CONSENSUS METHOD AND DATA VERIFICATION METHOD, APPARATUS, AND SYSTEM OF CONSORTIUM BLOCKCHAIN

Technical Field

The present file relates to the field of consortium blockchain technologies, and in particular, to a consensus method and a data verification method, apparatus, and system of a consortium blockchain.

Background

A consortium blockchain is a kind of blockchain applied between institutions, and various nodes thereof usually have corresponding entities, such as banking, insurance, security, and business associations. These institutions form an interests-related consortium to jointly maintain operation of the blockchain. In the prior art, a consensus on the consortium blockchain needs to be reached on data before it can be recorded by a new block generated by each node.

At present, when validity of block data of a certain node is verified, it is necessary to compare the block data with block data correspondingly stored by another node. Obviously, this method is relatively cumbersome and time-consuming in data tracing, and therefore, how to improve the convenience of block data verification is a technical problem that needs to be solved urgently.

Summary of the Invention

An objective of embodiments of the present specification is to provide a consensus method and a data verification method, apparatus, and system of a consortium blockchain, which can verify data in a block more conveniently.

To achieve the above objective, the embodiments of the present specification are implemented as follows:

In a first aspect, a consensus method of a consortium blockchain is provided, including:

when a target consensus node of a consortium blockchain performs a consensus operation on a target consensus proposal, sending a verification signature to another consensus node of

the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal;

receiving, by the target consensus node, a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

after the target consensus node reaches a consensus on proposal data of the target consensus, generating a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

In a second aspect, a data verification method of a consortium blockchain is provided, including:

extracting, from a target block of a target consensus node of a consortium blockchain, recorded proposal data and a verification signature from at least one consensus node in the consortium blockchain, wherein the proposal data in the target block comes from a target consensus proposal, and the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal; and

verifying the validity of the proposal data recorded in the target block based on a quantity of verification signatures extracted from the target block.

In a third aspect, a consensus node of a consortium blockchain is provided, including:

a sending module configured to, when a consensus operation is performed on a target consensus proposal, send a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal;

a receiving module configured to receive a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

a block generation module configured to, after a consensus is reached on proposal data of the target consensus, generate a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

In a fourth aspect, a consortium blockchain system is provided, including a plurality of consensus nodes, wherein a target consensus node among the plurality of consensus nodes performs the following when participating in a target consensus:

sending a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal;

receiving a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

after a consensus is reached on proposal data of the target consensus, generating a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

In a fifth aspect, a data verification apparatus of a consortium blockchain is provided, including:

an extraction module configured to extract, from a target block of a target consensus node of a consortium blockchain, recorded proposal data and a verification signature from at least one consensus node in the consortium blockchain, wherein the proposal data in the target block comes from a target consensus proposal, and the verification signature is used to represent at

least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal; and

a verification module configured to verify the validity of the proposal data recorded in the target block based on a quantity of verification signatures extracted from the target block.

Based on the solutions in the embodiments of the present specification, when performing a consensus operation on a target consensus, if proposal data meets a consensus verification item set by a target consensus node of a consortium blockchain itself for the target consensus proposal, a verification signature is sent to another consensus node. After the proposal data reaches a consensus, various consensus nodes may record the proposal data together with collected verification signatures in a block, so that when validity verification is performed on block data of a certain consensus node, a verification result can be directly determined only according to a verification signature of the block, without the need of tracing block data corresponding to other block nodes, so that the verification of the block data is more convenient.

Brief Description of the Drawings

To describe the technical solutions in the embodiments of the present application or the prior art more clearly, the accompanying drawings required for describing the embodiments or the prior art are briefly introduced below. It is apparent that the accompanying drawings described in the following are merely some embodiments recorded in the embodiments of the present application, and those of ordinary skill in the art may still derive other drawings from these accompanying drawings without creative efforts.

FIG. 1 is a schematic flowchart of a consensus method of a consortium blockchain according to an embodiment of the present specification;

FIG. 2 is a schematic flowchart of a data verification method of a consortium blockchain according to an embodiment of the present specification;

FIG. 3 is a schematic structural diagram of a consensus node of a consortium blockchain according to an embodiment of the present specification;

FIG. 4 is a schematic structural diagram of a consortium blockchain system according to an embodiment of the present specification;

FIG. 5 is a schematic structural diagram of a data verification apparatus according to an embodiment of the present specification; and

FIG. 6 is a schematic structural diagram of an electronic device according to an embodiment of the present specification.

Detailed Description

In order to enable those skilled in the art to better understand the technical solutions in the present specification, the technical solutions in the embodiments of the present specification will be described clearly and completely with reference to the accompanying drawings in the embodiments of the present specification. It is apparent that the described embodiments are merely some of rather than all the embodiments of the present application. Based on the embodiments of the present specification, all other embodiments derived by those of ordinary skill in the art without any creative efforts shall fall within the protection scope of the present specification.

As described above, at present, for a consortium blockchain, a consensus needs to be reached on data before it can be recorded by a new block generated by each node (generally means a consensus node). When authenticity of block data in a certain consensus node is verified subsequently, it is necessary to compare the block data with block data correspondingly stored by another node. Obviously, this verification method is relatively cumbersome and time-consuming in data tracing. This will cause a large service delay for a consortium blockchain system with large information throughput. Therefore, the present file aims to propose a technical solution that can more conveniently verify data in a block.

FIG. 1 is a flowchart of a consensus method of a consortium blockchain according to an embodiment of the present specification. The method shown in FIG. 1 may be performed by corresponding hardware in the following, and includes the following steps.

In S102, when a target consensus node of a consortium blockchain performs a consensus operation on a target consensus proposal, a verification signature is sent to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal.

It should be understood that the target consensus node in the embodiment of the present specification may refer to any consensus node in the consortium blockchain. For example, when a consensus protocol in the consortium blockchain classifies the consensus nodes into a consensus master node and a consensus backup node, the target consensus node refers to the consensus master node, or may also refer to the consensus backup node.

Different consensus nodes in the consortium blockchain may be provided with the same or at least partially different consensus verification items.

As an example introduction:

a consensus verification item set by at least part of consensus nodes in the consortium blockchain may include a verification required when a consensus operation is performed on the target consensus, for example, including at least one of the following:

verification on a hash value of a local last block, which is used to ensure traceability of a new block;

verification on a timestamp of the target consensus, which is used to ensure that a timestamp of a new block is later than a timestamp of the previous block; and

verification on proposal data of the target consensus, which is used to ensure that only proposal data on which a positive consensus is reached will be uploaded to the blockchain.

In addition, at least part of the consensus nodes in the consortium blockchain may also set exclusive consensus verification items according to their own service requirements. For example, a consensus node of a banking institution may perform risk verification on proposal data for security data it stores.

It should be understood that, in the embodiment of the present specification, a verification signature sent by the target consensus node belongs to representative data, and the data volume of this verification signature may be less than the data volume of an actual verification result. In other words, sending the verification signature at an execution stage of the target consensus will not generate a lot of data overhead.

In practical applications, the target consensus node may perform private key encryption on some unique information (such as time of the target consensus and a view number) of the target consensus based on a preset private key encryption algorithm, so as to generate a valid verification signature for the target consensus, which can effectively deter a malicious act that another consensus node privately counterfeits the verification signature of the target consensus node.

In S104, the target consensus node receives the verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal.

It should be understood that other consensus nodes may send the verification signatures with reference to the method shown in S102, which will not be repeated here.

In S106, after the target consensus node reaches a consensus on proposal data of the target consensus, a block recording a collected verification signature corresponding to the target consensus and the proposal data is generated, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

Specifically, a new block in this step can record the verification signature corresponding to the target consensus through a block header, which means that the verification signature corresponding to the target consensus may be used as digest data of the new block. Alternatively, the new block may record the verification signature corresponding to the target consensus through a block body, which means that the verification signature corresponding to the target consensus may be used as entity data of the new block.

It should be understood that according to the current consensus protocol mechanism, when the quantity of verification signatures in the new block reaches 2F+1 (F is a quantity of abnormal consensus nodes tolerable by the consortium blockchain), it indicates that the proposal data in the new block succeeds in verification by at least 2F+1 consensus nodes, thus having a function of proving the validity (authenticity) of the proposal data.

As can be known from the consensus method shown in FIG.1, in the solutions in the embodiments of the present specification, when performing a consensus operation on a target consensus, if proposal data meets a consensus verification item set by a target consensus node of a consortium blockchain itself for a target consensus proposal, a verification signature is sent to another consensus node. After the proposal data reaches a consensus, various consensus nodes may record the proposal data together with collected verification signatures in a block, so that when validity verification is subsequently performed on block data of a certain consensus node, a verification result can be directly determined only according to a verification signature of the block, without the need of tracing block data corresponding to other block nodes, so that the verification of the block data is more convenient.

Corresponding to the consensus method shown above in FIG. 1, a data verification method of a consortium blockchain is further provided in the embodiments of the present specification. FIG. 2 is a flowchart of a data verification method according to an embodiment of the present specification. The method shown in FIG. 2 may be performed by a corresponding apparatus in the following, and includes the following steps.

In S202, recorded proposal data and a verification signature from at least one consensus node in a consortium blockchain are extracted from a target block of a target consensus node of the consortium blockchain, wherein the proposal data in the target block comes from a target consensus proposal, and the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal.

In S204, the validity of the proposal data recorded in the target block is verified based on a quantity of verification signatures extracted from the target block.

For example, in this step, if the quantity of the verification signatures extracted from the target block reaches 2F+1, it is determined that the proposal data recorded in the target block succeeds in the validity verification.

As can be seen, based on the data verification method according to the embodiment of the present specification, when block data of a certain target consensus node is verified, a verification result can be directly determined only according to a verification signature in the block, without the need of tracing corresponding block data to other consensus nodes. Therefore, the verification method has been greatly simplified, which significantly improves the verification speed and reduces the verification overhead.

It should be noted here that the data verification method according to the embodiment of the present specification is applicable to a node of a consortium blockchain system. In other words, the node in the consortium blockchain system that is endowed with a data verification capability can verify data in a block based on the data verification method according to the embodiment of the present specification. In addition, the data verification method according to the embodiment of the present specification is also applicable to a client, and the client verifies authenticity of data in a block based on the data verification method according to the embodiment of the present specification, for example, realizes Simplified Payment Verification (SPV).

The consensus method and data verification method according to the embodiments of the present specification are described in detail below in combination with actual application scenarios.

In the present application scenario, consensus nodes of a consortium blockchain adopt a PBFT protocol to implement consensus. At a commit stage of the PBFT protocol, various

consensus nodes (including a consensus master node and a consensus backup node) multiplex a commit message to send verification signatures.

A consensus process of the PBFT protocol may include the following main steps.

The consensus master node generates proposal data of the current round of view, and the proposal data contains a transaction from a transaction pool of the consensus master node. It should be understood that in the consortium blockchain system, after receiving that a transaction is initiated by the client, the consensus master node may perform account validity verification on the transaction initiated by the client, and synchronize the transaction that succeeds in the account validity verification to its own transaction pool.

After that, based on an erasure coding technology, the consensus master node splits proposal data redundancy into a data block corresponding to the consensus backup node, and sends the split data block to the corresponding consensus backup node to ensure that transmission of the proposal data is fault-tolerant.

The consensus backup node that receives the data block sent by the consensus master node forwards the received data block to another consensus backup node in the consortium blockchain.

The consensus master node initiates consensus of this round of view, including:

A pre-prepare stage:

The master consensus node receives a request from a Client and assigns a number to the request. After that, the consensus master node broadcasts a pre-prepare message to each consensus backup node. This pre-prepare message mainly contains a view of the current consensus and a digest of the consensus master node, and at the same time also includes hash information corresponding to each data block calculated by the consensus master node based on the erasure coding technology.

A prepare stage:

After receiving the pre-prepare message, each consensus backup node participating in the consensus checks whether the pre-prepare message is valid.

Specifically, the consensus backup node may check whether the pre-prepare message is valid based on a set of verification items required to generate a verification signature. This set of verification items may include some verification items specified by the PBFT protocol itself, such as verification on the number n, verification on a consensus timestamp of this round, and verification on erasure code of prompt data. In addition, the set of verification items may also include an additional verification item that is not specified by the PBFT protocol, such as risk verification on the proposal data mentioned above.

If the pre-prepare message is valid, the procedure proceeds to the prepare stage. Then, a state of the consensus proposal on replica is determined to be prepared, and the consensus backup node adds the pre-prepare message to a local Log and sends the prepare message to another consensus backup node to wait for a commit stage.

If the pre-prepare message is invalid, the consensus backup node will repulse the proposal data of this consensus, and the consensus process ends.

A commit stage:

After each of all consensus nodes enters the prepared state, it sends its own verification signature to another consensus node through a commit message, and adds the commit message sent by itself to the local Log (representing its own approval).

Specifically, each consensus node in the consortium blockchain may encrypt some unique information (such as a view number and a consensus digest) of consensus in this round of view based on its own private key, and obtain a verification signature that has exclusive effect for this round of consensus.

When any consensus node discovers that there is a quorum (a quorum is a set of a certain quantity of replicas required to ensure all replica data consistency requirements and fault tolerance requirements) agrees the number assignment, it will broadcast a commit message to

all other nodes. At the same time, commit messages from other nodes will be received one after another. If each node receives 2F+1 commit messages (including one of its own, these commit messages from different nodes carry the same number n and view), it means that the consensus node has a certificate named committed certificate, and the request reaches a committed state on this consensus node. At this time, only through this consensus node, it can be concluded that the request has reached the prepared state in a quorum, that is, all consensus nodes of the same quorum have agreed to the assignment of the number n. When the request initiated by the Client reaches the committed state, it indicates that a consensus of the entire network has been reached.

After that, all consensus nodes locally generate a block that records the proposal data and the verification signatures collected based on the committed message.

Subsequently, when block data of a certain target consensus node in the consortium blockchain is verified, a corresponding process mainly includes the following step:

Proposal data in the target block in the target consensus node and all verification signatures corresponding to a consensus to which the proposal data belongs are extracted.

Assuming that in this application scenario, the verification signature is data encrypted by the consensus node based on its own private key, then the corresponding verification signature is parsed based on a public key of the consensus node in the consortium blockchain to verify the authenticity of each verification signature.

If the quantity of verification signatures that succeed in the verification reaches 2F+1, it is determined that the proposal data recorded in the target block is valid.

If the quantity of verification signatures that succeed in the verification does not reach 2F+1, it is determined that the proposal data recorded in the target block is invalid. Alternatively, the existing data verification method is implemented, and whether the proposal data recorded in the target block is valid is verified by tracing proposal data correspondingly recorded by blocks of other consensus nodes.

As can be known based on the above application scenario, the consensus method according to the embodiment of the present specification multiplexes the commit message of the PBFT protocol to send the verification signature. Based on the existing PBFT protocol, when a certain consensus node enters the commit stage, it means that the consensus node has completed verification on a hash value of a local last block, verification on a timestamp of this round of consensus, and verification on the proposal data of this round of consensus. Therefore, it can use the mechanism of commit message broadcast transmission to provide its own verification signature to other consensus nodes. In this way, sending verification signatures will not increase additional signaling overhead, and therefore will not cause excessive delays to consensus and data uploading to the blockchain.

It should be understood that the above application scenario is an introduction to the method according to the embodiment of the present specification. Appropriate changes can be made without departing from the above principles herein, and these changes should also be regarded as the protection scope of the embodiments of the present specification.

For example, the consensus method according to the embodiment of the present specification is also applicable to the HoneyBadgerBFT protocol. That is, after an Asynchronous Common Subset (ACS) stage of the HoneyBadgerBFT protocol ends (based on the HoneyBadgerBFT protocol, after the ACS stage ends, the consensus node will determine proposal data to be uploaded to the blockchain), each consensus node in the consortium blockchain sends its verification signature to another consensus node through an exclusive signature message (in the HoneyBadgerBFT protocol, the consensus node may complementally send some information through the signature message). After that, all consensus nodes locally generate a block that records the proposal data and the verification signature collected based on the signature message.

Corresponding to the consensus method shown above in FIG. 1, a consensus node of a consortium blockchain is further provided in the embodiments of the present specification. FIG.

3 is a structural diagram of consensus node 300 according to an embodiment of the present specification, including:

sending module 310 configured to, when a consensus operation is performed on a target consensus proposal, send a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal;

receiving module 320 configured to receive a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

block generation module 330 configured to, after a consensus is reached on proposal data of the target consensus, generate a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

In the embodiments of the present specification, when performing a consensus operation on a target consensus, if proposal data meets a consensus verification item set by a consensus node itself for a target consensus proposal, a verification signature is sent to another consensus node. After the proposal data reaches a consensus, various consensus nodes may record the proposal data together with collected verification signatures in a block, so that when validity verification is performed on block data of a certain consensus node, a verification result can be directly determined only according to a verification signature of the block, without the need of tracing block data corresponding to other block nodes, so that the verification of the block data is more convenient.

Optionally, the consensus nodes of the consortium blockchain perform the target consensus based on a Practical Byzantine Fault Tolerance (PBFT) protocol. The sending module 310 specifically sends a verification signature to another consensus node of the consortium blockchain through a commit message at a commit stage of the PBFT protocol.

Optionally, the consensus nodes of the consortium blockchain perform the target consensus based on a HoneyBadger Byzantine Fault Tolerance (HoneyBadgerBFT) protocol. The sending module 310 specifically sends a verification signature to another consensus node of the consortium blockchain based on a signature message after an ACS stage of the HoneyBadgerBFT protocol ends.

Optionally, different consensus nodes in the consortium blockchain are provided with the same or at least partially different consensus verification items.

A consensus verification item set by at least part of consensus nodes in the consortium blockchain includes at least one of the following:

verification on a hash value of a local last block, verification on a timestamp of the target consensus, and verification on proposal data of the target consensus.

Obviously, the consensus node according to the embodiment of the present specification can realize the steps and functions of the consensus node in the consensus method shown above in FIG. 1. The principles are the same, and thus will not repeated herein.

Corresponding to the consensus method shown above in FIG. 1, a consortium blockchain system is further provided in the embodiments of the present specification. FIG. 4 is a structural diagram of consortium blockchain system 400 according to an embodiment of the present specification, including: a plurality of consensus nodes 410.

Target consensus node 411 among the plurality of consensus nodes performs the following when participating in a target consensus: sending a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal; receiving a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and after a consensus is reached on proposal data of the target consensus, generating a block recording a collected verification signature corresponding to the target consensus and the

proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

In the consortium blockchain system according to the embodiment of the present specification, when performing a consensus operation on a target consensus, if proposal data meets a consensus verification item set by a target consensus node of a consortium blockchain itself for a target consensus proposal, a verification signature is sent to another consensus node. After the proposal data reaches a consensus, various consensus nodes may record the proposal data together with collected verification signatures in a block, so that when validity verification is performed on block data of a certain consensus node, a verification result can be directly determined only according to a verification signature of the block, without the need of tracing block data corresponding to other block nodes, so that the verification of the block data is more convenient.

Optionally, the consensus node of the consortium blockchain performs the target consensus based on the Practical Byzantine Fault Tolerance (PBFT) protocol; wherein sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain after a consensus operation is performed on a target consensus proposal includes: sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain through a commit message at a commit stage of the PBFT protocol.

Optionally, the consensus node of the consortium blockchain performs the target consensus based on the HoneyBadger Byzantine Fault Tolerance (HoneyBadgerBFT) protocol; wherein sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain after a consensus operation is performed on a target consensus proposal includes: sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain based on a signature message after an ACS stage of the HoneyBadgerBFT protocol ends.

Optionally, different consensus nodes in the consortium blockchain are provided with the same or at least partially different consensus verification items.

As an example introduction, a consensus verification item set by at least part of consensus nodes in the consortium blockchain includes at least one of the following:

verification on a hash value of a local last block, verification on a timestamp of the target consensus, and verification on proposal data of the target consensus.

Obviously, the consortium blockchain system according to the embodiment of the present specification can realize the steps and functions in the consensus method shown above in FIG. 1. The principles are the same, and thus will not repeated herein.

Corresponding to the consensus method shown above in FIG. 2, a data verification apparatus of a consortium blockchain is further provided in the embodiments of the present specification. FIG. 5 is a structural diagram of data verification apparatus 500 according to an embodiment of the present specification, including:

extraction module 510 configured to extract, from a target block of a target consensus node of a consortium blockchain, recorded proposal data and a verification signature from at least one consensus node in the consortium blockchain, wherein the proposal data in the target block comes from the target consensus proposal, and the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal; and

verification module 520 configured to verify the validity of the proposal data recorded in the target block based on a quantity of verification signatures extracted from the target block.

Obviously, based on the data verification apparatus according to the embodiment of the present specification, when block data of a certain target consensus node is verified, a verification result can be directly determined only according to a verification signature in the block, without the need of tracing corresponding block data to other consensus nodes.

Therefore, the verification method has been greatly simplified, which significantly improves the verification speed and reduces the verification overhead.

Optionally, during execution, if the quantity of the verification signatures extracted from the target block reaches 2F+1, verification module 520 determines that the proposal data recorded in the target block succeeds in the validity verification, wherein F is a quantity of abnormal consensus nodes tolerable by the consortium blockchain.

Obviously, the data verification apparatus according to the embodiment of the present specification can realize the steps and functions in the data verification method shown above in FIG. 2. The principles are the same, and thus will not repeated herein.

FIG. 6 is a schematic structural diagram of an electronic device according to an embodiment of the present specification. Please refer to FIG. 6, at a hardware level, the electronic device includes a processor, and optionally further includes an internal bus, a network interface, and a memory. The memory may include a memory, such as a high-speed Random-Access Memory (RAM), and may also include a non-volatile memory, such as at least one magnetic disk memory. Of course, the electronic device may also include hardware required by other services.

The processor, the network interface, and the memory may be connected to one another through an internal bus. The internal bus may be an Industry Standard Architecture (ISA) bus, a Peripheral Component Interconnect (PCI) bus, an Extended Industry Standard Architecture (EISA) bus, or the like. The bus may be classified into an address bus, a data bus, a control bus, and so on. For ease of presentation, only one bidirectional arrow is used in FIG. 6, but it does not indicate that there is only one bus or one type of bus.

The memory is configured to store a program. Specifically, the program may include program code including computer operation instructions. The memory may include a memory and a non-volatile memory, and provide instructions and data to the processor.

Optionally, the processor reads a corresponding computer program from the non-volatile memory into the memory and runs the consensus node shown in FIG. 3 at a logic level. The

processor executes the program stored in the memory, and is specifically configured to perform the following operations:

when a consensus operation is performed on a target consensus proposal, sending a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal;

receiving a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

after a consensus is reached on proposal data of the target consensus, generating a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

Alternatively, the processor reads a corresponding computer program from the non-volatile memory into the memory and runs the data verification apparatus shown in FIG. 5 at the logic level. The processor executes the program stored in the memory, and is specifically configured to perform the following operations:

extracting, from a target block of a target consensus node of a consortium blockchain, recorded proposal data and a verification signature from at least one consensus node in the consortium blockchain, wherein the proposal data in the target block comes from the target consensus proposal, and the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal; and

verifying the validity of the proposal data recorded in the target block based on a quantity of verification signatures extracted from the target block.

The above consensus method disclosed in the embodiment shown in FIG. 1 of the present specification or the data verification method disclosed in the embodiment shown in FIG. 2 may

be applied to the processor or implemented by the processor. The processor may be an integrated circuit chip with a signal processing capability. In the implementation process, various steps of the above method may be completed by an integrated logic circuit of hardware in the processor or instructions in the form of software. The above processor may be a general-purpose processor, including a Central Processing Unit (CPU), a Network Processor (NP), and the like; it may also be a Digital Signal Processor (DSP), an Application Specific Integrated Circuit (ASIC), a Field-Programmable Gate Array (FPGA), or other programmable logic devices, discrete gates or transistor logic devices, and discrete hardware components. The various methods, steps, and logical block diagrams disclosed in the embodiments of the present specification can be implemented or performed. The general-purpose processor may be a microprocessor, or the processor may also be any conventional processor or the like. The steps of the method disclosed in the embodiments of the present specification may be directly embodied as being performed and completed by a hardware decoding processor, or performed and completed by a combination of hardware and software modules in the decoding processor. The software module may be located in a mature storage medium in the field, such as a random access memory, a flash memory, a read-only memory, a programmable read-only memory, an electrically erasable programmable memory, or a register. The storage medium is located in the memory, and the processor reads information in the memory and completes the steps of the above method in combination with its hardware.

It should be understood that the electronic device according to the embodiment of the present specification can realize the function of the above consensus node in the embodiment shown in FIG. 1, or can realize the function of the above data verification apparatus in the embodiment shown in FIG. 2. The principles are the same, and thus will not repeated herein.

Of course, in addition to the software implementation, the electronic device in the present specification does not exclude other implementations, such as logic devices or a combination

of software and hardware. In other words, the execution body of the following processing procedure is not limited to various logic units, and may also be a hardware or logic device.

In addition, a computer-readable storage medium is further proposed in the embodiments of the present specification, and the computer-readable storage medium stores one or more programs including instructions.

Optionally, when the above instructions are executed by a portable electronic device that includes a plurality of application programs, the portable electronic device is enabled to perform the consensus method of the embodiment shown in FIG. 1, and is specifically used to perform the following steps:

when a consensus operation is performed on a target consensus proposal, sending a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal;

receiving a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

after a consensus is reached on proposal data of the target consensus, generating a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

Alternatively, when the above instructions are executed by a portable electronic device that includes a plurality of application programs, the portable electronic device is enabled to perform the data verification method of the embodiment shown in FIG. 2, and is specifically used to perform the following steps:

extracting, from a target block of a target consensus node of a consortium blockchain, recorded proposal data and a verification signature from at least one consensus node in the consortium blockchain, wherein the proposal data in the target block comes from the target

consensus proposal, and the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal; and

verifying the validity of the proposal data recorded in the target block based on a quantity of verification signatures extracted from the target block.

It should be understood that when executed by the portable electronic device including a plurality of application programs, the instructions enable the consensus node described above to realize the function in the embodiment shown in FIG. 1, or enable the above data verification apparatus to realize the function in the embodiment shown in FIG. 2. The principles are the same, and thus will not repeated herein.

Those skilled in the art should understand that the embodiments of the present specification can be provided as a method, a system, or a computer program product. Therefore, the present specification may be in the form of a complete hardware embodiment, a complete software embodiment, or an embodiment combining software and hardware. Moreover, the present specification may be in the form of a computer program product implemented on one or more computer-usable storage media (including, but not limited to, a magnetic disk memory, a CD-ROM, an optical memory, and the like) including computer-usable program code.

The specific embodiments of the present specification are described above. Other embodiments are within the scope of the appended claims. In some cases, the actions or steps recorded in the claims can be performed in an order different from the orders in the embodiments and can still achieve desired results. In addition, the processes depicted in the drawings do not necessarily require the particular order shown or a sequential order to achieve the desired results. In some embodiments, multitasking and parallel processing may also be feasible or may be advantageous.

The foregoing description is merely embodiments of the present specification, and is not used to limit the present specification. For those skilled in the art, the present specification may

have various alterations and changes. Any modifications, equivalent replacements, improvements, etc. made within the spirit and principle of the present specification shall be included in the scope of the claims. In addition, all other embodiments derived by those of ordinary skill in the art without any creative efforts shall fall within the protection scope of the present file.

CLAIMS

1. A consensus method of a consortium blockchain, comprising:

when a target consensus node of a consortium blockchain performs a consensus operation on a target consensus proposal, sending a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal, and wherein at least part of consensus nodes in the consortium blockchain set a consensus verification item that is configured to perform risk verification according to their own security data;

receiving, by the target consensus node, a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

after the target consensus node reaches a consensus on proposal data of the target consensus, generating a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

2. The method according to claim 1, wherein

the consensus nodes of the consortium blockchain perform the target consensus based on a Practical Byzantine Fault Tolerance (PBFT) protocol; and

sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain after a consensus operation is performed on a target consensus proposal comprises:

sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain through a commit message at a commit stage of the PBFT protocol.

3. The method according to claim 1, wherein

the consensus nodes of the consortium blockchain perform the target consensus based on a HoneyBadger Byzantine Fault Tolerance (HoneyBadgerBFT) protocol; and

sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain after a consensus operation is performed on a target consensus proposal comprises:

sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain based on a signature message after an ACS stage of the HoneyBadgerBFT protocol ends.

4. The method according to claim 1, wherein

different consensus nodes in the consortium blockchain are provided with the same or at least partially different consensus verification items.

5. The method according to claim 1, wherein

a consensus verification item set by at least part of consensus nodes in the consortium blockchain comprises at least one of the following:

verification on a hash value of a local last block, verification on a timestamp of the target consensus, and verification on proposal data of the target consensus.

6. A data verification method of a consortium blockchain, comprising:

extracting, from a target block of a target consensus node of a consortium blockchain, recorded proposal data and a verification signature from at least one consensus node in the consortium blockchain, wherein the proposal data in the target block comes from a target consensus proposal, and the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal, and wherein at least part of consensus nodes in the consortium blockchain set a consensus verification item that is configured to perform risk verification according to their own security data; and

verifying the validity of the proposal data recorded in the target block based on a quantity of verification signatures extracted from the target block.

7. The method according to claim 6, wherein

verifying the proposal data recorded in the target block based on the quantity of the verification signatures extracted from the target block comprises:

if the quantity of the verification signatures extracted from the target block reaches 2F+1, determining that the proposal data recorded in the target block succeeds in the validity verification, wherein F is a quantity of abnormal consensus nodes tolerable by the consortium blockchain.

8. A consensus node of a consortium blockchain, wherein at least part of consensus nodes in the consortium blockchain set a consensus verification item that is configured to perform risk verification according to their own security data, wherein the consensus node comprises:

a sending module configured to, when a consensus operation is performed on a target consensus proposal, send a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal;

a receiving module configured to receive a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

a block generation module configured to, after a consensus is reached on proposal data of the target consensus, generate a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

9. A consortium blockchain system, comprising a plurality of consensus nodes, wherein a target consensus node among the plurality of consensus nodes performs the following when participating in a target consensus:

sending a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal, and wherein at least part of consensus nodes in the consortium blockchain set a consensus verification item that is configured to perform risk verification according to their own security data;

receiving a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

after a consensus is reached on proposal data of the target consensus, generating a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

10. A data verification apparatus of a consortium blockchain, comprising:

an extraction module configured to extract, from a target block of a target consensus node of a consortium blockchain, recorded proposal data and a verification signature from at least one consensus node in the consortium blockchain, wherein the proposal data in the target block comes from a target consensus proposal, and the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal, and wherein at least part of consensus nodes in the consortium blockchain set a consensus verification item that is configured to perform risk verification according to their own security data; and

a verification module configured to verify the validity of the proposal data recorded in the target block based on a quantity of verification signatures extracted from the target block.