(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114138903 B
(45)授权公告日 2024.10.25

(21)申请号 202111456551.5

(22)申请日 2021.12.02

(65)同一申请的已公布的文献号
申请公布号 CN 114138903 A

(43)申请公布日 2022.03.04

(73)专利权人 杭州复杂美科技有限公司
地址 310000 浙江省杭州市西湖区文三路90号东部软件园6号楼7层702室

(72)发明人 马登极 王志文 吴思进

(51)Int.Cl.
G06F 16/27(2019.01)
G06F 16/22(2019.01)
G06F 16/23(2019.01)
G06Q 40/04(2012.01)

(56)对比文件
CN 114266665 A,2022.04.01

审查员 张力

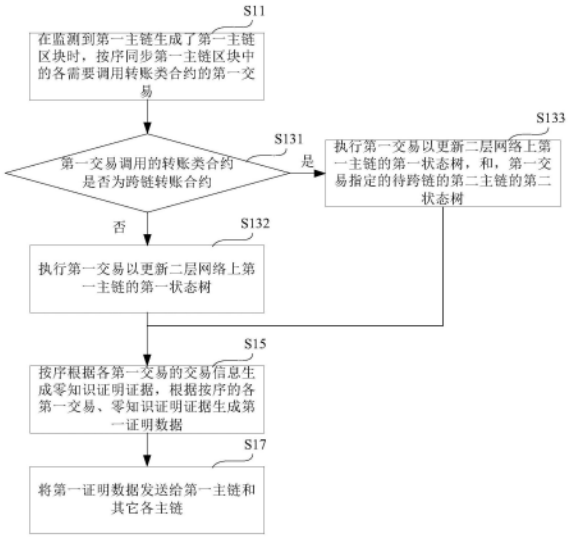
权利要求书2页 说明书6页 附图2页

(54)发明名称

多主链跨链方法、计算机设备和存储介质

(57)摘要

本发明提供一种多主链跨链方法、计算机设备和存储介质，该方法包括：在监测到第一主链生成了第一主链区块时，按序同步第一主链区块中的各需要调用转账类合约的第一交易；对各第一交易执行如下操作：判断第一交易调用的转账类合约是否为跨链转账合约：否，则执行第一交易以更新二层网络上第一主链的第一状态树；是，则执行第一交易以更新二层网络上第一主链的第一状态树，和，第一交易指定的待跨链的第二主链的第二状态树；按序根据各第一交易的交易信息生成零知识证明证据，根据按序的各第一交易、零知识证明证据生成第一证明数据；将第一证明数据发送给第一主链和其它各主链。本申请在节省成本的基础上防止双花。



CN 114138903 B

1.一种多主链跨链方法,其特征在于,二层网络上有分别对应于各主链的状态树,各所述状态树的初始根哈希相同,各主链配置有跨链验证合约,所述跨链验证合约中部署有验证交易信息的零知识证明电路,所述方法适用于二层网络的节点,所述方法包括:

在监测到第一主链生成了第一主链区块时,按序同步所述第一主链区块中的各需要调用转账类合约的第一交易;其中,所述转账类合约包括存款合约、取款合约、转账合约、跨链转账合约;

对各所述第一交易执行如下操作:

判断所述第一交易调用的转账类合约是否为跨链转账合约:

否,则执行所述第一交易以更新二层网络上所述第一主链的第一状态树;

是,则执行所述第一交易以更新二层网络上所述第一主链的第一状态树,和,所述第一交易指定的待跨链的第二主链的第二状态树;

按序根据各所述第一交易的交易信息生成零知识证明证据,根据按序的各所述第一交易、所述零知识证明证据生成第一证明数据;

将所述第一证明数据发送给所述第一主链和其它各主链,以供所述第一主链的主链节点:

通过所述跨链验证合约判断所述第一证明数据中的各所述第一交易与所述第一主链区块中的各所述第一交易的顺序是否相同:

相同,则将所述零知识证明证据输入所述零知识证明电路以验证所述第一证明数据中的各所述第一交易的交易信息是否正确:

验证正确,则结束;

所述第一证明数据还用于供其它各主链的主链节点:

将所述零知识证明证据输入所述零知识证明电路以验证所述第一证明数据中的各所述第一交易的交易信息是否正确:

验证正确,则执行各所述第一交易。

2.根据权利要求1所述的方法,其特征在于,还包括:

在监测到顺序不同,或,验证失败时,回滚所述第一状态树,或,回滚所述第一状态树和所述第二状态树至未执行各所述第一交易时的状态;

返回所述按序同步所述第一主链区块中的各需要调用转账类合约的第一交易以重新生成所述零知识证明证据和所述第一证明数据;

其中,其它各主链的主链节点在收到重新生成的所述第一证明数据后,验证所述第一证明数据中的各所述第一交易的交易信息是否正确前,还包括:

回滚所在主链至未执行各所述第一交易时的状态。

3.根据权利要求1所述的方法,其特征在于,其它各主链的主链节点在执行所述将所述零知识证明证据输入所述零知识证明电路以验证所述第一证明数据中的各所述第一交易的交易信息是否正确前,还包括:

接收由所述第一主链的主链节点,或,由中继服务器发送的各所述第一交易;

所述其它各主链的主链节点执行的所述将所述零知识证明证据输入所述零知识证明电路以验证所述第一证明数据中的各所述第一交易的交易信息是否正确包括:

通过所述跨链验证合约判断所述第一证明数据中的各所述第一交易与所述第一主链

节点或中继服务器发送的各所述第一交易的顺序是否相同：

相同，则将所述零知识证明证据输入所述零知识证明电路以验证所述第一证明数据中的各所述第一交易的交易信息是否正确。

4.根据权利要求1所述的方法，其特征在于，二层网络的节点在各主链上缴纳有若干押金，所述第一主链的主链节点在监测到顺序不同，或，验证失败时，扣除第一数量的押金；其它各主链的主链节点在验证失败时，扣除第一数量的押金。

5.一种计算机设备，其特征在于，所述设备包括：

一个或多个处理器；

存储器，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器执行如权利要求1-4中任一项所述的方法。

6.一种存储有计算机程序的存储介质，其特征在于，该程序被处理器执行时实现如权利要求1-4中任一项所述的方法。

多主链跨链方法、计算机设备和存储介质

技术领域

[0001] 本申请涉及区块链技术领域，具体涉及一种多主链跨链方法、计算机设备和存储介质。

背景技术

[0002] 当前基于二层网络的跨链方案一般是一对一的，一个二层网络对应一个主链。申请人希望提出一种一个二层网络对应多个主链的跨链方案，上述方案相较于现有技术，更加节省了成本，但也存在双花的问题。

发明内容

[0003] 鉴于现有技术中的上述缺陷或不足，期望提供一种在节省成本的基础上防止双花的多主链跨链方法、计算机设备和存储介质。

[0004] 第一方面，本发明提供一种适用于二层网络的节点的多主链跨链方法，二层网络上有分别对应于各主链的状态树，各状态树的初始根哈希相同，各主链配置有跨链验证合约，跨链验证合约中部署有验证交易信息的零知识证明电路，上述方法包括：

[0005] 在监测到第一主链生成了第一主链区块时，按序同步第一主链区块中的各需要调用转账类合约的第一交易；其中，转账类合约包括存款合约、取款合约、转账合约、跨链转账合约；

[0006] 对各第一交易执行如下操作：

[0007] 判断第一交易调用的转账类合约是否为跨链转账合约：

[0008] 否，则执行第一交易以更新二层网络上第一主链的第一状态树；

[0009] 是，则执行第一交易以更新二层网络上第一主链的第一状态树，和，第一交易指定的待跨链的第二主链的第二状态树；

[0010] 按序根据各第一交易的交易信息生成零知识证明证据，根据按序的各第一交易、零知识证明证据生成第一证明数据；

[0011] 将第一证明数据发送给第一主链和其它各主链，以供第一主链的主链节点：

[0012] 通过跨链验证合约判断第一证明数据中的各第一交易与第一主链区块中的各第一交易的顺序是否相同：

[0013] 相同，则将零知识证明证据输入零知识证明电路以验证第一证明数据中的各第一交易的交易信息是否正确：

[0014] 验证正确，则结束；

[0015] 第一证明数据还用于供其它各主链的主链节点：

[0016] 将零知识证明证据输入零知识证明电路以验证第一证明数据中的各第一交易的交易信息是否正确：

[0017] 验证正确，则执行各第一交易。

[0018] 第二方面，本发明还提供一种设备，包括一个或多个处理器和存储器，其中存储器

包含可由该一个或多个处理器执行的指令以使得该一个或多个处理器执行根据本发明各实施例提供的多主链跨链方法。

[0019] 第三方面,本发明还提供一种存储有计算机程序的存储介质,该计算机程序使计算机执行根据本发明各实施例提供的多主链跨链方法。

[0020] 本发明诸多实施例提供的多主链跨链方法、计算机设备和存储介质通过在监测到第一主链生成了第一主链区块时,按序同步第一主链区块中的各需要调用转账类合约的第一交易;对各第一交易执行如下操作:判断第一交易调用的转账类合约是否为跨链转账合约:否,则执行第一交易以更新二层网络上第一主链的第一状态树;是,则执行第一交易以更新二层网络上第一主链的第一状态树,和,第一交易指定的待跨链的第二主链的第二状态树;按序根据各第一交易的交易信息生成零知识证明证据,根据按序的各第一交易、零知识证明证据生成第一证明数据;将第一证明数据发送给第一主链和其它各主链的方法,在节省成本的基础上防止双花。

附图说明

[0021] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述,本申请的其它特征、目的和优点将会变得更明显:

[0022] 图1为本发明一实施例提供的一种多主链跨链方法的流程图。

[0023] 图2为本发明一实施例提供的一种设备的结构示意图。

具体实施方式

[0024] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是,此处所描述的具体实施例仅仅用于解释相关发明,而非对该发明的限定。另外还需要说明的是,为了便于描述,附图中仅示出了与发明相关的部分。

[0025] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0026] 申请人希望提出一种一个二层网络对应多个主链的跨链方案,上述方案相较于现有技术,更加节省了成本,但也存在双花的问题——如果运营方作弊存款后和另一条链的资产交换,另一条链将无法验证。举例,假设有3条主链(A链、B链、C链);A链上运行有资产AAA,B链上运行有资产BBB,C链上运行有资产CCC,AAA与BBB与CCC的兑换比例为1:1:1;假设运营方私自在二层网络中存款100AAA,并立即和二层网络中某一用户的BBB做了交换,这100AAA是凭空多出来的,最终会在A链上验证失败,但是运营者已经兑换了100BBB并提交到了B链,对B链造成危害。

[0027] 上述问题可以通过本申请的各实施例解决。

[0028] 图1为本发明一实施例提供的一种多主链跨链方法的流程图。如图1所示,在本实施例中,本发明提供一种适用于二层网络的节点的多主链跨链方法,二层网络上有分别对应于各主链的状态树,各状态树的初始根哈希相同,各主链配置有跨链验证合约,跨链验证合约中部署有验证交易信息的零知识证明电路,上述方法包括:

[0029] S11:在监测到第一主链生成了第一主链区块时,按序同步第一主链区块中的各需要调用转账类合约的第一交易;其中,转账类合约包括存款合约、取款合约、转账合约、跨链

转账合约;

[0030] 对各第一交易执行如下操作:

[0031] S131:判断第一交易调用的转账类合约是否为跨链转账合约:

[0032] 否,则执行步骤S132:执行第一交易以更新二层网络上第一主链的第一状态树;

[0033] 是,则执行步骤S133:执行第一交易以更新二层网络上第一主链的第一状态树,和,第一交易指定的待跨链的第二主链的第二状态树;

[0034] S15:按序根据各第一交易的交易信息生成零知识证明证据,根据按序的各第一交易、零知识证明证据生成第一证明数据;

[0035] S17:将第一证明数据发送给第一主链和其它各主链,以供第一主链的主链节点:

[0036] 通过跨链验证合约判断第一证明数据中的各第一交易与第一主链区块中的各第一交易的顺序是否相同:

[0037] 相同,则将零知识证明证据输入零知识证明电路以验证第一证明数据中的各第一交易的交易信息是否正确:

[0038] 验证正确,则结束;

[0039] 第一证明数据还用于供其它各主链的主链节点:

[0040] 将零知识证明证据输入零知识证明电路以验证第一证明数据中的各第一交易的交易信息是否正确:

[0041] 验证正确,则执行各第一交易。

[0042] 具体的,假设有3条主链(A链、B链、C链);A链上运行有资产AAA,B链上运行有资产BBB,C链上运行有资产CCC,AAA与BBB与CCC的兑换比例为1:1:1;二层网络上有A链的状态尔树TreeA、B链的状态树TreeB,C链的状态树TreeC,TreeA、TreeB、TreeC的初始根哈希相同;上述第一主链为A链,A链的主链节点按序根据tx1～tx10生成了主链区块block(100),其中,tx1、tx2为需要调用转账类合约的交易,tx1为用户甲请求存款100个AAA,tx2为用户B请求取款10个AAA;

[0043] 二层网络的节点执行步骤S11,在监测到A链生成了block(100)时,同步tx1、tx2;

[0044] 以tx1为例:

[0045] 二层网络的节点执行步骤S131,判断tx1调用的转账类合约是否为跨链转账合约:

[0046] 由于tx1调用的转账类合约是存款合约,则执行步骤S132:执行tx1(即将用户甲的状态数据+100)以更新二层网络上的TreeA;

[0047] tx2同理,此处不再赘述;

[0048] 二层网络的节点执行步骤S15,根据tx1、tx2的交易信息生成零知识证明证据proof1,并根据tx1、tx2、零知识证明证据生成证明数据proofchunk1;本领域技术人员应当理解,交易信息可以根据实际需求进行配置,一般包括交易发送方地址、交易接收方地址、交易类型、金额;

[0049] 二层网络的节点执行步骤S17,将证明数据proofchunk1发送给A链、B链和C链;

[0050] A链的主链节点通过跨链验证合约验证tx1、tx2是否与block(100)中的tx1、tx2的顺序相同;

[0051] 由于相同,则将零知识证明证据proof1输入零知识证明电路以验证证明数据中的tx1、tx2的交易信息是否正确;

[0052] 假设验证正确,则结束。

[0053] B链和C链的主链节点由于没有block(100)各交易的顺序,则B链和C链的主链节点将零知识证明证据proof1输入零知识证明电路以验证证明数据中的tx1、tx2的交易信息是否正确:

[0054] 假设验证正确,则执行tx1、tx2。

[0055] 上述实施例使得多条主链都在二层网络上维护一个共同账本,节省成本;以及,只有在交易顺序和交易信息均正确的基础上二层网络才能继续正常运行,防止双花。

[0056] 优选的,上述方法还包括:

[0057] 在监测到顺序不同,或,验证失败时,回滚第一状态树,或,回滚第一状态树和第二状态树至未执行各第一交易时的状态;

[0058] 返回按序同步第一主链区块中的各需要调用转账类合约的第一交易以重新生成零知识证明证据和第一证明数据;

[0059] 其中,其它各主链的主链节点在收到重新生成的第一证明数据后,验证第一证明数据中的各第一交易的交易信息是否正确前,还包括:

[0060] 回滚所在主链至未执行各第一交易时的状态。

[0061] 具体的,以block(100)为例,二层网络的节点在监测到顺序不同,或,验证失败时,回滚二层网络上的TreeA和TreeB至未执行tx1、tx2时的状态;

[0062] 二层网络的节点返回步骤“按序同步第一主链区块中的各需要调用转账类合约的第一交易”;最终,二层网络的节点将重新生成proof1和proofchunk1;

[0063] B链、C链的主链节点在收到重新生成的proofchunk2后,验证proofchunk1中的tx1、tx2的交易信息是否正确前,还需要将各自的主链回滚至未执行tx1、tx2时的状态。

[0064] 本领域技术人员应当理解,以B链为例,如果B链的主链节点在在收到重新生成的第一证明数据后,如果存在tx3(tx3的执行需用到tx1的执行结果),则B链的主链节点还应当回滚tx3。

[0065] 优选的,其它各主链节点在执行将零知识证明证据输入零知识证明电路以验证第一证明数据中的各第一交易的交易信息是否正确前,还包括:

[0066] 接收由第一主链的主链节点,或,由中继服务器发送的各第一交易;

[0067] 其它各主链的主链节点执行的将零知识证明证据输入零知识证明电路以验证第一证明数据中的各第一交易的交易信息是否正确包括:

[0068] 通过跨链验证合约判断第一证明数据中的各第一交易与第一主链节点或中继服务器发送的各第一交易的顺序是否相同:

[0069] 相同,则将零知识证明证据输入零知识证明电路以验证第一证明数据中的各第一交易的交易信息是否正确。

[0070] 具体的,B链、C链的主链节点在执行“将零知识证明证据输入零知识证明电路以验证第一证明数据中的各第一交易的交易信息是否正确”前,还包括:

[0071] 接收由A链的主链节点,或,由中继服务器发送的tx1、tx2;

[0072] 此时,B链、C链的主链节点有了交易顺序,则B链、C链的主链节点与A链的主链节点相同,也可以通过跨链验证合约判断proofchunk1中的tx1、tx2与A链的主链节点或中继服务器发送的tx1、tx2的顺序是否相同。

[0073] 优选的,二层网络的节点在各主链上缴纳有若干押金,第一主链的主链节点在监测到顺序不同,或,验证失败时,扣除第一数量的押金;其它各主链的主链节点在验证失败时,扣除第一数量的押金。

[0074] 假设A链～C链的主链节点均验证失败,则A链～C链的主链节点扣除二层网络的节点的第一数量的押金。

[0075] 上述实施例对二层网络的节点进行惩罚,进一步阻止双花。

[0076] 图2为本发明一实施例提供的一种设备的结构示意图。

[0077] 如图2所示,作为另一方面,本申请还提供了一种设备200,包括一个或多个中央处理单元(CPU)201,其可以根据存储在只读存储器(ROM)202中的程序或者从存储部分208加载到随机访问存储器(RAM)203中的程序而执行各种适当的动作和处理。在RAM203中,还存储有设备200操作所需的各种程序和数据。CPU201、ROM202以及RAM203通过总线204彼此相连。输入/输出(I/O)接口205也连接至总线204。

[0078] 以下部件连接至I/O接口205:包括键盘、鼠标等的输入部分206;包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分207;包括硬盘等的存储部分208;以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分209。通信部分209经由诸如因特网的网络执行通信处理。驱动器210也根据需要连接至I/O接口205。可拆卸介质211,诸如磁盘、光盘、磁光盘、半导体存储器等等,根据需要安装在驱动器210上,以便于从其上读出的计算机程序根据需要被安装入存储部分208。

[0079] 特别地,根据本公开的实施例,上述任一实施例描述的方法可以被实现为计算机软件程序。例如,本公开的实施例包括一种计算机程序产品,其包括有形地包含在机器可读介质上的计算机程序,所述计算机程序包含用于执行上述任一方法的程序代码。在这样的实施例中,该计算机程序可以通过通信部分209从网络上被下载和安装,和/或从可拆卸介质211被安装。

[0080] 作为又一方面,本申请还提供了一种计算机可读存储介质,该计算机可读存储介质可以是上述实施例的装置中所包含的计算机可读存储介质;也可以是单独存在,未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序,该程序被一个或者一个以上的处理器用来执行描述于本申请提供的方法。

[0081] 附图中的流程图和框图,图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分,该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个接连地表示的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这根据所涉及的功能而定。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以通过执行规定的功能或操作的专用的基于硬件的系统来实现,或者可以通过专用硬件与计算机指令的组合来实现。

[0082] 描述于本申请实施例中所涉及到的单元或模块可以通过软件的方式实现,也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中,例如,各所述单元可以是设置在计算机或移动智能设备中的软件程序,也可以是单独配置的硬件装置。其中,这

些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0083] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解,本申请中所涉及的发明范围,并不限于上述技术特征的特定组合而成的技术方案,同时也应涵盖在不脱离本申请构思的情况下,由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

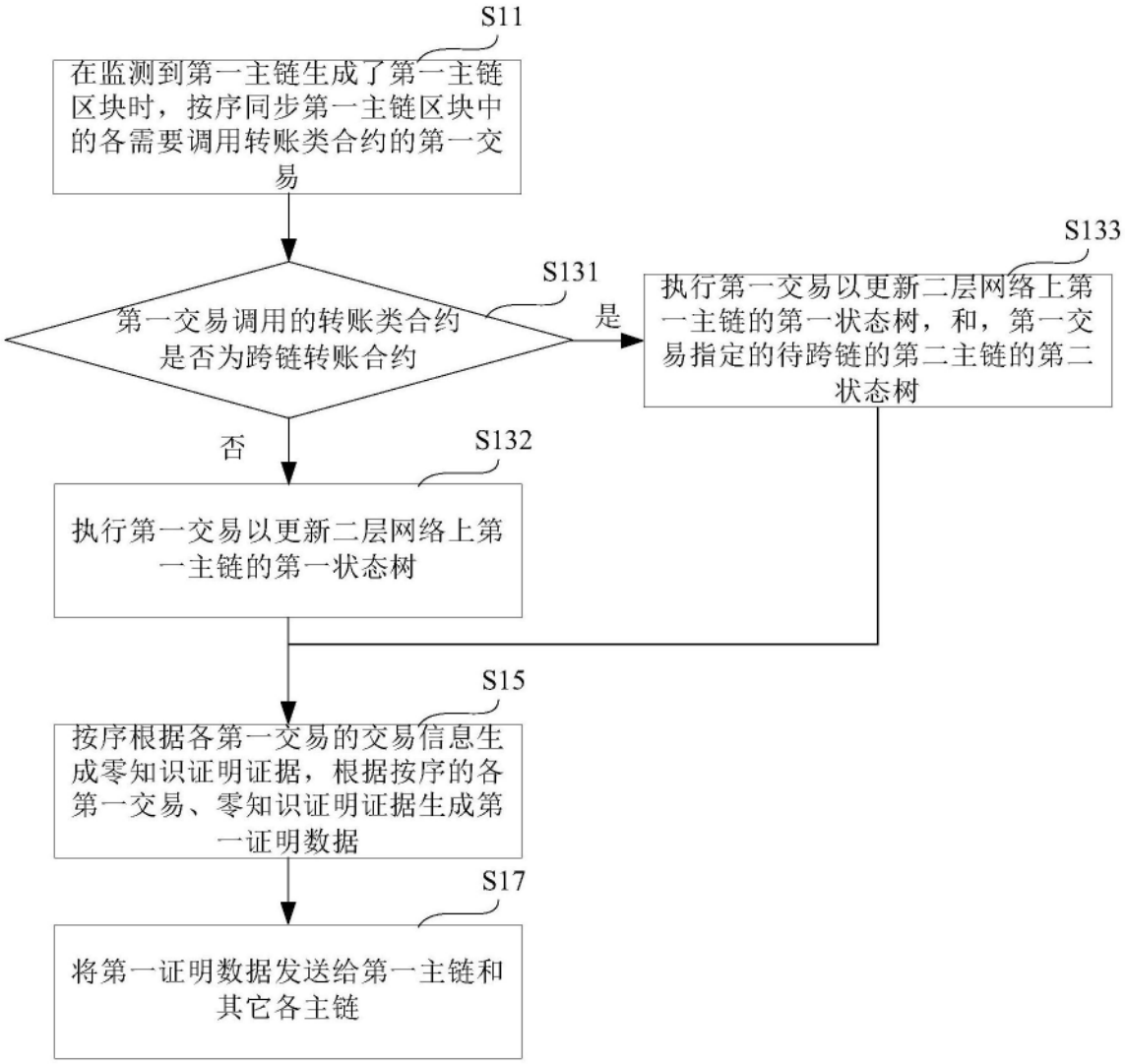

S11
在监测到第一主链生成了第一主链区块时，按序同步第一主链区块中的各需要调用转账类合约的第一交易
S131
第一交易调用的转账类合约是否为跨链转账合约
是
S133
执行第一交易以更新二层网络上第一主链的第一状态树，和，第一交易指定的待跨链的第二主链的第二状态树
否
S132
执行第一交易以更新二层网络上第一主链的第一状态树
S15
按序根据各第一交易的交易信息生成零知识证明证据，根据按序的各第一交易、零知识证明证据生成第一证明数据
S17
将第一证明数据发送给第一主链和其它各主链

图1

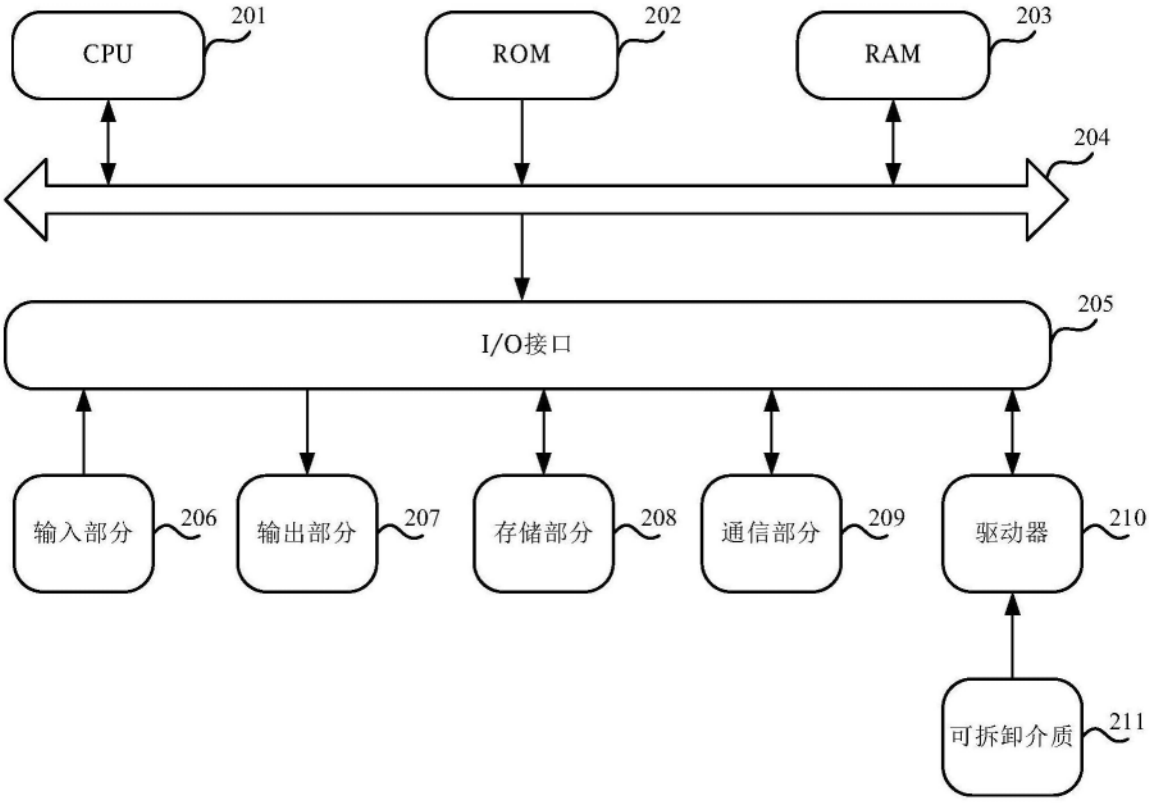

CPU
201
ROM
202
RAM
203
204
I/O接口
205
输入部分
206
输出部分
207
存储部分
208
通信部分
209
驱动器
210
可拆卸介质
211

图2