(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111066046 B
(45)授权公告日 2023.11.21

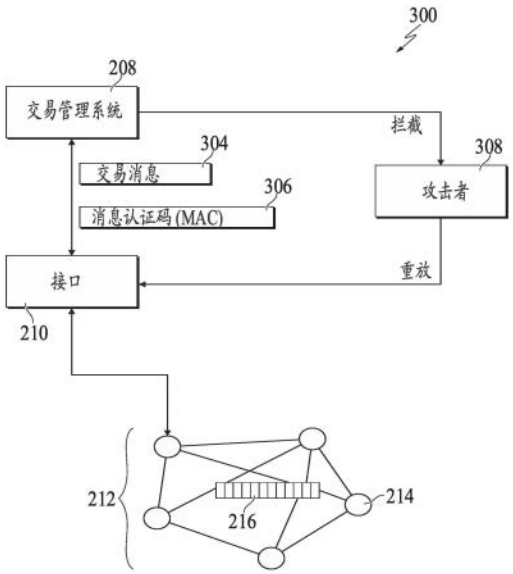
(21)申请号 201980003784.4
(22)申请日 2019.04.26
(65)同一申请的已公布的文献号
申请公布号 CN 111066046 A
(43)申请公布日 2020.04.24
(85)PCT国际申请进入国家阶段日
2020.02.05
(86)PCT国际申请的申请数据
PCT/CN2019/084510 2019.04.26
(87)PCT国际申请的公布数据
WO2019/137563 EN 2019.07.18
(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心
(72)发明人 吕宏
(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
专利代理师 艾佳
(51)Int.Cl.
G06Q 20/38(2006.01)
(56)对比文件
WO 2018205971 A1,2018.11.15
US 2017228731 A1,2017.08.10
CN 101901316 A,2010.12.01
CN 106295401 A,2017.01.04
CN 109064171 A,2018.12.21
US 2019268312 A1,2019.08.29
WO 2017011601 A1,2017.01.19
袁超.区块链中硬分叉期间的防御方案.现代计算机(专业版).2019,(第09期),全文.
审查员 崔小利
权利要求书1页 说明书11页 附图6页

(54)发明名称

抗重放攻击认证协议

(57)摘要

本文公开了用于增强区块链网络安全性的方法、系统和装置,包括编码在计算机存储介质上的计算机程序。本文的实施例包括:接收来自客户端的交易请求,其中,该交易请求包括请求被记录在区块链上的交易和基于对该交易进行哈希处理而计算出的交易哈希值;确定该交易哈希值先前未被存储在缓存资源或区块链中;将该交易哈希值存储在该缓存资源中;以及执行所述交易请求。



CN 111066046 B

1.一种计算机实现的用于增强区块链网络安全性的方法,包括:

区块链节点接收来自客户端的交易请求,其中,所述交易请求包括请求被记录在区块链上的交易和基于对所述交易进行哈希处理而计算出的交易哈希值;

所述区块链节点使用交易哈希值查询缓存资源,如果在所述缓存资源中查询不到所述交易哈希值,确定所述交易哈希值先前未被存储在所述缓存资源中;如果在所述缓存资源中查询到所述交易哈希值,进一步使用交易哈希值查询所述区块链,如果在所述区块链中查询不到所述交易哈希值,确定所述交易哈希值先前未被存储在所述区块链中;其中,所述缓存资源是布隆过滤器,其存储由所述区块链节点在接收所述交易请求之前接收到的交易哈希值;

如果所述交易哈希值先前未被存储在缓存资源或所述区块链中,将所述交易哈希值存储在所述缓存资源中;以及

执行所述交易请求。

2.如权利要求1所述的计算机实现的方法,其中,所述交易请求包括基于所述交易生成的数字签名。

3.如权利要求2所述的计算机实现的方法,其中,所述交易是第一交易,并且所述交易哈希值是第一交易哈希值,所述方法还包括:

所述区块链节点接收包括第二交易和第二交易哈希值的第二交易请求;

所述区块链节点确定所述第二交易哈希值先前被存储在所述缓存资源和所述区块链中;以及

所述区块链节点向所述客户端发送交易拒绝。

4.如权利要求1所述的计算机实现的方法,其中,所述交易是第一交易,并且所述交易哈希值是第一交易哈希值,并且所述方法还包括:

所述区块链节点接收包括第二交易和第二交易哈希值的第二交易请求;

所述区块链节点确定所述第二交易哈希值先前被存储在区块链中;以及

所述区块链节点向所述客户端发送交易拒绝。

5.如权利要求1所述的计算机实现的方法,其中,所述交易包括与区块链地址、交易金额和所述交易的时间中的一个或多个相关联的信息。

6.一种用于增强区块链网络安全性的系统,包括:

一个或多个处理器;以及

一个或多个计算机可读存储器,其耦接到所述一个或多个处理器并且其上存储有指令,所述指令能够由所述一个或多个处理器执行以执行权利要求1至5中任一项所述的方法。

7.一种用于增强区块链网络安全性的装置,所述装置包括用于执行权利要求1至5中任一项所述的方法的多个模块。

抗重放攻击认证协议

背景技术

[0001] 分布式账本(DLS),也可以被称为共识网络和/或区块链网络,使参与实体能够安全地且不可篡改地存储数据。在不引用任何特定用例的情况下,DLS通常被称为区块链网络。区块链网络的示例类型可以包括公有区块链网络、私有区块链网络和联盟区块链网络。联盟区块链网络针对选择的实体组群提供,该实体组群控制共识过程,并且联盟区块链网络包括访问控制层。

[0002] 在网络应用中,通过两个计算设备之间的网络连接传输的数据可能容易受到各种网络攻击,例如重放攻击。重放攻击涉及攻击者拦截在两个计算设备之间发送的一个或多个消息,并在随后的日期重发该消息(可能有一些修改)以提示执行由原始消息提示的相同行为。例如,攻击者可以拦截支付请求并将该请求中的目的地账户替换为他自己的账户。然后,攻击者可以发送修改后的支付请求以尝试将资金转账到自己的账户。

[0003] 在涉及与中央服务器交互的多个客户端的中心化系统中,可以实施抗重放攻击协议,例如,通过在每个消息中包括只能被使用一次的标识(例如,随机数)。中央服务器可以跟踪哪些随机数已被使用,并拒绝包含了已被包含在另一个消息中的随机数或无效随机数的消息。攻击者不能简单重放具有相同随机数的消息,因为中央服务器将拒绝该消息。在缺乏中央服务器的去中心化应用程序中,维护已使用的随机数列表可能具有挑战性,因为一旦接收到消息,不同的网络设备可能需要时间来更新随机数列表,由此留下一个可能接受使用相同随机数的消息的重放攻击的时间窗口。因此,需要用于增强区块链网络安全性的方法。

发明内容

[0004] 本文的实施例包括用于增强区块链网络上的数据安全性的计算机实现的方法。更具体地,本文的实施例涉及为连接到区块链网络的客户端实施抗重放攻击认证协议。

[0005] 本文还提供了与一个或多个处理器耦接且其上存储有指令的一个或多个非暂态计算机可读存储介质,当所述指令由一个或多个处理器执行时,促使所述一个或多个处理器执行根据本文提供的方法的实施例的操作。

[0006] 本文还提供了一种用于实施本文提供的方法的系统。该系统包括一个或多个处理器,以及耦接到所述一个或多个处理器并且其上存储有指令的计算机可读存储介质,当所述指令由所述一个或多个处理器执行时,所述指令将导致所述一个或多个处理器执行根据本文提供的方法的实施例的操作。

[0007] 应该了解,根据本文的方法可以包括本文描述的方面和特征的任何组合。也即,根据本文的方法不限于本文具体描述的方面和特征的组合,还包括所提供的方面和特征的任意组合。

[0008] 在附图和以下描述中阐述了本文的一个或多个实施例的细节。根据说明书、附图以及权利要求书,本文的其他特征和优点将是显而易见的。

附图说明

[0009] 图1描绘了可以用于执行本文实施例的环境的示例。

[0010] 图2描绘了根据本文实施例的概念性架构的示例。

[0011] 图3描绘了根据本文实施例在重放攻击下的分布式计算系统的示例。

[0012] 图4描绘了根据本文实施例用于实施抗重放攻击认证协议的处理的示例的泳道图。

[0013] 图5描绘了可根据本文实施例可以执行的处理的示例。

[0014] 图6描绘了根据本文实施例的装置的模块的示例。

[0015] 各附图中的相同附图标记表示相同的元件。

具体实施方式

[0016] 本文的实施例包括用于增强区块链网络上的数据安全性的计算机实现方法。更具体地，本文的实施例涉及针对连接到区块链网络的每一个客户端实施抗重放安全方案。在一些实施例中，动作包括：从客户端接收交易请求；确定该交易哈希先前未被存储在缓存资源或区块链中；将该交易哈希存储在缓存资源中；以及执行交易请求。

[0017] 为了提供本文实施例的进一步上下文，且如上所述，分布式账本系统(DLS)，其也可以被称为共识网络(例如，由点对点节点构成)，和区块链网络，使得参与实体能够安全地且不可篡改地进行交易和存储数据。虽然术语“区块链”通常与特定的网络和/或用例相关联，但是本文使用的区块链通常指不参考任何特定用例的DLS。

[0018] 区块链是以交易不可篡改的方式存储交易的数据结构。因此，区块链上记录的交易是可靠且可信的。区块链包括一个或多个区块。链中的每个区块通过包含在链中紧邻其前的前一区块的加密哈希值(cryptographic hash)而被链接到该前一区块。每个区块还包括时间戳、其自身的加密哈希值以及一个或多个交易。已经被区块链网络的节点验证的交易经哈希处理并被编码到默克尔(Merkle)树中。Merkle树是一种数据结构，在该树的叶节点处的数据是经哈希处理的，并且在该树的每个分支中的所有哈希值在该分支的根处被级联。此过程沿着树持续一直到整个树的根，在整个树的根处存储了代表树中所有数据的哈希值。声称是存储在树中的交易的哈希值可以通过确定其是否与树的结构一致而被快速验证。

[0019] 区块链是用于存储交易的去中心化或至少部分去中心化的数据结构，而区块链网络是通过广播、验证和确认交易等来管理、更新和维护一个或多个区块链的计算节点的网络。如上所述，区块链网络可以被提供为公有区块链网络、私有区块链网络或联盟区块链网络。本文参考联盟区块链网络进一步详细描述了本文的实施例。然而，可以预期，本文的实施例可以在任何适当类型的区块链网络中实现。

[0020] 通常，联盟区块链网络在参与实体之间是私有的。在联盟区块链网络中，共识过程由授权的节点集控制，该授权的节点集可以被称为共识节点，一个或多个共识节点由相应的实体(例如，金融机构、保险公司)操作。例如，由十(10)个实体(例如，金融机构、保险公司)组成的联盟可以操作联盟区块链网络，每个实体可以操作联盟区块链网络中的至少一个节点。

[0021] 在一些示例中，在联盟区块链网络内，全局区块链被提供为跨所有节点复制的区

块链。也就是说，所有共识节点相对于全局区块链处于完全状态共识。为了达成共识(例如，同意向区块链添加区块)，在联盟区块链网络内实施共识协议。例如，联盟区块链网络可以实施实用拜占庭容错(PBFT)共识，下面将进一步详细描述。

[0022] 鉴于以上上下文，本文进一步详述了本文的实施例。更具体地，如上所述，本文的实施例涉及为连接到区块链网络的客户端实施抗重放攻击认证协议。

[0023] 在一些实施例中，所公开的抗重放攻击认证协议使用唯一的交易哈希值来标记每个提出的交易，以防止攻击者重放被盗的客户端信息。

[0024] 图1描绘了可以用于执行本文实施例的环境100的示例。在一些示例中，示例环境100使得实体能够参与联盟区块链网络102。示例环境100包括计算设备106、108以及网络110。在一些示例中，网络110包括局域网(LAN)、广域网(WAN)、因特网或其组合，并且连接网络站点、用户设备(例如，计算设备)和后台系统。在一些示例中，可以通过有线和/或无线通信链路来访问网络110。

[0025] 在所描绘的示例中，计算系统106、108可以各自包括能够作为联盟区块链网络102中的节点参与的任何适当的计算系统。示例计算设备包括但不限于服务器、台式计算机、膝上型计算机、平板计算设备以及智能电话。在一些示例中，计算系统106、108承载一个或多个由计算机实现的服务，用于与联盟区块链网络102交互。例如，计算系统106可以承载第一实体(例如，用户A)的由计算机实现的、例如交易管理系统的服务，第一实体使用交易管理系统管理其与一个或多个其它实体(例如，其它用户)的交易。计算系统108可以承载第二实体(例如，用户B)的由计算机实现的、例如交易管理系统的服务，第二实体使用交易管理系统管理其与一个或多个其它实体(例如，其它用户)的交易。在图1的示例中，联盟区块链网络102被表示为节点的点对点网络(Peer-to-peer network)，并且计算系统106、108分别提供参与联盟区块链网络102的第一实体和第二实体的节点。

[0026] 图2描绘了根据本文实施例的示例性概念架构200。该示例性概念架构200包括实体层202、承载服务层204和区块链网络层206。在所描述的示例中，实体层202包括三个参与者，参与者A、参与者B和参与者C，每个参与者具有相应的交易管理系统208。

[0027] 在所描述的示例中，承载服务层204包括用于每个交易管理系统208的接口210。在一些示例中，各交易管理系统208使用协议(例如，超文本传输安全协议(HTTPS))通过网络(例如，图1的网络110)与相应的接口210通信。在一些示例中，每个接口210在相应的交易管理系统208和区块链网络层206之间提供通信连接。更具体地，接口210与区块链网络层206的区块链网络212通信。在一些示例中，接口210和区块链网络层206之间的通信是利用远程过程调用(RPC)进行的。在一些示例中，接口210“承载”用于相应交易管理系统208的区块链网络节点。例如，接口210提供用于访问区块链网络212的应用编程接口(API)。

[0028] 如本文所述，区块链网络212被提供为包括多个节点214的点对点网络，所述多个节点214将信息不可篡改地记录在区块链216中。尽管示意性地描绘了单个区块链216，但是在区块链网络212上提供并维护了区块链216的多个副本。例如，每个节点214存储区块链的一个副本。在一些实施例中，区块链216存储与在参与联盟区块链网络的两个或更多个实体之间执行的交易相关联的信息。

[0029] 区块链(例如，图2的区块链216)由一系列区块组成，每个区块存储数据。示例数据包括表示两个或更多个参与者之间的交易的交易数据。尽管本文通过非限制性示例使用了

“交易”,但是可以预期,任何适当的数据可以被存储在区块链中(例如,文档、图像、视频、音频)。示例交易可以包括但不限于有价物的交换(例如,资产、产品、服务、货币)。交易数据被不可篡改地存储在区块链内。也就是说,交易数据不能改变。其中,说明书中所涉及的货币、数字货币等均是法定货币。

[0030] 在存储在区块中之前,对交易数据进行哈希处理。哈希处理是将交易数据(作为字符串数据提供)转换为固定长度哈希值(也作为字符串数据提供)的处理。不可能对哈希值进行去哈希处理(un-hash)以获取交易数据。哈希处理确保即使交易数据的轻微改变也会导致完全不同的哈希值。此外,如上所述,哈希值具有固定长度。也就是说,无论交易数据的大小如何,哈希值的长度都是固定的。哈希处理包括通过哈希函数处理交易数据以生成哈希值。示例哈希函数包括但不限于输出256位哈希值的安全哈希算法(SHA)-256。

[0031] 多个交易的交易数据被哈希处理并被存储在区块中。例如,提供两个交易的哈希值,并对它们自身进行哈希处理以提供另一个哈希值。重复此处理,直到针对要被存储在区块中的所有交易提供单个哈希值为止。这个哈希值被称为Merkle根哈希值,并被存储在区块的头中。交易中的任何更改都会导致其哈希值发生变化,并最终导致Merkle根哈希值发生变化。

[0032] 通过共识协议将区块添加到区块链。区块链网络内的多个节点参与共识协议,并执行将区块添加到区块链中的工作。这样的节点被称为共识节点。上文介绍的PBFT用作共识协议的非限制示例。共识节点执行共识协议以将交易添加至区块链,并更新区块链网络的整体状态。

[0033] 更详细地,共识节点生成区块头,对区块中的所有交易进行哈希处理,并将哈希值成对地组合以生成进一步的哈希值,直到为区块中的所有交易提供单个哈希值(Merkle根哈希值)。这个哈希值被添加到区块头。共识节点还确定区块链中最近的区块(即,添加到区块链中的最后一个区块)的哈希值。共识节点还向区块头添加随机数(nonce)值和时间戳。

[0034] 通常,PBFT提供实用拜占庭状态机复制,其容忍拜占庭故障(例如,故障节点、恶意节点)。这在PBFT中通过假设将发生故障来实现(例如,假设存在独立节点故障和/或存在由共识节点发送的经操作的消息)。在PBFT中,共识节点以包括主共识节点和备共识节点的序列提供。主共识节点被周期性地改变,区块链网络内的所有共识节点将交易添加到区块链,以针对区块链网络的世界状态达成一致。在此处理中,消息在共识节点之间传输,并且每个共识节点证明从指定的对等节点接收消息,并验证该消息在传输期间未被修改。

[0035] 在PBFT中,共识协议被提供为所有共识节点以相同状态开始的多个阶段。首先,客户端向主共识节点发送请求以调用服务操作(例如,在区块链网络内执行交易)。响应于接收到该请求,主共识节点将该请求多播到备共识节点。备共识节点执行该请求,并且每个备共识节点向客户端发送回复。客户端等待直到接收到阈值数量的回复。在一些示例中,客户端等待接收f+1个回复,其中,f是区块链网络内可以容忍的故障共识节点的最大数量。最终结果是,足够数量的共识节点就要添加到区块链的记录的顺序达成一致,并且该记录被接受或拒绝。

[0036] 在一些区块链网络中,用密码学来维护交易的隐私。例如,如果两个节点想要保持交易隐私,以使得区块链网络中的其他节点不能够看出交易的细节,则这两个节点可以对交易数据进行加密处理。示例性密码学包括但不限于对称加密和非对称加密。对称加密是

指使用单个密钥既进行加密(从明文生成密文)又进行解密(从密文生成明文)的加密过程。在对称加密中,同一密钥可以对于多个节点可用,因此每个节点都可以对交易数据进行加密/解密。

[0037] 非对称加密使用密钥对,每个密钥对包括私钥和公钥,私钥仅对于相应节点是已知的,而公钥对于区块链网络中的任何或所有其他节点是已知的。节点可以使用另一个节点的公钥来加密数据,并且该加密的数据可以使用其他节点的私钥被解密。例如,再次参考图2,参与者A可以使用参与者B的公钥来加密数据,并将加密数据发送给参与者B。参与者B可以使用其私钥解密该加密数据(密文)并提取原始数据(明文)。使用节点的公钥加密的消息只能使用该节点的私钥进行解密。

[0038] 非对称加密用于提供数字签名,这使得交易中的参与者能够确认交易中的其他参与者以及交易的有效性。例如,节点可以对消息进行数字签名,而另一个节点可以根据参与者A的数字签名来确认该消息是由该节点发送的。数字签名也可以用于确保消息在传输过程中不被篡改。例如,再次参考图2,参与者A向参与者B发送消息。参与者A生成该消息的哈希值,然后使用其私钥加密该哈希值以提供作为加密哈希值的数字签名。参与者A将该数字签名附加到该消息上,并将该具有数字签名的消息发送给参与者B。参与者B使用参与者A的公钥解密该数字签名,并提取哈希值。参与者B对该消息进行哈希处理并比较哈希值。如果哈希值相同,则参与者B可以确认该消息确实来自参与者A,且未被篡改。

[0039] 图3描绘了在重放攻击下的分布式计算系统300的示例。分布式计算系统300包括客户端和服务器,彼此使用计算机网络可通信地耦接。分布式计算系统300可以具有类似于图2中描述的架构,交易管理系统208是客户端,并且接口210和节点214一起是服务器。在一示例中,交易管理系统208可以是在用户设备上运行的数字钱包应用程序。数字钱包应用程序可以管理用户账户的金融交易,并与节点214通信以在区块链216上注册新交易。示例金融交易包括发送和接收数字货币、执行智能合约、开立新用户账户等。

[0040] 在一些实施例中,交易管理系统208(客户端)和接口210(服务器)之间的通信信道使用一个或多个认证协议来确保数据完整性和数据安全性。例如,交易管理系统208可以用消息认证码(MAC)306标记每个交易消息304。交易消息304指定了交易管理系统208和节点214之间的交易内容,例如发送者的区块链地址、接收者的区块链地址、交易时间、数字货币的数额等。MAC 306是为交易消息304唯一地生成的,以验证交易并且用于对抗重放攻击,下面将进一步详细讨论。在一些示例中,交易管理系统208可以通过对交易消息304进行哈希处理来生成MAC 306。在一些示例中,可以通过对交易消息和与该交易消息相关联的密码进行哈希处理来生成MAC 306。

[0041] 在一些实施例中,攻击者308可以尝试在分布式计算系统300上进行重放攻击。例如,攻击者308可以首先拦截从交易管理系统208发送到接口210的数据,然后可以尝试使用拦截的数据来对接口210进行认证。攻击者308可以以不同方式使用拦截的数据。例如,攻击者308可以在与接口210或交易管理系统208的新通信会话中逐字重新发送拦截的数据。攻击者308还可以使用拦截的数据来尝试解密MAC 306。为了对抗这种重放攻击,接口210和/或交易管理系统208可以使用上面讨论的MAC 306实施用于已接收的消息的认证协议。

[0042] 该认证协议的有效性可以取决于用于生成MAC 306的技术。例如,如果MAC 306是交易管理系统208的密码的精确副本,则攻击者308可以将MAC 306重放到服务器并获得对

交易管理系统208的账户的访问。

[0043] 在另一示例中，使用交易管理系统208的账户密码*p*和由接口210发出的质询c的组合来生成MAC 306。例如，当交易管理系统208发起与接口210的通信会话时，接口210将随机生成的质询c发送到交易管理系统208。交易管理系统208可以将质询c级联到账户密码*p*，并使用哈希函数来生成哈希输出h(c||p)。示例哈希函数包括SHA-256、MD-5等。交易管理系统208接下来将质询c和哈希输出h(c||p)发送到接口210用于认证。结果，尽管攻击者308看到c和h(c||p)，但是攻击者308将不能够在不同的通信会话中重用h(c||p)，因为服务器(接口210)将发布一个不同的质询。

[0044] 然而，攻击者308可以尝试对哈希输出h(c||p)求逆(reverse)以获得密码*p*。例如，攻击者308可以使用彩虹表来对该哈希输出求逆。彩虹表是预计算的表，其将不同的哈希输出映射到特定哈希函数的哈希输入。为此，攻击者308可以伪装成合法服务器并向交易管理系统208发送虚假质询*c'*。攻击者308可以拥有预先计算的彩虹表，该彩虹表具有用于所使用的特定哈希函数的*c'*。如果攻击者308从毫无戒心的交易管理系统208接收到h(c'||p)，则攻击者308可能对该哈希函数求逆以获得密码*p*。结果，尽管该认证协议比前一个更安全，但是如果攻击者308会主动发出钓鱼质询*c'*，则它仍有安全漏洞。

[0045] 在另一示例中，使用服务器发布的质询*c*、客户端的密码*p*和随机数*n*的组合来生成MAC 306。随机数*n*是服务器和客户端选择的任意数字。在该认证协议下，交易管理系统208计算哈希输出h(n||c||p)并将该哈希输出连同质询c和随机数n一起发送到接口210。该认证协议可以防止攻击者308在新的通信会话中简单地重放所拦截的数据，并且还使得对具有钓鱼*c'*的哈希值进行求逆不可行，因为随机数*n*对于不同的交易是不同的。

[0046] 在上面的例子中，交易管理系统208和接口210之间的交易通过单调递增的数字来索引。出于安全目的，该索引可以用作随机数。例如，交易管理系统208可以本地跟踪交易索引，或者节点214进行连接测试(ping)以获得交易索引。然而，如果存在针对单个账户的多个交易管理系统，则在客户端之间协调以注册当前交易编号可能很复杂。此外，交易必须串行完成，而不是并行完成，因为每个交易都依赖于先前交易的计数器。如果一个交易使用了错误的随机数，则由于该数字不同，所有其后待处理交易都将被强制重新启动。在一些情况下，交易管理系统208管理多个时隙(slot)以启用并行交易。例如，每个时隙可以维护自己的索引号。但是，拥有大量时隙会增加计算成本。

[0047] 在另一示例中，通过使用时间戳进一步保护交易免受重放攻击。客户端不得不对服务器进行连接测试以接收每个交易的时间戳，并且交易必须在指定的时间窗口内完成。因此，即使攻击者成功拦截了由客户端发送的信息，攻击者也无法在时间窗口关闭时使用该信息。然而，获取最新的区块时间戳可能会增加计算成本，并且可能会在服务器和客户端不同步时拒绝合法请求。

[0048] 图4描绘了根据本文实施例的用于实施可被执行的认证协议的处理400的示例的泳道图。该认证协议可以对抗网络中的重放攻击，并且可以减轻客户端维护如图3所示的随机数集的责任。在一些实施例中，可以使用一个或多个计算设备执行的一个或多个计算机可执行程序来执行处理400。在客户端401和服务器403之间执行认证协议。在一些示例中，客户端401可以是可由用户操作的计算设备。服务器可以是区块链网络的一个或多个共识节点。

[0049] 作为第一步，客户端401通过在本地生成交易消息*m*(404)来发起交易(402)。例如，交易可以表示将指定数额的数字货币从客户端401控制的账户转账到区块链网络中的另一账户。客户端401使用由区块链网络协议指定的数据格式生成交易消息*m*。例如，交易消息*m*可以包括发送者的区块链地址、接收者的区块链地址、要交换的数字货币数额、挖矿奖励、时间戳等。这样，交易消息*m*与发起的交易唯一相关联。

[0050] 然后，客户端401计算交易消息*m*的交易哈希值h(m)(406)。用于计算交易哈希值h(*m*)的哈希函数可以与区块链网络用于生成区块的哈希函数相同。

[0051] 然后，客户端401可以生成用于在区块链上执行和记录交易的交易请求(408)。该交易请求可以包括交易消息*m*和交易哈希值h(*m*)。在某些情况下，客户端401可以使用其私钥对交易请求进行数字签名。如果交易请求被修改，则该数字签名将变为无效。

[0052] 客户端401接下来与服务器403建立通信会话(410)并将该交易请求发送到服务器(412)。

[0053] 在接收到该交易请求时，服务器403使用交易哈希值h(*m*)在区块链上搜索过去的交易。区块链上的每个交易都由唯一的哈希值索引，交易哈希值h(*m*)与区块链上的交易哈希值之间的匹配将表明该交易信息是重复的并且可能来自重放攻击。在一些实施例中，每个区块链可以包括多个区块，并且每个区块还可以包括多个交易。由于服务器403存储区块链的副本，因此服务器403搜索特定的交易哈希值可能在计算上是昂贵的。为了实施更有效的搜索策略，服务器403可以将现有的交易哈希值编入索引并将它们存储在缓存资源中。缓存资源可以比常规内存或数据库具有更快的访问速度。在某些情况下，缓存资源可以专用于存储交易哈希值。

[0054] 在某些情况下，在交易被记录在区块链上之后，可以从缓存资源中删除该交易哈希值。在这种情况下，服务器403可以搜索缓存资源和区块链以确定先前是否已经接收到交易哈希值h(*m*)。

[0055] 在某些情况下，无论交易是否被记录在区块链上，都可以在缓存哈希值中维护接收到的交易哈希值。在这种情况下，服务器403可以首先基于诸如布隆过滤器(bloom filter)的有效数据结构来搜索该缓存资源。

[0056] 布隆过滤器是用于确定元素是否是集合成员的概率性数据结构。对布隆过滤器的查询可能会返回假阳性(false positive)，但绝不会返回假阴性(false negative)。换句话说，查询返回“可能在集合中”或“绝对不在集合中”。因此，如果对布隆过滤器的查询指示某个交易哈希值不存在，则可以确定区块链上不存在该交易哈希值。另一方面，如果对布隆过滤器的查询指示该交易哈希值确实存在，则可以在整个区块链上进行进一步搜索以确定该交易哈希值是否实际存在。

[0057] 在接收到交易信息时，服务器403在与布隆过滤器相关联的缓存资源中搜索交易哈希值h(*m*)(414)。缓存资源可以存储先前接收到的交易哈希。如果搜索返回否定，表明区块链上不存在交易哈希，则相关联的交易是合法交易，并且服务器403继续进行交易(416)。然后将交易哈希存储到与布隆过滤器相关联的缓存资源中(418)。

[0058] 如果搜索返回肯定，则交易哈希值h(*m*)可能存在或可能不存在于区块链上。为了进一步确定区块链上h(*m*)的存在，服务器403执行交易哈希值h(*m*)的第二次搜索(420)。这次，服务器403将搜索与服务器403相关联的整个区块链以获得交易哈希值h(*m*)。如果搜索

返回否定，表明交易是合法的，则服务器403再次进行交易(416)并在区块链网络上广播该交易。如果该交易被验证，例如，通过工作量证明处理以确保客户端401具有足够的余额，则该交易将被记录在区块链上。

[0059] 如果第二次搜索返回肯定，则交易哈希值h(*m*)已经存在于区块链中。这表明客户端401正在尝试将先前使用的信息发送到服务器，即可能的重放攻击。结果，客户端401可以接收故障消息并中止交易(422)。

[0060] 图5描绘了根据本文实施例的用于实施抗重放攻击认证协议的处理500的示例的流程图。将从服务器的角度描述处理500，例如，图4中包括接口210和节点214的服务器403。服务器403可以是如图2所描绘的区块链网络212的服务器。

[0061] 作为第一步，服务器403建立来自例如图4的客户端401的客户端的通信会话(502)。通信会话允许客户端401和服务器403之间的双向数据交换。例如，交易请求可以包括由客户端401控制的数字资产的转账，并且客户端401可以请求服务器403在例如区块链216的区块链上记录交易。服务器403和客户端401共享某些秘密信息以用于认证目的。例如，服务器403可以存储客户端401的密码的副本。

[0062] 响应于建立通信会话，服务器403向客户端401发出质询(504)。质询是针对通信会话专门生成的随机或伪随机值。不同的通信会话将使用不同的质询。

[0063] 响应于发出质询，服务器403接收来自客户端401的交易请求(506)。例如，交易请求可以包括根据发布的质询、与客户端相关联的密码以及存储在由服务器403维护的区块链中的所请求的交易的哈希值而计算的哈希值。客户端401用来计算所请求的交易的哈希值的哈希函数与区块链网络212用来对区块链216上的交易进行哈希处理和索引的哈希函数相同。该交易请求包括交易消息哈希值(508)。

[0064] 然后，服务器403确定所请求的交易是否被包括在区块链216中(508)。例如，服务器403可以查询存储先前存储在区块链中的所有交易的哈希值的缓存资源。为了提高查询性能，服务器403可以使用布隆过滤器来确定区块链216是否已经包括所请求的交易的哈希值。

[0065] 如果服务器403确定所请求的交易的哈希值未被包括在区块链216中，则服务器403将继续进行交易(512)。例如，服务器403可以继续验证来自客户端301的密码。如果验证成功，则服务器403可以将当前交易广播到区块链网络212以进行验证。

[0066] 另一方面，如果服务器403确定所请求的交易的哈希值已经被包括在区块链216中，则服务器403将向客户端301发送交易拒绝(510)。重复交易哈希值的存在可以表明客户端301是恶意的并且正在重放被盗信息以获得服务器访问。

[0067] 图6是根据本文实施例的装置600的模块的示例的图。装置600可以是区块链节点的示例性实施例。装置600可以对应于上述实施例，并且装置600包括以下内容：接收模块602，用于接收来自客户端的交易请求，其中，该交易请求包括请求记录在区块链上的交易和基于对交易进行哈希处理而计算的交易哈希值；确定模块604，用于确定该交易哈希值先前未被存储在缓存资源或区块链中；存储模块606，用于将该交易哈希值存储在缓存资源中；执行模块608，用于执行该交易请求。

[0068] 本文中描述的技术产生一种或多种技术效果。在一些实施例中，所述技术使得区块链网络能够重复请求被区块链网络处理并被提交给共识处理之前，检测多次提交相同交

易请求的尝试(即,重放攻击)。这使得区块链网络能够避免处理这些无效交易,从而引起更大的交易吞吐量。在一些实施例中,该技术消除了必须在多个客户端之间协调的随机数或其他值的使用,从而导致更简单的客户端实施例和更少的无意重复请求的可能性。

[0069] 所描述的主题的实施例可以包括单独或组合的一个或多个特征。例如,在第一实施例中,用于增强区块链网络安全性的方法包括:接收来自客户端的交易请求,其中,该交易请求包括请求被记录在区块链上的交易和基于对交易进行哈希处理而计算的交易哈希值;确定该交易哈希值先前未被存储在缓存资源或区块链中;将该交易哈希值存储在缓存资源中;以及执行该交易请求。

[0070] 前述和其他所描述的实施例可以各自可选地包括以下特征中的一个或多个:

[0071] 第一特征,可以与以下任一特征组合,具体为:所述交易请求包括基于该交易生成的数字签名。

[0072] 第二特征,可以与先前或以下任一特征相组合,具体为:确定该交易哈希值先前未被存储在缓存资源中或者区块链中,包括:使用该交易哈希值查询缓存资源并确定该交易哈希值的相同副本未被存储在缓存资源中。

[0073] 第三特征,可以与先前或以下任一特征组合,具体为:缓存资源是布隆过滤器,其存储由区块链节点在接收所述交易请求之前接收到的交易哈希值。

[0074] 第四特征,可以与先前或以下任一特征组合,具体为:交易是第一交易并且交易哈希值是第一交易哈希值,区块链还接收包括第二交易和第二交易哈希值的第二交易请求;确定第二交易哈希值先前被存储在缓存资源和区块链中;并向客户端发送交易拒绝。

[0075] 第五特征,可以与先前或以下任一特征组合,具体为:所述交易是第一交易并且交易哈希值是第一交易哈希值,并且区块链节点还接收包括第二交易和第二交易哈希值的第二交易请求;确定第二交易哈希先前被存储在区块链中;并向客户端发送交易拒绝。

[0076] 第六特征,可以与先前或以下任一特征组合,具体为:该交易包括与区块链地址、交易金额和交易的时间中的一个或多个相关联的信息。

[0077] 本文中描述的主题、动作以及操作的实施例可以在数字电子电路、有形体现的计算机软件或固件、计算机硬件中实现,包括本文本文中公开的结构及其结构等同物,或者它们中的一个或多个的组合。本文中描述的主题的实施可以被实现为一个或多个计算机程序,例如,一个或多个计算机程序指令模块,被编码在计算机程序载体上,用于由数据处理装置执行或控制数据处理装置的操作。例如,计算机程序载体可以包括一个或多个计算机可读存储介质,其上编码有或存储有指令。载体可以是有形的非暂时性计算机可读介质,例如磁盘、磁光盘或光盘、固态驱动器、随机存取存储器(RAM)、只读存储器(ROM)或其他介质类型。可选地或附加地,载体可以是人工生成的传播信号,例如,机器生成的电、光学或电磁信号,其被生成来编码信息用于传输到合适的接收器装置以供数据处理装置执行。计算机存储介质可以是或部分是机器可读存储设备、机器可读存储基板、随机或串行访问存储器设备或它们中的一个或多个的组合。计算机存储介质不是传播信号。

[0078] 计算机程序也可以被称为或描述为程序、软件、软件应用程序、应用程序(app)、模块、软件模块、引擎、脚本或代码,可以以任何形式的编程语言编写,包括编译或解释性语言、说明或过程性语言;它可以被配置为任何形式,包括作为独立程序,或者作为模块、组件、引擎、子例程或适合在计算环境中执行的其他单元,该环境可以包括由通信数据网络互

联的在一个或多个位置的一台或多台计算机。

[0079] 计算机程序可以但非必须对应于文件系统中的文件。计算机程序可以被存储在保存其他程序或数据的文件的一部分中，例如，一个或多个脚本可以被存储在标记语言文档中；被存储在专用于所讨论的程序的单个文件中；或者被存储在多个协调文件中，协调文件例如是存储一个或多个模块、子程序或代码部分的多个文件。

[0080] 用于执行计算机程序的处理器包括，例如，通用微处理器和专用微处理器，以及任意种类的数码计算机的任意一个或多个处理器。通常，处理器将接收来自耦接到处理器的非暂态计算机可读介质的计算机程序的指令用于执行以及数据。

[0081] 术语“数据处理装置”包括用于处理数据的所有类型的装置、设备和机器，包括例如可编程处理器、计算机或者多处理器或计算机。数据处理装置可以包括专用逻辑电路，例如FPGA(现场可编程门阵列)、ASIC(专用集成电路)或GPU(图形处理单元)。除了硬件，该装置还可以包括为计算机程序创建执行环境的代码，例如，构成处理器固件、协议栈、数据库管理系统、操作系统或者它们中的一个或多个的组合的代码。

[0082] 本文中描述的处理和逻辑流程可以由一台或多台计算机执行一个或多个计算机程序来执行，以通过对输入数据进行运算并生成输出来执行操作。处理和逻辑流程也可以由例如FPGA、ASIC、GPU等的专用逻辑电路或专用逻辑电路与一个或多个编程计算机的组合来执行。

[0083] 适合于执行计算机程序的计算机可以基于通用微处理器和/或专用微处理器，或任何其他种类的中央处理单元。通常，中央处理单元将从只读存储器和/或随机存取存储器接收指令和数据。计算机的元件可以包括用于执行指令的中央处理单元以及用于存储指令和数据的一个或多个存储器设备。中央处理单元和存储器可以补充有专用逻辑电路或集成在专用逻辑电路中。

[0084] 通常，计算机还将包括或可操作地耦接到一个或多个存储设备，以从一个或多个存储设备接收数据或将数据传输到一个或多个存储设备。存储设备可以是例如磁盘、磁光盘或光盘、固态驱动器或任何其他类型的非暂态计算机可读介质。但是，计算机不需要具有这样的设备。因此，计算机可以耦接到本地和/或远程的一个或多个存储设备，例如一个或多个存储器。例如，计算机可以包括作为计算机的组成部件的一个或多个本地存储器，或者计算机可以耦接到云网络中的一个或多个远程存储器。此外，计算机可以嵌入在另一个设备中，例如移动电话、个人数字助理(PDA)、移动音频或视频播放器、游戏控制台、全球定位系统(GPS)接收器或例如通用串行总线(USB)闪存驱动器的便携式存储设备，仅举几例。

[0085] 组件可以通信地彼此“耦接”，例如直接地或经由一个或多个中间组件彼此电连接或光学连接。如果其中一个组件集成到另一个组件中，则这些组件也可以彼此“耦接”。例如，集成到处理器中的存储组件(例如，L2缓存组件)“耦接到”处理器。

[0086] 为了提供与用户的交互，本文中描述的主题的实施例可以在计算机上实现或配置为与该计算机通信，该计算机具有：显示设备，例如，LCD(液晶显示器)监视器，用于向用户显示信息；以及例如键盘和例如鼠标、轨迹球或触摸板等的指针设备的输入设备，用户可以通过该输入设备向该计算机提供输入。其他类型的设备也可以用于提供与用户的交互；例如，提供给用户的反馈可以是任何形式的感官反馈，例如视觉反馈、听觉反馈或触觉反馈；并且可以接收来自用户的任何形式的输入，包括声音、语音或触觉输入。此外，计算机可以

通过向用户使用的设备发送文档和从用户使用的设备接收文档来与用户交互;例如,通过对从web浏览器接收到的请求做出响应而向用户设备上的web浏览器发送web页面,或者通过与例如智能电话或电子平板电脑等的用户设备上运行的应用程序(app)进行交互。此外,计算机可以通过向个人设备(例如,运行消息应用的智能手机)发送文本消息或其他形式的消息并且接收作为回应来自用户的响应消息来与用户交互。

[0087] 本文使用与系统、装置和计算机程序组件有关的术语“被配置为”。对于被配置为执行特定操作或动作的一个或多个计算机的系统,意味着系统已经在其上安装了在运行中促使该系统执行所述操作或动作的软件、固件、硬件或它们的组合。对于被配置为执行特定操作或动作的一个或多个计算机程序,意味着该一个或多个程序包括当被数据处理装置执行时促使该装置执行所述操作或动作的指令。对于被配置为执行特定操作或动作的专用逻辑电路,意味着该电路具有执行所述操作或动作的电子逻辑。

[0088] 虽然本文包含许多具体的实施例细节,但是这些不应被解释为对由权利要求书本身限定的所请求保护的范围的限制,而是作为对特定实施例的具体特征的描述。在本申请多个单独实施例的上下文中描述的多个特定特征也可以在单个实施例中被组合实现。相反,在单个实施例的上下文中描述的各种特征也可以单独地或以任何合适的子组合在多个实施例中实现。此外,尽管上面的特征可以被描述为以某些组合起作用并且甚至最初如此被请求保护,但是在一些情况下,可以从要求保护的组合中删除来自该组合的一个或多个特征,并且权利要求书可以涉及子组合或子组合的变体。

[0089] 类似地,虽然以特定顺序在附图中描绘了操作并且在权利要求中叙述了操作,但是这不应该被理解为:为了达到期望的结果,要求以所示的特定顺序或依次执行这些操作,或者要求执行所有示出的操作。在一些情况下,多任务和并行处理可能是有利的。此外,上述实施例中各种系统模块和组件的划分不应被理解为所有实施例中都要求如此划分,而应当理解,所描述的程序组件和系统通常可以一起集成在单个软件产品中或者打包成多个软件产品。

[0090] 已经描述了主题的特定实施例。其他实施例在以下权利要求书的范围内。例如,权利要求书中记载的动作可以以不同的顺序执行并且仍然实现期望的结果。作为一个示例,附图中描绘的处理无需要求以所示的特定顺序或次序来实现期望的结果。在一些情况下,多任务和并行处理可能是有利的。

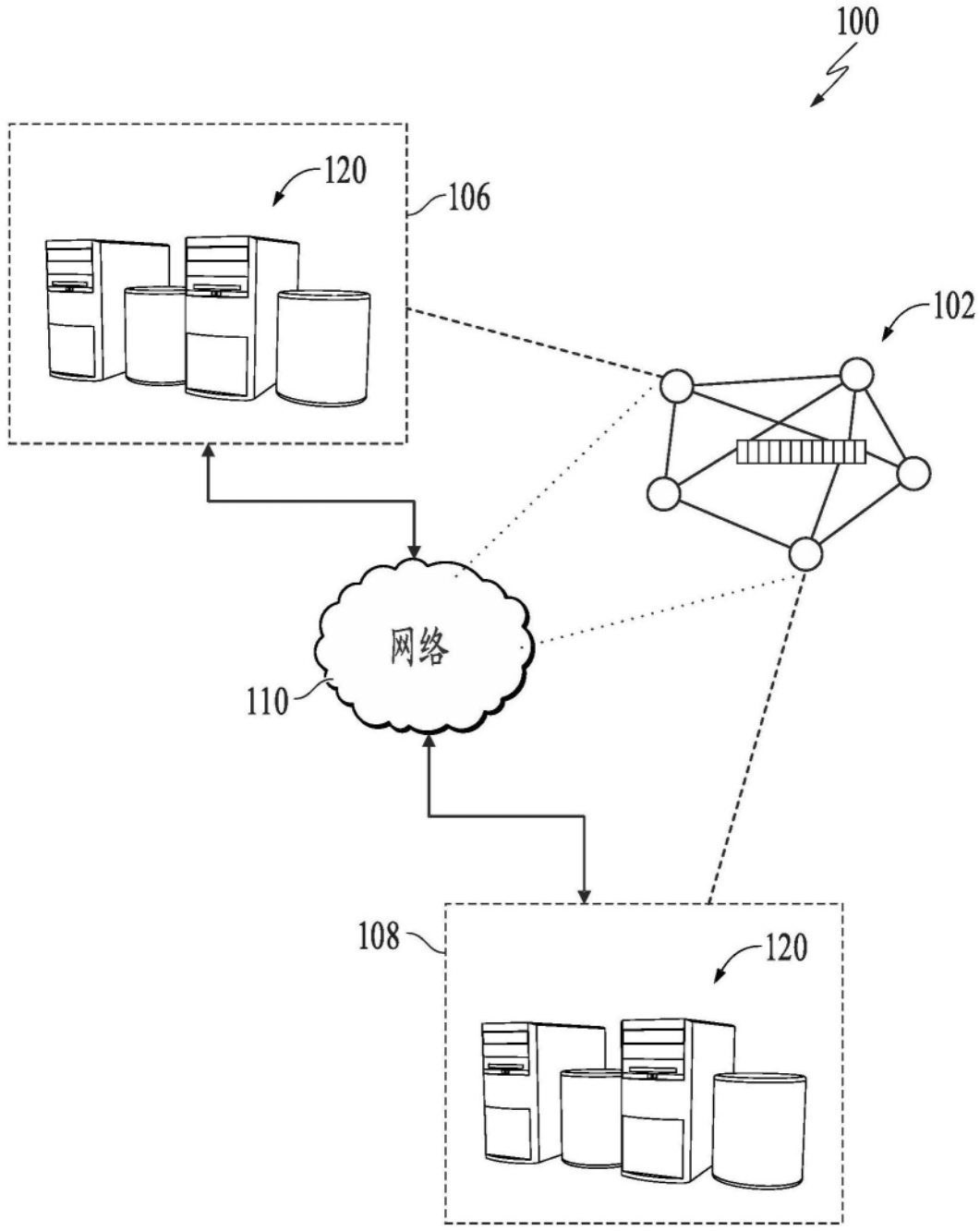


图1

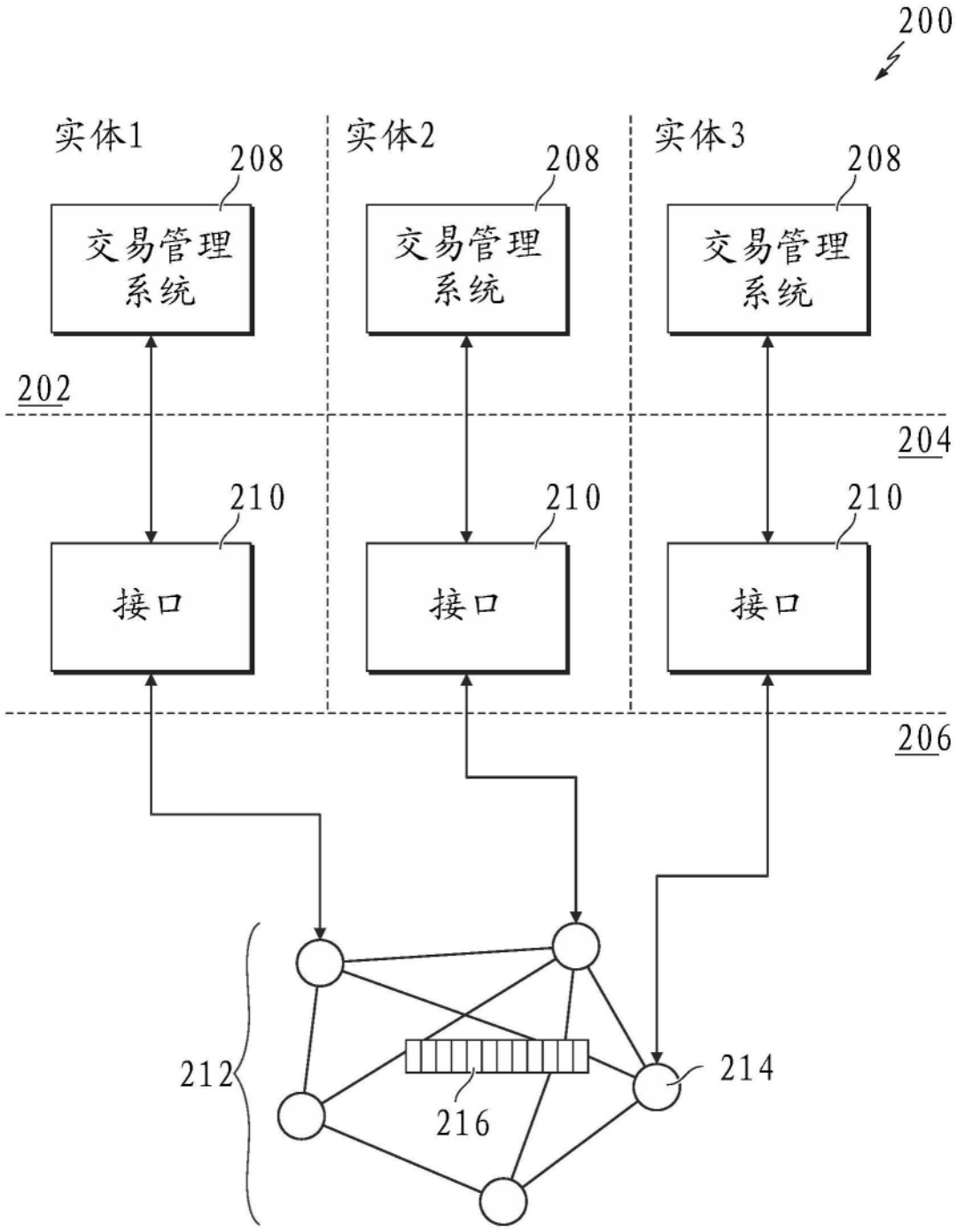

200
实体1
208
交易管理系统
实体2
208
交易管理系统
实体3
208
交易管理系统
202
204
210
接口
210
接口
210
接口
206
212
216
214

图2

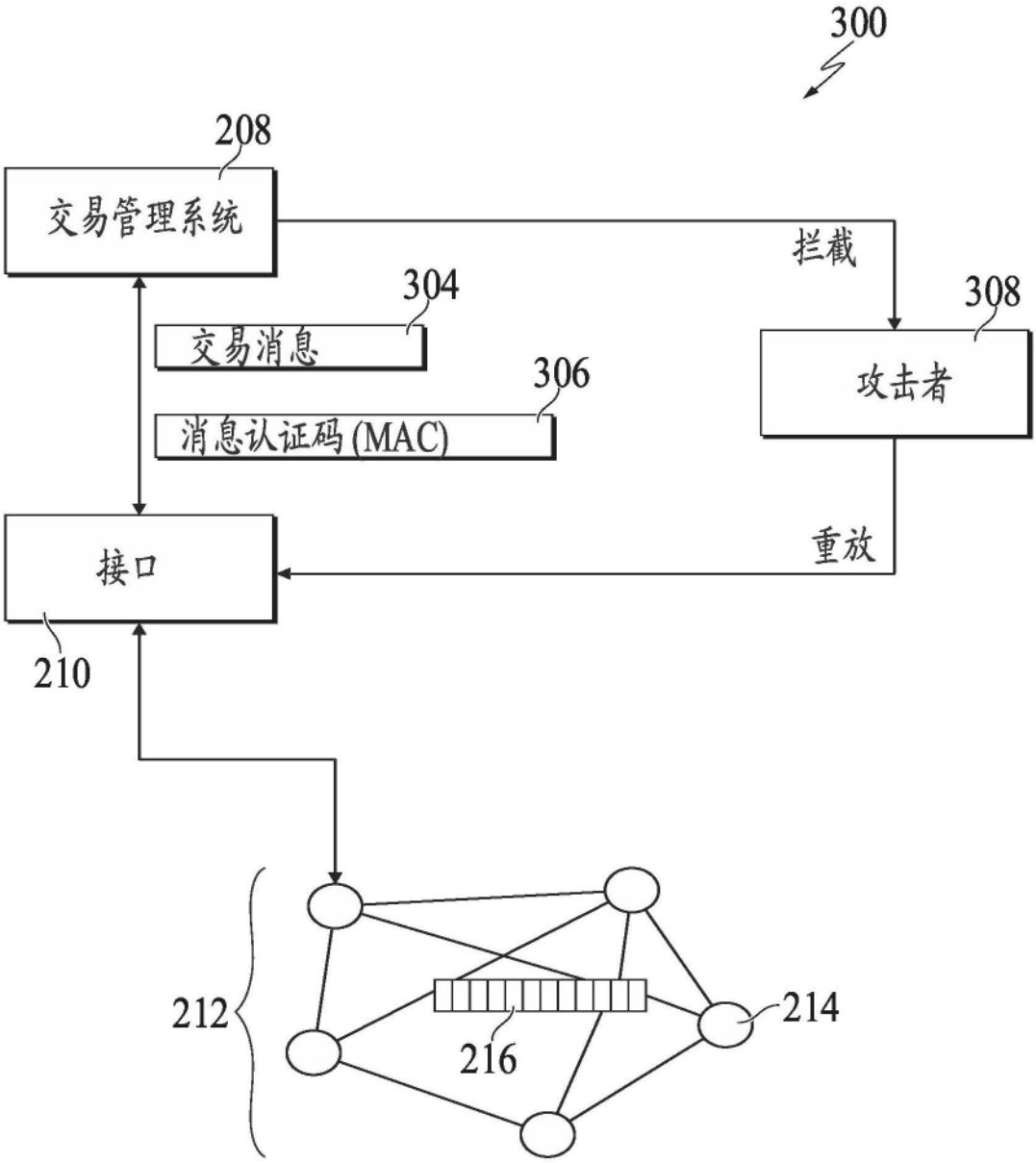

300
208
交易管理系统
拦截
304
交易消息
308
攻击者
306
消息认证码(MAC)
接口
重放
210
212
214
216

图3

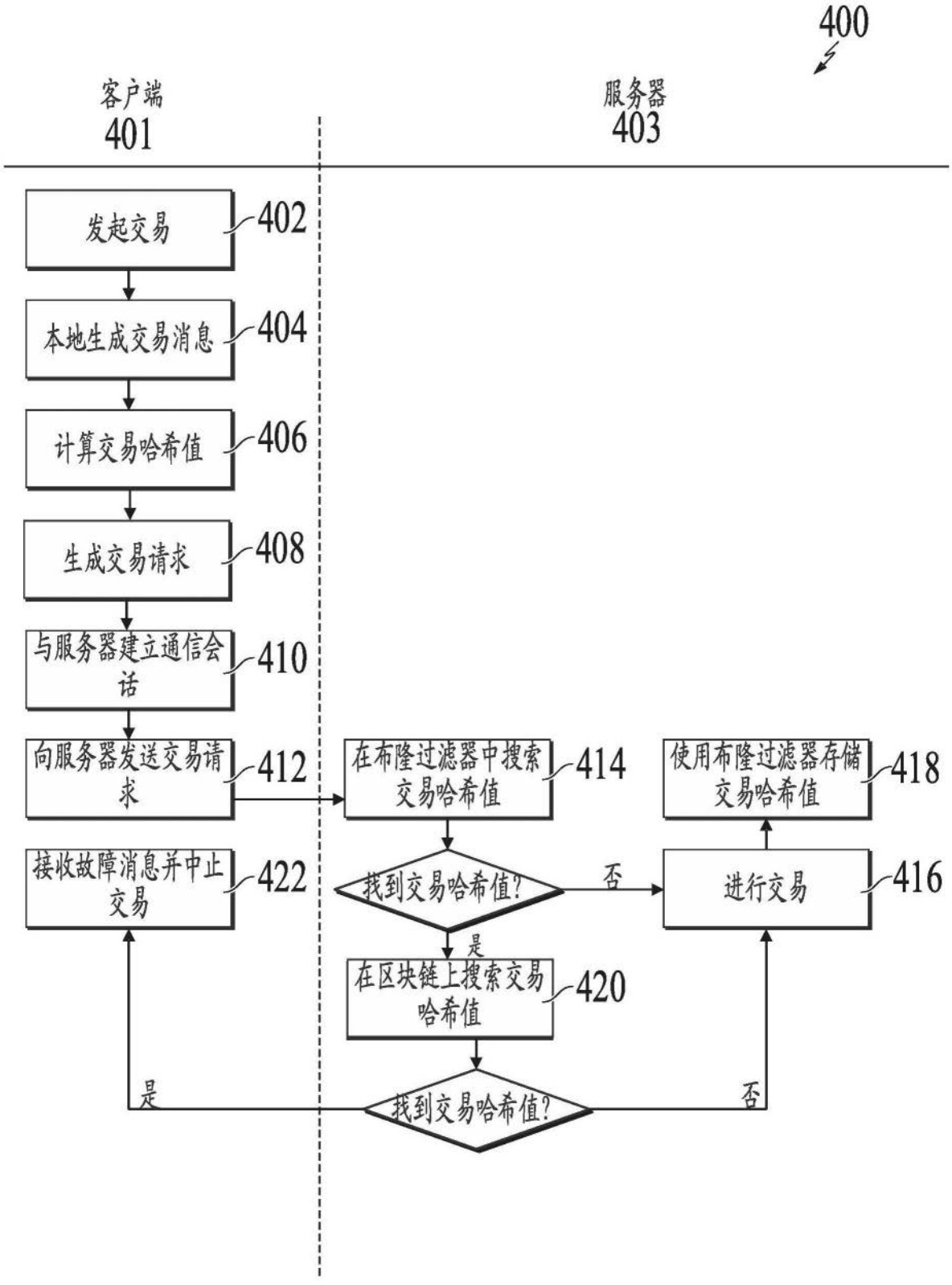

400
客户端
401
服务器
403
发起交易
402
本地生成交易消息
404
计算交易哈希值
406
生成交易请求
408
与服务器建立通信会话
410
向服务器发送交易请求
412
接收故障消息并中止交易
422
在布隆过滤器中搜索交易哈希值
414
找到交易哈希值?
否
是
进行交易
416
使用布隆过滤器存储交易哈希值
418
在区块链上搜索交易哈希值
420
找到交易哈希值?
是
否

图4

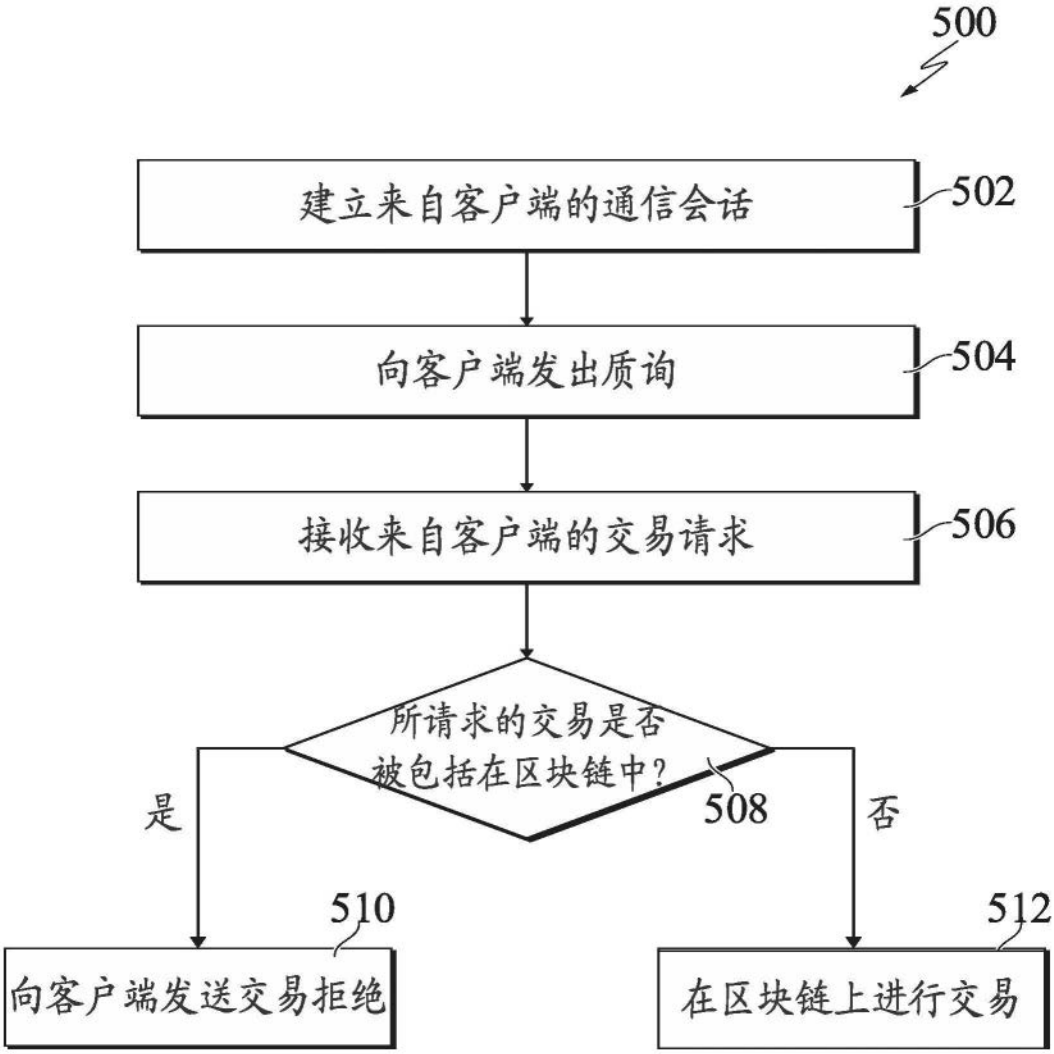

500
建立来自客户端的通信会话
502
向客户端发出质询
504
接收来自客户端的交易请求
506
所请求的交易是否
被包括在区块链中?
508
是
否
510
向客户端发送交易拒绝
512
在区块链上进行交易

图5

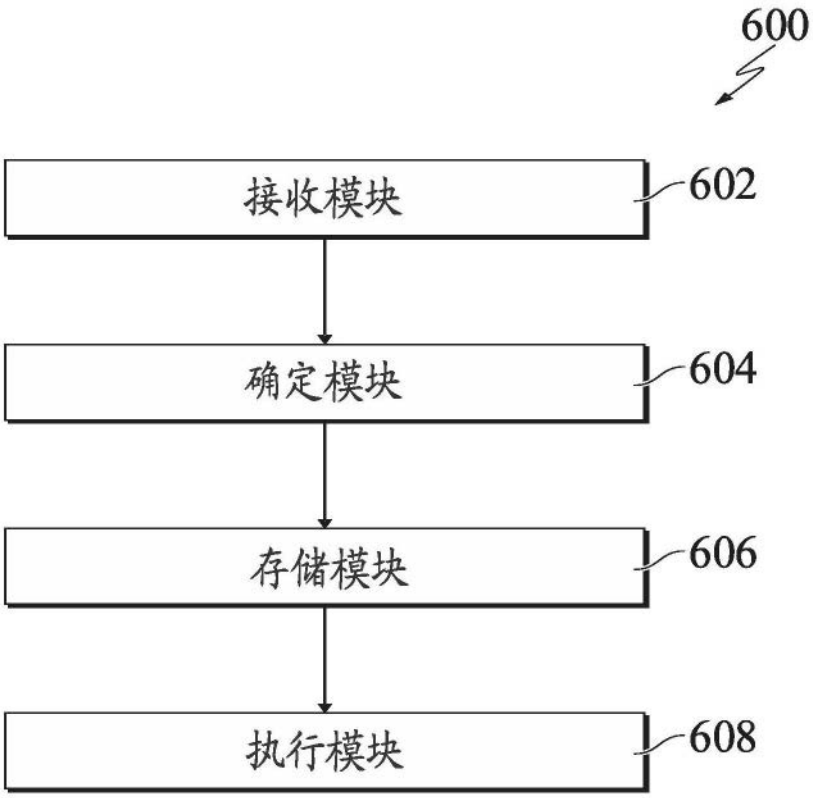


图6