

BLOCKCHAIN-BASED ASSET MANAGEMENT METHOD AND SYSTEM, SERVER AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] The present disclosure herein relates to the field of blockchain technology, especially to a blockchain-based asset management method and system, server and storage medium.

BACKGROUND

[0002] The asset management work of an enterprise refers to the effective management and control of various types of assets of the enterprise to protect the property safety of the enterprise, improve the efficiency of asset utilization, reduce operating costs, and enhance the competitiveness of the enterprise. Management and control include not only reasonable planning, but also accurate reimbursement. No matter how good the planning is, encountering chaotic asset reimbursements cannot effectively complete the asset management work of the enterprise. Therefore, reasonable planning and accurate reimbursement are an indispensable part of successfully completing enterprise asset management work.

[0003] In traditional asset management work, the reimbursement part is usually done by sending reimbursement requests and related certification materials to the corresponding staff members who have reimbursement needs. The staff members then complete the reimbursement work based on the reimbursement request and related certification materials. However, during this process, there is a possibility of tampering or forgery of the certification materials or reimbursement requests, which makes it difficult to effectively guarantee the authenticity of the final reimbursement results, leading to risks in the reimbursement work in asset management.

[0004] At present, the main focus is to deploy asset management work into the blockchain to reduce the occurrence of tampering or forgery of certification materials, thereby indirectly reducing the risk of asset management work. That is, personnel with reimbursement needs should first store relevant certification information directly in the blockchain to reduce the possibility of tampering with the certification information by involving other personnel; then send the reimbursement request to the corresponding asset management end, so that the asset management end can actively search for relevant certification information on the blockchain to complete the reimbursement work in asset management, thereby achieving the above purpose.

[0005] However, once the number of reimbursement requests increases, the existing methods will make the asset management end face multiple reimbursement requests at the same time. On the one hand, it will invisibly put pressure on the asset management end to receive requests, increase the probability of asset management end collapse, and fail to effectively reduce the risk of asset management work; on the one hand, it will invisibly put pressure on the asset management end to receive requests and increase the probability of the asset management end crashing, so that the purpose of reducing the risk of asset management work cannot be effectively achieved; on the other hand, it will also put pressure on the asset management end to process reimbursement work, increase the probability of errors in the asset management end processing process, and cannot effectively achieve the purpose of reducing the risk of asset management work.

SUMMARY

[0006] In order to reduce the risk of reimbursement work in asset management, embodiments of the present disclosure provide a blockchain-based asset management method and system, server and storage medium.

[0007] In the first aspect, this embodiment provides a blockchain-based asset management method, wherein the method comprises the steps:

obtaining a management information sent by a user end, judging whether a certification information in the management information is valid, and if valid, broadcasting the management information, wherein the management information includes a management request and corresponding certification information;

judging whether the broadcasting of the management information has been completed, and if so, sending the management request to an asset management end;

receiving corresponding pre-appropriation funds sent by the asset management end, which represent the allocation made by the asset management end according to the management request, and achieving a consensus on the pre-appropriation funds based on the certification information;

if the consensus is successful, sending an allocation instruction to the asset management end, representing that the asset management end can automatically disburse the pre-appropriation funds to the corresponding user; and

if the consensus is not successful, generating an adjustment information based on the certification information corresponding to the management request, and sending the adjustment information to the asset management end to adjust the

pre-appropriation funds sent by the asset management end to the corresponding user.

[0008] In some embodiments, broadcasting the management information includes:

obtaining a certification format of the certification information in the management information, judging whether the certification format is a preset format, and if so, broadcasting the management information across all nodes using an optimized strategy propagation method, wherein the optimized strategy propagation method is any one of hierarchical broadcasting, selecting trusted nodes, and limiting the broadcast range; and

if not, using a preset conversion model corresponding to the certification format to convert the certification information into a new certification information in the preset format, and broadcasting the new certification information and the corresponding management request across all nodes using the optimized strategy propagation method, wherein the new certification information and the corresponding management request constitute new management information.

[0009] In some embodiments, judging whether the broadcasting of the management information has been completed includes:

obtaining a memory pool status corresponding to each node at regular intervals, obtaining a number of nodes that have broadcast based on the memory pool status, judging whether the number of nodes is greater than a preset number of nodes, and if so, concluding that the broadcasting of the management information has been completed, wherein the preset number of nodes is not less than half of the total number of all nodes; and

otherwise, concluding that the broadcasting of the management information has not been completed.

[0010] In some embodiments, the method comprises the steps:

if the broadcasting of the management information has not been completed, obtaining a current broadcasting time, judging whether the broadcasting time is less than a preset reference broadcasting time, and if not, generating an alert signal representing the cessation of the asset management according to the management information; and

if it is less, continuing to wait for the next retrieval of the memory pool status corresponding to each node.

[0011] In some embodiments, achieving the consensus on the pre-appropriation funds based on the certification information includes:

each node obtains a total amount of funds in the corresponding certification information based on the obtained certification information, judges whether the total amount of funds is equal to the pre-appropriation funds based on a consensus mechanism, and if equal, the node stores a block data corresponding to the pre-appropriation funds in corresponding block;

if not equal, the node does not store the block data corresponding to the pre-appropriation funds in corresponding block;

judging whether a block height of the blocks corresponding to a preset number of qualified nodes are all the same, and if so, the consensus is successful; and

if not, the consensus is unsuccessful.

[0012] In some embodiments, generating the adjustment information based on the certification information corresponding to the management request includes:

subtracting the total amount of funds from the pre-appropriation funds to obtain a pre-appropriation difference, judging whether the pre-appropriation difference is greater than zero, and if it is greater than zero, the pre-appropriation difference serves as the basis for the asset management end to send a first adjustment information, indicating that less funds should be sent to the corresponding user on the basis of the pre-appropriation funds; and

if it is less than zero, the pre-appropriation difference serves as the basis for the asset management end to send a second adjustment information, indicating that more funds should be sent to the corresponding user on the basis of the pre-appropriation funds.

[0013] In some of the embodiments, if the consensus is not successful, further comprising generating an early warning signal, sending the early warning signal to the asset management end, and counting the number of times the early warning signal is generated.

[0014] In the second aspect, this embodiment provides a blockchain-based asset management system, the system comprises a blockchain end that includes an information receiving module, a broadcast module, an information output module, and a consensus module;

the information receiving module is used for obtaining a management information sent by a user end, and judging whether a certification information in the management information is valid;

the broadcast module is used if the certification information is valid,

broadcasting the management information, wherein the management information includes a management request and corresponding certification information; and judging whether the broadcasting of the management information has been completed;

the information output module is used if the broadcasting of the management information has been completed, sending the management request to an asset management end;

the consensus module is used for receiving corresponding pre-appropriation funds sent by the asset management end, which represent the allocation made by the asset management end according to the management request, and achieving a consensus on the pre-appropriation funds based on the certification information; and

the information output module is further used if the consensus is successful, sending an allocation instruction to the asset management end, representing that the asset management end can automatically disburse the pre-appropriation funds to the corresponding user; if the consensus is not successful, generating an adjustment information based on the certification information corresponding to the management request, and sending the adjustment information to the asset management end to adjust the pre-appropriation funds sent by the asset management end to the corresponding user.

[0015] In the third aspect, this embodiment provides a server, wherein the server comprises a processor and a memory, wherein a computer program that can run on the processor is stored on the memory, and when the computer program is executed by the processor, the blockchain-based asset management method as described in the first aspect is implemented.

[0016] In the fourth aspect, embodiments of the present disclosure provide a storage medium, wherein a computer program that can run on a processor is stored on the storage medium, wherein when the computer program is executed by the processor, the blockchain-based asset management method as described in the first aspect is implemented.

[0017] By adopting the above method, the blockchain end of the present disclosure first obtains the management information containing the management request and corresponding certification information sent by the user end, and then judges whether the certification information in the management information is valid. Only when the certification information is valid, the management information is broadcast, so that

the blockchain end pro-actively verifies whether the certification information is valid before broadcasting the management information, and does not disseminate invalid management information to the nodes to prepare for subsequent verification of whether the pre-appropriation funds are correct. After broadcasting the management information, it is also judged whether the broadcasting of the management information has been completed. Only after the blockchain end completes the broadcasting of the management information, the blockchain end sends the management request to the asset management end, ensuring that after receiving the pre-appropriation funds sent by the asset management end, the blockchain end can achieve the consensus based on the broadcast management information in a normal and orderly manner, reducing useless work such as subsequent management information sending and receiving pre-appropriation funds without completing the broadcasting. After all, the consensus results obtained by achieving consensus operations before completing the broadcast are not reliable.

[0018] The blockchain end will receive the corresponding pre-appropriation funds sent by the asset management end representing the asset management end according to the management request, and achieve the consensus based on the certification information that has been broadcast. If the consensus of the blockchain end is successful, it indicates that the pre-appropriation amount automatically divided to the allocation unit by the asset management end is accurate, then the blockchain end will send an allocation instruction to the asset management end, so that only the allocation unit will act in the asset management end, and the pre-appropriation funds in the allocation unit will be sent to the user in the corresponding management request, thus accurately completing the asset management work. In this way, even if the user end and the asset management end are subjected to external malicious attacks, the blockchain end will verify the validity of the certification information, broadcast and consensus, etc., to reduce the impact of the blockchain end from external malicious attacks, and reduce the risk of reimbursement work in asset management.

[0019] If the consensus on the blockchain end is not successful, it indicates that the asset management end may have been subjected to external malicious attacks, and the pre-appropriation amount automatically allocated to the allocation unit is inaccurate, that is, the reimbursement amount that the asset management end intends to allocate to the corresponding user is different from the amount of reimbursement requested by the user. Generating an adjustment information based on the certification information

corresponding to the management request, and sending the adjustment information to the asset management end to adjust the pre-appropriation funds sent by the asset management end to the corresponding user. In this way, even if the user end and the asset management end are subjected to external malicious attacks, the blockchain end will verify the validity of the certification information, broadcast and consensus, etc., if the consensus is unsuccessful, the asset management end will be sent to an adjustment information, allowing the asset management end to adjust the pre-appropriation funds sent to the corresponding users, accurately manage assets, and reduce the risk of reimbursement in asset management.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] FIG. 1 is a block diagram of a blockchain-based asset management method provided in this embodiment.

[0021] FIG. 2 is a block diagram of a method for broadcasting a management information provided by an embodiment of the present disclosure.

[0022] FIG. 3 is a block diagram of a method for achieving a consensus on the pre-appropriation funds based on a certification information provided by an embodiment of the present disclosure.

[0023] FIG. 4 is a framework diagram of a blockchain-based asset management system provided in this embodiment.

[0024] FIG. 5 is a structural block diagram of a server provided in this embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0025] In order to understand the purpose, technical solutions and advantages of the present disclosure more clearly, the present disclosure is described and illustrated below in conjunction with the accompanying drawings and embodiments. However, one of ordinary skilled in the art will understand that the present disclosure can be implemented without these details. It is obvious to those of ordinary skilled in the art that various changes can be made to the embodiments disclosed in the present disclosure, and the general principles defined in the present disclosure can be applied to other embodiments and application scenarios without departing from the principles and scope of the present disclosure. Accordingly, the present disclosure is not to be limited to the embodiments shown but is to be accorded the widest scope consistent with the scope of the present disclosure.

[0026] The embodiments of the present disclosure will be described in further detail below with reference to the accompanying drawings.

[0027] Blockchain is a chain composed of blocks one after another. Each block stores a certain amount of information, and they are connected into a chain in the order in which they were generated. This chain is stored in all servers. As long as one server in the entire system can work, the entire blockchain is safe. These servers are called nodes in the blockchain system, and each node can participate in the maintenance and management of the blockchain. Nodes are the fundamental components of blockchain, forming a blockchain network by means of communicating with each other, exchanging data, verifying information, etc., and providing storage space and arithmetic support for the entire blockchain system. If you want to modify the information in the blockchain, you must obtain the consent of more than half of the nodes and modify the information in all nodes, and these nodes are usually in the hands of different subjects, so it is extremely difficult to tamper with the information in the blockchain. Compared with traditional networks, blockchain includes two core characteristics: first, data is difficult to tamper with, and second, it is decentralized.

[0028] FIG. 1 is a block diagram of a blockchain-based asset management method provided in this embodiment. As shown in FIG. 1, the blockchain-based asset management method comprises the following steps:

Step 100: obtaining a management information sent by a user end, judging whether a certification information in the management information is valid, and if valid, broadcasting the management information, wherein the management information includes a management request and corresponding certification information.

[0029] Asset management requires the participation of three parties: the user end, the blockchain end and the asset management end. The user end is mainly used to assist users in transmitting management information to the blockchain end; the asset management end is mainly used to allocate corresponding funds to users; the blockchain end is mainly used to ensure that the management information provided by users is not tampered with by other parties, and check whether the funds that the asset management end intends to allocate to the corresponding users are correct. There is a communication connection channel between the user end, the blockchain end and the asset management end, and communication between each other can be achieved through this channel.

[0030] A management message includes a management request and a corresponding

set of certification information. The management request represents a reimbursement amount requested by a user for certain items during a specific period of time. The reimbursement amount is the total amount of funds requested by the user for reimbursement, and a management request corresponds one-to-one to a unique and determined user. The certification information represents information in at least one of transfer records, invoices or purchase records, used to prove the authenticity of a reimbursement request. A set of certification information includes at least one form of information, a set of certification information includes at least one sub-certification information, and each sub-certification information corresponds to an actual use of the reimbursement amount. For example, a piece of management information includes a management request from User A to reimburse 300 yuan for office supplies purchased on June 6, 2023, and a set of sub-certification information for purchasing paper for 100 yuan and sub-certification information for purchasing print cartridges for 200 yuan, then a set of certification information corresponding to the management request includes two sub-certification information. If the two sub-certification information both belong to one of the above ways of information, then the set of certification information includes information of one way; if the two sub-certification information belong to different ways of information, then the set of certification information includes two ways of information.

[0031] Each user corresponds to their own user end, and the user inputs management information into their own user end so that the user end can obtain the management information. Each user end establishes a communication connection with the blockchain end, so that once the user end receives the management information, it will automatically send the management information to the blockchain end through the established communication connection channel in order to enable the blockchain end to obtain the management information sent by the user end. Since the management request in the management information already carries the source that represents the management information, the blockchain end can distinguish each management information obtained, that is, which user is corresponding to each management information. Each user corresponds to their own user end, and the distributed characteristics of the blockchain allow the blockchain end to receive management information sent by multiple user ends at the same time. In this way, when multiple users send management information at the same time, the blockchain end can receive management information sent by these multiple user ends at the same

time without having to wait in line to send the management information, so that once a communication channel is established between the user end and the blockchain end, the management information can be quickly sent to the blockchain end based on this channel.

[0032] After obtaining management information, the blockchain end can obtain all the ways included in the certification information by checking the sub-certification information included in the certification information in the management information, which comprise one of seal, transfer time, or transfer party. If the certification information adopts the transfer record way, the transfer time and the transfer party of the certification information can be obtained by checking the management information; if the certification information adopts invoice way, the transfer party or the transfer party and seal of the certification information can be obtained by checking the management information; and if the certification information is the purchase record, the transfer time and the transfer party of the certification information can be obtained by checking the management information. The present disclosure defaults to the fact that the seals in the certification information are genuine seals. If the sub-certification information uses an invoice and there is no seal in the sub-certification information, then it is unnecessary to consider whether the transfer party is valid or not, and the sub-certification information will be invalid. The validity verification of the transfer party can be carried out by checking whether the attributes corresponding to the transfer party are consistent with the attributes purchased in the management request, and whether they belong to the specified purchasing attributes. If the attributes are consistent and belong to the specified purchasing attributes, the transfer party is valid; otherwise, the transfer party will be invalid. For example, if the attribute corresponding to the transfer party is an office supplies merchant, and the items purchased in the management request also belong to office supplies, and the office supplies belong to the specified purchasing attributes, then the transfer party is valid. The specified purchasing attributes include but are not limited to office supplies, public supplies, and cleaning supplies. The validity verification of the transfer time can be carried out by judging whether the transfer time is a working day and whether it is consistent with the time of the management request. If the transfer time is a working day and consistent with the time of the management request, then the transfer time is valid; otherwise, the transfer time will be invalid.

[0033] First, by checking the certification information in the management

information, you can get which sub-certification information is included in the certification information. Then, you can obtain all the ways included in the certification information through the way corresponding to each sub-certification information. Then, use the different ways mentioned above to verify the validity of all the methods contained in the certification information, if all methods are valid, then the certification information in the management information is valid; otherwise, the certification information in the management information is invalid. The management information is broadcast only if the certification information is valid, so that the blockchain end proactively verifies the validity of the certification information therein before broadcasting the management information, and does not disseminate invalid management information to the nodes in preparation for the subsequent verification of the correctness of the pre-appropriation funds.

[0034] FIG. 2 is a block diagram of a method for broadcasting a management information provided by an embodiment of the present disclosure. As shown in FIG. 2, broadcasting the management information includes the following steps:

Step 101: obtaining a certification format of the certification information in the management information, judging whether the certification format is a preset format, and if so, broadcasting the management information across all nodes using an optimized strategy propagation method, wherein the optimized strategy propagation method is any one of hierarchical broadcasting, selecting trusted nodes, and limiting the broadcast range.

[0035] Step 102: if not, using a preset conversion model corresponding to the certification format to convert the certification information into a new certification information in the preset format, and broadcasting the new certification information and the corresponding management request across all nodes using the optimized strategy propagation method, wherein the new certification information and the corresponding management request constitute new management information.

[0036] Each sub-certification information in the certification information may be any one of the certification formats in image format, Portable Document Format (PDF) format, and word format, the certification format of the certification information in the management information can be obtained by checking the suffix of each sub-certification information received, and the certification format of a set of certification information has at least one certification format. The preset format may be one of the above picture format, PDF format, and word format, and considering

that the corresponding photographs are also placed in the PDF format and the word format, and that in the case of the same amount of information, the certification information corresponding to the picture format requires less traffic during transmission process, this embodiment prioritizes the picture format as the preset format. If the certification format in a set of certification information has only a preset format, then the certification format is the preset format; and if the certification format in a set of certification information has other certification formats besides the preset format, then the certification format is not the preset format.

[0037] In the case that the certification format is the preset format, the node receiving the management information uses any one of the optimized strategy propagation method including hierarchical broadcasting, selecting trusted nodes, and limiting the broadcast range to broadcast the management information to the other nodes on the blockchain end. Hierarchical broadcasting realizes the entire broadcast by dividing the network into different levels and broadcasting to adjacent nodes first, thereby gradually expanding the broadcast range. Selecting trusted nodes is to select the specific nodes with higher bandwidth, stronger computing power, more reliable network connection, etc. as the trusted nodes in the network, and set it as the starting point for broadcasting. Limiting the broadcast range refers to limiting the range of each broadcast. By adopting the above optimized strategy propagation method, the speed of broadcasting management information to all nodes is improved.

[0038] In the case that the certification format is not the preset format, the node receiving the management information first converts the certification information into the new certification information in the preset format through the preset conversion model corresponding to the certification format. The preset conversion model may be a third-party format conversion tool or software deployed on the blockchain end, which can convert other certification formats that are not in the preset format to the preset format. It can also be a smart contract deployed on the blockchain end, which has corresponding programs for converting various certification formats to the preset format. The new certification information belonging to the preset format can be obtained from the certification information in other certification formats through the smart contract. The new certification information and the corresponding management request constitute the new management information, so that the node receiving the management information uses any one of the optimized strategy propagation method including hierarchical broadcasting, selecting trusted nodes, and limiting the

broadcast range to broadcast the converted new management information to the other nodes on the blockchain end. In this way, the certification information in the management information is unified in format before broadcasting the management information. On the one hand, compared with broadcasting all management information using the certification format before unification, it can save the traffic consumed during the broadcast process, and alleviate the pressure on the blockchain end; on the other hand, compared with first broadcasting the management information without format conversion, and then using smart contracts deployed on each node to perform format conversion, it will reduce the number of smart contract deployments, and alleviate the pressure on the blockchain end.

[0039] Step 200: judging whether the broadcasting of the management information has been completed, and if so, sending the management request to an asset management end.

[0040] After broadcasting the management information, it is necessary to further judge whether the broadcasting of the management information has been completed. Only after the blockchain end completes the broadcasting of the management information, the blockchain end sends the management request to the asset management end, ensuring that after receiving the pre-appropriation funds sent by the asset management end, the blockchain end can achieve the consensus based on the broadcast management information in a normal and orderly manner, reducing useless work such as subsequent management information sending and receiving pre-appropriation funds without completing the broadcasting. After all, the consensus results obtained by achieving consensus operations before completing the broadcast are not reliable. Judging whether the broadcasting of the management information has been completed includes the following steps:

Step 201: obtaining a memory pool status corresponding to each node at regular intervals, obtaining a number of nodes that have broadcast based on the memory pool status, judging whether the number of nodes is greater than a preset number of nodes, and if so, concluding that the broadcasting of the management information has been completed, wherein the preset number of nodes is not less than half of the total number of all nodes.

[0041] Step 202: otherwise, concluding that the broadcasting of the management information has not been completed.

[0042] Each node in the blockchain has a memory pool to maintain transactions that

have not yet been packaged into blocks, and when a node receives the broadcast management information, it will be added to the memory pool. The above-mentioned memory pool status is specifically the first status in which broadcast management information is stored, or the second status in which broadcast management information is not stored. By checking whether the management information is present in the memory pool corresponding to each node at fixed intervals, the memory pool status corresponding to each node can be obtained, and the number of nodes that have been broadcast can be obtained by counting the number of memory pools in the first status. The total number of nodes on the blockchain end is known. The above-mentioned preset number of nodes shall not be less than half of the total number of all nodes on the blockchain end. If the number of nodes in the first status is greater than the preset number of nodes, it indicates that the blockchain end has completed the broadcasting and can send the management request to the asset management end.

[0043] If the number of nodes in the first status is not greater than the preset number of nodes, it indicates that the blockchain has not completed the broadcasting. At this time, the current broadcasting time can be obtained. Judging whether the broadcasting time is less than the preset reference broadcasting time, and if not, generating an alert signal representing the cessation of the asset management according to the management information. If it is less, continuing to wait for the next retrieval of the memory pool status corresponding to each node.

[0044] The reference broadcasting time expected for a broadcast is stored on the blockchain end, and the reference broadcasting time represents the maximum broadcasting time allowed by the blockchain end. The above broadcasting time represents the actual time it takes for the blockchain end to broadcast a piece of management information. If the broadcasting time is not less than the reference broadcasting time, it means that the time for the blockchain end to broadcast this management information has exceeded the maximum allowed broadcasting time. This broadcast may be abnormal and generate an alert signal representing that asset management based on the management information has been stopped. The blockchain end will no longer broadcast, nor will it send management requests to the asset management end. According to the alert signal, the staff will know the status of the asset management work in a timely manner and know that the asset management work has not been completed. If the broadcasting time is less than the reference

broadcasting time, it means that the time for the blockchain end to broadcast this management information has not exceeded the maximum allowed broadcasting time. It can continue to wait for a fixed time and then obtain the memory pool status corresponding to each node next time, and continue to judge whether the broadcasting of the management information is completed. In this way, as long as the broadcasting of the management information has not been completed and the broadcasting time is less than the reference broadcasting time, it will continue to wait for the next time to obtain the memory pool status corresponding to each node, and complete the broadcasting of the management information to the greatest extent possible.

[0045] Step 300: receiving corresponding pre-appropriation funds sent by the asset management end, which represent the allocation made by the asset management end according to the management request, and achieving a consensus on the pre-appropriation funds based on the certification information.

[0046] After the asset management end receives the management request sent by the blockchain end, the asset management unit in the asset management end automatically divides it into the allocation unit for appropriation based on the reimbursement amount expressed in the management request. The allocation unit is only subject to allocation instructions or adjustment information control sent by the blockchain end. After funds are stored in the allocation unit, it will automatically be sent to the blockchain end to represent that the asset management end will allocate corresponding pre-appropriation funds according to the management request. After receiving the pre-appropriation funds, the blockchain end automatically broadcasts to all nodes, so that the nodes on the blockchain end achieve consensus on the pre-appropriation funds based on the received certification information. FIG. 3 is a block diagram of a method for achieving a consensus on a pre-appropriation funds based on a certification information provided by an embodiment of the present disclosure. As shown in FIG. 3, achieving the consensus on the pre-appropriation funds based on the certification information includes the following steps:

Step 301: each node obtains a total amount of funds in the corresponding certification information based on the obtained certification information, judges whether the total amount of funds is equal to the pre-appropriation funds based on a consensus mechanism, and if equal, the node stores a block data corresponding to the pre-appropriation funds in corresponding block.

[0047] Step 302: if not equal, the node does not store the block data corresponding

to the pre-appropriation funds in corresponding block.

[0048] Step 303: judging whether a block height of the blocks corresponding to a preset number of qualified nodes are all the same, and if so, the consensus is successful.

[0049] Step 304: if not, the consensus is unsuccessful.

[0050] If a node on the blockchain end does not have a set of certification information in the current management information, a set of certification information in the current management information can be obtained from a nearby node that stores a set of certification information in the current management information, so that each node on the blockchain end has a set of certification information in the current management information. By reading each sub-certification information in the set of certification information, the sub-amount corresponding to each sub-certification information can be obtained, and then the total amount of funds in the certification information can be obtained by superimposing the sub-amounts corresponding to all sub-certification information in the set of certification information. A consensus mechanism is stored on the blockchain, and all nodes on the blockchain are able to fairly and honestly compare the total amount of funds numerically with the received pre-appropriated funds based on the consensus mechanism. If the node determines that the two values are equal, then the block data is stored in the node in the corresponding block that is consistent with or the opposite of the value represented by the pre-appropriation funds. If the node determines that the two values are not equal, then the node takes no action, that is, no block data is stored in the corresponding block that is consistent with or opposite to the value represented by the pre-appropriation funds. When each block completes data storage, the height of the block will increase by one.

[0051] The above-mentioned preset standard number is the number set by the consensus mechanism in Step 301. This preset standard number is at least not less than half of the number of nodes that can achieve consensus. By obtaining the corresponding block height of each node, and then counting the number of first nodes corresponding to the same block height. If the largest number among the number of first nodes is not less than the preset standard number, it means that the block heights of the blocks corresponding to each node of the preset standard number is all the same, then the blockchain end successfully achieved a consensus on the pre-appropriation funds. If the largest number among the number of first nodes is less than the preset

standard number, it means that the block heights of the blocks corresponding to each node without the preset standard number is all the same, then the blockchain end fails to achieve a consensus on the pre-appropriation funds. In this way, by simply comparing the block heights of the blocks corresponding to the nodes in the blockchain to the same number and the preset standard number, it is possible to easily and intuitively judge whether the consensus on the pre-appropriation funds has been successful.

[0052] Step 400, if the consensus is successful, sending an allocation instruction to the asset management end, representing that the asset management end can automatically disburse the pre-appropriation funds to the corresponding user.

[0053] Step 500, if the consensus is not successful, generating an adjustment information based on the certification information corresponding to the management request, and sending the adjustment information to the asset management end to adjust the pre-appropriation funds sent by the asset management end to the corresponding user.

[0054] If the consensus of the blockchain end is successful, it indicates that the pre-appropriation amount automatically divided to the allocation unit by the asset management end is accurate, then the blockchain end will send an allocation instruction to the asset management end, so that only the allocation unit will act in the asset management end, and the pre-appropriation funds in the allocation unit will be sent to the user in the corresponding management request, thus accurately completing the asset management work. In this way, even if the user end and the asset management end are subjected to external malicious attacks, the blockchain end will verify the validity of the certification information, broadcast and consensus, etc., to reduce the impact of the blockchain end from external malicious attacks, and reduce the risk of reimbursement work in asset management.

[0055] If the consensus on the blockchain end is not successful, it indicates that the asset management end may have been subjected to external malicious attacks, and the pre-appropriation amount automatically allocated to the allocation unit is inaccurate, that is, the reimbursement amount that the asset management end intends to allocate to the corresponding user is different from the amount of reimbursement requested by the user. The blockchain end will generate adjustment information by calculating the difference between the amount represented by the certification information and the pre-appropriation funds, and then send the adjustment information to the allocation

unit in the asset management end. Based on the value represented by the adjustment information, the allocation unit will judge whether to require the asset management end to automatically reallocate the amount represented by the adjustment information to the allocation unit, or to transfer the amount stored in its own allocation unit out of the amount represented by the adjustment information, and return the transferred amount to the asset management unit in the asset management end. After the amount in the allocation unit is adjusted, the last amount stored in the allocation unit is what the asset management end needs to send to the user in the corresponding management request. In this way, even if the user end and the asset management end are subjected to external malicious attacks, the blockchain end will verify the validity of the certification information, broadcast and consensus, etc., if the consensus is unsuccessful, the asset management end will be sent to an adjustment information, allowing the asset management end to adjust the pre-appropriation funds sent to the corresponding users, accurately manage assets, and reduce the risk of reimbursement in asset management.

[0056] Generating the adjustment information based on the certification information corresponding to the management request includes: subtracting the total amount of funds from the pre-appropriation funds to obtain a pre-appropriation difference, judging whether the pre-appropriation difference is greater than zero, and if it is greater than zero, the pre-appropriation difference serves as the basis for the asset management end to send a first adjustment information, indicating that less funds should be sent to the corresponding user on the basis of the pre-appropriation funds; and if it is less than zero, the pre-appropriation difference serves as the basis for the asset management end to send a second adjustment information, indicating that more funds should be sent to the corresponding user on the basis of the pre-appropriation funds. The adjustment information includes the first adjustment information and the second adjustment information. That is, the pre-appropriation difference is greater than zero, indicating that the amount in the allocation unit is greater than the amount that actually needs to be sent to the user in the corresponding management request, then the first adjustment information generated by the blockchain end is an information that allows the allocation unit to transfer the amount stored in its own allocation unit out of the amount represented by the adjustment information, and return the transferred amount to the asset management unit in the asset management end based on the numerical value represented by the adjustment information. The

pre-appropriation difference is less than zero, indicating that the amount in the allocation unit is less than the amount that actually needs to be sent to the user in the corresponding management request, then the second adjustment information generated by the blockchain end is an information that allows the allocation unit to automatically allocate the amount represented by the adjustment information to the allocation unit based on the numerical value represented by the adjustment information. The allocation unit on the asset management end will take corresponding actions after receiving the first adjustment information or the second adjustment information, so as to accurately complete the asset management work.

[0057] In addition, if the consensus on the blockchain end is not successful, the blockchain end will also generate an early warning signal and send the early warning signal to the asset management end, which plays a role in allowing the asset management end to timely understand whether the amount of allocations made according to management requests is accurate. The blockchain end also counts the number of times warning signals are generated, so that it can provide a reference for subsequent evaluation of the asset management end's own security.

[0058] FIG. 4 is a framework diagram of a blockchain-based asset management system provided in this embodiment. As shown in FIG. 4, a blockchain-based asset management system comprises a blockchain end that includes an information receiving module, a broadcast module, an information output module, and a consensus module.

[0059] The information receiving module is used for obtaining a management information sent by a user end, judging whether a certification information in the management information is valid. The broadcast module is used if the certification information is valid, broadcasting the management information, wherein the management information includes a management request and corresponding certification information; judging whether the broadcasting of the management information has been completed. The information output module is used for sending the management request to an asset management end if the broadcasting of the management information is completed. The consensus module is used for receiving corresponding pre-appropriation funds sent by the asset management end, which represent the allocation made by the asset management end according to the management request, and achieving a consensus on the pre-appropriation funds based on the certification information. The information output module is further used if the

consensus is successful, sending an allocation instruction to the asset management end, representing that the asset management end can automatically disburse the pre-appropriation funds to the corresponding user; if the consensus is not successful, generating an adjustment information based on the certification information corresponding to the management request, and sending the adjustment information to the asset management end to adjust the pre-appropriation funds sent by the asset management end to the corresponding user.

[0060] The other functions performed by the aforementioned information receiving module, broadcast module, information output module, and consensus module, as well as the technical details of each function, are the same or similar to the corresponding features in the previously described blockchain-based asset management method and will therefore not be described in detail.

[0061] FIG. 5 is a structural block diagram of a server provided in this embodiment. As shown in FIG. 5, the server includes a processor 51 and a memory 52. The memory 52 stores a computer program 53 that can run on the processor 51. When the computer program 53 is executed by the processor, the blockchain-based asset management method provided in the embodiments of the present disclosure are implemented.

[0062] The memory 52 can be a Read Only Memory (ROM) or other types of static storage devices that can store static information and instructions, Random Access Memory (RAM) or other types of dynamic storage devices that can store information and instructions. It can also be Electrically Erasable Programmable Read Only Memory (EEPROM), Compact Disc Read Only Memory (CD-ROM) or other optical disc storage, including compressed discs, laser discs, disc, digital versatile discs, Blu-ray discs, etc., magnetic disk storage media or other magnetic storage devices, or any other medium that can be used to carry or store desired program codes in the form of instructions or data structures and can be accessed by a computer, but not limited to these. Memory 52 may be an internal storage unit in some embodiments.

[0063] The processor 51 may be a central processing unit, a general purpose processor, a data signal processor, a specific integrated circuit, a field programmable gate array or other programmable logic devices, transistor logic devices, hardware components or any combination thereof. For executing program codes or processing data stored in the memory 52.

[0064] The processor 51 and the memory 52 are connected via a bus. The bus may

include a path that carries information between the above-mentioned components. The bus can be a peripheral component interconnection standard bus or an extended industry standard structure bus, etc. The bus can be divided into an address bus, a data bus, a control bus, etc. For ease of presentation, only one thick line is used in FIG. 5, but it does not mean that there is only one bus or one type of bus.

[0065] FIG. 5 only shows a server with a memory 52, a processor 51, and a bus. It can be understood in the art that the structure shown in FIG. 5 does not limit the server. It can be a bus type structure or a star type structure. The server may also include more or fewer components than shown, some combinations of components, or different component arrangements. Other existing or future electronic equipment shall, where applicable, be included in the scope of protection and are incorporated herein by reference.

[0066] The embodiment of the present disclosure provides a computer-readable storage medium. The computer-readable storage medium stores a computer program. When it is run on a computer, the computer can execute the aforementioned blockchain-based asset management method in the embodiment.

[0067] It should be understood that although various steps in the flow chart of the accompanying drawings are shown in sequence as indicated by arrows, these steps are not necessarily executed in the order indicated by arrows. Unless explicitly stated in the present disclosure, the execution of these steps is not strictly limited in order, and they can be executed in other orders.

[0068] The above are only some of the embodiments of the present disclosure, and it should be noted that for those ordinary skilled in the art, a number of improvements and modifications can be made without departing from the principles of the present disclosure, and these improvements and modifications should also be regarded as the scope of protection of the present disclosure.

CLAIMS

What is claimed is:

1. A blockchain-based asset management method, wherein the method comprises the steps:

obtaining a management information sent by a user end, judging whether a certification information in the management information is valid, and if valid, broadcasting the management information, wherein the management information includes a management request and corresponding certification information; the management request represents a reimbursement amount requested by a user for certain items during a specific period of time, and the certification information represents information in at least one of transfer records, invoices or purchase records, used to prove the authenticity of a reimbursement request;

judging whether the broadcasting of the management information has been completed, and if so, sending the management request to an asset management end;

receiving corresponding pre-appropriation funds sent by the asset management end, which represent the allocation made by the asset management end according to the management request, and achieving a consensus on the pre-appropriation funds based on the certification information;

if the consensus is successful, sending an allocation instruction to the asset management end, representing that the asset management end can automatically disburse the pre-appropriation funds to the corresponding user;

if the consensus is not successful, generating an adjustment information based on the certification information corresponding to the management request, and sending the adjustment information to the asset management end to adjust the pre-appropriation funds sent by the asset management end to the corresponding user; and

judging whether the certification information in the management information is valid comprises: obtaining all the methods included in the certification information, which comprise one of seal, transfer time, or transfer party; verifying whether all the methods included in the certification information are valid using the corresponding validation methods for each method, if all are valid, the certification information in the management information is valid; otherwise, the certification information in the management information is invalid.

2. The method according to claim 1, wherein broadcasting the management

information comprises:

obtaining a certification format of the certification information in the management information, judging whether the certification format is a preset format, and if so, broadcasting the management information across all nodes using an optimized strategy propagation method, wherein the optimized strategy propagation method is any one of hierarchical broadcasting, selecting trusted nodes, and limiting the broadcast range; and

if not, using a preset conversion model corresponding to the certification format to convert the certification information into a new certification information in the preset format, and broadcasting the new certification information and the corresponding management request across all nodes using the optimized strategy propagation method, wherein the new certification information and the corresponding management request constitute new management information.

3. The method according to claim 1, wherein judging whether the broadcasting of the management information has been completed comprises:

obtaining a memory pool status corresponding to each node at regular intervals, obtaining a number of nodes that have broadcast based on the memory pool status, judging whether the number of nodes is greater than a preset number of nodes, and if so, concluding that the broadcasting of the management information has been completed, wherein the preset number of nodes is not less than half of the total number of all nodes; and

otherwise, concluding that the broadcasting of the management information has not been completed.

4. The method according to claim 3, wherein the method comprises the steps:

if the broadcasting of the management information has not been completed, obtaining a current broadcasting time, judging whether the broadcasting time is less than a preset reference broadcasting time, and if not, generating an alert signal representing the cessation of the asset management according to the management information; and

if it is less, continuing to wait for the next retrieval of the memory pool status corresponding to each node.

5. The method according to claim 2, wherein achieving the consensus on the pre-appropriation funds based on the certification information comprises:

each node obtains a total amount of funds in the corresponding certification

information based on the obtained certification information, judges whether the total amount of funds is equal to the pre-appropriation funds based on a consensus mechanism, and if equal, the node stores a block data corresponding to the pre-appropriation funds in corresponding block;

if not equal, the node does not store the block data corresponding to the pre-appropriation funds in corresponding block;

judging whether a block height of the blocks corresponding to a preset number of qualified nodes are all the same, and if so, the consensus is successful; and

if not, the consensus is unsuccessful.

6. The method according to claim 5, wherein generating the adjustment information based on the certification information corresponding to the management request comprises:

subtracting the total amount of funds from the pre-appropriation funds to obtain a pre-appropriation difference, judging whether the pre-appropriation difference is greater than zero, and if it is greater than zero, the pre-appropriation difference serves as the basis for the asset management end to send a first adjustment information, indicating that less funds should be sent to the corresponding user on the basis of the pre-appropriation funds; and

if it is less than zero, the pre-appropriation difference serves as the basis for the asset management end to send a second adjustment information, indicating that more funds should be sent to the corresponding user on the basis of the pre-appropriation funds.

7. The method according to claim 1, wherein if the consensus is not successful, further comprising generating an early warning signal, sending the early warning signal to the asset management end, and counting the number of times the early warning signal is generated.

8. A blockchain-based asset management system, wherein the system comprises a blockchain end that includes an information receiving module, a broadcast module, an information output module, and a consensus module;

the information receiving module is used for obtaining a management information sent by a user end, and judging whether a certification information in the management information is valid;

the broadcast module is used if the certification information is valid, broadcasting the management information, wherein the management information

includes a management request and corresponding certification information; the management request represents a reimbursement amount requested by a user for certain items during a specific period of time, and the certification information represents information in at least one of transfer records, invoices or purchase records, used to prove the authenticity of a reimbursement request; and judging whether the broadcasting of the management information has been completed;

the information output module is used if the broadcasting of the management information has been completed, sending the management request to an asset management end;

the consensus module is used for receiving corresponding pre-appropriation funds sent by the asset management end, which represent the allocation made by the asset management end according to the management request, and achieving a consensus on the pre-appropriation funds based on the certification information;

the information output module is further used if the consensus is successful, sending an allocation instruction to the asset management end, representing that the asset management end can automatically disburse the pre-appropriation funds to the corresponding user; if the consensus is not successful, generating an adjustment information based on the certification information corresponding to the management request, and sending the adjustment information to the asset management end to adjust the pre-appropriation funds sent by the asset management end to the corresponding user; and

judging whether the certification information in the management information is valid comprises: obtaining all the methods included in the certification information, which comprise one of seal, transfer time, or transfer party; verifying whether all the methods included in the certification information are valid using the corresponding validation methods for each method, if all are valid, the certification information in the management information is valid; otherwise, the certification information in the management information is invalid.

9. A server, wherein the server comprises: a processor and a memory, wherein a computer program that can run on the processor is stored on the memory, and when the computer program is executed by the processor, the blockchain-based asset management method as described in any one of claims 1 to 7 being implemented.

10. A computer-readable storage medium, wherein a computer program that can run on a processor is stored on the computer-readable storage medium, wherein when

the computer program is executed by the processor, the blockchain-based asset management method as described in any one of claims 1 to 7 being implemented.