ELECTION METHOD AND APPARATUS FOR REPRESENTATIVE NODE DEVICE, COMPUTER DEVICE, AND STORAGE MEDIUM

[0001] This application claims priority to Chinese Patent Application No. 201811046270.0, titled "METHOD AND APPARATUS FOR ELECTING REPRESENTATIVE NODE DEVICE, COMPUTER DEVICE, AND STORAGE MEDIUM" filed with the Chinese Patent Office on September 7, 2018, which is incorporated by reference in its entirety.

FIELD

[0002] The present disclosure relates to the technical field of blockchain, and in particular to a method and an apparatus for electing a representative node device, a computer device, and a storage medium.

BACKGROUND

[0003] In recent years, with the development of network technologies, a blockchain system is widely applied to life. The blockchain system may include multiple node devices. Each node device may store transaction data by utilizing blocks and connect the blocks sequentially in chronological order to form a chain data structure, so as to form a distributed account book in the blockchain system.

[0004] At present, node devices may generate a block through the following process. When a transaction occurs on any node device, the node device may record transaction data and broadcast the transaction data in a blockchain system, so that other node devices in the blockchain system receive the transaction data. After the node devices in the blockchain system receive the transaction data, the node devices may package the transaction data to generate a new block, and perform verification on the new block based on a consensus mechanism. After the new block is verified, each node device may add the new block to a blockchain configured on nodes.

[0005] In the foregoing process in which the node devices generate a block, a representative node device may be elected to replace all the node devices to generate a block, to improve working efficiency of the blockchain system. Any node device in the blockchain system may become the representative node device, node devices have different qualifications because the node devices are

different in terms of performance or authority. In addition, there may be a malicious node device that constantly transmits erroneous information in the blockchain system. Once an unqualified node device or a malicious node device is elected as the representative node device, normal operation of the blockchain system is affected. In this case, there is an urgent need for a method for electing a representative node device that can ensure normal operation of the blockchain system.

SUMMARY

[0006] According to embodiments of the present disclosure, a method and an apparatus for electing a representative node device, a computer device, and a storage medium are provided.

[0007] A method for electing a representative node device is provided. The method is performed by a first node device, the first node device is any node device in a blockchain system, and the method includes:

receiving candidate addition transaction data, where the candidate addition transaction data carries credential data, the credential data indicates that the first node device meets a qualification requirement for a candidate node device;

storing the candidate addition transaction data on a target blockchain of the blockchain system in a case that multiple node devices among the blockchain system verify the candidate addition transaction data by consensus; and

participating in an election of the representative node device according to the candidate addition transaction data stored on the target blockchain.

[0008] An apparatus for electing a representative node device is provided. The apparatus includes: a receiving module, a storage module and an election module. The receiving module is configured to receive candidate addition transaction data. The candidate addition transaction data carries credential data, and the credential data indicates that a first node device meets a qualification requirement for a candidate node device. The storage module is configured to store the candidate addition transaction data on a target blockchain of a blockchain system in a case that multiple node devices in the blockchain system verify the candidate addition transaction data by consensus. The election module is configured to participate in an election of the representative node device according to the candidate addition transaction data stored on the target blockchain.

[0009] A computer device is provided, including a processor and a memory. The memory stores computer-readable instructions. The computer-readable instructions, when executed by the processor, cause the processor to perform the following operations:

receiving candidate addition transaction data, where the candidate addition transaction data carries credential data, the credential data indicates that the first node device meets a qualification requirement for a candidate node device;

storing the candidate addition transaction data on a target blockchain of the blockchain system in a case that multiple node devices in the blockchain system verify the candidate addition transaction data by consensus; and

participating in an election of the representative node device according to the candidate addition transaction data stored on the target blockchain.

[0010] A non-volatile computer-readable storage medium is provided, which stores computer-readable instructions. The computer-readable instructions, when executed by one or more processors, cause the one or more processors to perform the following operations:

receiving candidate addition transaction data, where the candidate addition transaction data carries credential data, the credential data indicates that the first node device meets a qualification requirement for a candidate node device;

storing the candidate addition transaction data on a target blockchain of the blockchain system in a case that multiple node devices in the blockchain system verify the candidate addition transaction data by consensus; and

participating in an election of the representative node device according to the candidate addition transaction data stored on the target blockchain.

[0011] Details of one or more embodiments of the present disclosure are provided in the accompanying drawings and description below. Other features, objectives, and advantages of the present disclosure become apparent from the specification, the accompanying drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] To describe the technical solutions of the embodiments of the present disclosure more clearly, the accompanying drawings required for describing the embodiments are described briefly hereinafter. Apparently, the accompanying drawings in the following description show only some embodiments of the present disclosure, and a person of ordinary skill in the art may derive other accompanying drawings from the accompanying drawings without creative efforts.

[0013] FIG. 1 is a schematic structural diagram of a blockchain system according to an embodiment of the present disclosure.

[0014] FIG. 2 is a flowchart of a method for electing a representative node device according to an embodiment of the present disclosure.

[0015] FIG. 3 is a flowchart of a qualification auditing process for a node device according to an embodiment of the present disclosure.

[0016] FIG. 4 is a schematic structural diagram of an apparatus for electing a representative node device according to an embodiment of the present disclosure.

[0017] FIG. 5 is a schematic structural diagram of a server according to an embodiment of the present disclosure.

DETAILED DESCRIPTION OF EMBODIMENTS

[0018] To enable the objectives, technical solutions, and advantages of the present disclosure clearer, embodiments of the present disclosure are described in detail with reference to the accompanying drawings.

[0019] FIG. 1 is a schematic structural diagram of a blockchain system according to an embodiment of the present disclosure. Referring to FIG. 1, the blockchain system includes multiple node devices on which a same blockchain is configured. The multiple node devices may be multiple servers belonging to a same organization, multiple servers belonging to different organizations, or multiple terminals of a user. This is not limited in the embodiments of the present disclosure. The term "multiple" mentioned in the embodiments of the present disclosure refers to "more than one".

[0020] The multiple node devices each can receive transaction data. When the blockchain system uploads the transaction data to the blockchain, different nodes play different roles. Thus, the node devices may be classified into representative node devices and non-representative node devices. A representative node device is configured to generate a block and perform verification on the block by consensus. A non-representative node device is configured to receive the block verified by the representative node device by consensus, perform verification on the block, and store the verified block on a target blockchain. Depending on performances, the non-representative node devices may be classified into ordinary node devices and candidate node devices.

[0021] In addition, in the embodiments of the present disclosure, a target server is further provided. The target server may serve as an auditor, and is configured to receive a candidate

application request transmitted by at least one node device in the blockchain system, perform a qualification audit on the node device in response to the candidate application request, and generate credential data. The target server may transmit the credential data to the audited node device, so that the node device, by means of the credential data that meets a preset rule, becomes the candidate node device of the representative node device in the blockchain system.

[0022] In some embodiments, an example of a process of recording transaction data in the blockchain system is as follows. In a case that any node device in the blockchain system receives the transaction data, the node device broadcasts the received transaction data in the blockchain system, so that other node devices receive the transaction data. After the representative node device in the blockchain system receives the transaction data, the representative node device generates a block based on the transaction data, so that representative node devices perform verification on the block by consensus. After the representative node devices verify the block by consensus, the representative node device broadcasts the block in the blockchain system. After receiving the block broadcasted by the representative node device, the non-representative node device performs verification on the block. After being verified, the block is stored on the target blockchain configured on the non-representative node device.

[0023] The consensus described in the embodiments of the present disclosure indicates that multiple node devices in the blockchain system separately perform verification on data. In a case that verification performed by any node device succeeds, a verification success message is broadcasted in the blockchain system. In a case that the verification success message received by any node device meets a preset consensus policy, it is determined that the data is verified by consensus.

[0024] For example, descriptions are provided by an example in which verification by consensus is performed by the representative node devices in the blockchain system. The verification by consensus may be performed through the proof of work (POW) mechanism. The process is described as follows. The representative node device in the blockchain system generates a block. The representative node device calculates a hash value of a block header of the generated block and determines whether the hash value is less than a current target value. In a case that the hash value is greater than the target value, the representative node device changes a random number in the generated block accordingly and recalculates the hash value. In a case that the hash value calculated by the representative node device is less than the target value, the representative node device broadcasts a first block to other representative node devices or broadcast the first block in the blockchain system. Other representative node devices perform verification on the first block

after receiving the first block. In a case that most of the other representative node devices all agree with validity of the first block, the first block is verified by consensus.

[0025] In the system provided in the embodiments of the present disclosure, it is unnecessary to check whether transaction data can be stored after all node devices in the blockchain system generate a block and most of the node devices in the blockchain system reach a consensus on the generated block. In fact, the representative node devices generate a block and perform verification on the block by consensus, and the non-representative node device completes verification, so that transaction data can be recorded in the blockchain system, thereby improving working efficiency of the blockchain system.

[0026] Further, to illustrate a process of electing a representative node device in the blockchain system, descriptions are provided below by a specific embodiment.

[0027] FIG. 2 is a flowchart of a method for electing a representative node device according to an embodiment of the present disclosure. Referring to FIG. 2, the method according to this embodiment of the present disclosure includes the following steps S201 to S218.

[0028] In S201, a first node device transmits a candidate application request to a target server. The candidate application request carries qualification information of the first node device.

[0029] The first node device is any node device in the blockchain system. The target server may be one or more servers in the blockchain system, or one or more servers outside the blockchain system. The target server may be provided with at least one terminal device. A user functioning as an auditor may log in to the terminal device to perform a qualification audit on the node device in the blockchain system. It may be understood that the target server may be any node device in the blockchain system, or a server of a third-party organization associated with the blockchain system.

[0030] The first node device transmits the candidate application request to the target server, so that the target server performs a qualification audit on the first node device based on the qualification information carried in the candidate application request, to check whether the first node device can become a candidate node device.

[0031] The qualification information of the first node device carried in the candidate application request may include any one of the following: device performance of the first node device; a deposit of a preset amount that has been paid by the first node device to the target server; and a credit value of a user account corresponding to the first node device. Practically, the qualification information may include other content, and this is not limited in this embodiment.

[0032] If the blockchain system currently subjects to a first election, the first node device may be a non-representative node device. If the blockchain system does not subject to the first election currently, the first node device is any ordinary node device. That is, the first node device is neither a representative node device, nor a candidate node device.

[0033] In S202, the target server, after receiving the candidate application request, performs a qualification audit on the first node device; and generates credential data in a case that the first node device meets a qualification requirement for a candidate node device.

[0034] In this case, the first node device may be referred to as a first target node device. That is, in a case that the first target node device meets the qualification requirement for the candidate node device, the credential data is generated. The credential data may indicate that the first target node device meets the qualification requirement for the candidate node device.

[0035] The target server may transmit, after receiving the candidate application request, the qualification information carried in the candidate application request to at least one terminal device configured on the target server, so that the user performs a qualification audit on the node device through the terminal device.

[0036] The qualification audit is performed as follows. When the qualification information meets the qualification requirement for the candidate node device, the audit is passed. For example, the audit is passed in a case that device performance of the node device meets a preset performance condition; or the audit is passed in a case that the node device has paid a deposit of a preset amount; or the audit is passed in a case that credit of a user corresponding to the node device meets a preset credit condition. In a case that the first node device passes the qualification audit, the first node device is eligible to become the candidate node device. It may be understood that the first target node device may be any node device in the blockchain system. If the first target node device meets the qualification requirement for the candidate node device, the first target node device may be the first node device.

[0037] In a case that the qualification audit on the first node device (the first target node device) is passed, credential data is generated by the terminal device. The credential data may include a consent identifier, generation time of a credential, a validity period of the credential, and a signature of the user. It may be understood that the target server may transmit, after receiving the candidate application request, qualification information carried in the candidate application request to multiple terminal devices configured on the target server, so that multiple users perform a qualification audit on the node device through the terminal devices. In addition, the credential data may include multiple consent identifiers, generation time of multiple credentials, validity periods of

the multiple credentials, and signatures of the multiple users. The consent identifier indicates that the user agrees that the first node device can become the candidate node device. The validity period may be utilized for performing verification on validity of the credential data, thereby preventing a non-candidate node device from becoming a representative node device by means of credential data maliciously obtained. The signature is a signature added by the user to the qualification information. In a case that the qualification audit on the first node device is not passed, the terminal device may not generate credential data. The terminal device transmits the generated credential data to the target server. The target server summarizes all pieces of credential data. Alternatively, the terminal device may feed back an audit result only to the target server. The target server generates credential data based on the audit result of the terminal device participating in the audit.

[0038] Alternatively, the target server may perform a qualification audit on the first node device. In a case that the first node device passes the qualification audit performed by the target server, credential data is generated by the target server. The credential data includes: a consent identifier, generation time of a credential, a validity period of the credential, and a signature of the target server. The signature refers to a signature added by the target server to the qualification information for the first node device by utilizing a private key of the target server.

[0039] The target server may perform an audit off-line or on-line. In a case that the audit is performed off-line, an on-line operation of the target server is not affected, and the qualification information is processed and analyzed manually, so that effectiveness and credibility of the audit can be improved. In a case that the audit is performed on-line, a real-time property of the audit is improved, and labor costs are reduced.

[0040] In S203, the target server transmits the credential data to the first node device.

[0041] The target server transmits the credential data to the first node device, so that the first node device initiates a candidate addition transaction in the blockchain system based on the credential data.

[0042] In S204, the first node device broadcasts candidate addition transaction data in the blockchain system based on the credential data. The candidate addition transaction data includes the credential data and a list of candidate node devices. The list of candidate node devices includes multiple first target node devices, and the credential data includes credential data corresponding to multiple first target node devices.

[0043] The first node device initiates a candidate addition transaction in the blockchain system, so that the first node device may become a candidate node device. All node devices in the blockchain system receive the broadcasted candidate addition transaction data.

[0044] In this embodiment of the present disclosure, an example in which the first node device applies to become the candidate node device, and the first node device transmits the candidate addition transaction data is utilized for description. In some embodiments, any node device in the blockchain system may transmit the candidate addition transaction data, and the candidate addition transaction data may be received by any node device in the blockchain system. Specific implementations are not limited in the embodiments of this application.

[0045] In S205, second node devices receive the candidate addition transaction data.

[0046] The second node devices are node devices other than the first node device. The terms "first", "second", and "third" and so on described in the embodiments of the present disclosure are intended to distinguish different node device, rather than distinguish functions of the node devices.

[0047] In S206, multiple node devices in the blockchain system store the candidate addition transaction data into a target blockchain of the blockchain system in a case that the multiple node devices in the blockchain system verify the candidate addition transaction data by consensus.

[0048] In the embodiment of the present disclosure, the multiple node devices verifying the candidate addition transaction data by consensus may include that multiple representative node devices in the blockchain system verify the candidate addition transaction data by consensus. The multiple representative node devices in the blockchain system may be multiple representative node devices among the second node devices. The multiple representative node devices may perform verification on the candidate addition transaction data in at least one of the following verification manners:

[0049] (1) A representative node device performs verification on validity of the candidate addition transaction data based on whether the credential data include a preset number of consent identifiers. In a case that the credential data includes the preset number of consent identifiers, the representative node device determines that the candidate addition transaction data is valid. In a case that the number of representative node devices determining that the candidate addition transaction data is valid among the multiple representative node devices meets a preset consensus reaching condition, a consensus is reached. The preset consensus reaching condition may include that: all the representative node devices determine validity or a preset number or a preset ratio of representative

node devices among all representative node devices determine validity, and this is not limited in the embodiment of the present disclosure.

[0050] (2) A representative node device verifies validity of the candidate addition transaction data based on a validity period of the credential data. In a case that the validity period of the credential data does not expire, the representative node device determines that the candidate addition transaction data is valid. When multiple representative node devices determine that the candidate addition transaction data is valid, a consensus is reached. The credential data may include multiple validity periods, and the validity periods may be inconsistent. A validity period that expires earliest among the multiple validity periods may be adopted to determine whether the candidate addition transaction data is valid.

[0051] For a blockchain system subjecting to a first election, a preset initial representative node device may function as a node device participating in a consensus process this time. Subsequently, multiple representative node devices are elected. The multiple elected representative node devices may be switched to a running state of a representative node device, to participate in a process of block generation and consensus of the entire blockchain system. A node device that is not elected as a representative node device is in a running state of a non-representative node device, and does not participate in the process of block generation and consensus of the entire blockchain system.

[0052] In the foregoing steps S201 to S206, multiple candidate node devices in the blockchain system are determined according to the qualification audit performed on the node devices in the blockchain by the target server.

[0053] In this case, any node device in the entire blockchain system knows an identity of the first target node device as the candidate node device. Therefore, in the blockchain system, an election may be performed on the multiple candidate node devices indicated by the candidate addition transaction data, that is, the multiple first target node devices, to elect a representative node device.

[0054] Any node device in the blockchain may participate in an election of the representative node device according to the candidate addition transaction data stored on the target blockchain.

[0055] A specific election process is described as follows.

[0056] In S207, the first node device receives voting transaction data of a user.

[0057] Transaction data in the blockchain system may include voting transaction data and other transaction data. The voting transaction data may be generated based on a voting target of a user in the blockchain system. The voting transaction data may include: a transaction type, a list of node devices to be voted, a private key signature of a voting user, and the like.

[0058] In this embodiment, a voting target of a user is the candidate node device stored in the blockchain system.

[0059] In this embodiment of the present disclosure, a process of electing a representative node device is described by an example in which a user votes by logging in to the first node device to elect a representative node device. Alternatively, a user may log in to another node device of the blockchain system to vote, and this is not limited in the present disclosure.

[0060] In S208, the first node device broadcasts the voting transaction data in the blockchain system.

[0061] In S209, the second node devices receive the voting transaction data.

[0062] In S210, the second node devices receive the voting transaction data for candidate node devices; in a case that the multiple node devices in the blockchain system verify the voting transaction data by consensus, the voting transaction data is stored on the target blockchain of the blockchain system.

[0063] In this embodiment of the present disclosure, the multiple node devices verifying the voting transaction data by consensus may include that multiple representative node devices currently working in the blockchain system verify the voting transaction data by consensus.

[0064] In S211, in a case that the number of generated blocks reaches a second preset number, the first node device determines multiple first blocks from blocks of the target blockchain. The multiple first blocks are configured to store the voting transaction data of the candidate node devices.

[0065] In S211, the first node device may search the blocks of the target blockchain based on a voting transaction type, to obtain a block storing the voting transaction type as the first block.

[0066] In this embodiment of the present disclosure, multiple elections may be performed during an operation process of the blockchain system, to avoid a system operation problem caused by an exception of a specific representative node device, for example, a specific representative node device operating in an abnormal state or having a credit problem, thereby ensuring stable operation of the blockchain system based on the representative node device.

[0067] An election is performed only when the number of the generated blocks reaches the second preset number, so that a switching frequency of a representative node device, that is, how often a representative node device is switched, can be ensured, thereby avoiding frequent switching of the representative node device and avoiding affecting normal operation of the entire blockchain system. The generated blocks are blocks generated after a previous election.

[0068] It may be understood that the generated blocks not only include blocks generated based on voting transaction data, but also include blocks generated based on other transaction data. Practically, the generated blocks may further include blocks generated based on voting transaction data and other transaction data. Details are not described in this embodiment of the present disclosure.

[0069] All the node devices in the blockchain system execute step S211, and details are not described in this embodiment of the present disclosure.

[0070] In S212, the first node device determines, according to the voting transaction data stored in the multiple first blocks, the number of votes of each of the candidate node devices in the blockchain system.

[0071] The voting transaction data includes a transaction type, a list of node devices to be voted, a private key signature of a voting user, and the like. Therefore, according to the voting transaction data stored on respective first blocks, the number of votes obtained by each node device may be counted.

[0072] In this embodiment of the present disclosure, in the blockchain system, voting is performed in an incremental voting manner. The incremental voting refers to indicating a node device to be voted in a voting transaction and reserving historical voting results. For example, a user has voted for three node devices A, B and C, and an object of this voting is a node device D. During this voting, the user may directly vote for the node device D. A list of node devices to be voted in the voting transaction data carries a public key of the node device D. That is, the user votes for, through multiple rounds of voting, the four node devices A, B, C, and D.

[0073] Based on the foregoing incremental voting manner, a vote for a node device to be voted may be withdrawn. For example, a user has already voted for three node devices A, B and C. If the user wants to withdraw the vote for the node device C next time, the user may directly indicate withdrawal of the vote for the node device C in the voting transaction data during next voting.

[0074] Another manner may be adopted during voting and vote counting, and this is not limited in the present disclosure.

[0075] Steps S211 to S212 describe examples of how to obtain the voting transaction data corresponding to the candidate node devices. Another manner may be adopted in this process, and this is not limited in the present disclosure.

[0076] In S213, the first node device determines an election result in a descending order of the numbers of votes. The election result includes public keys of a third preset number of representative node devices in the blockchain system and the number of votes of each representative node device.

[0077] The third preset number may be equal to the number of representative node devices currently working. That is, the third preset number is set, so that the representative node devices currently working can all be replaced with the elected representative node devices. Alternatively, the third preset number may be changed. For example, the third preset number may be changed according to the number of node devices in the blockchain system. In a case that the number of the node devices is increased, the third preset number may be increased.

[0078] The first node device may determine whether it is a newly elected representative node device according to the determined election result. That is, any node device in the blockchain system may determine, according to an election result obtained through counting, whether it is a newly elected representative node device, and identities of other representative node devices that are newly elected this time.

[0079] Steps S212 to S213 describe an implementation of a process of determining, by the first node device according to the numbers of votes of the multiple candidate node devices, multiple representative node devices in the blockchain system. That is, a process of determining, according to the voting transaction data stored in the multiple first blocks, the third preset number of representative node devices in the blockchain system is described. Practically, another election manner may be adopted, and this is not limited in the present disclosure.

[0080] In S214, the representative node devices currently working are switched to a candidate node device state for operation, and the representative node devices that are newly elected this time are switched to a representative node device state for operation.

[0081] Steps S207 to S214 describe a representative node device election process of the blockchain system. The blockchain system may delete the candidate node device, and a specific deletion process is described as follows.

[0082] In S215, any candidate node device broadcasts candidate deletion transaction data in the blockchain system. The candidate deletion transaction data indicates that the candidate node device withdraws from the election.

[0083] In this case, a node device that meets a qualification requirement for a candidate node device and withdraws from the election may be referred to as a second target node device. That is, the candidate deletion transaction data indicates that the first target node device is deleted from the candidate node devices.

[0084] In a case that any candidate node device no longer wants to be elected as a representative node device, the candidate node device may initiate a candidate deletion transaction in the blockchain system. That is, candidate deletion transaction data is broadcasted, so that each node device no longer votes for the candidate node device in a next election, after receiving the transaction data.

[0085] In S216, each node device receives the candidate deletion transaction data.

[0086] In S217, in a case that multiple node devices in the blockchain system verify the candidate deletion transaction data by consensus, the multiple node devices in the blockchain system store the candidate deletion transaction data on the target blockchain.

[0087] When the representative node devices currently working in the blockchain system verify the candidate deletion transaction data by consensus, the representative node devices may package the candidate deletion transaction data and generate a block, and transmit the block to each non-representative node device. The non-representative node device stores the candidate deletion transaction data into the blockchain configured by the non-representative node device, so that all the node devices in the blockchain system maintain a list of candidate node devices together. Therefore, in the next election, the candidate node device loses qualification, and the user does not vote for the candidate node device.

[0088] In S218, the second target node device is switched to an ordinary node device state for operation.

[0089] The second target node has paid a deposit to the target server, to become a representative node device. However, at this point, the second target node device has been switched to the ordinary node device state, indicating that the second target node device cannot become a representative node device. In this case, the target server needs to refund the deposit paid by the candidate node device along an original path. That is, the method further includes: receiving target transaction data, the target transaction data being used for indicating to refund the deposit to an

account of the second target node device. The target transaction data can be initiated by the target server as a node device in the blockchain system, or initiated by the target server through any node device in the blockchain system, and this is not limited in the embodiments of the present disclosure.

[0090] Steps S215 to S218 describe a candidate node device deletion process, and may be performed in any time period in which there is a candidate node device in the blockchain system. No limitation is imposed in this embodiment. In addition, the candidate node device may be deleted in another manner, and this is not limited in this embodiment.

[0091] According to the method provided in this embodiment of the present disclosure, a qualification audit is performed on node devices in the blockchain system by a target server, and credential data is transmitted to the audited node devices based on an audit result, to prove that the node devices may become candidate node devices. The node devices may initiate, based on the credential data, a candidate addition transaction in the blockchain system, and determine candidate node devices according to a preset rule, so that the blockchain system can elect representative nodes device only from the candidate node devices, thereby improving efficiency of an election for the representative node devices in the blockchain system.

[0092] Further, in the election process, the numbers of votes of respective node devices in the blockchain system are counted once a second preset number of blocks are generated, to elect representative node devices. In this way, a switching frequency of representative node devices can be controlled, so that the representative node devices are not frequently switched, and the blockchain system can normally operate. The representative node device replaces all the node devices in the blockchain system to generate a block and perform verification on the block by consensus, thereby not only improving the working efficiency of the blockchain system by avoiding a case that all the nodes devices perform the above process, but also ensuring qualification of the representative node devices, so that the blockchain system operates more efficiently. In addition, a candidate node device that does not meet the qualification requirement is deleted, thereby further ensuring qualification of the representative node devices, and thus improving working efficiency of the representative node devices.

[0093] In the foregoing embodiment, one target server is utilized to audit node devices in the blockchain system. In some embodiments, multiple target servers may be utilized to audit node devices in the blockchain system, as described below.

[0094] FIG. 3 is a flowchart of a qualification auditing process for a node device according to an embodiment of the present disclosure. Referring to FIG 3, the method according to this embodiment includes the following steps S301 to S305.

[0095] In S301, a first node device transmits a candidate application request to target servers A1 to An. The candidate application request carries qualification information of the first node device.

[0096] The target servers A1 to An are configured to perform a qualification audit on the node device in the blockchain system. If the target servers A1 to An perform verification on a node device and a verification result is positive, the first node device may be determined as a candidate node device. In this embodiment of the present disclosure, descriptions are provided by only an example in which multiple target servers perform a qualification audit together. In this embodiment, step S301 may be implemented in the following two manners.

[0097] In a first manner, the first node device transmits the candidate application request to one of the multiple target servers. The target server transmits the candidate application request to other target servers, so that other target servers can receive the candidate application request.

[0098] In a second manner, the first node device transmits the candidate application request to all of the multiple target servers, so that all the target servers can receive the candidate application request. Alternatively, the first node device may transmit the candidate application request to some of the target servers, and the target servers forward the received candidate application request to other target servers, so that the other target servers can receive the candidate application request. Specific transmitting manners are not limited in this embodiment of the present disclosure.

[0099] The candidate application request refers to a request through which the first node device applies to any target server for becoming a candidate device node. The qualification information of the first node device carried in the candidate application request may include any one of the following: device performance of the first node device; a deposit of a preset amount that has been paid by the node device to the target server; and a credit value of a user account corresponding to the first node device. Practically, the qualification information may include other content, and this is not limited in this embodiment

[0100] In S302, the target servers A1 to An separately perform a qualification audit on the first node device and generate credential data, after receiving the candidate application request.

[0101] After the target servers A1 to An audit the qualification information of the first node device, credential transaction data is generated respectively for the target servers which verify the qualification information. The credential data may include a consent identifier, generation time of a credential, a validity period of the credential, and a signature of the target server. The consent identifier refers to an identifier indicating that the target server consents that the first node device becomes the candidate node device. The validity period can prevent a non-candidate node device from becoming a representative node device by means of credential data that expires. The signature is a signature added by the target server to the qualification information by utilizing a private key of the target server. Alternatively, the credential data generated by the target server may be credential data generated based on audit results of terminal devices associated with the target servers, for example, step S202. Details are not provided in this embodiment of the present disclosure.

[0102] In S303, multiple target servers separately transmit the credential data to the first node device. The multiple target servers are servers of an auditor.

[0103] The multiple target servers separately transmit the credential data to the first node device, so that the first node device receives the credential data and initiates a candidate addition transaction to the blockchain system based on the credential data.

[0104] In some embodiments, one target server may be selected from the multiple target servers, and other target servers that verify the audit may transmit credential data generated by themselves to the selected target server. The target server summarizes all the pieces of credential data, and transmits the summarized credential data to the first node device.

[0105] In S304, the first node device broadcasts the candidate addition transaction data in the blockchain system based on the received credential data. The candidate addition transaction data includes the credential data and a list of candidate node devices.

[0106] The first node device initiates the candidate addition transaction to any node device of the blockchain system, so that the first node device may become a candidate node device.

[0107] Steps S301 to S304 describe a process in which multiple target servers perform an audit to determine whether a node device has a qualification of becoming a candidate node device. For a process in which the first node device becomes the candidate node device and a process of electing representative node devices in the blockchain system, one may refer to steps S205 to S218. Details are not provided herein.

[0108] In this embodiment, multiple target servers are configured to audit the node devices in the blockchain system, to avoid that the audit cannot be performed normally due to a fault of a

specific target server. A qualification of a node device that passes the audit performed by the multiple target servers is more reliable.

[0109] All the foregoing optional technical solutions may be arbitrarily combined to form an optional embodiment of the present disclosure, and details are not described herein.

[0110] FIG. 4 is a schematic structural diagram of an apparatus for electing a representative node device according to an embodiment of the present disclosure. Referring to FIG. 4, the apparatus includes a first receiving module 401, a first storage module 402, and an election module 403.

[0111] The first receiving module 401 is connected to the first storage module 402 and is configured to receive candidate addition transaction data. The candidate addition transaction data carries credential data, and the credential data indicates that a first target node device meets a qualification requirement for a candidate node device.

[0112] The first storage module 402 is connected to the election module 403 and is configured to store the candidate addition transaction data on a target blockchain of the blockchain system in a case that multiple node devices in the blockchain system verify the candidate addition transaction data by consensus.

[0113] The election module 403 is configured to participate in an election of the representative node device according to the candidate addition transaction data stored on the target blockchain.

[0114] In an embodiment, the credential data includes signature data of multiple auditing users.

[0115] In an embodiment, the device further includes:

a transmitting module, configured to transmit a candidate application request to a target server, the candidate application request carrying qualification information of the node device.

[0116] In an embodiment, the target server is any node device in the blockchain system; or

the target server is a server of a third party organization associated with the blockchain system.

[0117] In an embodiment, the first target node device meets at least one of the following conditions:

device performance of the first target node device meets a preset performance condition;

the first target node device has paid a preset amount of deposit; and

credit of a user corresponding to the first target node device meets a preset credit condition.

[0118] In an embodiment, the multiple node devices in the blockchain system verifying the candidate addition transaction data by consensus includes that multiple representative node devices in the blockchain system verify the candidate addition transaction data by consensus.

[0119] In an embodiment, the device further includes:

a second receiving module, configured to receive candidate deletion transaction data, the candidate deletion transaction data indicating deleting a second target node device from the candidate node devices; and

a second storage module, configured to store the candidate deletion transaction data on the target blockchain of the blockchain system in a case that the multiple node devices in the blockchain system verify the candidate deletion transaction data by consensus.

[0120] In an embodiment, the device further includes:

a third receiving module, configured to receive target transaction data, the target transaction data being used for indicating to refund the deposit to an account of the second target node device.

[0121] According to the apparatus provided in this embodiment of the present disclosure, a qualification audit is performed on node devices in the blockchain system by an auditor, and credential data is transmitted to the audited node devices based on an audit result, to prove whether the node devices can become candidate node devices. The node devices may initiate, based on the credential data, a candidate addition transaction in the blockchain system, and determine candidate node devices according to a preset rule, so that the blockchain system can elect representative nodes device only from the candidate node devices, thereby improving efficiency of an election for the representative node devices in the blockchain system.

[0122] FIG. 5 is a schematic structural diagram of a server according to an embodiment of the present disclosure. The server 500 may vary due to different configurations or different performances, and may include one or more central processing units (CPUs) 501 and one or more memories 502. The memory 502 stores computer-readable instructions, and the computer-readable

instructions are loaded and executed by the processor 501 to implement the methods according to the foregoing method embodiments. Practically, the server may further include components such as a wired or wireless network interface, a keyboard, and an input/output interface, to facilitate inputs/outputs. The server may further include another component configured to implement functions of a device, and details are not described herein.

[0123] In an exemplary embodiment, a computer-readable storage medium, for example, a memory including instructions, is further provided. The instructions may be executed by a processor in a terminal, to perform the method for electing a representative node device in the foregoing embodiments. For example, the computer-readable storage medium may be a read-only memory (ROM), a random access memory (RAM), a compact disc read-only memory (CD-ROM), a magnetic tape, a floppy disk, an optical data storage device, or the like.

[0124] A person of ordinary skill in the art may understand that all or some of the steps of the foregoing embodiments may be implemented by using hardware, or may be implemented by a program instructing relevant hardware. The program may be stored in a computer-readable storage medium. The above-mentioned storage medium may be a read-only memory, a magnetic disk, an optical disc, and the like.

[0125] The foregoing descriptions are merely preferred embodiments of the present disclosure, and are not intended to limit the present disclosure. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of the present disclosure falls within the protection scope of the present disclosure.

CLAIMS

1. A method for electing a representative node device, performed by a first node device, the first node device being any node device in a blockchain system, the method comprising:

broadcasting candidate newly addition transaction data, the candidate newly addition transaction data including credential data, the credential data indicating that the first node device meets a qualification requirement for a candidate node device;

storing the candidate newly addition transaction data on a target blockchain of the blockchain system upon a plurality of node devices in the blockchain system achieving consensus on the candidate newly addition transaction data; and

performing an election process of a representative node device based on the candidate newly addition transaction data stored on the target blockchain.

2. The method according to claim 1, wherein the credential data comprises signature data of a plurality of auditing users.

3. The method according to claim 1 or 2, wherein before the broadcasting candidate newly addition transaction data, the method further comprises:

transmitting a candidate application request to a target server, the candidate application request including qualification information of the first node device.

4. The method according to claim 3, wherein the target server is any node device in the blockchain system; or

the target server is a server of a third party organization associated with the blockchain system.

5. The method according to any one of claims 1 to 4, wherein the first node device meeting a qualification requirement for a candidate node device comprises at least one of the following: device performance of the first node device meeting a preset performance condition, the first node device having paid a preset amount of deposit, and credit of a user corresponding to the first node device meeting a preset credit condition.

6. The method according to any one of claims 1 to 5, wherein the plurality of node devices in the blockchain system achieving consensus on the candidate newly addition transaction data is characterized in that a plurality of representative node devices in the blockchain system achieving consensus on the candidate newly addition transaction data.

7. The method according to any one of claims 1 to 6, wherein after the storing the candidate newly addition transaction data on a target blockchain of the blockchain system, the method further comprises:

receiving candidate deletion transaction data, wherein the candidate deletion transaction data is data for indicating deleting a second target node device from the candidate node devices; and

storing the candidate deletion transaction data on the target blockchain of the blockchain system when the plurality of node devices in the blockchain system achieves consensus on the candidate deletion transaction data.

8. The method according to claim 7, wherein after the storing the candidate deletion transaction data on the target blockchain of the blockchain system, the method further comprises:

receiving target transaction data, wherein the target transaction data is data for refunding a deposit to an account of the second target node device.

9. A node device in a blockchain system, the node device performs the method according to any one of claims 1 to 8.

10. A computer program for causing a node device in a blockchain system to perform the method according to any one of claims 1 to 8.