(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107220820 B
(45)授权公告日 2019.10.01

(21)申请号 201710344407.X

(22)申请日 2017.05.16

(65)同一申请的已公布的文献号
申请公布号 CN 107220820 A

(43)申请公布日 2017.09.29

(73)专利权人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 郭锐 李茂材 王宗友 梁军 张建俊 赵琦 朱大卫 屠海涛 刘斌华

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 朱雅男

(51)Int.Cl.
G06Q 20/10(2012.01)
G06Q 20/38(2012.01)
G06Q 20/42(2012.01)

(56)对比文件
CN 105809062 A,2016.07.27,
CN 106656839 A,2017.05.10,
CN 106407430 A,2017.02.15,

审查员 唐田田

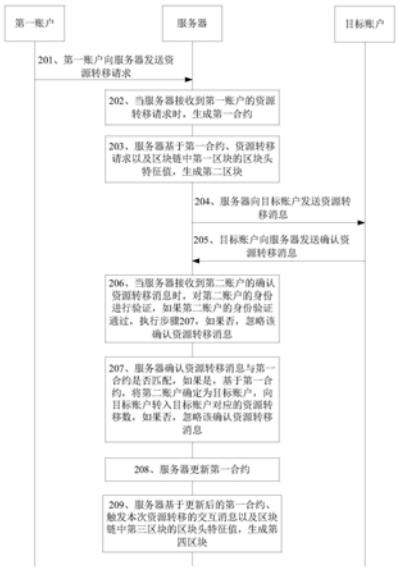
权利要求书2页 说明书11页 附图4页

(54)发明名称

资源转移方法、装置及存储介质

(57)摘要

本发明公开了一种资源转移方法、装置及存储介质，属于网络技术领域。该方法包括：接收第一账户的资源转移请求，所述资源转移请求用于请求将所述第一账户的资源转移至目标账户；生成第一合约，所述第一合约用于指示所述第一账户的资源转移条件；基于所述第一合约、所述资源转移请求以及区块链中第一区块的区块头特征值，生成第二区块，所述第一区块为所述区块链上所述第二区块的上一个区块，所述第二区块用于记录本次资源转移请求事件；当符合所述第一合约指示的资源转移条件时，基于所述第一合约进行资源转移。本发明提高了资源转移的可靠性和安全性。



CN 107220820 B

1.一种资源转移方法,其特征在于,所述方法包括:

接收第一账户的资源转移请求,所述资源转移请求用于请求将所述第一账户的资源转移至目标账户;

生成第一合约,所述第一合约用于指示所述第一账户的资源转移条件;

基于所述第一合约的特征值、所述资源转移请求以及区块链中第一区块的区块头特征值,生成第二区块,所述第一区块为所述区块链上所述第二区块的上一个区块,所述第二区块用于记录本次资源转移请求事件;

当符合所述第一合约指示的资源转移条件时,基于所述第一合约进行资源转移。

2.根据权利要求1所述的方法,其特征在于,所述当符合所述第一合约指示的资源转移条件时,基于所述第一合约进行资源转移,包括:

接收第二账户的确认资源转移消息;

如果所述第二账户的身份验证通过,且所述确认资源转移消息与所述第一合约匹配,将所述第二账户确定为所述目标账户,基于所述第一合约向所述目标账户转入所述目标账户对应的资源转移数。

3.根据权利要求2所述的方法,其特征在于,所述如果所述第二账户的身份验证通过,且所述确认资源转移消息与所述第一合约匹配,将第二账户确定为所述目标账户,基于所述第一合约向所述目标账户转入所述目标账户对应的资源转移数,包括:

如果所述确认资源转移消息中的合约公钥对所述确认资源转移消息中的合约私钥签名验证通过,且所述确认资源转移消息中的账户公钥对所述确认资源转移消息中的账户私钥签名验证通过,获取所述确认资源转移消息中的合约公钥对应的合约标识;

如果所述确认资源转移消息中的合约公钥对应的合约标识与所述第一合约的合约标识相同,且所述第二账户与所述目标账户相同,且所述确认资源转移消息中的资源转移数匹配所述第一合约的资源转移数,且所述确认资源转移消息的接收时间不晚于所述第一合约的到期时间,基于所述第一合约,将所述第二账户确定为所述目标账户,向所述目标账户转入所述目标账户对应的资源转移数。

4.根据权利要求1所述的方法,其特征在于,所述当符合所述第一合约指示的资源转移条件时,基于所述第一合约进行资源转移,包括:

接收第二账户的拒绝资源转移消息;

如果所述第二账户的身份验证通过,且所述拒绝资源转移消息与所述第一合约匹配,基于所述第一合约,将所述第二账户确定为所述目标账户,向所述第一账户退回所述目标账户对应的资源转移数。

5.根据权利要求1所述的方法,其特征在于,所述当符合所述第一合约指示的资源转移条件时,基于所述第一合约进行资源转移,包括:

当检测到所述第一合约达到所述第一合约的到期时间时,基于所述第一合约,向所述第一账户退回所述第一合约中的资源转移数。

6.根据权利要求1所述的方法,其特征在于,所述当符合所述第一合约指示的资源转移条件时,基于所述第一合约进行资源转移之后,所述方法还包括:

更新所述第一合约,更新后的第一合约用于指示所述第一账户的剩余资源转移条件;

基于更新后的第一合约、触发本次资源转移的交互消息以及所述区块链中第三区块的

区块头特征值，生成第四区块，所述第三区块为所述区块链上所述第四区块的上一个区块，所述第四区块用于记录本次资源转移完成事件。

7.根据权利要求1所述的方法，其特征在于，所述方法还包括：

将合约私钥发送至所述目标账户，使得所述目标账户基于所述合约私钥得到合约私钥签名和合约公钥，所述合约私钥由所述第一账户发送得到。

8.一种资源转移装置，其特征在于，所述装置包括：

接收模块，用于接收第一账户的资源转移请求，所述资源转移请求用于请求将所述第一账户的资源转移至目标账户；

合成生成模块，用于生成第一合约，所述第一合约用于指示所述第一账户的资源转移条件；

区块生成模块，用于基于所述第一合约的特征值、所述资源转移请求以及区块链中第一区块的区块头特征值，生成第二区块，所述第一区块为所述区块链上所述第二区块的上一个区块，所述第二区块用于记录本次资源转移请求事件；

资源转移模块，用于当符合所述第一合约指示的资源转移条件时，基于所述第一合约进行资源转移。

9.根据权利要求8所述的装置，其特征在于，所述资源转移模块用于：

接收第二账户的确认资源转移消息；

如果所述第二账户的身份验证通过，且所述确认资源转移消息与所述第一合约匹配，将所述第二账户确定为所述目标账户，基于所述第一合约向所述目标账户转入所述目标账户对应的资源转移数。

10.根据权利要求8所述的装置，其特征在于，所述资源转移模块用于：

接收第二账户的拒绝资源转移消息；

如果所述第二账户的身份验证通过，且所述拒绝资源转移消息与所述第一合约匹配，基于所述第一合约，将所述第二账户确定为所述目标账户，向所述第一账户退回所述目标账户对应的资源转移数。

11.根据权利要求8所述的装置，其特征在于，所述资源转移模块用于：

当检测到所述第一合约达到所述第一合约的到期时间时，基于所述第一合约，向所述第一账户退回所述第一合约中的资源转移数。

12.根据权利要求8所述的装置，其特征在于，所述装置还包括：

合约更新模块，用于更新所述第一合约，更新后的第一合约用于指示所述第一账户的剩余资源转移条件；

所述区块生成模块，还用于基于更新后的第一合约、触发本次资源转移的交互消息以及所述区块链中第三区块的区块头特征值，生成第四区块，所述第三区块为所述区块链上所述第四区块的上一个区块，所述第四区块用于记录本次资源转移完成事件。

13.一种计算机可读存储介质，其特征在于，所述存储介质中存储有至少一条指令，所述指令由处理器加载并执行以实现如权利要求1至权利要求7中任一项所述的方法。

14.一种服务器，其特征在于，所述服务器包括处理器和存储器，所述存储器中存储有至少一条指令，所述指令由所述处理器加载并执行以实现如权利要求1至权利要求7中任一项所述的方法。

资源转移方法、装置及存储介质

技术领域

[0001] 本发明涉及网络技术领域，特别涉及一种资源转移方法、装置及存储介质。

背景技术

[0002] 随着网络技术的发展，账户之间可以方便的基于网络进行交互，例如，基于网络进行聊天、互动游戏、资源转移例如延时转账等，延时转账是指转账款在接收方确认后才进行的转账。

[0003] 以资源转移中的延时转账过程为例，在进行延时转账时，假设账户A向账户B发送了一个红包，红包金额为X元，则服务器可以将账户A的X元转账至一个中间账户M，如果账户B确认接收该红包，则服务器可以将中间账户M中的X元转账至账户B，完成账户A到账户B的延时转账过程。

[0004] 在实现本发明的过程中，发明人发现现有技术至少存在以下问题：

[0005] 由于服务器存在被恶意账户侵入的安全隐患，收款账户、转账金额等转账信息很可能被恶意篡改，导致资源转移过程的安全性和可靠性差。

发明内容

[0006] 为了解决现有技术的问题，本发明实施例提供了一种资源转移方法、装置及存储介质和服务器。所述技术方案如下：

[0007] 第一方面，提供了一种资源转移方法，所述方法包括：

[0008] 接收第一账户的资源转移请求，所述资源转移请求用于请求将所述第一账户的资源转移至目标账户；

[0009] 生成第一合约，所述第一合约用于指示所述第一账户的资源转移条件；

[0010] 基于所述第一合约、所述资源转移请求以及区块链中第一区块的区块头特征值，生成第二区块，所述第一区块为所述区块链上所述第二区块的上一个区块，所述第二区块用于记录本次资源转移请求事件；

[0011] 当符合所述第一合约指示的资源转移条件时，基于所述第一合约进行资源转移。

[0012] 第二方面，提供了一种资源转移装置，所述装置包括：

[0013] 接收模块，用于接收第一账户的资源转移请求，所述资源转移请求用于请求将所述第一账户的资源转移至目标账户；

[0014] 合成生成模块，用于生成第一合约，所述第一合约用于指示所述第一账户的资源转移条件；

[0015] 区块生成模块，用于基于所述第一合约、所述资源转移请求以及区块链中第一区块的区块头特征值，生成第二区块，所述第一区块为所述区块链上所述第二区块的上一个区块，所述第二区块用于记录本次资源转移请求事件；

[0016] 资源转移模块，用于当符合所述第一合约指示的资源转移条件时，基于所述第一合约进行资源转移。

[0017] 第三方面，提供了一种计算机可读存储介质，所述存储介质中存储有至少一条指令，所述指令由处理器加载并执行以实现上述第一方面中任一项所述的方法。

[0018] 第四方面，提供了一种服务器，所述服务器包括处理器和存储器，所述存储器中存储有至少一条指令，所述指令由所述处理器加载并执行以实现上述第一方面中任一项所述的方法。

[0019] 本发明实施例通过在接收到第一账户的资源转移请求时，生成第一合约，并基于第一合约、资源转移请求和区块链中第一区块的区块头特征值，生成第二区块，并当符合第一合约指示的资源转移条件时，基于第一合约进行资源转移，能够基于区块链中前后区块之间的关联关系，使得区块中任一资源转移过程中的信息被篡改时都能通过下一区块检测到，避免了恶意账户篡改或抵赖被转移的资源，保证了资源转移过程的安全性和可靠性，而且，由于合约的信息也记录在区块链中，使得合约被篡改时也能通过区块链中已记录的合约的信息被检测到，进一步保证了合约的安全性和正确性，提高了资源转移的安全性和可靠性。

附图说明

[0020] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0021] 图1是本发明实施例提供的一种资源转移的实施环境示意图；

[0022] 图2是本发明实施例提供的一种资源转移方法的流程图；

[0023] 图3是本发明实施例提供的一种合约标识生成流程图；

[0024] 图4是本发明实施例提供的一种资源转移装置的框图；

[0025] 图5A是本发明实施例提供的一种资源转移装置的框图；

[0026] 图5B是本发明实施例提供的一种资源转移装置的框图；

[0027] 图6是本发明实施例提供的一种服务器结构示意图。

具体实施方式

[0028] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0029] 图1是本发明实施例提供的一种资源管理的实施环境示意图。参见图1，该实施环境中包括：资源管理系统101和终端102。该资源管理系统101可以包括多个节点，每个节点可以对应一个服务器，该多个节点可存储相同的一条区块链，该区块链由多个区块组成，每个区块均存储有不同的信息，一条区块链上的区块按照时间顺序进行存储。在本发明实施例中，每个区块可以存储资源转移过程中的一个交互消息和基于该交互消息生成的合约的特征值。该终端102是指该资源管理系统所服务的用户所在终端，用于与资源管理系统进行交互，从而从该用户的账户向其他账户转移资源，或者基于资源管理系统的管理在账户中储存资源等。该资源管理系统101用于管理用户的账户中的资源，并在资源转移过程中生成合约，将交互信息和合约的信息存储至区块链上的区块。用户的账户是指与登录该终端102

的用户所关联的账户，如，用户的网银、微信零钱或游戏账户等，该账户中可以存储有用户的资源，这些资源为进行网络交易时可使用的资源，例如，用户的网银中所包含货币资源、微信零钱中所存储的货币资源、游戏账户中的虚拟货币或卡包中的数字票据等。

[0030] 本发明实施例中，每个节点已配置了相同的合约模板，该合约模板是指待确定参数的代码，资源管理系统101可以根据接收到的与账户间的交互消息和合约模板，生成一个实体化的合约，也即是生成一段可以运行在区块链上的代码，从而根据合约进行资源转移过程。为了方便管理每个账户的资源，资源管理系统101也可以为每个账户维护一个合约列表。当然，为了保证合约的安全性，资源管理系统101可以仅在合约列表中生成新的合约或在已生成的合约中添加更新信息，而禁止已生成的合约中的信息被修改。

[0031] 需要说明的是，当资源管理系统101中的任一节点确定当前区块中需要存入的输入信息或生成合约时，该资源管理系统101中的其他节点便可以根据共识算法获取该输入信息或合约，并在当前区块中也存入该输入信息，且在合约列表中存入该合约，使得资源管理系统101中全部节点上存储的信息保持一致。

[0032] 图2是本发明实施例提供的一种资源转移方法的流程图，参见图2，该方法可以应用于图1所示的资源管理系统中的服务器与终端上的账户的交互过程，包括以下步骤：

[0033] 201、第一账户向服务器发送资源转移请求，资源转移请求用于请求将第一账户的资源转移至目标账户。

[0034] 其中，第一账户是指该服务器所服务的任一用户的账户，可唯一标识该用户。该步骤中，该用户可以在终端上选择目标账户和资源转移数，使得终端生成该资源转移请求，并将该资源转移请求发送至服务器。需要说明的是，本发明实施例对目标账户的数量和资源转移数不做具体限定。

[0035] 以该资源为网银为例，当检测到对转账选项的触发操作时，终端可以显示转账界面，该转账界面中可以包括账户通信列表和转账金额输入框，进而，终端可以获取用户在转账金额输入框中输入的转账金额作为资源转移数，并获取用户在账户通信列表中选择的一个或多个目标账户。当然，用户还可以为每个目标账户分别设置转账金额。

[0036] 本发明实施例中，该资源转移请求还携带合约标识。合约标识用于唯一标识第一账户发起的一次资源转移过程，使得服务器能够依据该合约标识将该资源转移过程中的涉及的事件记录在区块链上，避免了恶意账户篡改或抵赖被已转移的资源，提高资源转移过程中已转移资源的不可否认性和资源转移的可靠性。

[0037] 在不同的应用场景下，该合约标识可以采用的不同的方式得到。例如，为了保证公共区块链的场景下资源转移过程的安全性，参见图3，本发明实施例提供了一种合约标识生成流程图，该生成流程中，终端可以根据第一账户私钥，通过椭圆曲线算法(选择的曲线可以为secp256k1)计算出第一账户公钥，并对第一账户公钥进行哈希计算，采用的哈希算法可以为SHA256(Secure Hash Algorithm 256，256位哈希算法)和RIPEMD160(RACE Integrity Primitives Evaluation Message Digest，160位原始完整性校验消息摘要算法)的结合，进而，终端可以将得到的哈希值进行编码，得到该合约标识，编码方式可以BASE58(58位基础编码)。其中，第一账户私钥可以为随机生成的一串字符，其位数可以为256比特。又例如，在私有区块链的场景下，由于私有区块链具备严格的访问控制，且参与资源转移过程的账户均为一个组织的内部账户，因此资源转移过程中无需考虑交互方之外的

恶意账户的介入，也就无需考虑合约标识被伪造的安全隐患，则该合约标识可以为任一字符，如，终端通过数字自增长的方式得到一个数字，作为该合约标识。

[0038] 202、当服务器接收到第一账户的资源转移请求时，生成第一合约，第一合约用于指示第一账户的资源转移条件。

[0039] 其中，第一合约是指可以运行在区块链上的代码。该步骤中，当服务器接收到该资源转移请求时，可以基于已配置的合约模板以及该资源转移请求中的各项信息，将该各项信息作为合约模板中的各项参数，生成该第一合约。

[0040] 具体地，为了方便服务器管理各个账户的合约，服务器为每个账户维护一个合约列表，因此服务器可以根据资源转移请求中的第一账户，在第一账户的合约列表中生成第一合约。该第一合约中可以包括合约标识、资源转移数、目标账户、第一合约的到期时间以及合约生成时间等信息。该第一合约的到期时间可以由服务器根据当前时间以及预设期限的和值得到。需要说明的是，为了保证整个资源转移过程中的资源数平衡，服务器是将第一账户中与资源转移数对应的资源转移至该第一合约。

[0041] 在实际的应用场景中，该资源转移请求中可以包括多个目标账户，如果第一账户为每个目标账户设置了资源转移数，则服务器可以在生成第一合约时将每个目标账户和其对应的资源转移数对应存储。或者，如果第一账户没有设置各个目标账户对应的资源转移数，则服务器可以在生成第一合约时将资源转移请求中的资源转移数随机地分配给目标账户。

[0042] 当然，服务器还可以对第一账户进行验证，如果验证通过，则生成第一合约。本发明实施例对验证方式不做限定。例如，服务器将资源转移数与该第一账户的资源总数进行比较，如果资源转移数小于该资源总数，则生成第一合约，否则，提示该第一账户资源转移失败。

[0043] 203、服务器基于第一合约、资源转移请求以及区块链中第一区块的区块头特征值，生成第二区块，第一区块为区块链上第二区块的上一个区块，第二区块用于记录本次资源转移请求事件。

[0044] 该步骤中，服务器可以从区块链中获取第一区块的区块头中的所有信息，并基于该第一区块的区块头中的所有信息得到第一区块的区块头特征值，并对将要存入第二区块的区块主体中的第一合约的信息和资源转移请求进行特征值计算，得到第二区块的区块主体特征值，进而，将第一区块的区块头特征值、第二区块的区块主体特征值(还可以包括版本号、难度值和时间戳)存储至第二区块的区块头；将第一合约的信息和资源转移请求存储至第二区块的区块主体，生成该第二区块，使得第二区块与第一区块通过第一区块的区块头特征值相关，因而实现了将区块链中的区块串联起来的目的，使得对区块中任何信息(包括合约的信息和资源转移请求)的篡改，均能够通过区块的区块头中所存储的上一个区块的区块头特征值的追溯而检测到，从而保证了资源转移过程的安全性。

[0045] 在实际的应用场景中，考虑到第一合约的信息格式可能与区块链中各存储格式不匹配，服务器可以基于第一合约的特征值、资源转移请求以及第一区块的区块头特征值，生成第二区块。该实现方式中，服务器可以对第一合约的各项信息进行哈希计算，将得到的哈希值作为第一合约的特征值，并将第一合约的特征值和资源转移请求存储至第二区块。通过该实现方式，由于对第一合约中任何信息的篡改，都会使被篡改的第一合约的特征值发

生改变，而存储在区块链上的第一合约的特征值不可更改，因此对第一合约的任何篡改都可以根据区块链上的第一合约的特征值检测到，从而保证了合约的安全性。

[0046] 204、服务器向目标账户发送资源转移消息。

[0047] 该步骤中，服务器可以基于第一合约，生成资源转移消息，并将资源转移消息发送至目标账户所在终端。该资源转移消息可以包括第一账户和资源转移数值等信息。具体地，服务器可以基于合约中每个目标账户对应的资源转移数，生成该目标账户的资源转移消息，并将其发送至该目标账户。

[0048] 本发明实施例中，为了避免合约标识被伪造，提高资源转移过程的安全性，服务器可以将合约私钥发送至目标账户，使得目标账户基于合约私钥得到合约私钥签名和合约公钥，合约私钥由第一账户发送得到。而为了保证合约私钥的安全性，第一账户在发送该的合约私钥时可以采用事先约定的加密算法对该合约私钥进行加密，使得目标账户也可以采用该事先约定的解密算法对该加密后的合约私钥进行解密，得到该合约私钥。需要说明的是，该合约私钥可以由第一账户在发送资源转移请求之外的另一个业务包发送至服务器，由服务器从该业务包中提取出目标账户和合约私钥，并将合约私钥转发至目标账户。当然，如果第一账户不是基于合约私钥生成合约标识，而是通过其他方式生成合约标识，如在私有区块链的场景下可以采用数字自增长的方式生成该合约标识，则第一账户无需发送该合约私钥，而是由服务器直接将合约标识发送至目标账户，使得在目标账户确认或拒绝资源转移时，服务器能够根据目标账户携带的合约标识查找到与目标账户确认或决绝的资源所对应的合约。

[0049] 205、目标账户向服务器发送确认资源转移消息。

[0050] 该步骤中，当目标账户所在终端接收到资源转移消息时，可以根据资源转移消息，生成并显示资源接收界面，该资源接收界面可以包括目标账户对应的资源转移数、第一账户、确认选项和拒绝选项等信息，当检测到目标账户对确认选项的触发操作时，该终端可以生成确认资源转移消息，并将其发送至服务器，当检测到目标账户对拒绝选项的触发操作时，该终端可以生成拒绝资源转移消息，并将其发送至服务器。当然，该目标账户也可以选择忽略该资源转移消息，如，关闭该资源接收界面。

[0051] 需要说明的是，为了证明确认资源转移的账户身份，该终端可以采用目标账户的账户私钥对将要发送的确认信息的摘要信息进行签名，得到账户私钥签名，该确认消息可以包括第一账户、目标账户和目标账户对应的资源转移数，而为了保证目标账户所确认的资源与第一合约的资源对应，终端还可以采用已得到的合约私钥对该确认信息的摘要信息进行签名，得到合约私钥签名，进而，终端可以根据已配置的与第一账户相同的公钥算法得到合约私钥对应的合约公钥，并获取与账户私钥配对的账户公钥，基于该账户公钥、账户私钥签名、合约公钥、合约私钥签名、目标账户对应的资源转移数以及确认信息，生成该确认资源转移消息。生成拒绝资源转移消息的过程同理，将确认信息替换为拒绝信息即可。

[0052] 206、当服务器接收到第二账户的确认资源转移消息时，对第二账户的身份进行验证，如果第二账户的身份验证通过，执行步骤207，如果否，忽略该确认资源转移消息。

[0053] 该步骤中，服务器可以提取确认资源转移消息中的各项信息，并基于提取的信息验证第二账户是否为第一账户所选择的目标账户。具体地，服务器可以基于确认资源转移消息中的合约公钥、合约私钥签名、账户公钥和账户私钥签名进行验证，如果该合约公钥对

该合约私钥签名验证通过，且该账户公钥对该账户私钥签名验证通过，则可以获取确认资源转移消息中的合约公钥对应的合约标识，并执行步骤207，如果任一项验证未通过，则可以忽略该资源转移消息。

[0054] 在验证过程中，服务器可以通过合约公钥对合约私钥签名进行解密，如果解密后的摘要信息与确认资源转移消息中的确认消息的摘要信息相同，可以确认该合约公钥对合约私钥签名验证通过；服务器还可以通过该账户公钥对账户私钥签名进行解密，如果解密后的摘要信息也与确认资源转移消息中的确认消息的摘要信息相同，可以确认该账户公钥对该账户私钥签名验证通过。在获取合约标识时，服务器可以从确认资源转移消息中提取出合约公钥，并根据已配置的与第一账户相同的合约标识算法和编码方式，得到该合约公钥对应的合约标识。

[0055] 通过上述基于密钥的验证过程，既通过账户密钥验证了该确认资源转移消息来自于第二账户，也通过合约密钥验证了该第二账户为第一账户所选择的目标账户，因此在该双重验证的机制下，进一步提高了资源转移过程的安全性和准确性。

[0056] 207、服务器确认资源转移消息与第一合约是否匹配，如果是，基于第一合约，将第二账户确定为目标账户，向目标账户转入目标账户对应的资源转移数，如果否，忽略该确认资源转移消息。

[0057] 该步骤中，服务器可以将确认资源转移消息中的信息与第一合约的信息进行比较，并根据比较结果，确认资源转移消息是否与第一合约匹配。

[0058] 为使确认匹配的条件更为严格，从而提高资源转移过程的正确性和安全性，服务器可以分别判断确认资源转移消息中的合约公钥对应的合约标识与第一合约的合约标识相同、第二账户是否与目标账户相同、确认资源转移消息中的资源转移数是否匹配第一合约的资源转移数、确认资源转移消息的接收时间是否不晚于第一合约的到期时间，如果上述判断结果均为是，则符合第一合约指示的资源转移条件，服务器执行第一合约的代码，将第二账户确定为目标账户，，向目标账户转入目标账户对应的资源转移数，如果上述任一判断结果为否，则服务器可以忽略该确认资源转移消息。需要说明的是，在实际的应用场景中，也可以采用其中的至少一项判断条件作为资源转移的依据，本发明实施例不限定以哪几项判断条件作为依据，也不限定上述判断条件的判断时序。

[0059] 由于该第一账户可能同时向多个目标账户进行资源转移，该步骤也可以具体为：服务器根据确认资源转移消息中的第一账户，在第一账户的合约列表中查找是否存在与根据确认资源转移消息得到的合约标识相同的合约标识，如果是，则提取该合约标识对应的目标账户、每个目标账户对应的资源转移数以及第一合约的到期时间，进而，服务器可以判断该确认资源转移消息的接收时间是否不晚于第一合约的到期时间，如果是，可以判断该第二账户是否与任一目标账户相同，如果是，可以继续判断该确认资源转移消息中的资源转移数是否与第一合约中该目标账户对应的资源转移数相同，如果是，则可以向目标账户转入该目标账户对应的资源转移数。需要说明的是，为了提高合约的安全性，可以限制合约列表的操作权限，例如，该合约列表仅允许被读取和写入，而禁止被修改。

[0060] 本发明实施例通过在接收到第一账户的资源转移请求时，生成第一合约，并基于第一合约、资源转移请求和区块链中第一区块的区块头特征值，生成第二区块，并当符合第一合约指示的资源转移条件时，基于第一合约进行资源转移，能够基于区块链中前后区块

之间的关联关系，使得区块中任一资源转移过程中的信息被篡改时都能通过下一区块检测到，避免了恶意账户篡改或抵赖被转移的资源，保证了资源转移过程的安全性和可靠性，而且，由于合约的信息也记录在区块链中，使得合约被篡改时也能通过区块链中已记录的合约的信息被检测到，进一步保证了合约的安全性和正确性，提高了资源转移的安全性和可靠性。

[0061] 而且，现有技术中的一个中间账户往往同时为多个账户服务，使得该中间账户中可能同时储存了多个账户的转账款，导致中间账户可能错误地将收款用户A的转账款转账至收款用户B，资源转移过程的容错性低。而本发明实施例在每个账户发起资源转移时，均可以为该账户实时生成一个用于本次资源转移过程的合约，不仅能够方便管理各个账户的资源转移过程、简化了账户体系的设计、保证了账户资源数的平衡性，而且提高了资源转移过程的容错性，更加避免了一个中间账户同时为大量账户服务时系统性能受限的问题。

[0062] 而且，本发明实施例还可以灵活地应用在多种资源转移过程中，例如，多个账户抢红包、待接收资源者主动拒绝资源或者引入第三方仲裁共同分配资源的场景。其中，第三方仲裁共同分配资源的场景如：第三方账户从一次资源转移过程中抽取百分比的资源数。

[0063] 需要说明的是，上述步骤206和207的执行时序是示例性的，事实上，服务器也可以先执行步骤207再执行步骤206，或者为了提高资源转移效率，同时执行步骤206和207。还要说明的是，步骤206-207为本发明实施例中当符合第一合约指示的资源转移条件时，服务器基于第一合约进行资源转移的一种可能实现方式，事实上，也存在其他情况能够符合第一合约指示的资源转移条件。本发明实施例以情况1和情况2为例进行说明：

[0064] 情况1、服务器接收第二账户的拒绝资源转移消息；如果第二账户的身份验证通过，且拒绝资源转移消息与第一合约匹配，基于第一合约，将第二账户确定为目标账户，向第一账户退回目标账户对应的资源转移数。

[0065] 该情况下，服务器可以根据拒绝资源转移消息中的合约公钥、合约私钥签名、账户公钥、账户公钥签名以及拒绝消息对第二账户的身份进行验证，如果验证不通过，可以忽略该决绝资源转移消息，如果验证通过，则确认该拒绝资源转移消息中的信息与第一合约的信息是否匹配，如果是，可以将第二账户确定为目标账户，并向第一账户退回该目标账户对应的资源转移数，如果否，则忽略该拒绝资源转移消息。其中，具体验证过程与步骤206中的验证过程同理；具体确认匹配的过程与步骤207中确认匹配的过程同理，将确认资源转移消息替换为拒绝资源转移消息，且确认信息替换为拒绝信息即可实现。

[0066] 情况2、当服务器检测到第一合约达到第一合约的到期时间时，基于第一合约，向第一账户退回第一合约中的资源转移数。

[0067] 该情况下，服务器可以周期性检测各个合约是否达到该合约的到期时间，如果是，则可以向第一账户退回第一合约中的资源转移数，如果否，则本次检测过程可以忽略该合约。

[0068] 基于上述资源转移过程，该第一账户已转移的资源和该第一账户的剩余资源(实际是指第一账户请求转移的资源中的剩余资源)有以下可以有五种情况：

[0069] 一、该第一合约达到第一合约的到期时间，该资源转移数退回至第一账户中，该第一账户的剩余资源数为零。

[0070] 二、目标账户为一个，该第一账户请求转移的资源全部转移至目标账户，则该第一

账户的剩余资源数为零。

[0071] 三、目标账户为一个，该第一账户请求转移的资源被目标账户拒绝，资源转移数退回至第一账户中，该第一账户的剩余资源数为零。

[0072] 四、目标账户为多个，该第一账户请求转移的资源部分转移至目标账户，则该第一账户的剩余资源数大于零且小于资源转移请求中的资源转移数。

[0073] 五、目标账户为多个，该第一账户请求转移的资源被目标账户拒绝，该目标账户对应的资源转移数退回至第一账户中，该第一账户的剩余资源数大于零且小于资源转移请求中的资源转移数。

[0074] 对于情况一至三，由于该第一账户发起的资源转移过程已全部完成，为了避免在该资源转移过程中的任一方反悔或抵赖，且避免重复执行该第一合约向目标账户或第一账户进行转移，从而提高资源转移过程的严谨性和安全性，服务器可以将第一合约设置为已完成状态，本发明实施例对设置的方式不做具体限定，例如，服务器可以为第一合约添加合约已完成标识，或者，在该第一合约中添加已转移资源的账户和对应的转移资源数，由于该转移资源数与第一账户请求转移的资源数相同，相当于标识该第一合约已完成全部资源的转移，或者，在该第一合约中添加一条新的资源转移数，且该资源转移数为零，以使服务器基于该资源第一合约中的合约已完成标识或者最新的资源转移数不会再执行资源转移。

[0075] 需要说明的是，为了保证合约正确执行，且资源转移过程正确，每次发生资源转移，该第一合约均会更新，但为了避免已进行资源转移的账户抵赖或篡改合约，更新时不是修改该第一合约中已经存储的信息，而是在第一合约中添加更新信息，服务器后续在基于该第一合约进行资源转移时，需要基于第一合约中最新的更新信息进行资源转移，例如，基于第一合约中更新信息的时间戳，获取最新添加的更新信息，并基于该最新添加的更新信息进行资源转移。

[0076] 在将该第一合约设置为已完成状态时，服务器可以基于已完成状态的第一合约、触发本次资源转移完成的消息以及区块链中第五区块的区块头特征值，生成第六区块，第五区块为区块链上第六区块的上一个区块，第六区块用于记录触发本次资源转移完成的事件。其中，触发本次资源转移完成的消息可以为服务器检测到第一合约达到第一合约的到期时间的消息，或者，目标用户的确认资源转移消息或者目标用户的拒绝资源转移消息。

[0077] 对于情况四和情况五，本发明实施例继续以步骤208和步骤209进行说明：

[0078] 208、服务器更新第一合约，更新后的第一合约用于指示第一账户的剩余资源转移条件。

[0079] 该步骤中，考虑到第一账户的资源已部分转移至一个目标账户或者部分退回至第一账户，因此，为了能够继续为多个目标账户中的其他账户进行资源转移，服务器可以基于第一合约、已确认(或拒绝)资源转移目标账户以及已转移资源数，在第一合约中添加更新信息，完成第一合约的更新过程，该更新信息根据已进行的资源转移过程得到，该更新信息可以有多种表达形式。例如，该更新信息包括已进行资源转移的账户(第一账户或目标账户)和对应的资源转移数，使得服务器后续可以根据该更新信息和第一合约中已记录的信息，确定当前的目标账户和每个目标账户对应的资源转移数。又例如，该更新信息包括除该已进行资源转移的账户之外的剩余目标账户、以及剩余目标账户对应的资源转移数，则服务器后续可以直接根据该更新信息进行资源转移。

[0080] 需要说明的是，由于目标账户可能有多个，而基于每个目标账户的交互消息，该第一合约均会更新，因此，该第一合约中可能记录多次更新信息，服务器在基于该第一合约进行资源转移时，可以按照更新信息的时间戳，基于最新的更新信息进行资源转移。

[0081] 209、服务器基于更新后的第一合约、触发本次资源转移的交互消息以及区块链中第三区块的区块头特征值，生成第四区块，第三区块为区块链上第四区块的上一个区块，第四区块用于记录本次资源转移完成事件。

[0082] 该步骤中，服务器可以基于更新后的第一合约的信息(如更新后的第一合约的特征值)、确认资源转移消息(或拒绝资源转移消息)以及区块链中第三区块的区块头特征值，生成该第四区块。具体生成过程与步骤203的区块生成过程同理。

[0083] 事实上，后续在该第一合约的到期时间之前，如果服务器接收到某个目标账户的确认资源转移消息或者拒绝资源转移消息时，还可以继续基于步骤206和207的验证过程和确认匹配过程进行确定是否进行资源转移，并在确定资源转移时，更新合约并生成新的区块。或者，如果直到达到该第一合约的到期时间时，服务器也没有收到任何目标账户的交互消息，则可以将该第一合约中的剩余资源转移数退回至第一账户，并将第一合约设置为已完成状态和并生成新的区块。

[0084] 在该第一账户向多个目标账户转移资源时，如果该多个目标账户中的一些目标账户已经确认(或拒绝)资源转移，而另一些目标账户还没有进行确认或者拒绝，则该第一合约的资源转移数不会一次性全部转移，则为了保证该第一账户请求转移的全部资源可以转移，为用户提供完善的资源转移服务，服务器还需要根据该第一账户的剩余资源继续进行资源转移，通过更新第一合约并生成第四区块，不仅能够避免前次资源转移过程中已转移资源的账户抵赖或篡改转移记录，还能够依据该更新后的第一合约准确地执行下一次资源转移过程，进一步使得资源转移过程中的资源数保持平衡。

[0085] 图4是本发明实施例提供的一种资源转移装置的框图，参见图4，该装置包括：

[0086] 接收模块401，用于接收第一账户的资源转移请求，资源转移请求用于请求将第一账户的资源转移至目标账户；

[0087] 合成生成模块402，用于生成第一合约，第一合约用于指示第一账户的资源转移条件；

[0088] 区块生成模块403，用于基于第一合约、资源转移请求以及区块链中第一区块的区块头特征值，生成第二区块，第一区块为区块链上第二区块的上一个区块，第二区块用于记录本次资源转移请求事件；

[0089] 资源转移模块404，用于当符合第一合约指示的资源转移条件时，基于第一合约进行资源转移。

[0090] 本发明实施例通过在接收到第一账户的资源转移请求时，生成第一合约，并基于第一合约、资源转移请求和区块链中第一区块的区块头特征值，生成第二区块，并当符合第一合约指示的资源转移条件时，基于第一合约进行资源转移，能够基于区块链中前后区块之间的关联关系，使得区块中任一资源转移过程中的信息被篡改时都能通过下一区块检测到，避免了恶意账户篡改或抵赖被转移的资源，保证了资源转移过程的安全性和可靠性，而且，由于合约的信息也记录在区块链中，使得合约被篡改时也能通过区块链中已记录的合约的信息被检测到，进一步保证了合约的安全性和正确性，提高了资源转移的安全性和可

靠性。

[0091] 在一种可能实现方式中，资源转移模块404用于：

[0092] 接收第二账户的确认资源转移消息；

[0093] 如果第二账户的身份验证通过，且确认资源转移消息与第一合约匹配，将第二账户确定为目标账户，基于第一合约向目标账户转入目标账户对应的资源转移数。

[0094] 在一种可能实现方式中，资源转移模块404用于：

[0095] 如果确认资源转移消息中的合约公钥对确认资源转移消息中的合约私钥签名验证通过，且确认资源转移消息中的账户公钥对确认资源转移消息中的账户私钥签名验证通过，获取确认资源转移消息中的合约公钥对应的合约标识；

[0096] 如果确认资源转移消息中的合约公钥对应的合约标识与第一合约的合约标识相同，且第二账户与目标账户相同，且确认资源转移消息中的资源转移数匹配第一合约的资源转移数，且确认资源转移消息的接收时间不晚于第一合约的到期时间，基于第一合约，将第二账户确定为目标账户，向目标账户转入目标账户对应的资源转移数。

[0097] 在一种可能实现方式中，资源转移模块404用于：

[0098] 接收第二账户的拒绝资源转移消息；

[0099] 如果第二账户的身份验证通过，且拒绝资源转移消息与第一合约匹配，基于第一合约，将第二账户确定为目标账户，向第一账户退回目标账户对应的资源转移数。

[0100] 在一种可能实现方式中，资源转移模块404用于：

[0101] 当检测到第一合约达到第一合约的到期时间时，基于第一合约，向第一账户退回第一合约中的资源转移数。

[0102] 在一种可能实现方式中，区块生成模块403用于：

[0103] 基于第一合约的特征值、资源转移请求以及第一区块的区块头特征值，生成第二区块。

[0104] 在一种可能实现方式中，基于图4的装置组成，参见图5A，该装置还包括：合约更新模块405，用于更新第一合约，更新后的第一合约用于指示第一账户的剩余资源转移条件；

[0105] 区块生成模块403，还用于基于更新后的第一合约、触发本次资源转移的交互消息以及区块链中第三区块的区块头特征值，生成第四区块，第三区块为区块链上第四区块的上一个区块，第四区块用于记录本次资源转移完成事件。

[0106] 在一种可能实现方式中，基于图4的装置组成，参见图5B，该装置还包括：

[0107] 发送模块406，用于将合约私钥发送至目标账户，使得目标账户基于合约私钥得到合约私钥签名和合约公钥，合约私钥由第一账户发送得到。

[0108] 上述所有可选技术方案，可以采用任意结合形成本发明的可选实施例，在此不再一一赘述。

[0109] 需要说明的是：上述实施例提供的资源转移装置在转移资源时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的资源转移装置与资源转移方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0110] 图6是本发明实施例提供的一种服务器结构示意图。参见图6，该服务器包括处理

组件622,其进一步包括一个或多个处理器,以及由存储器632所代表的存储器资源,用于存储可由处理部件622的执行的指令,例如应用程序。存储器632中存储的应用程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外,处理组件622被配置为执行指令,以执行上述资源转移方法中服务器侧执行的方法。

[0111] 服务器还可以包括一个电源组件626被配置为执行服务器的电源管理,一个有线或无线网络接口650被配置为将服务器连接到网络,和一个输入输出(I/O)接口658。服务器可以操作基于存储在存储器632的操作系统,例如Windows Server™,Mac OS X™,Unix™,Linux™,FreeBSD™或类似。

[0112] 在示例性实施例中,还提供了一种计算机可读存储介质,例如包括指令的存储器632,上述指令可由处理组件622执行以完成上述资源转移方法中服务器侧执行的方法。例如,该计算机可读存储介质可以是ROM、RAM(Random Access Memory,随机存取存储器)、CD-ROM(Compact Disc Read-Only Memory,光盘只读存储器)、磁带、软盘和光数据存储设备等。

[0113] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成,也可以通过程序来指令相关的硬件完成,所述的程序可以存储于一种计算机可读存储介质中,上述提到的存储介质可以是只读存储器,磁盘或光盘等。

[0114] 以上所述仅为本发明的可选实施例,并不用以限制本发明,凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

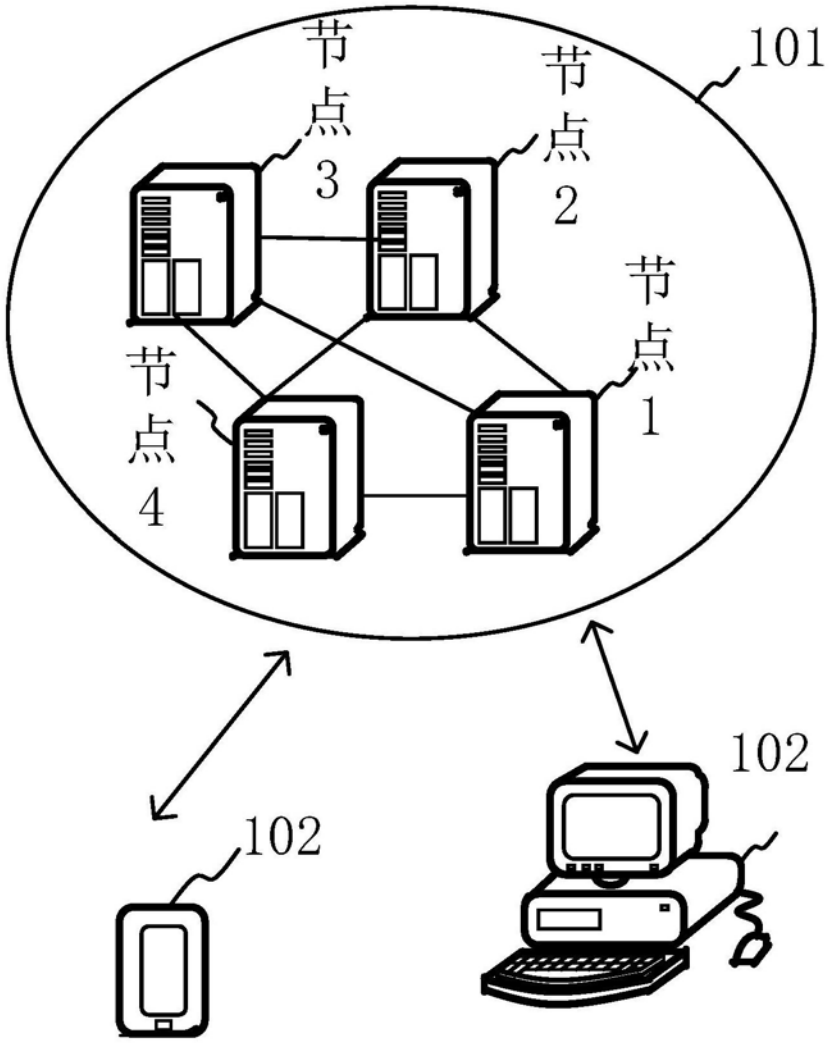


图1

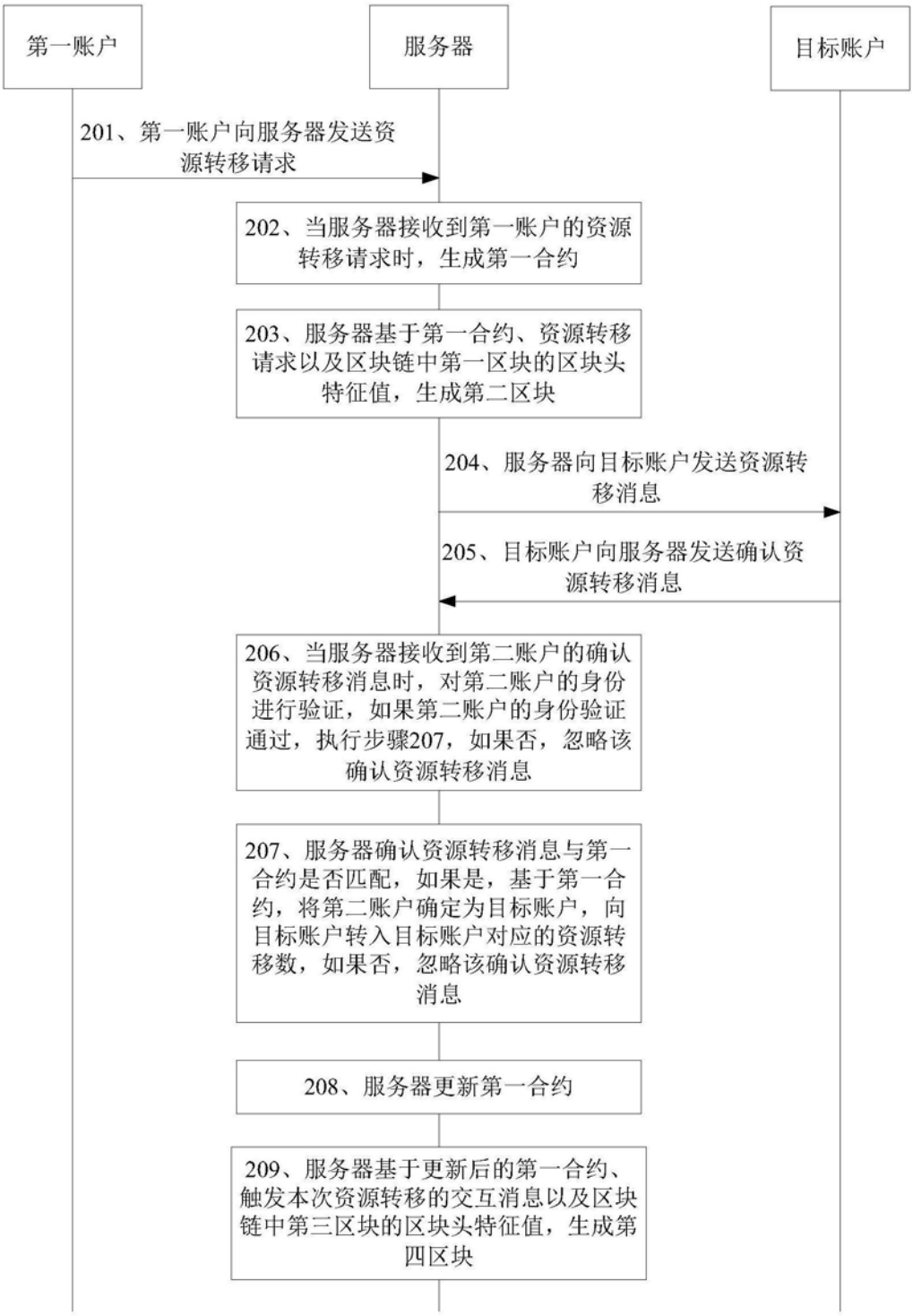

第一账户
服务器
目标账户
201、第一账户向服务器发送资源转移请求
202、当服务器接收到第一账户的资源转移请求时，生成第一合约
203、服务器基于第一合约、资源转移请求以及区块链中第一区块的区块头特征值，生成第二区块
204、服务器向目标账户发送资源转移消息
205、目标账户向服务器发送确认资源转移消息
206、当服务器接收到第二账户的确认资源转移消息时，对第二账户的身份进行验证，如果第二账户的身份验证通过，执行步骤207，如果否，忽略该确认资源转移消息
207、服务器确认资源转移消息与第一合约是否匹配，如果是，基于第一合约，将第二账户确定为目标账户，向目标账户转入目标账户对应的资源转移数，如果否，忽略该确认资源转移消息
208、服务器更新第一合约
209、服务器基于更新后的第一合约、触发本次资源转移的交互消息以及区块链中第三区块的区块头特征值，生成第四区块

图2


私钥
椭圆曲线
公钥
哈希算法、
编码
私钥

图3

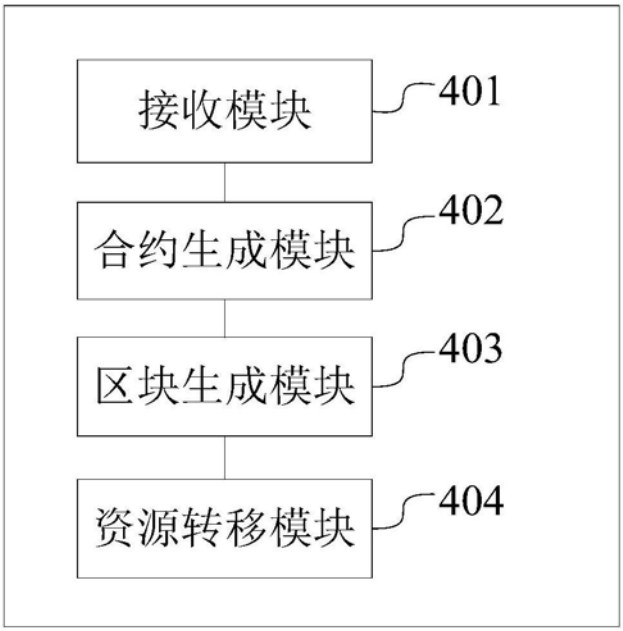

接收模块
401
合约生成模块
402
区块生成模块
403
资源转移模块
404

图4

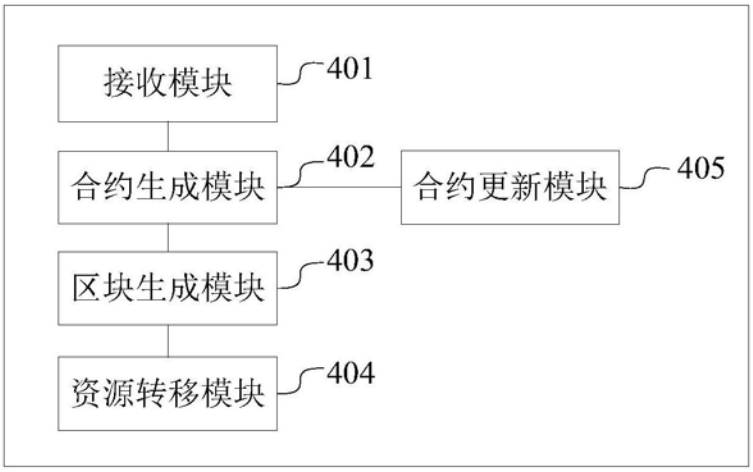

接收模块
401
合约生成模块
402
合约更新模块
405
区块生成模块
403
资源转移模块
404

图5A

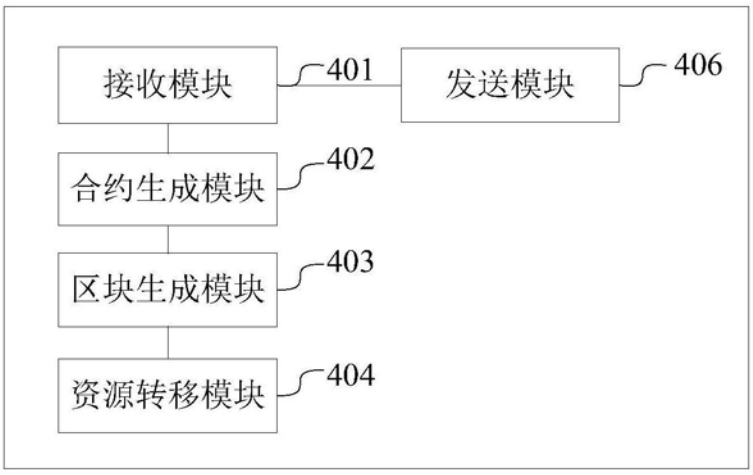

接收模块
401
发送模块
406
合约生成模块
402
区块生成模块
403
资源转移模块
404

图5B

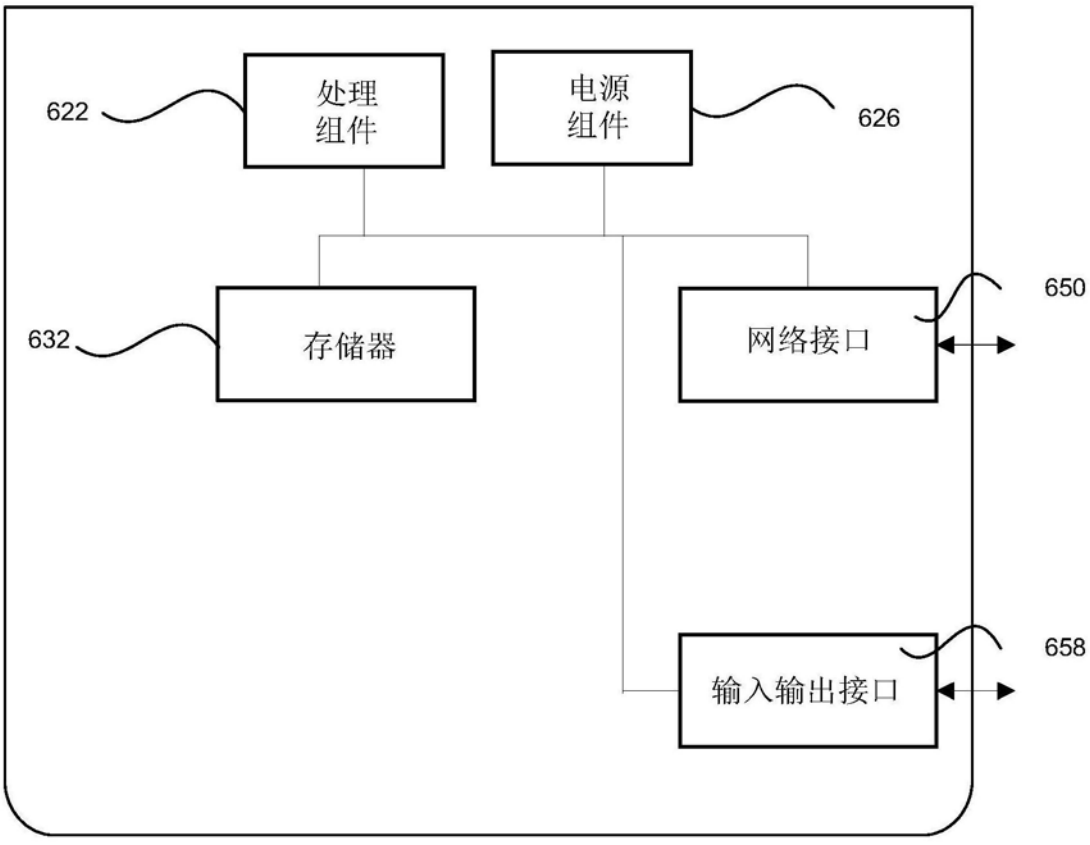

622
处理组件
电源组件
626
632
存储器
网络接口
650
输入输出接口
658

图6