



(12)发明专利申请

(10)申请公布号 CN 110413621 A

(43)申请公布日 2019.11.05

(21)申请号 201910704233.2

(22)申请日 2019.07.31

(71)申请人 中国工商银行股份有限公司

地址 100140 北京市西城区复兴门内大街
55号

(72)发明人 李曼潇 张叶飞 刘朝伟 王舒榕
曾雨峰 巨龙

(74)专利代理机构 北京三友知识产权代理有限公司 11127

代理人 王涛 任默闻

(51)Int.Cl.

G06F 16/22(2019.01)

G06F 16/27(2019.01)

G06Q 40/04(2012.01)

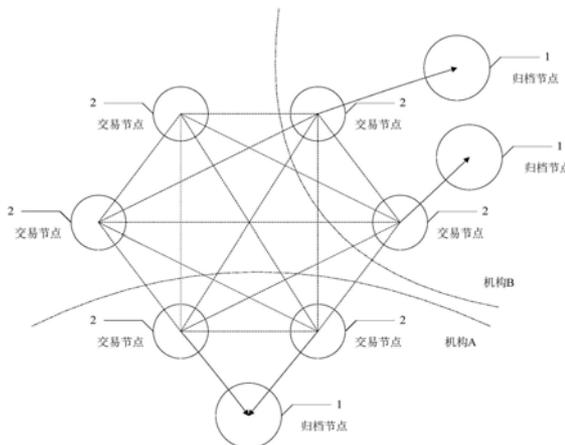
权利要求书4页 说明书13页 附图8页

(54)发明名称

基于区块链的离线归档系统及方法

(57)摘要

一种基于区块链的离线归档系统及方法,具体包含归档节点和交易节点;交易节点根据归档参数配置归档节点信息;接收区块链用户发起的归档请求完成交易共识,当交易共识完成后解析归档请求获得归档参数并计算获得符合归档参数的一个或多个在线数据区块,将在线数据区块清理并生成同样结构的归档数据区块后;根据被清理的在线数据区块通过哈希算法计算生成历史数据指纹;将历史数据指纹及归档数据区块发送至归档节点信息对应的归档节点;根据归档节点反馈的确认信息删除本地临时目录中存储数据生成归档成功信息,将归档成功信息反馈区块链用户;归档节点根据历史数据指纹及归档数据区块完成数据归档并反馈确认信息至交易节点。



1. 一种基于区块链的离线归档系统,其特征在于,所述系统包含一个或多个归档节点和多个交易节点;

所述交易节点之间通过网络连接,所述归档节点与所述交易节点一对一或一对多连接;

所述交易节点用于根据预设归档参数配置归档节点信息及数据归档的本地临时目录;接收区块链用户发起的归档请求,根据所述归档请求与区块链上其他交易节点完成交易共识,当交易共识完成后解析所述归档请求获得归档参数;根据所述归档参数计算获得符合所述归档参数的一个或多个在线数据区块,将所述在线数据区块清理并生成同样结构的一个或多个归档数据区块后存入所述本地临时目录;根据被清理的所述在线数据区块通过哈希算法计算生成历史数据指纹;将所述历史数据指纹存入所述本地临时目录后,将所述本地临时目录中所述历史数据指纹及所述归档数据区块发送至所述归档节点信息对应的归档节点;以及,根据所述归档节点反馈的确认信息删除所述本地临时目录中存储数据生成归档成功信息,将所述归档成功信息发送至发起归档请求的区块链用户;

所述归档节点用于根据所述历史数据指纹及所述归档数据区块完成数据归档,当归档完成后反馈确认信息至所述交易节点。

2. 根据权利要求1所述的基于区块链的离线归档系统,其特征在于,所述归档节点包含参数配置模块、数据传输模块、数据合并模块、数据查询模块和数据验证模块;

所述参数配置模块用于配置数据归档的相关参数,所述相关参数包含全量归档数据的存储路径、增量归档数据的临时存储路径、归档服务对外的端口和URL信息;

所述数据传输模块用于与各个交易节点建立网络连接,接收交易节点的请求并进行应答;当所述请求为数据传输请求时,还用于在临时目录保存所述历史数据指纹及所述归档数据区块后产生的增量归档数据;

所述数据合并模块用于根据所述交易节点传输的触发信号对所述归档数据传输模块产生的所述增量归档数据做遍历,把遍历到的数据合并到全量归档数据目录;

所述数据查询模块用于对外提供归档区块数据查询服务,根据交易节点在查询请求中指定的网络ID、节点ID和查询区块的高度获得对应区块信息,并将所述区块信息反馈至所述交易节点;

所述数据验证模块用于对已归档数据做验证以及在将所述增量归档数据合并到全量归档数据目录之前对增量归档数据做验证。

3. 根据权利要求2所述的基于区块链的离线归档系统,其特征在于,所述数据验证模块包含:通过从最新区块开始一直到创世区块验证每个区块记录的prehash等于前一个区块数据做hash计算的结果的验证方式,对已归档数据做验证以及在将所述增量归档数据合并到全量归档数据目录之前对增量归档数据做验证。

4. 根据权利要求2所述的基于区块链的离线归档系统,其特征在于,所述交易节点包含:通讯模块、共识模块、交易执行模块、归档数据处理模块、临时数据清理模块、归档数据查询模块和数据验证模块;

所述通讯模块分别与区块链客户端、其他交易节点、归档节点建立网络连接,用于为所述交易节点提供数据交互通道;

所述共识模块用于与其他交易节点根据约定好的共识算法对交易进行共识处理,根据

共识的结果确定交易的执行顺序并把交易打包成区块交由所述交易执行模块；

所述交易执行模块用于根据所述执行顺序处理所述区块中的交易；当所述交易为归档交易时，将所述归档交易的交易数据交由所述归档数据处理模块；

所述归档数据处理模块用于根据所述归档交易的交易参数指定的归档区块高度或者归档时间点，计算出小于归档区块的全部区块数据或者小于归档时间点生成的全部区块，根据全部区块及归档参数生成归档指南区块和在线数据区块后，将所述归档指南区块和在线数据区块存入至本地临时目录；根据所述归档节点信息将本地临时目录中存储的全部文件打包后发送至对应的归档节点；

所述临时数据清理模块用于根据所述归档节点反馈的确认信息删除所述本地临时目录中存储数据生成归档成功信息，并交由所述通讯模块将所述归档成功信息发送至发起归档请求的区块链用户；

所述归档数据查询模块用于将区块链用户发起的查询请求提交至所述数据查询模块，以及将所述数据查询模块反馈的所述区块信息交由所述区块链用户；

所述数据验证模块用于通过从最新区块开始一直到创世区块验证每个区块记录的prehash等于前一个区块数据做hash计算的结果的验证方式，对在线的区块数据做验证。

5. 根据权利要求4所述的基于区块链的离线归档系统，其特征在于，所述归档数据处理模块包含归档数据计算模块、归档数据传输模块和归档数据合并模块；

所述归档数据计算模块用于根据所述归档交易的交易参数指定的归档区块高度或者归档时间点，计算出小于归档区块的全部区块数据或者小于归档时间点生成的全部区块，获得归档区块；根据归档区块及归档参数生成归档指南区块、归档数据索引区块、归档数据区块；将所述归档指南区块存入在线数据存储目录，并将被归档的在线数据区块于在线数据存储目录中清理；将归档数据索引区块、归档数据区块存入本地临时目录；

所述归档数据传输模块用于根据所述归档节点信息将本地临时目录中存储的全部文件打包后发送至对应的归档节点；

所述归档数据合并模块用于当所述归档数据传输模块完成数据传输后生成触发信号，将所述触发信号发送至所述数据合并模块。

6. 根据权利要求5所述的基于区块链的离线归档系统，其特征在于，所述归档指南区块包含清理指南点、历史数据指纹、清理起始区块高度、清理截止区块高度、清理起始区块入账时间和清理截止区块入账时间；

所述清理指南点为本次离线归档执行后，记录未被归档的第一个在线数据区块的区块高度；

所述历史数据指纹为本次离线归档执行后，被归档的一个或多个在线数据区块做哈希计算得到的计算结果；

所述清理起始区块高度为本次离线归档执行中，被归档的在线数据区块的区块高度的最小值；

所述清理截止区块高度为本次离线归档执行中，被归档的在线数据区块的区块高度的最大值；

所述清理起始区块入账时间为本次离线归档执行中，被归档的区块高度最小的在线数据区块的时间戳；

所述清理截止区块入账时间为本次离线归档执行中,被归档的区块高度最大的在线数据区块的时间戳。

7. 根据权利要求6所述的基于区块链的离线归档系统,其特征在于,所述在线数据区块包含区块高度、上一区块哈希、交易数据和时间戳;

所述区块高度为根据在线数据区块生成顺序从小到大编号的序号信息;

所述上一区块哈希为区块高度比当前区块小一的在线数据区块做哈希运算的结果;

所述交易数据为包含在在线数据区块中的一个或多个交易的交易参数和执行结构;

所述时间戳为区块的生成时间。

8. 根据权利要求7所述的基于区块链的离线归档系统,其特征在于,所述归档节点包含数据存储模块,所述数据存储模块用于存储归档数据索引区块和归档数据区块;所述归档数据索引区块和所述归档数据区块用于对应存储所述归档数据传输模块传输的打包文件;

其中,所述归档数据索引区块包含上一区块哈希、历史数据指纹、清理起始区块高度、清理截止区块高度、清理起始区块入账时间和清理截止区块入账时间;

所述归档数据区块包含区块高度、上一区块哈希和交易数据和时间戳。

9. 一种基于区块链的离线归档方法,其特征在于,所述方法包含:

根据预设归档参数配置归档节点信息及数据归档的本地临时目录;

接收区块链用户发起的归档请求,根据所述归档请求与区块链上其他交易节点完成交易共识,当交易共识完成后解析所述归档请求获得归档参数;

根据所述归档参数计算获得符合所述归档参数的一个或多个在线数据区块,将所述在线数据区块清理并生成同样结构的一个或多个归档数据区块后存入所述本地临时目录;

根据被清理的所述在线数据区块通过哈希算法计算生成历史数据指纹;

将所述历史数据指纹存入所述本地临时目录后,将所述本地临时目录中所述历史数据指纹及所述归档数据区块发送至所述归档节点信息对应的归档节点;

根据所述归档节点反馈的确认信息删除所述本地临时目录中存储数据生成归档成功信息,将所述归档成功信息发送至发起归档请求的区块链用户。

10. 根据权利要求9所述的基于区块链的离线归档方法,其特征在于,所述方法还包含:

接收区块链用户发起的查询请求,根据所述查询请求获得对应的网络ID、节点ID和查询区块的高度;

根据所述查询区块的高度查询对应区块是否已被归档,当所述区块已被归档时,获得对应的区块的历史数据指纹;

将所述网络ID、所述节点ID、所述历史数据指纹和所述查询区块的高度发送至归档节点,由所述归档节点根据所述网络ID、所述节点ID、所述历史数据指纹和所述查询区块的高度查询对应的区块并接收所述归档节点反馈的查询结果;

将所述查询结果反馈至区块链用户。

11. 根据权利要求9所述的基于区块链的离线归档方法,其特征在于,所述方法还包含:

获取当前交易节点的内存情况和单个区块的占用内存大小,根据内存情况和单个区块的占用内容大小计算获得在线区块的并发验证数量,根据所述并发验证数量对当前交易节点内区块分组获得多组待验证区块数据;根据所述待验证区块数据的区块高度,从高到低进行依次对所述待验证区块数据进行验证获得验证结果;

获取归档节点的归档区块的验证结果；

将所述归档区块的验证结果与所述在线区块的验证结果比较，根据比较结果获得区块归档验证情况。

12. 根据权利要求11所述的基于区块链的离线归档方法，其特征在于，根据所述待验证区块数据的区块高度，从高到低进行依次对所述待验证区块数据进行验证获得验证结果包含：对所述待验证区块数据中各区块分别进行验证，将各区块的验证结果两两比较，当比较结果符合预设规则时以所述待验证区块数据中区块高度最小的区块为所述待验证区块数据的验证结果；将所述待验证区块数据的验证结果与相邻的所述待验证区块数据的验证结果进行比较，当比较结果符合预设规则时以所述待验证区块数据中区块高度最小的所述待验证区块数据的验证结果作为在线区块的验证结果。

13. 根据权利要求12所述的基于区块链的离线归档方法，其特征在于，将所述归档区块的验证结果与所述在线区块的验证结果比较，根据比较结果获得区块归档验证情况包含：将在线区块中区块高度最小的区块记录的上一区块哈希与归档区块中区块高度最大的区块记录的上一区块哈希比较，当两者相同时区块归档验证通过。

14. 一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求9至13任一所述方法。

15. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有执行权利要求9至13任一所述方法的计算机程序。

基于区块链的离线归档系统及方法

技术领域

[0001] 本发明涉及区块链技术处理系统,尤其是一种基于区块链的离线归档系统及方法。

背景技术

[0002] 区块链系统的数据记录包含区块信息,区块信息有着持续增长并且不可篡改的特点;每个区块都包含一个时间戳和前一区块的指针,这样设计使得区块链数据不可篡改,一旦记录下来,在一个区块中的数据将不可逆转;因此网络中数据持续增长。直接清理区块的历史数据会导致从新区块到创世区块间数据验证受阻,因此业内亟需针对区块链系统提出一种数据在线清理与离线归档的方法。

发明内容

[0003] 本发明目的在于提供一种基于区块链的离线归档系统及方法,使区块链用户可以在区块链网络不停机且不影响系统原有交易的情况下,对存量区块数据做清理和归档,在归档期间和归档结束后均支持对归档区块数据的查询。

[0004] 为达上述目的,本发明所提供的基于区块链的离线归档系统,具体包含一个或多个归档节点和多个交易节点;所述交易节点之间通过网络连接,所述归档节点与所述交易节点一对一或一对多连接;所述交易节点用于根据预设归档参数配置归档节点信息及数据归档的本地临时目录;接收区块链用户发起的归档请求,根据所述归档请求与区块链上其他交易节点完成交易共识,当交易共识完成后解析所述归档请求获得归档参数;根据所述归档参数计算获得符合所述归档参数的一个或多个在线数据区块,将所述在线数据区块清理并生成同样结构的一个或多个归档数据区块后存入所述本地临时目录;根据被清理的所述在线数据区块通过哈希算法计算生成历史数据指纹;将所述历史数据指纹存入所述本地临时目录后,将所述本地临时目录中所述历史数据指纹及所述归档数据区块发送至所述归档节点信息对应的归档节点;以及,根据所述归档节点反馈的确认信息删除所述本地临时目录中存储数据生成归档成功信息,将所述归档成功信息发送至发起归档请求的区块链用户;所述归档节点用于根据所述历史数据指纹及所述归档数据区块完成数据归档,当归档完成后反馈确认信息至所述交易节点。

[0005] 在上述基于区块链的离线归档系统中,优选的,所述归档节点包含参数配置模块、数据传输模块、数据合并模块、数据查询模块和数据验证模块;所述参数配置模块用于配置数据归档的相关参数,所述相关参数包含全量归档数据的存储路径、增量归档数据的临时存储路径、归档服务对外的端口和URL信息;所述数据传输模块用于与各个交易节点建立网络连接,接收交易节点的请求并进行应答;当所述请求为数据传输请求时,还用于在临时目录保存所述历史数据指纹及所述归档数据区块后产生的增量归档数据;所述数据合并模块用于根据所述交易节点传输的触发信号对所述归档数据传输模块产生的所述增量归档数据做遍历,把遍历到的数据合并到全量归档数据目录;所述数据查询模块用于对外提供归

档区块数据查询服务,根据交易节点在查询请求中指定的网络ID、节点ID和查询区块的高度获得对应区块信息,并将所述区块信息反馈至所述交易节点;所述数据验证模块用于对已归档数据做验证以及在将所述增量归档数据合并到全量归档数据目录之前对增量归档数据做验证。

[0006] 在上述基于区块链的离线归档系统中,优选的,所述数据验证模块包含:通过从最新区块开始一直到创世区块验证每个区块记录的prehash等于前一个区块数据做hash计算的结果的验证方式,对已归档数据做验证以及在将所述增量归档数据合并到全量归档数据目录之前对增量归档数据做验证。

[0007] 在上述基于区块链的离线归档系统中,优选的,所述交易节点包含:通讯模块、共识模块、交易执行模块、归档数据处理模块、临时数据清理模块、归档数据查询模块和数据验证模块;所述通讯模块分别与区块链客户端、其他交易节点、归档节点建立网络连接,用于为所述交易节点提供数据交互通道;所述共识模块用于与其他交易节点根据约定好的共识算法对交易进行共识处理,根据共识的结果确定交易的执行顺序并把交易打包成区块交由所述交易执行模块;所述交易执行模块用于根据所述执行顺序处理所述区块中的交易;当所述交易为归档交易时,将所述归档交易的交易数据交由所述归档数据处理模块;所述归档数据处理模块用于根据所述归档交易的交易参数指定的归档区块高度或者归档时间点,计算出小于归档区块的全部区块数据或者小于归档时间点生成的全部区块,根据全部区块及归档参数生成归档指南区块和在线数据区块后,将所述归档指南区块和在线数据区块存入至本地临时目录;根据所述归档节点信息将本地临时目录中存储的全部文件打包后发送至对应的归档节点;所述临时数据清理模块用于根据所述归档节点反馈的确认信息删除所述本地临时目录中存储数据生成归档成功信息,并交由所述通讯模块将所述归档成功信息发送至发起归档请求的区块链用户;所述归档数据查询模块用于将区块链用户发起的查询请求提交至所述数据查询模块,以及将所述数据查询模块反馈的所述区块信息交由所述区块链用户;所述数据验证模块用于通过从最新区块开始一直到创世区块验证每个区块记录的prehash等于前一个区块数据做hash计算的结果的验证方式,对在线的区块数据做验证。

[0008] 在上述基于区块链的离线归档系统中,优选的,所述归档数据处理模块包含归档数据计算模块、归档数据传输模块和归档数据合并模块;

[0009] 所述归档数据计算模块用于根据所述归档交易的交易参数指定的归档区块高度或者归档时间点,计算出小于归档区块的全部区块数据或者小于归档时间点生成的全部区块,获得归档区块;根据归档区块及归档参数生成归档指南区块、归档数据索引区块、归档数据区块;将所述归档指南区块存入在线数据存储目录,并将被归档的在线数据区块于在线数据存储目录中清理;将归档数据索引区块、归档数据区块存入本地临时目录;所述归档数据传输模块用于根据所述归档节点信息将本地临时目录中存储的全部文件打包后发送至对应的归档节点;所述归档数据合并模块用于当所述归档数据传输模块完成数据传输后生成触发信号,将所述触发信号发送至所述数据合并模块。

[0010] 在上述基于区块链的离线归档系统中,优选的,所述归档指南区块包含清理指南点、历史数据指纹、清理起始区块高度、清理截止区块高度、清理起始区块入账时间和清理截止区块入账时间;所述清理指南点为本次离线归档执行后,记录未被归档的第一个在线

数据区块的区块高度;所述历史数据指纹为本次离线归档执行后,被归档的一个或多个在线数据区块做哈希计算得到的计算结果;所述清理起始区块高度为本次离线归档执行中,被归档的在线数据区块的区块高度的最小值;所述清理截止区块高度为本次离线归档执行中,被归档的在线数据区块的区块高度的最大值;所述清理起始区块入账时间为本次离线归档执行中,被归档的区块高度最小的在线数据区块的时间戳;所述清理截止区块入账时间为本次离线归档执行中,被归档的区块高度最大的在线数据区块的时间戳。

[0011] 在上述基于区块链的离线归档系统中,优选的,所述在线数据区块包含区块高度、上一区块哈希、交易数据和时间戳;所述区块高度为根据在线数据区块生成顺序从小到大编号的序号信息;所述上一区块哈希为区块高度比当前区块小一的在线数据区块做哈希运算的结果;所述交易数据为包含在在线数据区块中的一个或多个交易的交易参数和执行结构;所述时间戳为区块的生成时间。

[0012] 在上述基于区块链的离线归档系统中,优选的,所述归档节点包含数据存储模块,所述数据存储模块用于存储归档数据索引区块和归档数据区块;所述归档数据索引区块和所述归档数据区块用于对应存储所述归档数据传输模块传输的打包文件;其中,所述归档数据索引区块包含上一区块哈希、历史数据指纹、清理起始区块高度、清理截止区块高度、清理起始区块入账时间和清理截止区块入账时间;所述归档数据区块包含区块高度、上一区块哈希和交易数据和时间戳。

[0013] 本发明还提供一种基于区块链的离线归档方法,所述方法包含:根据预设归档参数配置归档节点信息及数据归档的本地临时目录;接收区块链用户发起的归档请求,根据所述归档请求与区块链上其他交易节点完成交易共识,当交易共识完成后解析所述归档请求获得归档参数;根据所述归档参数计算获得符合所述归档参数的一个或多个在线数据区块,将所述在线数据区块清理并生成同样结构的一个或多个归档数据区块后存入所述本地临时目录;根据被清理的所述在线数据区块通过哈希算法计算生成历史数据指纹;将所述历史数据指纹存入所述本地临时目录后,将所述本地临时目录中所述历史数据指纹及所述归档数据区块发送至所述归档节点信息对应的归档节点;根据所述归档节点反馈的确认信息删除所述本地临时目录中存储数据生成归档成功信息,将所述归档成功信息发送至发起归档请求的区块链用户。

[0014] 在上述基于区块链的离线归档方法中,优选的,所述方法还包含:接收区块链用户发起的查询请求,根据所述查询请求获得对应的网络ID、节点ID和查询区块的高度;根据所述查询区块的高度查询对应区块是否已被归档,当所述区块已被归档时,获得对应的区块的历史数据指纹;将所述网络ID、所述节点ID、所述历史数据指纹和所述查询区块的高度发送至归档节点,由所述归档节点根据所述网络ID、所述节点ID、所述历史数据指纹和所述查询区块的高度查询对应的区块并接收所述归档节点反馈的查询结果;将所述查询结果反馈至区块链用户。

[0015] 在上述基于区块链的离线归档方法中,优选的,所述方法还包含:获取当前交易节点的内存情况和单个区块的占用内存大小,根据内存情况和单个区块的占用内容大小计算获得在线区块的并发验证数量,根据所述并发验证数量对当前交易节点内区块分组获得多组待验证区块数据;根据所述待验证区块数据的区块高度,从高到低进行依次对所述待验证区块数据进行验证获得验证结果;获取归档节点的归档区块的验证结果;将所述归档区

块的验证结果与所述在线区块的验证结果比较,根据比较结果获得区块归档验证情况。

[0016] 在上述基于区块链的离线归档方法中,优选的,根据所述待验证区块数据的区块高度,从高到低进行依次对所述待验证区块数据进行验证获得验证结果包含:对所述待验证区块数据中各区块分别进行验证,将各区块的验证结果两两比较,当比较结果符合预设规则时以所述待验证区块数据中区块高度最小的区块为所述待验证区块数据的验证结果;将所述待验证区块数据的验证结果与相邻的所述待验证区块数据的验证结果进行比较,当比较结果符合预设规则时以所述待验证区块数据中区块高度最小的所述待验证区块数据的验证结果作为在线区块的验证结果。

[0017] 在上述基于区块链的离线归档方法中,优选的,将所述归档区块的验证结果与所述在线区块的验证结果比较,根据比较结果获得区块归档验证情况包含:将在线区块中区块高度最小的区块记录的上一区块哈希与归档区块中区块高度最大的区块记录的上一区块哈希比较,当两者相同时区块归档验证通过。

[0018] 本发明还提供一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述计算机程序时实现上述方法。

[0019] 本发明还提供一种计算机可读存储介质,所述计算机可读存储介质存储有执行上述方法的计算机程序。

[0020] 本发明的有益技术效果在于:解决了由于区块链特性导致的数据持续增长和不可随意清理的问题,引入数据离线归档有下面几点好处;利用对被归档数据计算历史数据指纹并记录,可以保证被归档数据依然有不可篡改的特征;利用原有的多节点共识机制,可以保证归档交易的严格准入,只有得到全网共识节点的认可才能执行数据清理和归档;利用远端数据备份服务器的动态配置,可以保证归档数据既可以集中存放在一台数据备份服务器,也可以存放在多台数据备份服务器上,做到了数据存储的灵活配置;利用远端数据备份服务器对外提供查询或验证功能,可以保证区块链系统能够查询到被归档数据,并验证归档数据不被篡改;集成数据归档功能到在线服务,保证了清理期间不需要停机且不影响其他交易;优化了在线数据校验过程,原来的数据校验是从最新区块一直验证到创世区块,验证过程占用系统的CPU和内存资源较多,而且数据量大的时候验证过程持续时间较长,引入数据归档后,线上数据验证只需要从最新区块一直验证到线上未被归档的第一个区块,归档数据的验证可以在归档服务器上执行,一方面加快了线上验证过程、一方面一定程度上释放了线上交易节点服务器的硬件资源。

附图说明

[0021] 此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,并不构成对本发明的限定。在附图中:

[0022] 图1为一种区块链系统支持离线归档与归档数据查询的网络结构图;

[0023] 图2为一种归档节点的结构图;

[0024] 图3为一种交易节点的结构图;

[0025] 图4为一种区块链系统中在线清理与离线归档的在线数据结构;

[0026] 图5为一种区块链系统中在线清理与离线归档的离线数据结构;

[0027] 图6A和图6B为一种区块链离线归档系统的在线清理与离线归档处理交易的流程

图；

[0028] 图7为一种区块链离线归档系统的查询交易的流程图；

[0029] 图8为一种区块链离线归档系统的归档交易的共识准入的流程图；

[0030] 图9为一种区块链离线归档系统的区块防篡改验证的流程图。

具体实施方式

[0031] 以下将结合附图及实施例来详细说明本发明的实施方式，借此对本发明如何应用技术手段来解决技术问题，并达成技术效果的实现过程能充分理解并据以实施。需要说明的是，只要不构成冲突，本发明中的各个实施例及各实施例中的各个特征可以相互结合，所形成的技术方案均在本发明的保护范围之内。

[0032] 另外，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0033] 为达上述目的，本发明所提供的基于区块链的离线归档系统，具体包含一个或多个归档节点和多个交易节点；所述交易节点之间通过网络连接，所述归档节点与所述交易节点一对一或一对多连接；所述交易节点用于根据预设归档参数配置归档节点信息及数据归档的本地临时目录；接收区块链用户发起的归档请求，根据所述归档请求与区块链上其他交易节点完成交易共识，当交易共识完成后解析所述归档请求获得归档参数；根据所述归档参数计算获得符合所述归档参数的一个或多个在线数据区块，将所述在线数据区块清理并生成同样结构的一个或多个归档数据区块后存入所述本地临时目录；根据被清理的所述在线数据区块通过哈希算法计算生成历史数据指纹；将所述历史数据指纹存入所述本地临时目录后，将所述本地临时目录中所述历史数据指纹及所述归档数据区块发送至所述归档节点信息对应的归档节点；以及，根据所述归档节点反馈的确认信息删除所述本地临时目录中存储数据生成归档成功信息，将所述归档成功信息发送至发起归档请求的区块链用户；所述归档节点用于根据所述历史数据指纹及所述归档数据区块完成数据归档，当归档完成后反馈确认信息至所述交易节点。实际工作中，本发明所提供的基于区块链的离线归档系统如图1所示，包括多个归档节点1和多个交易节点2，参与网络组建的可以是一个或者多个机构，每个机构可以有一个或多个归档节点和交易节点。其中所有交易节点2相互之间进行网络连接，一个机构可以有一个或者多个归档节点1，归档节点1与该机构交易节点2之间的网络连接可以是一对一（机构B）也可以是一对多（机构A）。

[0034] 所述“归档节点1”为一台服务器或多台相互备份的服务器，通过为交易节点2提供离线数据备份功能，为整个区块链网络的用户提供数据备份服务。归档节点1还会为各个区块链成员提供归档数据查询、归档数据合并、离线区块数据防篡改验证服务，支持在线区块链系统查询已归档的区块数据、支持多次数据归档后的底层数据合并处理、支持对离线归档区块数据未被篡改做验证。

[0035] 所述“交易节点2”是指区块链中对交易进行接收、广播、共识、执行和存储的网络节点，一般是各区块链成员的可信服务器、工作站等，负责把用户的请求封装成交易再广播到其他交易节点，或者根据区块链共识算法的规则对其他交易节点广播的交易进行共识，对于共识通过的交易会进行智能合约处理，最后根据处理的结果生成区块并进行持久化保

存。交易节点2持久化存储所有交易记录,这部分结果记录在区块。交易节点2可以通过联合若干个(两个或以上)可信任的其他交易节点2,为区块链成员提供在线区块数据清理和区块数据离线归档功能。

[0036] 在本发明一实施例中,所述归档节点包含参数配置模块、数据传输模块、数据合并模块、数据查询模块和数据验证模块;所述参数配置模块用于配置数据归档的相关参数,所述相关参数包含全量归档数据的存储路径、增量归档数据的临时存储路径、归档服务对外的端口和URL信息;所述数据传输模块用于与各个交易节点建立网络连接,接收交易节点的请求并进行应答;当所述请求为数据传输请求时,还用于在临时目录保存所述历史数据指纹及所述归档数据区块后产生的增量归档数据;所述数据合并模块用于根据所述交易节点传输的触发信号对所述归档数据传输模块产生的所述增量归档数据做遍历,把遍历到的数据合并到全量归档数据目录;所述数据查询模块用于对外提供归档区块数据查询服务,根据交易节点在查询请求中指定的网络ID、节点ID和查询区块的高度获得对应区块信息,并将所述区块信息反馈至所述交易节点;所述数据验证模块用于对已归档数据做验证以及在将所述增量归档数据合并到全量归档数据目录之前对增量归档数据做验证,例如通过从最新区块开始一直到创世区块验证每个区块记录的prehash等于前一个区块数据做hash计算的结果的验证方式,对已归档数据做验证以及在将所述增量归档数据合并到全量归档数据目录之前对增量归档数据做验证。具体的,请参考图2所示,所述归档节点1包含:参数配置模块11、数据传输模块12、数据合并模块13、数据查询模块14、数据验证模块15。

[0037] 所述参数配置模块11负责配置数据归档相关参数,包括全量归档数据的存储路径、增量归档数据的临时存储路径、归档服务对外的端口和URL等信息。

[0038] 所述数据传输模块12负责与各个交易节点2建立网络连接,接收交易节点2的请求并进行应答。该请求类型是数据传输请求,在临时目录保存做完归档数据计算后产生的增量归档数据。

[0039] 所述数据合并模块13负责对归档数据传输模块12产生的增量数据做遍历,把遍历到的数据合并到全量归档数据目录,最终把合并结果成功或者失败返回给发起合并请求的交易节点2。

[0040] 所述数据查询模块14负责对外提供归档区块数据查询服务,查询归档数据的交易节点2在请求中指定网络ID、节点ID和查询区块的高度,归档节点1返回该区块的全部信息。

[0041] 所述数据验证模块15负责在归档节点启动时对全部已归档数据做校验、在归档数据合并模块13执行前对增量归档数据做验证,具体验证方法是从最新区块开始一直到创世区块,验证每个区块记录的prehash等于前一个区块数据做hash计算的结果。若验证通过,直接做后续处理;若验证不通过,记录报错日志并发送预警信息给区块链用户。

[0042] 在本发明一实施例中,所述交易节点包含:通讯模块、共识模块、交易执行模块、归档数据处理模块、临时数据清理模块、归档数据查询模块和数据验证模块;所述通讯模块分别与区块链客户端、其他交易节点、归档节点建立网络连接,用于为所述交易节点提供数据交互通道;所述共识模块用于与其他交易节点根据约定好的共识算法对交易进行共识处理,根据共识的结果确定交易的执行顺序并把交易打包成区块交由所述交易执行模块;所述交易执行模块用于根据所述执行顺序处理所述区块中的交易;当所述交易为归档交易时,将所述归档交易的交易数据交由所述归档数据处理模块;所述归档数据处理模块用于

根据所述归档交易的交易参数指定的归档区块高度或者归档时间点,计算出小于归档区块的全部区块数据或者小于归档时间点生成的全部区块,根据全部区块及归档参数生成归档指南区块和在线数据区块后,将所述归档指南区块和在线数据区块存入至本地临时目录;根据所述归档节点信息将本地临时目录中存储的全部文件打包后发送至对应的归档节点;所述临时数据清理模块用于根据所述归档节点反馈的确认信息删除所述本地临时目录中存储数据生成归档成功信息,并交由所述通讯模块将所述归档成功信息发送至发起归档请求的区块链用户;所述归档数据查询模块用于将区块链用户发起的查询请求提交至所述数据查询模块,以及将所述数据查询模块反馈的所述区块信息交由所述区块链用户;所述数据验证模块用于通过从最新区块开始一直到创世区块验证每个区块记录的prehash等于前一个区块数据做hash计算的结果的验证方式,对在线的区块数据做验证。其中,所述归档数据处理模块可包含归档数据计算模块、归档数据传输模块和归档数据合并模块;所述归档数据计算模块用于根据所述归档交易的交易参数指定的归档区块高度或者归档时间点,计算出小于归档区块的全部区块数据或者小于归档时间点生成的全部区块,获得归档区块;根据归档区块及归档参数生成归档指南区块、归档数据索引区块、归档数据区块;将所述归档指南区块存入在线数据存储目录,并将被归档的在线数据区块于在线数据存储目录中清理;将归档数据索引区块、归档数据区块存入本地临时目录;所述归档数据传输模块用于根据所述归档节点信息将本地临时目录中存储的全部文件打包后发送至对应的归档节点;所述归档数据合并模块用于当所述归档数据传输模块完成数据传输后生成触发信号,将所述触发信号发送至所述数据合并模块。

[0043] 具体的,请参考图3所示,所述交易节点2包含:通讯模块21、共识模块22、交易执行模块23、数据存储模块24、归档数据计算模块25、归档数据传输模块26、归档数据合并模块27、临时数据清理模块28、归档数据查询模块29、数据验证模块30。

[0044] 所述通讯模块21分别与区块链客户端、其他交易节点2、归档节点1建立网络连接。与区块链客户端建立restful网络连接,交易节点2作为服务端,接收区块链客户端的交易请求,然后通过与其他交易节点2建立RPC网络连接,把交易广播到其他交易节点2,进行后续的区块链共识处理。通讯模块21还会向归档节点1发起请求,该请求可以是归档传输请求,也可以是归档合并请求,也可以是归档区块查询请求,归档节点1返回处理结果。

[0045] 所述共识模块22是交易共识处理的逻辑装置,根据业务规则对交易的合法性进行判断,在合法性验证通过后,与其他交易节点2根据约定好的共识算法对交易进行共识处理,这里的共识算法可以是POW (Proof Of Work,工作量证明)、POS (Proof Of Stake,股权证明)、DPOS (Delegated Proof Of Stake,委托股权证明)、PBFT (Practical Byzantine Fault Tolerance,实用拜占庭容错)等。最后根据共识的结果确定交易的执行顺序,把交易打包成区块,并把区块交给执行模块23执行。

[0046] 所述交易执行模块23负责把区块中的交易按顺序执行,如果发现交易类型是归档交易,会把交易数据交给归档数据计算模块25处理,否则由其他类型交易处理模块处理,最终交易执行完毕会由数据存储模块24处理。

[0047] 所述数据存储模块24负责持久化存储交易执行的结果。

[0048] 所述归档数据计算模块25负责归档交易的计算处理,根据归档交易参数指定的归档区块高度(或者归档时间点),计算出小于归档区块的全部区块数据(或者小于归档时间

点生成的全部区块),然后按照图4的数据结构计算出结果,计算结果存放在临时目录。

[0049] 所述归档数据传输模块26负责归档交易的传输处理,调用归档节点1的数据传输模块12服务,把归档数据计算模块25的计算结果,即临时目录的全部文件打包发送给归档节点1。

[0050] 所述归档数据合并模块27负责触发归档节点1上的数据合并模块13,执行归档数据合并,并根据返回的执行结果继续临时数据清理模块28的处理或者报错退出。

[0051] 所述临时数据清理模块28是归档交易执行的最后一步,在前面全部操作都成功的情况下,清理前面的归档数据计算模块25生成的临时目录数据。

[0052] 所述归档数据查询模块29负责归档数据查询交易的处理,在判断查询的数据已归档后,触发归档节点1的数据查询模块14。

[0053] 所述数据验证模块30负责对在线的区块数据做验证,具体验证方法是从最新区块开始一直到未被归档的第一个区块,验证每个区块记录的prehash等于前一个区块数据做hash计算的结果。若验证通过,直接做后续处理;若验证不通过,记录报错日志并发送预警信息给区块链用户。若需要对被归档数据做验证,交易节点2触发归档节点1的数据验证模块15,根据返回结果确认验证通过或者验证失败。

[0054] 请参考图4所示,本发明中交易节点的数据结构为在线数据结构,所述在线数据结构可包含包含:归档指南区块3、在线数据区块4。

[0055] 所述归档指南区块3包含:清理指南点31、历史数据指纹32、清理起始区块高度33、清理截止区块高度34、清理起始区块入账时间35、清理截止区块入账时间36、其它数据37。所述清理指南点31是本次离线归档执行后,记录未被归档的第一个在线数据区块4的区块高度41。所述历史数据指纹32是本次离线归档执行后,被归档的一个或多个在线数据区块4做哈希计算得到的结果,如果被篡改,会在归档节点1和归档数据索引区块5同名字段的比对中发现。所述清理起始区块高度33是本次离线归档执行中,被归档的在线数据区块4的区块高度41的最小值。所述清理截止区块高度34是本次离线归档执行中,被归档的在线数据区块4的区块高度41的最大值。所述清理起始区块入账时间35是本次离线归档执行中,被归档的区块高度41最小的在线数据区块4的时间戳45。所述清理截止区块入账时间36是本次离线归档执行中,被归档的区块高度41最大的在线数据区块4的时间戳45。所述其它数据37是做归档数据查询可能会用到的其他查询条件。

[0056] 所述在线数据区块4包含:区块高度41、上一区块哈希42、交易数据43、时间戳44、其他数据45。所述区块高度41是一个自然数,按照在线数据区块4生成顺序从小到大编号。所述上一区块哈希42是区块高度比当前区块小一的在线数据区块4做哈希运算的结果,保证在线数据区块4不被篡改,如果是创世区块可以不需要这个字段。所述交易数据43是包含在在线数据区块4中的一个或多个交易的信息,包含交易参数、执行结果等。所述时间戳44记录生成区块的时间。所述其他数据45是伴随区块生成需要的一些其他信息。

[0057] 再请参考图5所示,本发明中归档节点的数据结构为离线数据结构,所述离线数据结构包含:归档数据索引区块5、归档数据区块6。

[0058] 所述归档数据索引区块5包含:上一区块哈希值51、历史数据指纹52、清理起始区块高度53、清理截止区块高度54、清理起始区块入账时间55、清理截止区块入账时间56、其它数据57。所述上一区块哈希值51是上一个归档数据索引区块5做哈希运算得到的结果,保

证归档数据索引区块5不被篡改,如果是第一个归档数据索引区块5可以不需要这个字段。所述历史数据指纹52是本次离线归档执行后,被归档的一个或多个在线数据区块4做哈希计算得到的结果。所述清理起始区块高度53是本次离线归档执行中,被归档的在线数据区块4的区块高度41的最小值。所述清理截止区块高度54是本次离线归档执行中,被归档的在线数据区块4的区块高度41的最大值。所述清理起始区块入账时间55是本次离线归档执行中,被归档的区块高度41最小的在线数据区块4的时间戳45。所述清理截止区块入账时间56是本次离线归档执行中,被归档的区块高度41最大的在线数据区块4的时间戳45。所述其它数据57是数据归档中可能要记录并在后面校验用到的信息。

[0059] 所述归档数据区块6包含:区块高度61、上一区块哈希62、交易数据63、时间戳64、其他数据65。所述区块高度61和区块高度41的定义一致。所述上一区块哈希62和上一区块哈希42的定义一致。所述交易数据63和交易数据43的定义一致。所述时间戳64和时间戳44的定义一致。所述其他数据65和其他数据45的定义一致。

[0060] 请参考图6A所示,本发明还提供一种基于区块链的离线归档方法,所述方法包含:S101根据预设归档参数配置归档节点信息及数据归档的本地临时目录;S102接收区块链用户发起的归档请求,根据所述归档请求与区块链上其他交易节点完成交易共识,当交易共识完成后解析所述归档请求获得归档参数;S103根据所述归档参数计算获得符合所述归档参数的一个或多个在线数据区块,将所述在线数据区块清理并生成同样结构的一个或多个归档数据区块后存入所述本地临时目录;S104根据被清理的所述在线数据区块通过哈希算法计算生成历史数据指纹;S105将所述历史数据指纹存入所述本地临时目录后,将所述本地临时目录中所述历史数据指纹及所述归档数据区块发送至所述归档节点信息对应的归档节点;S106根据所述归档节点反馈的确认信息删除所述本地临时目录中存储数据生成归档成功信息,将所述归档成功信息发送至发起归档请求的区块链用户。

[0061] 具体的,请参考图6B所示,在实际工作中,整个区块链网络系统接收到归档请求时,归档节点1和交易节点2的处理步骤如下:

[0062] 步骤S701:交易节点2启动后,根据预设的归档参数配置好归档节点1的IP、端口、URL地址、用户、密码等,数据归档的本地临时目录等信息。

[0063] 步骤S702:交易节点2配置好归档参数后,通讯模块21开始接收来自区块链用户的归档请求。

[0064] 步骤S703:交易节点2接收到归档请求后,开始和网络中其他交易节点2做交易共识,共识成功继续归档处理S704,共识失败停止归档并组装报错信息后执行S715。

[0065] 步骤S704:交易节点2在网络共识成功后,解析归档请求的参数,包括网络ID、节点ID、清理高度等(按高度清理就是清理高度、按时间清理就是清理时间)。

[0066] 步骤S705:交易节点2的归档数据计算模块25,以请求参数是清理的区块高度(简称清理高度)为例,要求请求的清理高度大于全部归档指南区块3的清理指南点31、清理高度小于在线数据区块4的最大的区块高度41。满足前面两个条件后,交易节点2挑选出区块高度41小于清理高度的一个或多个在线数据区块4,这些区块都将被清理并生成同样结构的一个或多个归档数据区块6,暂存在临时目录。在交易节点2生成一个归档指南区块3,清理指南点31记录的就是本次清理指定的清理高度,根据本次被清理的一个或多个在线数据区块4用哈希算法计算出新的归档指南区块3的历史数据指纹32(一方面保证了这段归档区

块的不可篡改性,一方面用于索引到归档节点1的对应数据),记录归档指南区块3的清理起始区块高度33、清理截止区块高度34、清理起始区块入账时间35、清理截止区块入账时间36、其它数据37。在临时目录生成一个归档数据索引区块5,上一区块哈希值51记录的是上一次归档生成的归档数据索引区块5做哈希运算的结果,历史数据指纹52、清理起始区块高度53、清理截止区块高度54、清理起始区块入账时间55、清理截止区块入账时间56记录和归档指南区块3对应字段一样,其它数据57记录交易的其他关键信息。

[0067] 步骤S706:交易节点2完成归档数据计算后,归档数据传输模块26可以通过FTP或者其他方式将临时目录的归档数据传输给归档节点1。

[0068] 步骤S707:归档节点1的数据传输模块12接收归档数据,并根据网络ID、节点ID暂存在对应临时目录,返回传输结果给交易节点2。

[0069] 步骤S708:交易节点2判断传输结果,如果传输成功继续S709,如果传输失败停止归档流程并执行S714。

[0070] 步骤S709:交易节点2在传输成功后,归档数据合并模块27触发请求归档节点1做归档数据合并,请求参数是网络ID和节点ID。

[0071] 步骤S710:归档节点1接收到合并请求后,数据合并模块13把归档数据临时目录合并到正式的归档数据目录下,返回合并结果给交易节点2。

[0072] 步骤S711:交易节点2判断合并结果,如果合并成功继续S712,如果合并失败停止归档流程并执行S714。

[0073] 步骤S712:交易节点2合并成功后,临时数据清理模块执行清理,删除临时目录下不需要的数据,最后打包归档成功信息。

[0074] 步骤S713:交易节点2的通讯模块21返回归档成功信息给区块链用户。

[0075] 步骤S714:交易节点2记录归档失败的断点信息(用于下一次归档完成断点再续),最后打包归档失败信息。

[0076] 步骤S715:交易节点2的通讯模块21返回归档失败信息给区块链用户。

[0077] 在本发明一实施例中,所述方法还包含:接收区块链用户发起的查询请求,根据所述查询请求获得对应的网络ID、节点ID和查询区块的高度;根据所述查询区块的高度查询对应区块是否已被归档,当所述区块已被归档时,获得对应的区块的历史数据指纹;将所述网络ID、所述节点ID、所述历史数据指纹和所述查询区块的高度发送至归档节点,由所述归档节点根据所述网络ID、所述节点ID、所述历史数据指纹和所述查询区块的高度查询对应的区块并接收所述归档节点反馈的查询结果;将所述查询结果反馈至区块链用户。具体请参考图7所示,整个区块链网络系统接收到查询请求后,归档节点1和交易节点2的处理步骤如下:

[0078] 步骤S801:交易节点2的通讯模块21,接收到来自客户端的交易请求后,判断是交易区块查询请求后,归档数据查询模块29检查请求参数合法性,以请求参数是查询的区块高度(简称查询高度)为例,要求查询高度小于或等于在线数据区块4的最大的区块高度41。

[0079] 步骤S802:交易节点2的归档数据查询模块29,判断查询数据的状态。若查询高度大于或等于全部归档指南区块3的清理指南点31,说明查询的数据未被归档,执行S807。若查询高度小于任一归档指南区块3的清理指南点31,说明查询的数据已归档,执行S803。

[0080] 步骤S803:交易节点2的归档数据查询模块29判断查询数据已归档后,将查询请求

(包含网络ID、节点ID、历史数据指纹、查询高度等信息)转发归档节点1的数据验证模块15。

[0081] 步骤S804:归档节点1的数据验证模块15验证历史数据指纹合法性,验证通过后转发数据查询模块14处理,验证失败后报错返回交易节点2。

[0082] 步骤S805:历史数据指纹验证通过后,归档节点1的数据查询模块14处理查询请求并返回结果,结果响应交易节点2。

[0083] 步骤S806:历史数据指纹验证失败后,交易节点2的归档数据查询模块29接收结果,并打包给通讯模块21。

[0084] 步骤S807:交易节点2的在线数据查询模块处理查询请求并打包给通讯模块21。

[0085] 步骤S808:交易节点2的通讯模块21返回查询结果。

[0086] 在本发明一实施例中还提供一种区块链离线归档系统的归档交易的共识准入的流程图,请参考图8所示,交易节点2的处理步骤如下:

[0087] 步骤S901:交易节点2启动后,根据预设的归档参数配置好:哪些交易节点2参与离线归档(图示是机构A、B共四个节点)、哪些交易节点2参与归档交易共识(图示里面是机构A一个节点、机构B两个节点)。

[0088] 步骤S902:整个区块链网络系统接收到归档请求时,参与归档交易共识的交易节点2(图示里面是机构A一个节点、机构B两个节点)广播归档交易共识消息,归档交易共识消息的内容包括但不限于“归档区块高度”、“共识节点ID”、“共识节点签名信息”等。

[0089] 步骤S903:参与离线归档的交易节点2(图示是机构A、B共四个节点)接收来自其他交易节点2的归档交易共识消息,若超过一定数目的共识消息一致,认为全网共识成功,继续归档请求的处理;若接收到的一致的一致共识消息数目不超过阈值,认为归档交易共识失败,返回归档失败信息给区块链用户。不参与离线归档的交易节点2接收到归档交易共识请求后直接丢弃,忽略请求。

[0090] 在本发明一实施例中,所述方法还包含:获取当前交易节点的内存情况和单个区块的占用内存大小,根据内存情况和单个区块的占用内容大小计算获得在线区块的并发验证数量,根据所述并发验证数量对当前交易节点内区块分组获得多组待验证区块数据;根据所述待验证区块数据的区块高度,从高到低进行依次对所述待验证区块数据进行验证获得验证结果;获取归档节点的归档区块的验证结果;将所述归档区块的验证结果与所述在线区块的验证结果比较,根据比较结果获得区块归档验证情况;具体的,上述实施例使用时,首先获取当前交易节点的可用内存M、单个区块的大小m和待验证区块的数目N,待验证区块是从区块高度最大的区块到未被归档的区块高度最小的区块,根据可用内存和单个区块的大小计算在线区块并发验证的最大数量 $N_{max} = \text{向下取整}(M/m)$,并发验证数量是 $n = \min(N, N_{max})$,根据所述并发验证数量n对当前交易节点的待验证区块分组,每组区块数量是n,获得多组待验证区块数据;每组区块的验证在一个线程或进程中处理,不同组区块的验证并行处理,根据所述待验证区块数据的区块高度,从高到低进行依次对所述待验证区块数据进行验证获得验证结果;获取归档节点的归档区块的验证结果;将所述归档区块的验证结果与所述在线区块的验证结果比较,根据比较结果获得区块归档验证情况;其中,根据所述待验证区块数据的区块高度,从高到低进行依次对所述待验证区块数据进行验证获得验证结果包含:对所述待验证区块数据中各区块分别进行验证,将各区块的验证结果两两比较,当比较结果符合预设规则时以所述待验证区块数据中区块高度最小的区块为所述

待验证区块数据的验证结果;将所述待验证区块数据的验证结果与相邻的所述待验证区块数据的验证结果进行比较,当比较结果符合预设规则时以所述待验证区块数据中区块高度最小的所述待验证区块数据的验证结果作为在线区块的验证结果。

[0091] 在上述实施例中,将所述归档区块的验证结果与所述在线区块的验证结果比较,根据比较结果获得区块归档验证情况包含:将在线区块中区块高度最小的区块记录的上一区块哈希与归档区块中区块高度最大的区块记录的上一区块哈希比较,当两者相同时区块归档验证通过。具体的,请参考图9所示,本发明还提供了一种区块链离线归档系统的区块防篡改验证的流程图,归档节点1和交易节点2的处理步骤如下:步骤S1001:交易节点2执行区块验证时,分为两个步骤:线上区块验证和归档区块验证,两个步骤可以并发执行。归档区块验证通过发区块验证请求给归档节点1,要求归档节点1返回验证通过或者验证不通过的结果,除了这个结果外,还附加返回最大高度的区块的哈希计算结果。步骤S1002:由于内存和CPU限制,现有的线上区块验证过程一般是串行计算,从最大高度的区块开始一直验证到创世区块,验证方法是验证每个区块中存储的“前一区块哈希”等于高度小一的区块计算哈希的结果,相等则认为前一区块验证通过,没有被篡改,往前推一个区块继续验证。本专利一方面减少了交易节点2需要验证的区块总数,一方面优化区块验证过程为并发计算。交易节点1先计算可用的内存、单个区块的大小,确认一次最多可以并发验证多少区块,然后并发启动对应数目的区块验证(并发方式包括但不限于多线程、多进程、GPU等方式),需要验证的区块包括高度最大的区块一直到未被归档的高度最小的区块,验证通过的区块标记为已验证,若全部线上区块验证通过则等待归档节点1返回归档区块验证的结果做合并,若出现一个区块验证不通过,则标记验证不通过、终止线上区块验证的全部并发过程、通知归档节点1结束归档区块验证,若线上区块未验证完成则继续读取未处理的区块做验证。步骤S1003:归档节点1开始归档区块验证,先计算可用的内存、单个区块的大小,确认一次最多可以并发验证多少区块,然后并发启动对应数目的区块验证(并发方式包括但不限于多线程、多进程、GPU等方式),需要验证的区块包括高度最大的区块一直到创世区块,验证通过的区块标记为已验证,若全部归档区块验证通过则返回验证结果给交易节点2为验证通过并返回“最大高度区块的哈希”计算结果,若出现一个区块验证不通过,则标记验证不通过、终止归档区块验证的全部并发过程、通知交易节点2结束归档区块验证。步骤S1004:交易节点2接收到归档节点1的验证结果响应后,判断验证结果,如果验证不通过则终止线上区块验证,返回验证失败给区块链用户,如果验证通过则暂存验证结果并等待线上区块验证结束。线上区块验证结束后,比较线上高度最小区块记录的“前一区块哈希”等于归档节点1返回“最大高度区块的哈希”,如果验证不通过则返回验证失败给区块链用户,如果验证通过则返回验证成功给区块链用户。

[0092] 本发明还提供一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述计算机程序时实现上述方法。

[0093] 本发明还提供一种计算机可读存储介质,所述计算机可读存储介质存储有执行上述方法的计算机程序。

[0094] 本发明的有益技术效果在于:解决了由于区块链特性导致的数据持续增长和不可随意清理的问题,引入数据离线归档有下面几点好处:利用对被归档数据计算历史数据指纹并记录,可以保证被归档数据依然有不可篡改的特征;利用原有的多节点共识机制,可以

保证归档交易的严格准入,只有得到全网共识节点的认可才能执行数据清理和归档;利用远端数据备份服务器的动态配置,可以保证归档数据既可以集中存放在一台数据备份服务器,也可以存放在多台数据备份服务器上,做到了数据存储的灵活配置;利用远端数据备份服务器对外提供查询或验证功能,可以保证区块链系统能够查询到被归档数据,并验证归档数据不被篡改;集成数据归档功能到在线服务,保证了清理期间不需要停机且不影响其他交易;优化了在线数据校验过程,原来的数据校验是从最新区块一直验证到创世区块,验证过程占用系统的CPU和内存资源较多,而且数据量大的时候验证过程持续时间较长,引入数据归档后,线上数据验证只需要从最新区块一直验证到线上未被归档的第一个区块,归档数据的验证可以在归档服务器上执行,一方面加快了线上验证过程、一方面一定程度上释放了线上交易节点服务器的硬件资源。

[0095] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0096] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0097] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0098] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0099] 以上所述的具体实施例,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上所述仅为本发明的具体实施例而已,并不用于限定本发明的保护范围,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

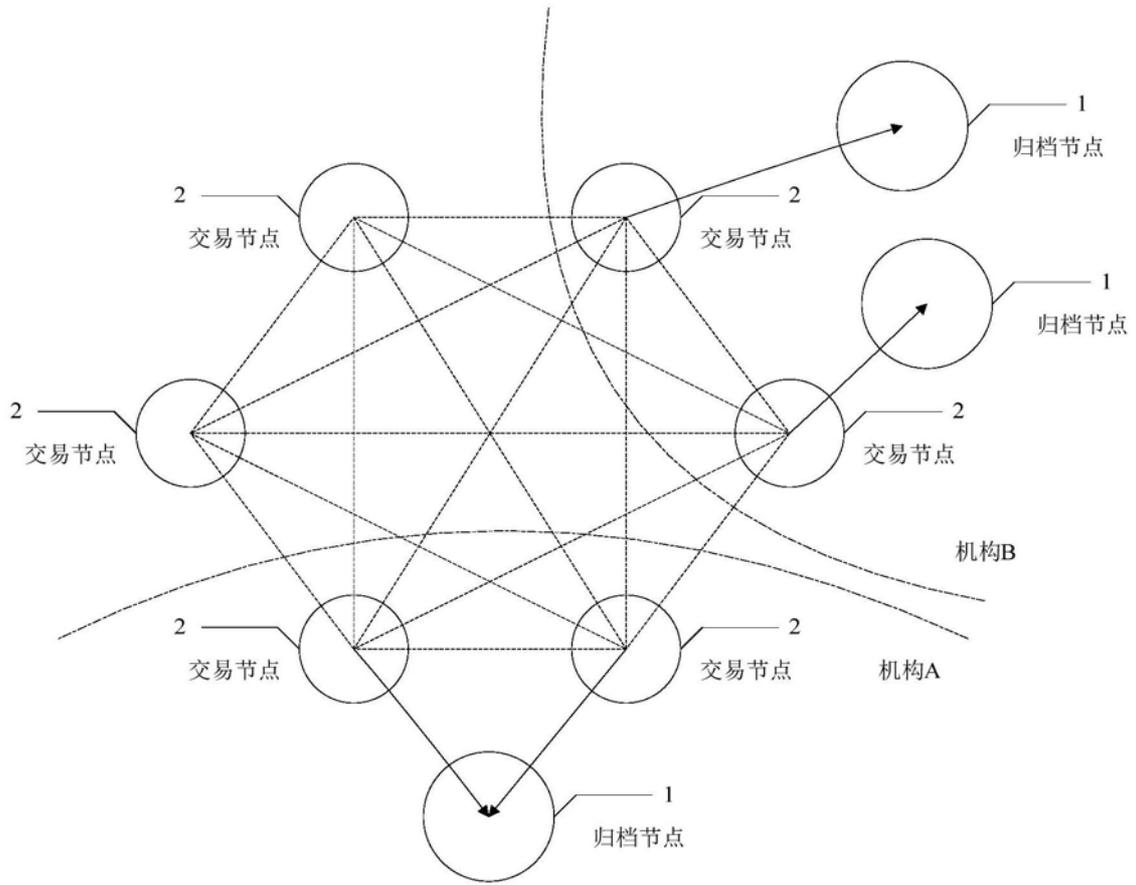


图1

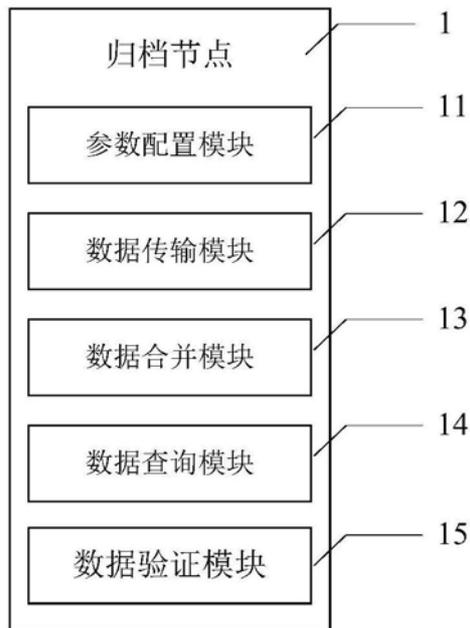


图2

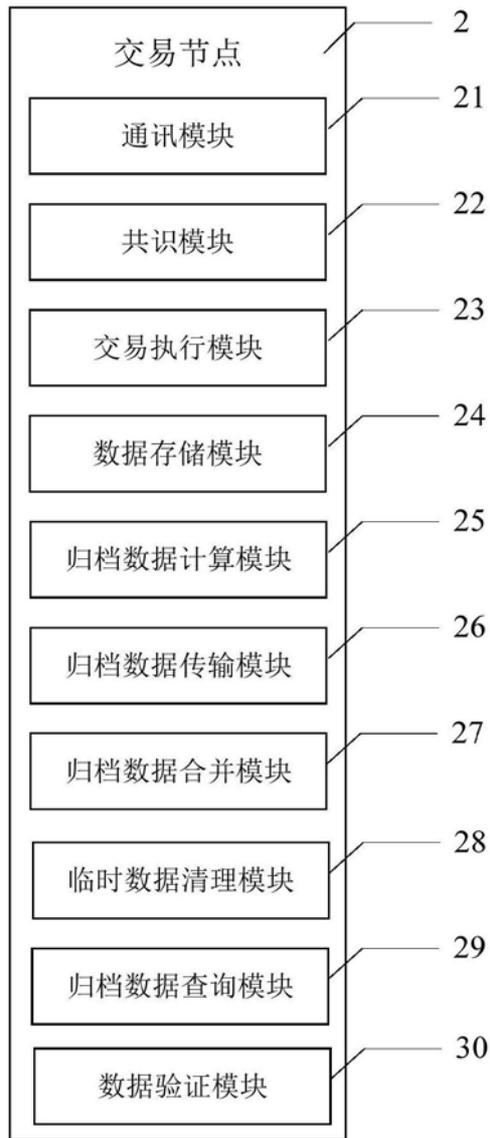


图3

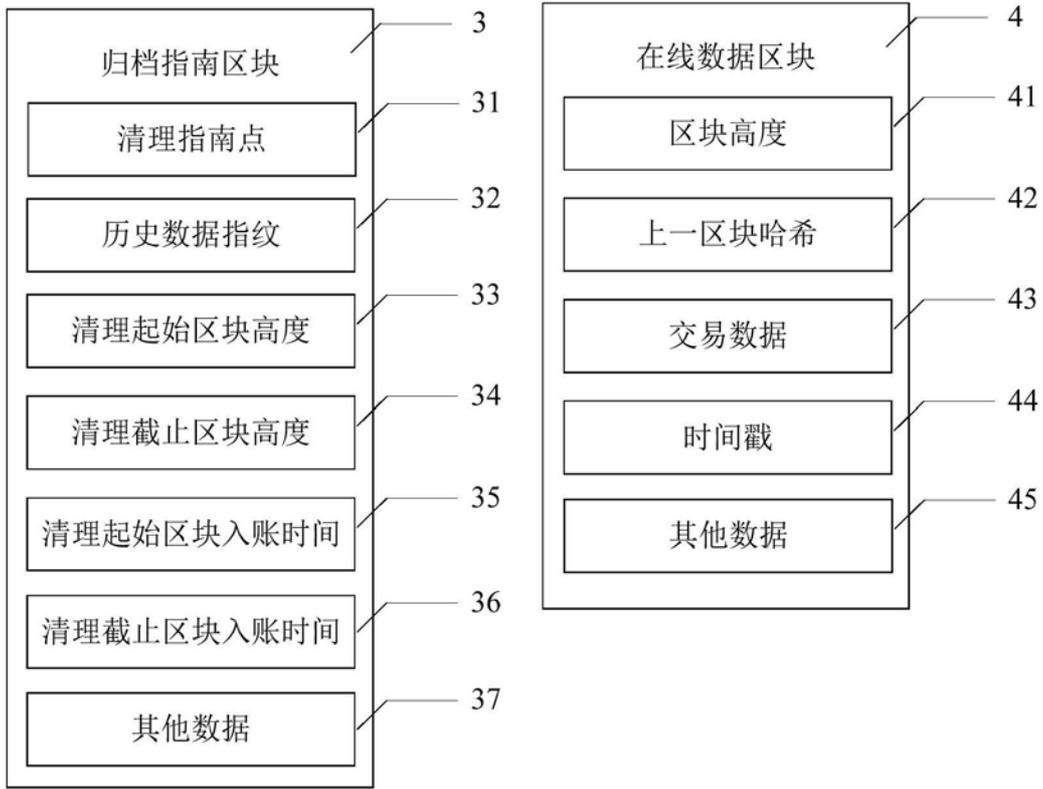


图4

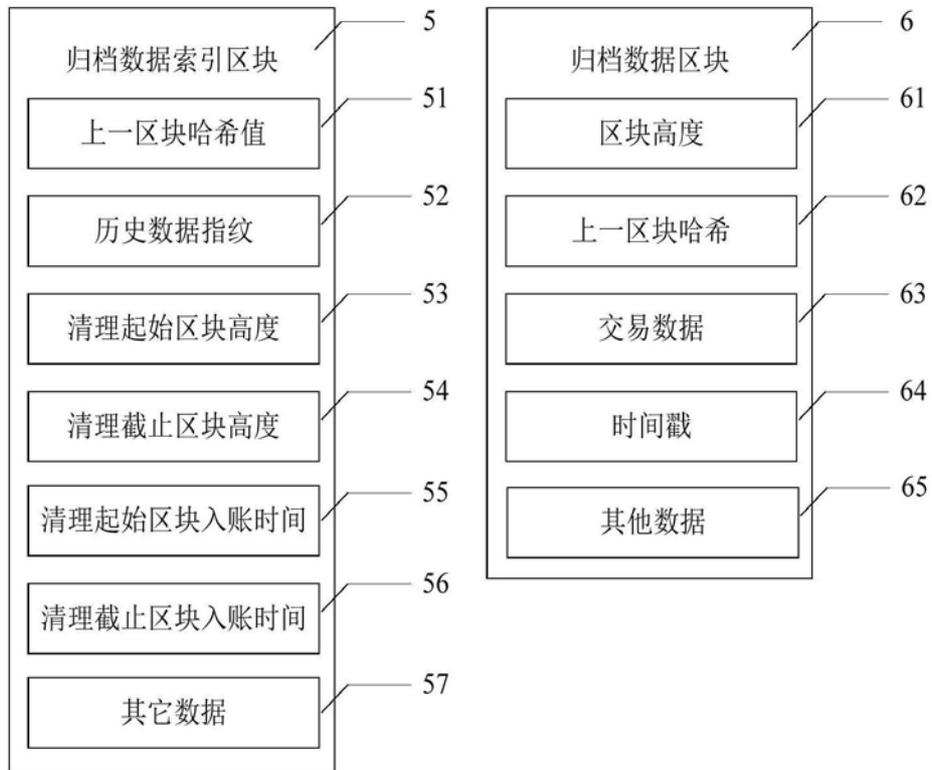


图5

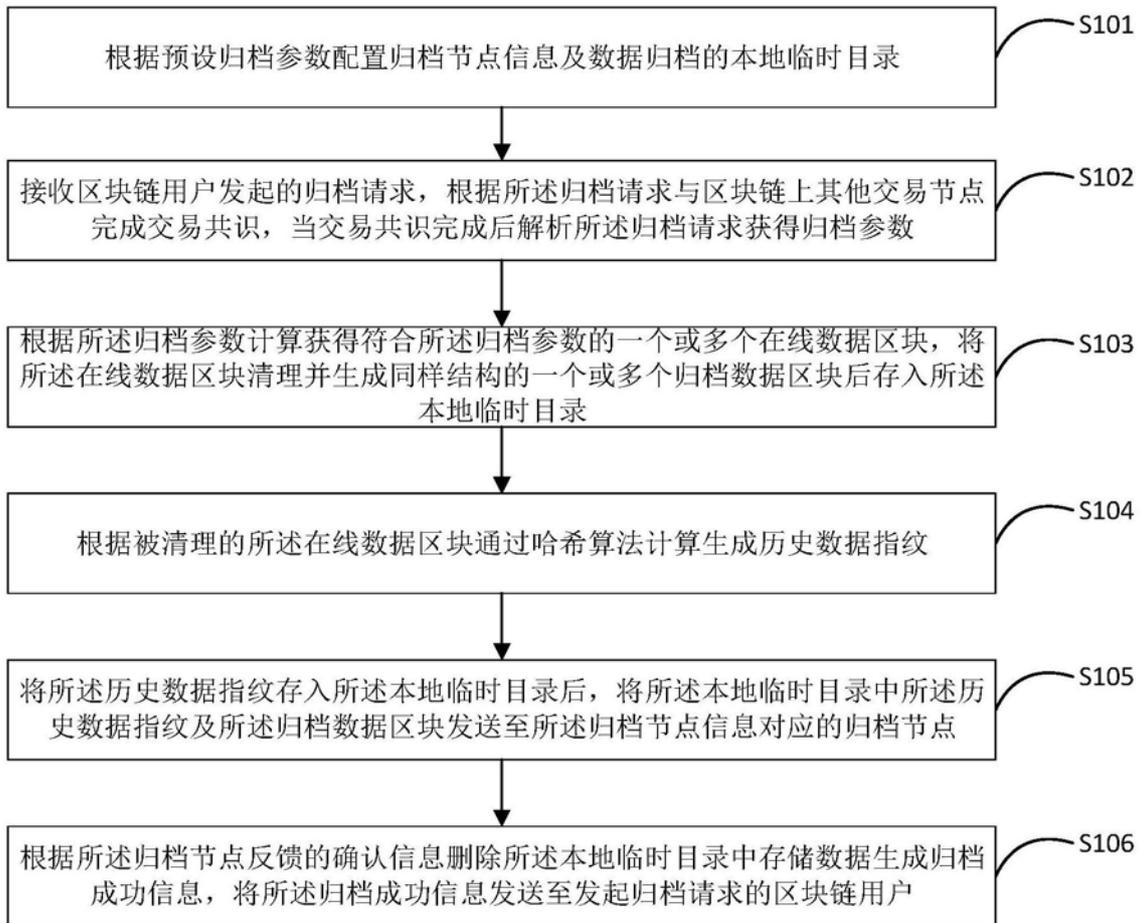


图6A

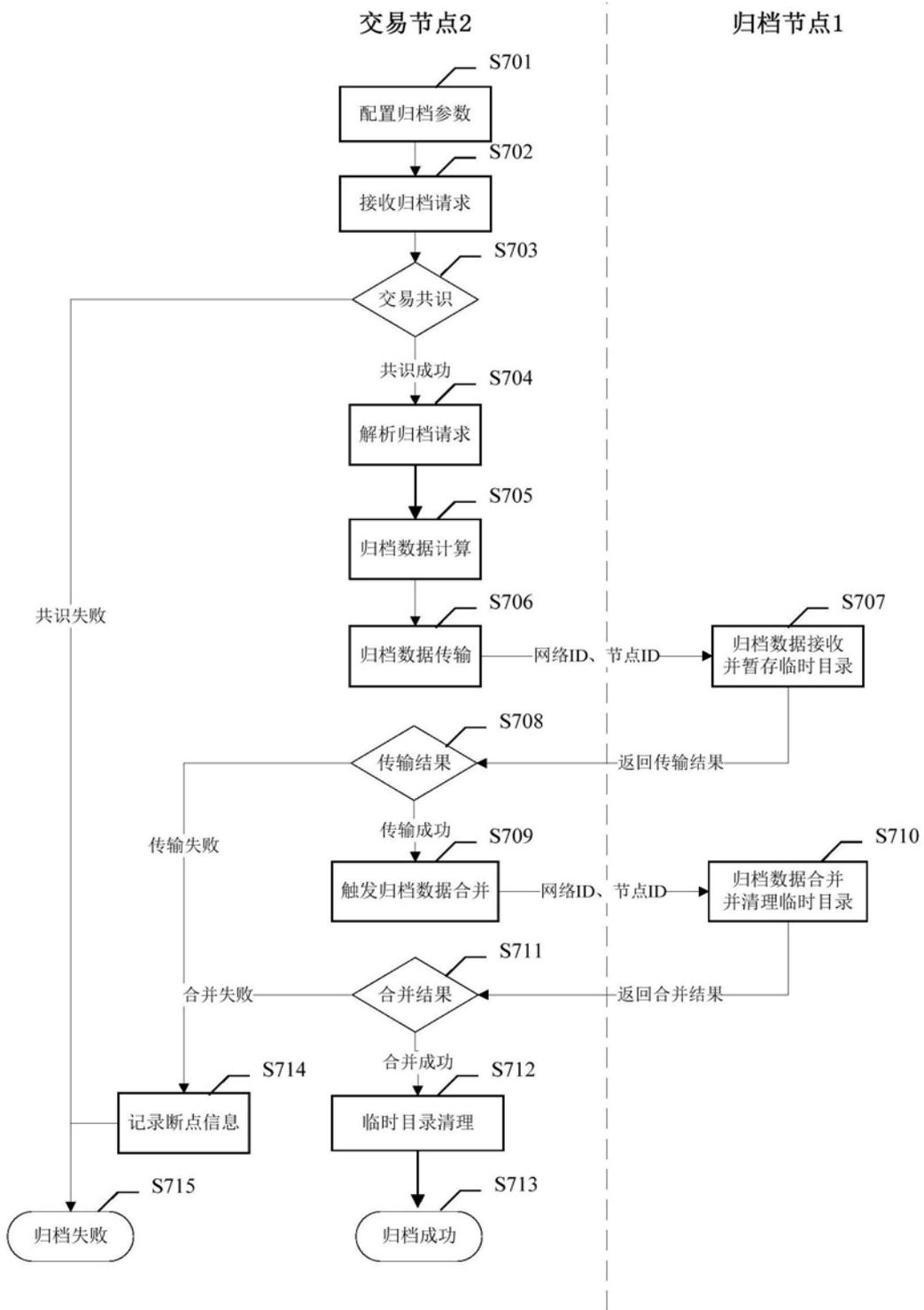


图6B

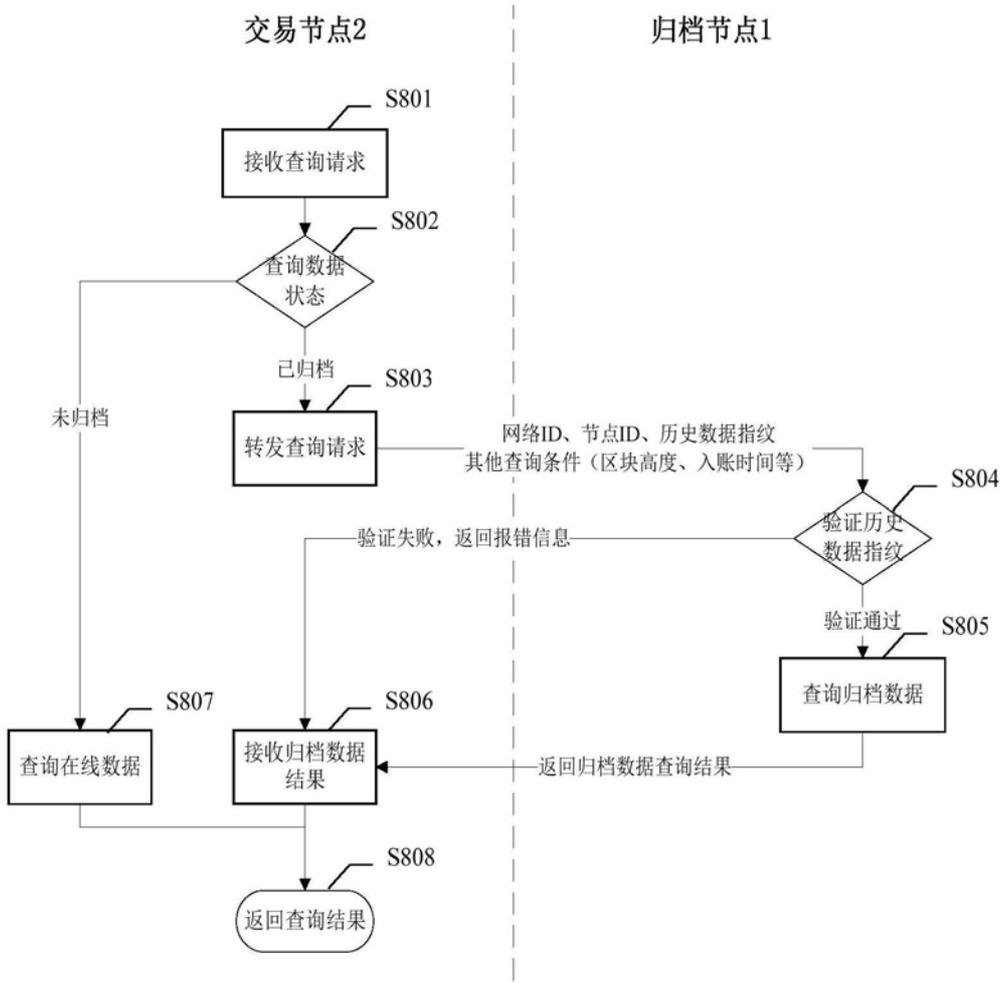


图7

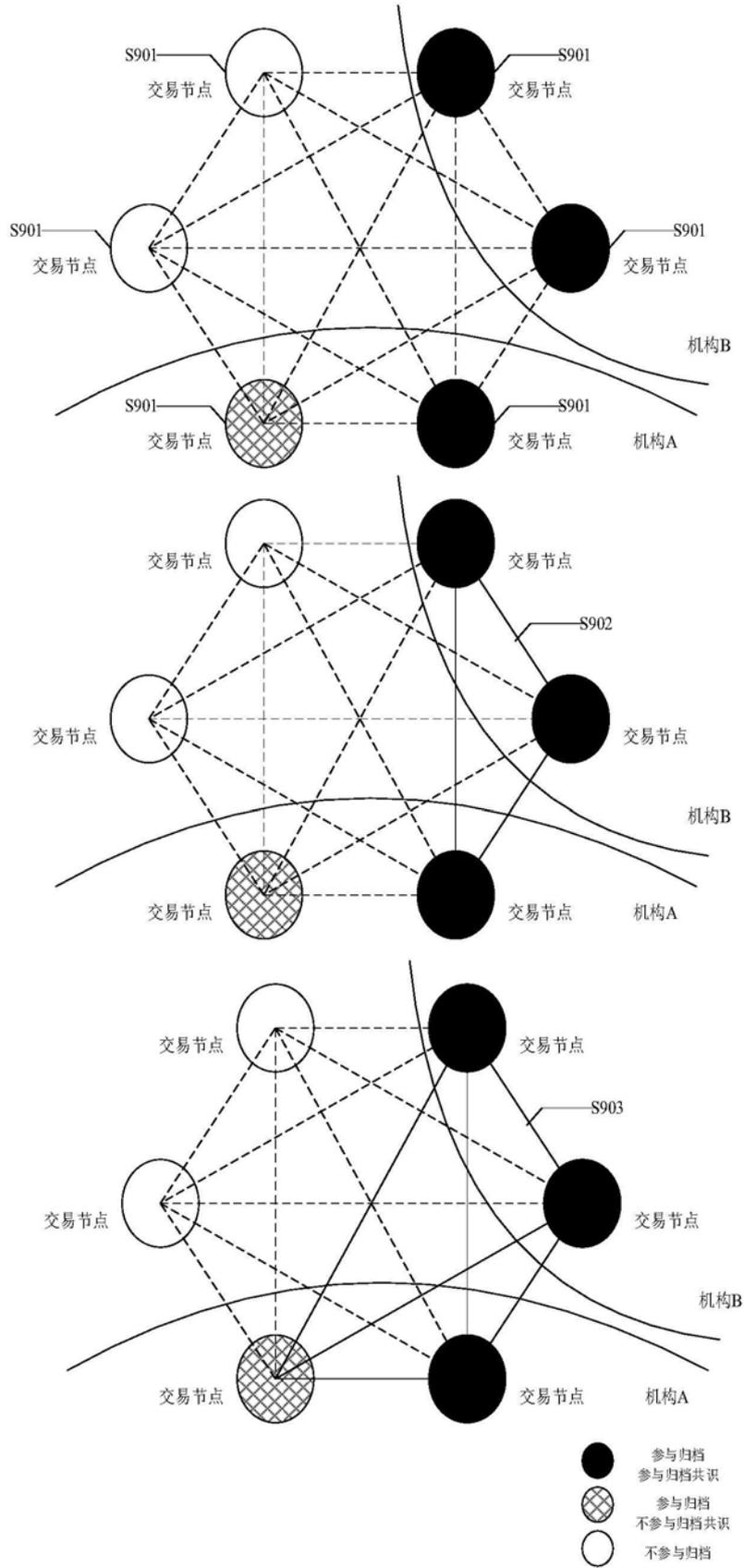


图8

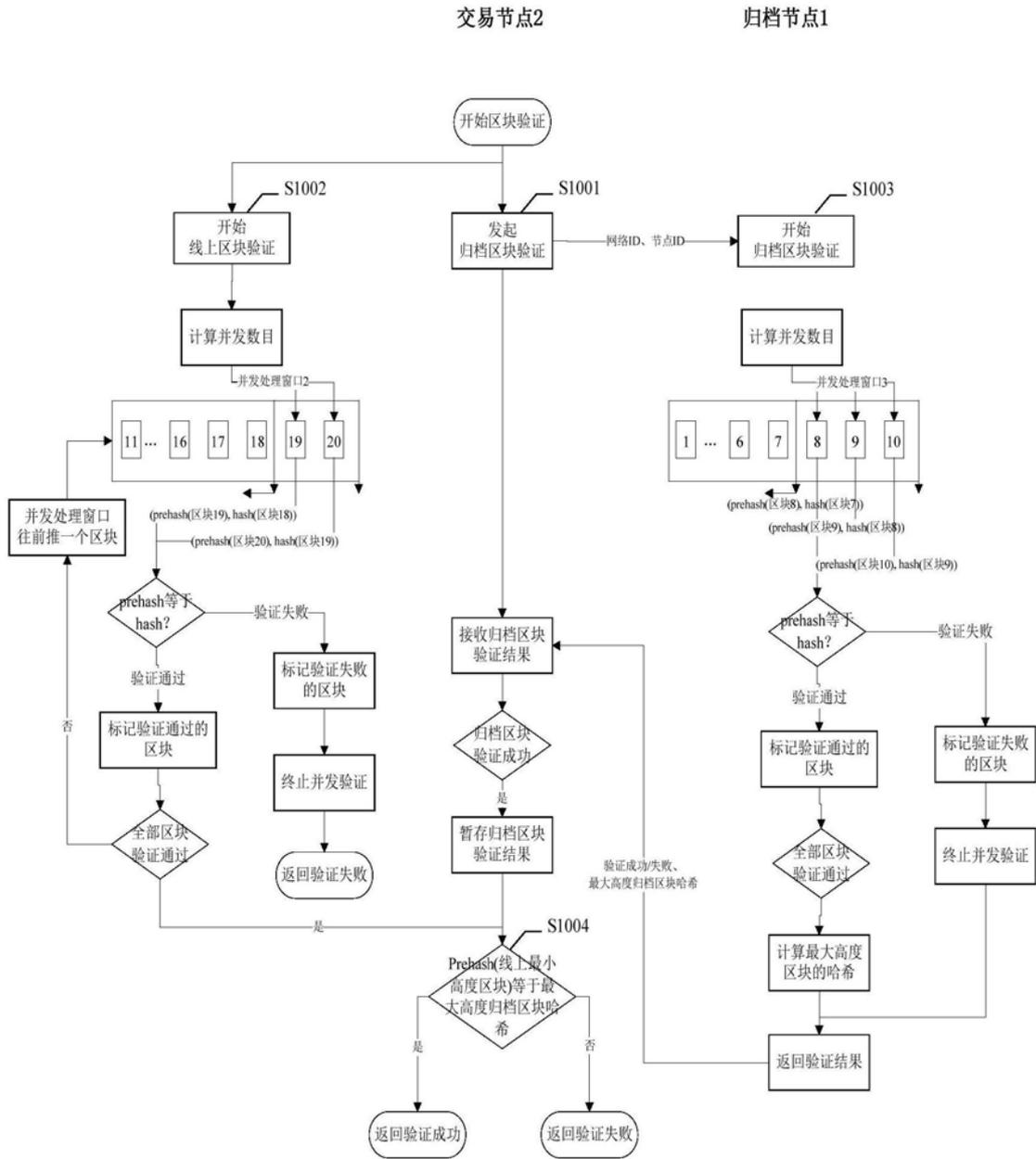


图9