program product being configured to implement the block processing method on the second node side.

[0207] To sum up, the foregoing embodiments are merely intended for describing the technical solutions of the embodiments of the present disclosure, but not for limiting the present

disclosure. Although the embodiments of the present disclosure is described in detail with reference to the foregoing embodiments, it is to be understood by a person of ordinary skill in the art that modifications can still be made to the technical solutions described in the foregoing embodiments or equivalent replacements may be made to some technical features thereof, without departing from the spirit and scope of the technical solutions of the embodiments of the present disclosure.

CLAIMS

1. A block processing method, the method being executed by a first node in a blockchain, the blockchain further comprising a second node, the first node being a leader node, the second node being a follower node, and the method comprising:

packaging, by the first node, first transaction information in a transaction queue of the first node into a candidate block, and broadcasting the candidate block through the blockchain, wherein the first transaction information in the broadcasted candidate block is not verified by the first node;

performing, by the first node, verification on the first transaction information in the candidate block to generate a first verification result, and executing a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result;

broadcasting, by the first node, a first node processing result through the blockchain, the first node processing result comprising the first verification result and the first transaction execution result;

receiving, by the first node, a second node processing result broadcast by the second node through the blockchain, the second node processing result comprising a second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and a second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block; and

performing, by the first node, consensus on the candidate block according to the first node processing result and the second node processing result, saving, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and saving the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

2. The method according to claim 1, wherein before the packaging, by the first node, first transaction information in a transaction queue of the first node into a candidate block, the method further comprises:

checking, by the first node, whether the transaction queue meets a preset block generation condition; and

triggering, in a case that the transaction queue meets the block generation condition, the operation of packaging, by the first node, the first transaction information in the transaction queue of the first node into the candidate block.

3. The method according to claim 2, wherein the checking, by the first node, whether the transaction queue meets a preset block generation condition comprises:

checking, by the first node, whether a quantity of pieces of transaction information stored in the transaction queue exceeds a first threshold, determining, in a case that the quantity of pieces of transaction information exceeds the first threshold, that the transaction queue meets the block generation condition, and determining, in a case that the quantity of pieces of transaction information does not exceed the first threshold, that the transaction queue does not meet the block generation condition.

4. The method according to claim 2, wherein the checking, by the first node, whether the transaction queue meets a preset block generation condition comprises:

checking, by the first node, whether a volume of data stored in the transaction queue exceeds a second threshold, determining, in a case that the volume of data exceeds the second threshold, that the transaction queue meets the block generation condition, and determining, in a case that the volume of data does not exceed the second threshold, that the transaction queue does not meet the block generation condition.

5. The method according to claim 2, wherein the checking, by the first node, whether the transaction queue meets a preset block generation condition comprises:

checking, by the first node, whether a time difference between a previous time of generating a block for the transaction queue and a current time exceeds a block generation time threshold, determining, in a case that the time difference exceeds the block generation time threshold, that the transaction queue meets the block generation condition, and determining, in a case that the time difference does not exceed the block generation time threshold, that the transaction queue does not meet the block generation condition.

6. The method according to claim 1, further comprising:

receiving, by the first node, transaction information transmitted by at least one client to the blockchain; or receiving, by the first node, transaction information obtained by the second

node from at least one client; and

putting, by the first node, the transaction information of the at least one client into the transaction queue.

7. The method according to claim 1, further comprising:

packaging, by the first node, second transaction information in the transaction queue into the candidate block while packaging the first transaction information into the candidate block, and broadcasting the candidate block through the blockchain;

performing, by the first node, verification on the second transaction information in the candidate block to generate a third verification result, and executing a transaction indicated by the second transaction information in the candidate block to generate a third transaction execution result;

broadcasting, by the first node, a third node processing result through the blockchain, the third node processing result comprising the third verification result and the third transaction execution result;

receiving, by the first node, a fourth node processing result broadcast by the second node through the blockchain, the fourth node processing result comprising: a fourth verification result generated by the second node by performing verification on the second transaction information in the candidate block, and a fourth transaction execution result generated by the second node by executing the transaction indicated by the second transaction information in the candidate block; and

performing, by the first node, consensus on the candidate block according to the third node processing result and the fourth node processing result, saving, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and saving the third transaction execution result in a case that the transaction indicated by the second transaction information is executed successfully.

8. The method according to any one of claims 1 to 7, wherein the saving, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully comprises:

saving, by the first node in a case that a consensus on the candidate block is reached successfully, header information of the candidate block and the first transaction information that is successfully verified.

9. A block processing method, the method being executed by a second node in a blockchain, the blockchain further comprising a first node, the first node being a leader node, the second node being a follower node, and the method comprising:

receiving, by the second node, a candidate block broadcast by the first node through the blockchain, and obtaining first transaction information from the candidate block, wherein the first transaction information in the broadcasted candidate block is not verified by the first node;

performing, by the second node, verification on the first transaction information in the candidate block to generate a second verification result, and executing a transaction indicated by the first transaction information in the candidate block to generate a second transaction execution result;

broadcasting, by the second node, a second node processing result through the blockchain, the second node processing result comprising the second verification result and the second transaction execution result; and

saving, by the second node, the candidate block in a case that the first transaction information is verified successfully, and saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

10. The method according to claim 9, wherein after the broadcasting, by the second node, a second node processing result through the blockchain, the method further comprises:

receiving, by the second node, a first node processing result broadcast by the first node through the blockchain, the first node processing result comprising: a first verification result generated by the first node by performing verification on the first transaction information in the candidate block, and a first transaction execution result generated by the first node by executing the transaction indicated by the first transaction information in the candidate block; and

performing, by the second node, consensus on the candidate block according to the first node processing result and the second node processing result, and triggering, in a case that a consensus on the candidate block is reached successfully, the operation of saving, by the second node, the candidate block in a case that the first transaction information is verified successfully, and the operation of saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

11. The method according to claim 9, wherein after the broadcasting, by the second node, a second node processing result through the blockchain, the method further comprises:

receiving, by the second node, a notification message transmitted by the first node in a case that a consensus on the candidate block is reached successfully on the first node; and

triggering, by the second node according to the notification message, the operation of saving, by the second node, the candidate block in a case that the first transaction information is verified successfully, and the operation of saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

12. The method according to any one of claims 9 to 11, further comprising:

receiving, by the second node, the candidate block broadcast by the first node through the blockchain, and obtaining second transaction information from the candidate block;

performing, by the second node, verification on the second transaction information in the candidate block to generate a fourth verification result, and executing a transaction indicated by the second transaction information in the candidate block to generate a fourth transaction execution result;

broadcasting, by the second node, a fourth node processing result through the blockchain, the fourth node processing result comprising the fourth verification result and the fourth transaction execution result; and

saving, by the second node, the candidate block in a case that the second transaction information is verified successfully, and saving the fourth transaction execution result in a case that the transaction indicated by the second transaction information is executed successfully.

13. A block processing method, the method being executed by a first node in a blockchain, the blockchain further comprising a second node, the first node being a leader node, the second node being a follower node, and the method comprising:

putting, by the first node in response to at least one client transmitting transaction information to the blockchain, the transaction information transmitted by the client into a transaction queue of the first node;

checking, by the first node, whether the transaction queue meets a preset block generation condition;

packaging, by the first node in response to the transaction queue meeting the block generation condition, first transaction information in the transaction queue of the first node into a candidate block, adding a signature to the candidate block, and broadcasting the candidate block through the blockchain, wherein the first transaction information in the broadcasted candidate block is not verified by the first node;

performing, by the first node, verification on the first transaction information in the candidate block to generate a first verification result, and executing a transaction indicated by the first transaction information in the candidate block to generate a first transaction execution result;

adding, by the first node, a signature to a first node processing result, and then broadcasting the first node processing result through the blockchain, the first node processing result comprising the first verification result and the first transaction execution result;

receiving, by the first node, a second node processing result broadcast by the second node through the blockchain, the second node processing result comprising: a second verification result generated by the second node by performing verification on the first transaction information in the candidate block, and a second transaction execution result generated by the second node by executing the transaction indicated by the first transaction information in the candidate block; and

performing, by the first node according to the first node processing result and the second node processing result, consensus on the candidate block by using a distributed consensus algorithm, saving, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and saving the first transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

14. The method according to claim 13, further comprising:

packaging, by the first node, second transaction information in the transaction queue into the candidate block while packaging the first transaction information into the candidate block, adding a signature to the candidate block, and then broadcasting the candidate block through the blockchain;

performing, by the first node, verification on the second transaction information in the candidate block to generate a third verification result, and executing a transaction indicated by the second transaction information in the candidate block to generate a third transaction

execution result;

adding, by the first node, a signature to a third node processing result, and then broadcasting the third node processing result through the blockchain, the third node processing result comprising the third verification result and the third transaction execution result;

receiving, by the first node, a fourth node processing result broadcast by the second node through the blockchain, the fourth node processing result comprising: a fourth verification result generated by the second node by performing verification on the second transaction information in the candidate block, and a fourth transaction execution result generated by the second node by executing the transaction indicated by the second transaction information in the candidate block; and

performing, by the first node, consensus on the candidate block according to the third node processing result and the fourth node processing result, saving, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully, and saving the third transaction execution result in a case that the transaction indicated by the second transaction information is executed successfully.

15. The method according to claim 13 or 14, wherein the saving, by the first node, the candidate block in a case that a consensus on the candidate block is reached successfully comprises:

saving, by the first node in a case that a consensus on the candidate block is reached successfully, header information of the candidate block and the first transaction information that is successfully verified, the header information of the candidate block comprising: a hash value of a previous block of the candidate block, a root of Merkle tree, a root of state, a receipt root, a signature of node, and a nonce.

16. A block processing method, the method being executed by a second node in a blockchain, the blockchain further comprising a first node, the first node being a leader node, the second node being a follower node, and the method comprising:

receiving, by the second node, a candidate block broadcast by the first node through the blockchain, and obtaining first transaction information from the candidate block, wherein the first transaction information in the broadcasted candidate block is not verified by the first node;

performing, by the second node, verification on the first transaction information in the candidate block to generate a second verification result, and executing a transaction indicated by the first transaction information in the candidate block to generate a second transaction execution result;

adding, by the second node, a signature to a second node processing result, and broadcasting the second node processing result through the blockchain, the second node processing result comprising the second verification result and the second transaction execution result; and

saving, by the second node, the candidate block in a case that the first transaction information is verified successfully, and saving the second transaction execution result in a case that the transaction indicated by the first transaction information is executed successfully.

17. A blockchain node, the blockchain node being a first node in a blockchain, the first node comprising: a processor and a memory,

the memory being configured to store instructions; and

the processor being configured to execute the instructions in the memory, to perform the method according to any one of claims 1 to 8, or perform the method according to any one of claims 13 to 15.

18. A blockchain node, the blockchain node being a second node in a blockchain, the second node comprising a processor and a memory,

the memory being configured to store instructions; and

the processor being configured to execute the instructions in the memory, to perform the method according to any one of claims 9 to 12, or perform the method according to claim 16.

19. A block processing system, the block processing system comprising: a first node and a second node,

the first node being configured to perform the method according to any one of claims 1 to 8, and the second node being configured to perform the method according to any one of claims 9 to 12;

or

the first node being configured to perform the method according to any one of claims 13

to 15, and the second node being configured to perform the method according to claim 16.

20. A computer-readable storage medium, comprising instructions, when run on a computer, causing the computer to perform the method according to any one of claims 1 to 8, or perform the method according to any one of claims 9 to 12, or perform the method according to any one of claims 13 to 15, or perform the method according to claim 16.