(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110537355 B
(45)授权公告日 2022.06.17

(21)申请号 201880026072.X
(22)申请日 2018.04.16
(65)同一申请的已公布的文献号
申请公布号 CN 110537355 A
(43)申请公布日 2019.12.03
(30)优先权数据
1706132.6 2017.04.18 GB
(85)PCT国际申请进入国家阶段日
2019.10.18
(86)PCT国际申请的申请数据
PCT/IB2018/052619 2018.04.16
(87)PCT国际申请的公布数据
WO2018/193355 EN 2018.10.25
(73)专利权人 区块链控股有限公司
地址 安提瓜和巴布达圣约翰
(72)发明人 P·希门尼斯-德尔加多
(74)专利代理机构 隆天知识产权代理有限公司 72003
专利代理师 石海霞 李晔
(51)Int.Cl.
H04L 67/10(2022.01)
H04L 12/18(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 106548091 A,2017.03.29
CN 106385319 A,2017.02.08
CN 105719185 A,2016.06.29
CN 106534097 A,2017.03.22
CN 105939331 A,2016.09.14
US 2016292672 A1,2016.10.06
US 2016261404 A1,2016.09.08
u2.RANDAO:A DAO working as RNG of Ethereum.《https://github.com/randao/randao》.2016,

审查员 刘莹

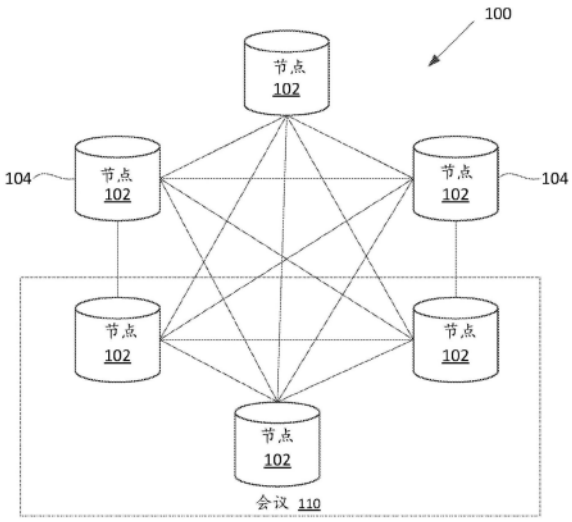
权利要求书2页 说明书20页 附图9页

(54)发明名称

基于安全区块链的共识

(57)摘要

可以提供一种计算机实现的方法。该计算机实现的方法包括:i)由区块链网络中的节点向会议池广播交易,以加入由节点群组形成的会议;ii)在会议已接受来自请求者的激活脚本的请求之后,由节点准备以与会议相关联的公钥加密地锁定的区块链交易;iii)通过所述节点与所述节点群组中的其他节点合作而合作地生成用于该交易的有效加密签名以耗用该交易;iv)在区块链交易已被解锁之后,从多个信息提供系统接收数据;v)确定从多个信息提供系统接收到的数据的中心点;以及vi)通过所述节点与所述节点群组中的其他节点合作而基于中心点激活脚本。



CN 110537355 B

1.一种计算机实现的方法,包括:

由区块链网络中的节点向会议池广播交易,以加入由节点群组形成的会议;

在所述会议已接受来自请求者的激活脚本的请求之后,由所述节点准备以与所述会议池相关联的公钥加密锁定的区块链交易,所述区块链交易被配置成允许多个信息提供系统向该区块链交易添加输入,其中,所述输入包括相应的解决方案数据证明;

在所述输入已被添加到所述区块链交易之后,由所述节点与所述群组中的其他节点合作而合作地生成用于所述区块链交易的有效加密签名以解锁所述区块链交易;

在所述交易已被解锁之后,从所述多个信息提供系统接收数据;

基于所述解决方案数据证明确定从至少一个所述信息提供系统接收到的数据对应于已提交的解决方案;

响应于基于所述解决方案数据证明确定从至少一个所述信息提供系统接收到的数据不与已提交的解决方案相对应,所述方法还包括:

确定从所述多个信息提供系统接收到的所述数据的中心点;

由所述节点与所述会议的其他节点合作而基于所述中心点激活所述脚本;以及

响应于基于所述解决方案数据证明确定从至少一个所述信息提供系统接收到的数据不与已提交的解决方案相对应而丢弃所述数据。

2.根据权利要求1所述的计算机实现的方法,还包括:

由所述节点基于所述中心点对提供接近所述中心点的数据的所述信息提供系统的子集进行识别;以及

由所述节点与所述群组中的其他节点合作授权将令牌转移到所述子集中的每个信息提供系统。

3.根据权利要求2所述的计算机实现的方法,其中,包括在所述转移中的所述令牌包括从所述请求者接收到的进入所述会议池中的一个或多个令牌。

4.根据权利要求2或3所述的计算机实现的方法,其中,所述请求包括阈值指示符,并且其中,所述子集是基于所述阈值指示符而被识别的。

5.根据权利要求4所述的计算机实现的方法,其中,所述阈值指示符是从所述请求者接收到的。

6.根据权利要求1所述的计算机实现的方法,其中,所述输入包括出于安全而待锁定的令牌。

7.根据权利要求1所述的计算机实现的方法,其中,所述信息提供系统在所述区块链交易中包括基于公钥的散列、所述请求的解决方案、和盐值。

8.根据权利要求7所述的计算机实现的方法,其中,从所述多个信息提供系统接收到的数据包括所述公钥、所述请求的所述解决方案和所述盐值,所述方法还包括:

基于所述公钥、所述请求的解决方案和所述盐值生成散列;以及

将所生成的散列与包括在所述区块链交易中的散列进行比较。

9.根据权利要求1所述的计算机实现的方法,其中,还包括:

检测恶意方的恶意活动,其中所述恶意方为所述会议的所述节点之一;以及

使用私钥份额来没收由所述恶意方先前转移到所述会议池的令牌之中的至少一部分。

10.根据权利要求9所述的计算机实现的方法,其中,没收包括转移到不可耗用帐户。

11.一种计算机可读存储介质,包括计算机可执行指令,所述计算机可执行指令在被执行时配置处理器以进行权利要求1至10中任一项所述的方法。

12.一种电子装置,包括:

接口装置;

处理器,耦接到所述接口装置;

存储器,耦接到所述处理器,所述存储器上存储有计算机可执行指令,所述计算机可执行指令在被执行时配置所述处理器以进行权利要求1至10中任一项所述的方法。

13.根据权利要求12所述的电子装置,其中,所述处理器包括可信执行环境,并且其中,所述计算机可执行指令在所述可信执行环境内执行。

基于安全区块链的共识

技术领域

[0001] 本发明一般涉及分布式账本，更具体而言，涉及用于激活与这样的分布式帐本相关联的脚本的方法和系统。本发明特别适合用于基于分布式帐本上不可用的信息来激活这样的脚本，但不限于此。

背景技术

[0002] 在本文中，我们使用术语“区块链”来包括所有形式的电子、基于计算机的分布式账本。它们包括区块链和交易链技术、许可的账本和未经许可的账本、共享账本及其变体。区块链技术最广为人知的应用是比特币账本，但是也提出并开发了其他区块链实施方式。虽然本文中出于方便和说明的目的可以引用比特币，但是应当注意，本发明不限于与比特币区块链一起使用，替代性的区块链实施方式和协议也落入本发明的范围内。

[0003] 区块链是一种基于共识的电子账本，它被实现为基于计算机的分散式、分布式系统，该系统由区块组成，而区块相应地由交易和其他信息组成。对于比特币而言，每个交易是一个数据结构，该数据结构对区块链系统中的参与者之间的数字资产的控制转移进行编码，并包括至少一个输入和至少一个输出。每个区块包含前一个区块的散列，以致于这些区块变为链接在一起，以创建自区块链开始以来就已经写入区块链的所有交易的永久、不可更改的记录。交易包含嵌入其输入和输出中称为脚本的小程序，它们指定如何以及通过谁来访问交易的输出。在比特币平台上，这些脚本是使用基于堆栈的脚本语言来编写的。

[0004] 为了将交易写入区块链，必须对其进行“验证”。某些网络节点充当矿工并进行工作以确保每次交易都有效，而无效交易从网络中被拒绝。例如，安装在节点上的软件客户端对引用的的交易以及未耗用的交易输出(UTXO)进行该验证工作。可通过执行其锁定和解锁脚本来进行验证。如果锁定和解锁脚本的执行评估为TRUE，并且如果满足某些其他条件(例如包括足够的开采费用)，则交易有效并且可以被写入区块链。因此，为了将交易写入区块链，该交易必须i)由接收交易的节点来验证-如果交易被验证，则节点将其中继到网络中的其他节点；ii)被加入由矿工建造的新区块；iii)被开采，即加入过去交易的公共账本。当向区块链添加足够数量的区块以使交易实际上不可逆时，认为交易被确认。

[0005] 虽然区块链技术由于加密货币实现方式的使用而广为人知，但是数字企业家已经开始探索比特币所基于的加密安全系统以及可以存储在区块链上以实现新系统的数据这两者的使用。如果区块链可用于并不限于加密货币领域的自动化任务和过程，这将是非常有利的。这样的解决方案将能够利用区块链的好处(例如，事件的永久性、防篡改记录，分布式处理等)，同时在其应用中更通用。

[0006] 区块链技术已经被用于提供用于智能合约的平台。智能合约是执行合同条款的计算机化交易协议。当在区块链上实现时，智能合约是存储在区块链上并且由区块链交易触发的计算机化协议，该计算机化协议在被执行时可以使数据写入到区块链。当在区块链上实现时，智能合约对于区块链网络的所有用户都是可见的。

[0007] 智能合约通常必须由消息或交易激活。也就是说，智能合约通常必须由外部代理

触碰(poke)而用于待执行的代码。此外,智能合约通常不能访问区块链本身之外的信息。在不访问这样的信息的情况下,智能合约可能不能够确定合同的哪些条款将被执行/实施。为了获得这样的外部信息,有时使用可信外部代理来提供对于区块链之外且对于智能合约来说是所需的信息的访问。对可信外部代理的依赖降低了智能合约的自主性和自执行特性。对可信外部代理的依赖可能会降低智能合约的安全性和可用性。

发明内容

[0008] 因此,根据本发明,提供一种如所附权利要求限定的方法。

[0009] 如下更详细所述,可以在区块链网络上形成会议(congress)。会议可以是开放成员资格群组,区块链网络中的任何节点可以在向与会议相关联的池提交足够的权益时加入该开放成员资格群组。例如,节点可通过将诸如数字货币(例如比特币)、令牌或其他权益或价值的数字资产转移到与会议相关联的账户来加入会议。有利地,会议可以用于安全地激活诸如智能合约之类的脚本。例如,会议可以用于将数据从外部源可靠地提供到脚本。该会议可以用于在其中节点之间的消息转移是不安全的的分布式系统中安全地达成共识。例如,会议可以将数据从外部源可靠地提供到脚本,并且数据可以被安全地提供,即使会议中的节点之间的通信可能不安全亦是如此。

[0010] 因此,根据本发明,可以提供一种计算机实现的方法。该计算机实现的方法可以包括:i)由区块链网络中的节点向会议池广播交易,以加入由节点群组形成的会议;ii)在会议已经从请求者接受激活脚本的请求之后,由节点准备可支付给会议池的交易,该交易被配置成允许多个信息提供系统向交易添加输入;iii)在输入已被添加到交易之后,由该节点与节点群组中的其他节点合作而合作地生成用于交易的有效签名以耗用该交易;iv)在交易已经被耗用之后,从多个信息提供系统接收数据;v)确定从多个信息提供系统接收到的数据的中心点;vi)由该节点与节点群组中的其他节点合作而基于中心点激活脚本。

[0011] 在一些实施方式中,提供了一种计算机实现的方法。该计算机实现的方法可以包括:i)由区块链网络中的节点向会议池广播交易,以加入由节点群组形成的会议;ii)在会议已经从请求者接受激活脚本的请求之后,由节点准备以与会议相关联的公钥加密地锁定的区块链交易,该区块链交易被配置成允许多个信息提供系统向区块链交易添加输入;iii)在输入已被添加到区块链交易之后,由该节点与节点群组中的其他节点合作而合作地生成用于交易的有效签名以解锁区块链交易;iv)在交易已被解锁之后,从多个信息提供系统接收数据;v)确定从多个信息提供系统接收到的数据的中心点;vi)由该节点与节点群组中的其他节点合作而基于中心点激活脚本。

[0012] 在一些实施方式中,计算机实现的方法包括:i)由所述节点基于所述中心点对提供接近中心点的数据的信息提供系统的子集进行识别;以及ii)由所述节点与所述群组的其他节点合作授权将数字资产(即,令牌)转移到该子集中的每个信息提供者(即,转移到该子集中的每个信息提供系统)。

[0013] 在一些实施方式中,包括在转移中的数字资产(即,令牌)包括从请求者接收到的进入会议池的一个或更多个数字资产(即,令牌)。在一些实施方案中,请求包括阈值指示符,并且其中,子集是基于阈值指示符来识别的。可以从请求者接收阈值指示符。

[0014] 在一些实施方式中,对交易的输入(即,对区块链交易的输入)包括相应的解决方

案数据证明，并且该方法包括基于解决方案数据证明确定从所述信息提供系统中的至少一个信息提供系统接收到的数据对应于已提交的解决方案。

[0015] 在一些实施方式中，对交易的输入(即，对区块链交易的输入)包括解决方案数据的相应证明，并且该方法还包括：i)确定从所述信息提供系统中的至少一个信息提供系统接收到的数据不与从该信息提供系统接收到的解决方案数据证明相对应；以及响应于基于所述解决方案数据证明确定出从所述信息提供系统中的所述至少一个信息提供系统接收的所述数据不与已提交的解决方案相对应而丢弃所述数据。

[0016] 在一些实施方式中，对交易的输入包括作为安全存款(即，出于安全而被锁定)而持有的数字资产(即，令牌)。

[0017] 在一些实施方式中，信息提供系统在交易中(即，在区块链交易中)包括基于公钥的散列、请求的解决方案和盐值，并且在一些实施方案中，从多个信息提供系统接收的数据包括公钥、请求的解决方案和盐值。该方法还可以包括：i)基于公钥、请求的解决方案和盐值生成散列；以及ii)将所生成的散列与包括在交易中(即，在区块链交易中)的散列进行比较。

[0018] 在一些实施方式中，计算机实现的方法还包括：i)检测恶意方的恶意行为，恶意方为会议的节点之一；以及ii)使用私钥份额来没收由所述恶意方先前转移到所述会议池的令牌的至少一部分。没收可以包括转移到不可耗用帐户。

[0019] 根据本发明，可以提供一种电子设备。该电子设备包括接口设备、耦接至接口设备的处理器、和耦接至处理器的存储器。存储器上存储有计算机可执行指令，该计算机可执行指令在被执行时配置处理器以进行本文所述的方法。

[0020] 根据本发明，可以提供一种计算机可读存储介质。所述计算机可读存储介质包括计算机可执行指令，所述计算机可执行指令在被执行时配置处理器以进行本文所述的方法。

附图说明

[0021] 参考本文所述的实施方案，本发明的这些和其他方案将变得显而易见并得以阐明。下面仅通过示例并参考附图来描述本发明的实施例，其中：

[0022] 图1示出示例性区块链网络的方框图。

[0023] 图2示出可以充当区块链网络中的节点的示例性电子装置的方框图。

[0024] 图3是发起会议的示例性方法的流程图。

[0025] 图4是加入会议的示例性方法的流程图。

[0026] 图5是没收数字资产的示例性方法的流程图。

[0027] 图6是重新分配密钥份额的示例性方法的流程图。

[0028] 图7是重新分配密钥份额的另一个示例性方法的流程图。

[0029] 图8是返回存款的示例性方法的流程图。

[0030] 图9是示例区块链网络的框图。

[0031] 图10是用于请求激活脚本的示例方法的流程图。

[0032] 图11是用于促进脚本的激活的示例方法的流程图。

具体实施方式

[0033] 区块链网络

[0034] 首先参考图1。图1以方框图形式示出与区块链相关联的示例性区块链网络100。区块链网络可以是公共区块链网络，它是一个点对点的开放成员网络，任何人可以加入其中，无需邀请或经过其他成员同意。运行区块链协议(区块链网络100在该协议下操作)的实例的分布式电子装置可以参与区块链网络100。这种分布式电子装置可称为节点102。区块链协议例如可以是比特币协议。

[0035] 运行区块链协议且形成区块链网络100的节点102的电子装置可以是各种类型的装置，例如包括台式计算机、膝上型计算机、平板计算机、服务器、诸如智能电话这样的移动装置、诸如智能手表这样的可穿戴计算机、或其他电子装置。

[0036] 区块链网络100的节点102使用合适的通信技术相互耦接，所述通信技术可包括有线和无线通信技术。这种通信遵循与区块链相关联的协议。例如，在区块链是比特币区块链的情况下，可以使用比特币协议。

[0037] 节点102维护区块链上所有交易的全局账本。因此，全局账本是分布式账本。每个节点102可以存储全局账本的完整副本或部分副本。对于通过工作量证明来保护的区块链，影响全局账本的节点102的交易由其他节点102验证，从而维护全局账本的有效性。当区块链是基于工作量证明的区块链时，也通过检查随区块提交的工作量证明来证实区块。

[0038] 至少一部分节点102作为区块链网络100的矿工104操作。图1的区块链网络100是工作量证明区块链，其中矿工104执行昂贵的计算，以便促进区块链上的交易。例如，工作量证明区块链可能要求矿工解决加密问题。在比特币中，矿工104找到一个随机数，使得区块头部通过SHA-256散列到一个小于当前难度所定义的值的数字。工作量证明算法所需的散列功率意味着在一定数量的区块在其顶部被开采之后，交易被认为实际上是不可逆的。解决加密问题的矿工104为区块链创建新区块，并将新区块广播到其他节点102。在接受应该将区块添加到区块链之前，其他节点102证实矿工104实际上已经解决了加密问题并因此展示了足够的工作量证明。通过节点102的共识将区块添加到区块链(即，添加到分布式全局账本)。

[0039] 矿工104创建的区块包括已经由节点102广播到区块链的交易。例如，区块可包括从与节点102的其中一个相关联的地址到与节点102的其中另一个相关联的地址的交易。通过这种方式，区块充当从一个地址到另一个地址的交易的记录。要求该交易被包括在区块中的一方证明：他们被授权通过使用与其公钥相对应的私钥对请求进行签名来发起转移(例如，在比特币的情况下，耗用比特币)。如果请求被有效地签名，则仅将转移添加到区块中。

[0040] 对于比特币而言，在公钥和地址之间存在一对一对应关系。也就是说，每个公钥与单个地址相关联。因此，本文中对于将数字资产转移至公钥或从公钥转移数字资产(例如，支付到公共密钥中)以及将数字资产转移至与所述公共密钥相关联的地址或从所述地址转移数字资产的任何引用都指的是共同的操作。

[0041] 有些节点102可能不是作为矿工操作，而是作为验证节点参与。交易验证可能涉及检查(一个或多个)签名、确认对有效UTXO的引用等。

[0042] 图1的示例包括五个节点102，其中三个作为矿工104参与。实际上，节点102或矿工

104的数量可以不同。在很多区块链网络中，节点102和矿工104的数量可以远大于图1所示的数量。

[0043] 如下所述，各种节点102可以合作形成将在本文中称为会议110的群组。在所示示例中，将三个节点102示出为会议110的参与方。但是，会议110成员的实际数量可能大得多。

[0044] 会议110是开放成员群组，它可以由任何节点102在向与会议110相关联的池提交足够的权益时加入。例如，节点可通过向与会议110相关联的账户转移数字资产(诸如数字货币(例如比特币)、令牌、或其他权益或价值)来加入会议。加入会议的节点102可以是区块链网络中的任何节点，包括采矿节点和非采矿节点。在会议的至少一部分应用中，充当会议成员的节点在他们下载(但不一定保留)完整区块链的意义上监视区块链。

[0045] 下面更详细地讨论用于加入、离开和参与会议110的技术。

[0046] 作为节点操作的电子装置

[0047] 图2是示出示例性电子装置200的组件的方框图，示例性电子装置200可以充当点对点区块链网络100(图1)中的节点102(图1)。示例性电子装置200也可称为处理装置。电子装置可以采用各种形式，例如包括台式计算机、膝上型计算机、平板计算机、服务器、诸如智能手机这样的移动装置、诸如智能手表这样的可穿戴计算机、或其他类型的形式。

[0048] 电子装置200包括处理器210、存储器220和接口装置230。这些组件可以直接或间接地相互耦接并且可以相互通信。例如，处理器210、存储器220和接口装置230可以经由总线240相互通信。存储器220存储计算机软件程序，其包括用于进行本文所述功能的机器可读指令和数据。例如，存储器可包括处理器可执行指令，当通过处理器210执行时，可执行指令使得电子装置进行本文所述的方法。处理器可执行指令可包括指令，当由处理器210执行时，该指令使得电子装置实现与区块链网络100(图1)相关联的协议。例如，指令可包括用于实现比特币协议的指令。

[0049] 存储器220可以存储区块链网络100(图1)的全局账本或其一部分。也就是说，存储器220可以存储区块链的所有区块或一部分区块，例如最新的区块，或者一些区块中的一部分信息。

[0050] 虽然存储器220在图2中用单个方框示出，但是实际上，电子装置200可包括多个存储器组件。存储器组件可以是各种类型，例如包括RAM、HDD、SSD、闪存驱动器等。不同类型的存储器可以适合于不同的目的。此外，虽然存储器220与处理器210分开示出，但是处理器210也可包括嵌入式存储器。

[0051] 如图2所示，处理器210可包括诸如可信执行环境(TEE)250这样的安全区域。TEE 250是隔离执行环境，其为电子装置200提供额外的安全性，例如隔离执行、可信应用的完整性和资产机密性。TEE 250提供了这样的执行空间：该执行空间保证在TEE 250内加载的计算机指令和数据在机密性和完整性方面受到保护。TEE 250可用于保护重要资源(例如密钥)的完整性和机密性。TEE 250至少部分地在硬件级别实现，使得在TEE 250内执行的指令和数据受到保护，以防止来自电子装置200其余部分以及诸如电子装置的所有者这样的外方的访问和操纵。TEE 250内的数据和计算从操作包括TEE 250的节点102的一方得到保护。

[0052] TEE 250可以操作以将飞地实例化，然后一次一个添加存储器的页面，同时累积地进行散列。也可以在远程机器(可以是开发者机器或另一个机器)上进行类似的操作，以便远程机器确定并存储预期的散列。因此，飞地的内容可以由任何远程机器证实，以确保飞地

运行批准的算法。可通过比较散列来进行证实。飞地完全建成后，将其锁定。可以在TEE 250中运行代码并向代码发送秘密，但代码不能更改。最终散列可通过证明密钥来进行签名，并且可使其对于数据所有者可用，以在数据所有者向飞地发送任何秘密之前证实它。

[0053] TEE 250可用于保护与由会议110(图1)使用的会议公钥相关联的私钥份额的机密性和完整性。例如，TEE 250可以用于私钥份额的生成和存储。TEE 250目的是确保没有成员能够直接获得在TEE 250飞地内保持的私钥份额，或者通过成员间通信或跨飞地通信获得关于其他私钥份额的信息。协议对于飞地阈值的损害也是稳健的。此外，TEE 250可以启用远程证明，该远程证明可以由节点102(图1)用来向其他节点102证明TEE 250是可信的并且正在运行用于会议110所实施的协议的、被批准的计算机可执行指令。远程证明可以由TEE 250通过运行特定代码段并在飞地内部发送该代码的散列来提供，代码的散列由用于飞地的内部证明密钥签名。

[0054] 当先前在电子装置200上使用私钥份额的会议110的成员选择离开会议时，TEE 250可用于证明私钥份额的安全删除。电子装置200可通过TEE 250中提供的远程证明协议向其他会议成员提供删除证明。在允许成员撤回其成员存款之前，可能需要删除证明。也就是说，存款的返回可以以证明成员的飞地内的私人密钥份额的删除为条件。

[0055] TEE 250可以配备有安全随机数发生器，安全随机数发生器是在TEE的飞地内部，其可用于生成私钥、随机询问、或其他随机数据。TEE 250还可以被配置为从外部存储器读取数据，并且可以被配置为将数据写入外部存储器。这些数据可通过仅在飞地内部保持的秘密密钥加密。

[0056] 可以使用各种平台(诸如可信平台模块(TPM)或英特尔软件保护扩展(SGX))来实现TEE 250。例如，SGX支持远程证明，这使得飞地能够从正在执行特定飞地的处理器获取签名的声明，所述特定飞地具有称为引用的给定成员。诸如英特尔证明服务(IAS)这样的第三方证明服务可以证明这些签名的声明源自符合SGX规范的可信CPU。

[0057] 电子装置200充当区块链网络100(图1)中的节点102(图1)，并且可以加入或者以其他方式参加会议110(图1)。当一组数字资产持有者汇集数字资产(例如数字货币、令牌或区块链网络100(图1)支持的其他权益或价值)时，会议110形成。

[0058] 会议和阈值签名

[0059] 会议110可以是许可或非许可群组。也就是说，区块链网络100(图1)中的任何节点102(图1)(即，通过监视和存储区块链中的至少一部分信息的任何节点)可以加入会议110。为了加入会议110，节点102将一个或多个数字资产转移到与会议110相关联的数字资产池(即，转移到与一个或多个数字资产相关联的公共群组地址，该一个或多个数字资产相应地与其他成员相关联)。该数字资产池可被称为会议池。例如，节点102可通过将这样的数字资产转移(即，存放)到与会议池相关联的地址(即，转移到又可称为公共群组地址的“会议地址”)来加入会议110。数字资产被置于具有单个公钥(称为会议公钥)的群组阈值签名的控制之下。会议议员持有分布式产生的私钥份额。持有的份额数量可以与存放在池中的金额成比例。

[0060] 由会议110控制的数字资产(包括转移到会议地址的任何数字资产)被置于阈值签名方案的控制之下。在阈值签名方案下，需要一组总私钥份额持有超过阈值的成员来产生有效签名，该签名允许数字资产被转移离开会议110的控制。即，必须将至少阈值数量的私

钥份额生成有效签名用于为会议110控制的数字资产的任何向外转移。

[0061] 会议公钥阻碍会议110的成员存放在会议池中的以换取私钥份额的数字资产,以及通过会议110的成员或非成员存放在与会议池相关联的地址的任何数字资产(即,在会议的全部、部分、或有条件控制下放置)(该任何数字资产由于获得私钥份额之外的原因而已经被存放)。非成员或成员可出于各种原因将数字资产存放在与会议相关联的地址。在下面更详细解释的一个示例中,成员或非成员可将数字资产存入会议110,以将这些资产移动到另一个区块链,另一个区块链可称为替代链,例如侧链。侧链可以是与主区块链平行(即平行于主链)运行的区块链。

[0062] 因为同一会议公钥可以控制成员存款(即由会议成员提供的以换取私钥份额的数字资产)以及成员或非成员处于其他目的提供的数字资产,所以到与会议相关联的地址的至少一部分存款可能会被特别标记,以表明存款的类型。例如,将数字资产转移到会议地址的交易可包括标记、标识符或指示正在进行的存款的性质的其他属性。举例来说,不是为了加入会议或增加会议成员资格中权益的目的而进行的将数字资产转移到会议地址的交易可包括特殊标识符,以指示存款是为了其他目的而进行的。在管理私钥生成时,可通过与会议110相关联的节点102来使用这些标识符。更具体而言,为了加入群组而存放数字资产的节点102被分配用于会议110的私钥份额(作为进行数字资产存放的结果),而为了其他目的(例如,转移到侧链)存放数字资产的其他节点102不一定持有会议的会议私钥份额(即,对应于会议公钥)。

[0063] 会议110可以充当自治群组,其中通过没收全部或部分成员存款的威胁来强制执行合作行为。非合作或恶意成员可能由于加入由很多诚实成员参与的合作协议而被没收这种数字资产。也就是说,为了确保所有节点102都按照预定协议或准则进行操作,进入会议池的成员存款可能会被没收。没收意味着永久阻止被视为没收的成员存款的返回。形成由于恶意活动而未返回的成员存款的(一个或多个)数字资产可以留在会议池中但不返回(例如,如果达成共识(在替代链上)它们不应该被返回),立即或在将来被转移到另一个不可耗用的地址,或以其他方式没收,并且没收的性质可能取决于会议是否充当用于侧链的担保验证者集合(bonded validator set)。

[0064] 此外,当会议成员希望离开会议110时,他们可以撤回其成员存款(即,要求会议110将成员存款转移回该成员的个人地址)。但是,仅当群组成员(即会议)使用多个私钥份额(其数量超过生成有效数字签名所需的阈值)来批准撤回时才进行资金的撤回。

[0065] 会议110实现的阈值签名方案可以是各种类型。阈值签名方案允许在n方之间共享签名权,只要至少阈值数量的私钥份额有助于生成有效签名。小于阈值的任何子集都不能生成有效签名。更具体而言,每一方都控制私人签名密钥的份额,并且必须使用阈值数量的密钥份额、通过组合部分签名来生成有效签名。任何小于阈值的密钥份额子集都不能生成有效签名。

[0066] 阈值签名方案可以是椭圆曲线数字签名算法(ECDSA)方案。例如,ECDSA方案可以是Ibrahim等人在“A robust threshold elliptic curve digital signature providing anew verifiable secret sharing scheme”,2003 EIII 46th Midwest Symposium on Circuits and Systems,1:276-280(2003)中提出的类型。该阈值签名方案是数字签名方案的扩展,其是基于椭圆曲线加密的算法,其中需要来自n个密钥份额持有者一方的t+1个密

钥份额来重建私钥。该方案可用于构建有效签名，而无需重建私钥，并且没有任何一方必须向另一方透露其密钥份额。

[0067] 因为t+1密钥份额足以重建秘密，所以根据该技术的最大允许对手(adversary)数量为t。在Ibrahim等人的模型中，对手是一个破坏持有秘密份额的一方并可以访问该秘密份额的实体。对手可以是各种类型。例如，拜占庭对手是可能假装参与协议而实际上他们发送不正确的信息的对手。Ibrahim提出的ECDSA方案对于高达t<＝n/4个恶意对手是稳健的。这种稳健性可以上升到t<＝n/3，但代价是更高的复杂性。

[0068] Ibrahim等人的ECDSA方案对于阻止t<＝n/3个阻止对手是稳健的。阻止对手能够防止破坏方参与协议或中途停止参与。

[0069] 该ECDSA方案包括可由节点102用来识别恶意或不合作方的各种机制。例如，可验证的秘密共享(VSS)可用于共享Shamir秘密共享(SSS)所需的多项式。SSS是一种秘密共享的形式，其中将秘密分成若干部分并将其各自独有的部分提供给每个参与者。这些部分可用于重建秘密。在不一致的份额被提供给不同节点102的情况下，或者在将与广播至所有节点的盲目份额不同的份额秘密地发送到节点的情况下，节点102可以使用VSS来识别恶意节点102或成员。可通过节点102中的任何一个来识别不一致的份额。可通过包括允许节点102将其份额验证为一致的辅助信息来使得可以验证秘密的共享。

[0070] 向个别节点发送不正确的份额(即，与广播的盲目份额不同的份额)可以被份额的预期接收节点识别。被秘密发送到节点的不正确份额的识别可以使用公共可验证的秘密共享(PVSS)技术公开验证。这样的技术可以避免在不使用PVSS的情况下可能发生的欺骗发送者的识别时出现的可能延迟，并且在发送不正确的份额时，不正确份额的接收者离线或从网络的实质部分切断。

[0071] 诸如向不同节点提供不一致份额的不当行为可以由会议110解决，以阻止恶意行为。例如，当节点102(图1)被其他节点102识别为恶意方时，超过阈值(例如，t+1)的多个节点102(即，与会议成员相关联的节点)可以合作惩罚恶意方。例如，节点102可以采取涉及由恶意方存放到会议的数字资产(诸如数字货币、令牌或其他权益或价值)的动作。例如，会议可通过将数字货币、令牌、权益或价值转移到不可耗用的地址来烧毁它们，或者会议可通过与其他节点达成共识来没收这些数字资产以拒绝对这些数字资产到恶意方的返回进行授权。非不当行为节点的节点102还可通过合作排除不当行为节点来阻止不当行为(例如，通过有效地将密钥份额无效；例如，通过将节点从参与会议协议中排除，或通过重新共享私钥而不是向不当行为节点分配份额)。

[0072] 可通过使用TEE来增强上述ECDSA技术。例如，基于Ibrahim等人的阈值ECDSA签名技术考虑一种强大的对手形式，在这里称为拜占庭对手。这种类型的对手可以任意行为，例如，他们不仅拒绝参与签名过程或中途停止参与，而且还可能假装诚实地参与并发送不正确的信息。但是，通过使用TEE，并产生用于在存储秘密的私钥份额的TEE的飞地内签名的数据，可以提供额外的安全性，因为极不可能大量损害飞地。例如，如果每个TEE被分配不超过一个密钥份额，那么可以合理地预期可能受损的TEE的数量不接近拜占庭对手的稳健性阈值，假设n足够大。这允许协议是安全的，如果相对于密钥份额的总数，它可以容忍一小部分恶意对手。

[0073] 例如，如果所有节点都具有TEE，则只有在TEE的制造商未被破坏的情况下，并且只

能通过很大的努力和费用才能通过对节点的物理访问来实现对存储在飞地内的秘密的获取。这种制造商等级的破坏预计是可管理的。例如，如果制造商错误地声称很多公钥对应于真正的TEE，则他们可以直接访问私钥份额，并可能发起攻击。但是，这种攻击需要足够数量的密钥份额，以允许制造商在没有其他节点帮助的情况下产生有效签名。这将意味着累积大部分的总权益，这将是非常昂贵的。此外，通过实施攻击，将摧毁权益持有的大部分价值。

[0074] 当使用TEE时，考虑协议对“破坏的节点”的稳健性是有用的。破坏的节点使得TEE外部的硬件被破坏，但TEE的完整性未受损害。破坏的节点可以控制飞地接收和不接收什么信息。具体而言，破坏的节点可以停止、即避免参与协议。如果要求提供给协议的信息通过在飞地(其中在证明期间认证对应的公钥)中秘密持有的私钥来签名，则私钥与飞地本身一样可信。因此，破坏的节点不能向协议发送任意(认证的)信息，并且可能仅通过停止或试图欺骗飞地不正确地行动(例如，通过向其提供过时信息)来尝试干扰。因此，对于破坏的节点，成功的攻击将需要收集足够数量的部分签名，以产生完整签名。通过TEE，Ibrahim等人的协议对于2t个破坏的节点是稳健的。因为如果n-2t>＝2t+1就可以产生签名，那么大小为2t+1<＝(n+1)/2的任何合格的密钥份额子集就足矣。因此，在使用TEE时，可将阈值签名方案的阈值配置为大于或等于密钥份额的50％的数字，从而在存在破坏的节点的情况下产生有效签名。

[0075] 也可以使用其他阈值签名方案。例如，阈值签名方案可以是Goldfeder等人在“Securing Bitcoin Wallets Via a New DSA/ECDSA threshold signature scheme”，(2015)中提出的类型的ECDSA阈值方案。该协议允许t+1方产生有效签名。因此，对手必须控制以产生有效签名的密钥份额的数量等于对手必须拥有以重建私钥的密钥份额的数量。在需要一致同意以产生有效签名的情况下，该技术可以提供有效的方案。在最一般的情况下，该方案强加空间要求，其随着会议成员的数量呈指数级扩展，因为对于任意阈值，需要为n个玩家中的t+1个玩家的任何可能子集重复整个协议。因此，对于n和t两者的大值，将需要存储大量的密钥份额。为了减轻这种存储要求，可将标准比特币多重签名与阈值签名组合。具体而言，可以使用多重签名锁定数字资产，从而将每个私钥划分为多个份额。在空间要求方面，这种技术将使得更大的会议更有效率。还可通过在多个等级以反复的方式为出自较小大小的参与方中的大量参与者组成方案来改进扩展属性。例如，可将阈值签名方案与Cohen等人在“Efficient Multiparty Protocols via Log-Depth Threshold Formulas (2013)，Advances in Cryptology-CRYPTO 2013 pp 185-202”提出中的技术组合。

[0076] 可以使用其他阈值方案，包括非ECDSA签名方案。例如，节点102可以使用基于Schnorr方案的阈值方案来实现会议110。

[0077] 区块链网络100(图1)中的节点102(图1)可以基于所选择的阈值签名方案来实现会议协议。这样的节点102可包括存储在存储器220(图2)中的、实现会议协议的计算机可执行指令。在由处理器210(图2)执行时，这样的指令使得节点102(诸如参考图2所述的类型的电子装置200)进行会议协议的一个或多个方法。这些方法可包括图4至图8和图10的方法300、400、500、600、700、800、1000中的任何一个或组合。因此，会议协议可包括图4至图8和图10的方法300、400、500、600、700、800、1000中的一个或多个的组合。可通过节点同与其他会议成员相关联的其他节点合作来进行这些方法。

[0078] 会议启动

[0079] 下面参考图3，示出启动会议110的方法300。方法300可以由初始信任方进行，以建立会议110。即，与初始信任方相关联的节点102可以进行方法300。

[0080] 方法300包括在操作302提供会议公钥。可将会议公钥提供给其他节点102，以允许其他节点在他们希望加入会议时支付到会议公钥。也就是说，其他人可将数字资产转移到与会议公钥相关联的地址，从而加入会议。

[0081] 在操作304，进行方法300的节点102允许支付到公钥，直到满足一个或多个条件。例如，针对确定的时间段或者确定的区块数量，节点可以允许支付到公钥。在满足条件之后(例如，在该时间段期满或开采所述数量的区块之后)，进行方法300的节点102在操作306识别该会议的初始成员。

[0082] 在识别出包括会议的初始成员资格的各方之后，在操作307，根据阈值签名方案将私钥划分为私钥份额。然后在操作308，将私钥份额从进行方法300的节点102分配到所识别的各方。私钥份额与阈值签名方案相关联，阈值签名方案可以是本文所述的类型。

[0083] 在操作308期间，被识别为会议成员的节点102合作生成新的私钥份额和新的公钥。由初始信任方发送到这些节点的原始密钥份额可用于签名和广播交易，以将会议池中的所有数字资产发送到新的公钥，新的公钥随后成为会议公钥。也就是说，在操作408期间，建立新的群组公共地址，并且在会议的控制下的数字资产被转移到该新地址，该新地址成为群组的新地址并与会议公钥相关联。在确认该转移之后，会议可以无信任地操作。新的群组公共地址形成为将来可以从希望加入会议110的其他节点接收数字资产的存款的地址，或者用于如上所述的其他目的。现在认为会议成员加入了会议，并且这些节点现在可以在没有初始信任方的帮助下运行。此外，初始信任方不再在会议的操作中扮演任何角色。

[0084] 会议启动后加入会议

[0085] 下面参考图4，图4示出加入会议的方法400。图4的方法400可以结合图3的方法300操作，但是，图4的方法400是由在进行图3的方法300的节点所操作的相同区块链网络100(图1)中操作的节点102中的不同节点进行的。图4的方法400包括在操作402获得会议公钥。会议公钥可以直接从发起会议的一方获得，例如进行图3的方法300的节点，也可以从第三方获得，例如包括在区块链网络100(图1)之外操作的第三方系统。例如，可以从可通过公共互联网访问的公共web服务器获得会议公钥。

[0086] 进行方法400的节点102在操作404通过广播从与节点102相关联的私人账户到会议地址(即，与会议公钥相关联的地址)的数字资产的交易来支付到会议公钥。更具体而言，节点102广播交易以将一个或多个数字资产转移到与会议公钥相关联的公共群组地址。公共群组地址是会议池的地址。会议池包括与会议的其他成员相关联的其他数字资产。因此，在操作404的交易一旦被矿工104(图1)添加到区块中，就将数字资产转移到包括其他成员的数字资产的会议池。公共群组地址可以从希望加入会议的各方接收转移，也可以从不希望加入会议的各方接收转移。不希望加入会议的各方将数字资产转移到会议池，以便通过使用会议所采用的阈值签名方案，使得会议能够对这些数字资产进行全面、部分或有条件的控制。

[0087] 在操作404的交易可包括标记、标识符或其他属性，其指示转移数字资产的一方希望加入会议并且存款是为此目的而进行的。

[0088] 在通过会议池存放数字资产之后，进行方法400的节点102在操作406接收私钥份

额。然后，节点102通过运行协议的单个实例在操作408重新生成私钥份额。可以在节点102的TEE内进行私钥份额的生成。

[0089] 在操作408，节点102生成要在阈值签名方案中使用的私钥份额，其中至少必须使用私钥份额的阈值来代表会议为交易生成有效签名。其他私钥份额的持有者是会议的其他成员，他们通过将相应的数字资产转移到公共群组地址，而在许可或未经许可的基础上加入会议。

[0090] 为了重新生成私钥份额，在操作408，现有的会议成员可以合作更新密钥份额。例如，节点102可以生成阶数为t且具有常数项零的随机多项式$f_{n+1}^{0}(x)$。然后，节点102可以计算点$f_{n+1}^{0}(n+1)$并将其设置为它们的私钥份额。然后，节点102可以将该多项式$f_{n+1}^{0}(i)$上的点分配给每个现有的会议成员i＝1，...，n。然后，每个现有的会议成员(i＝1，...，n)将接收到的值添加到其现有的私钥份额中，以获得新的私钥份额。节点102现在具有等同于所有其他成员的私钥份额，并且对应的公钥保持不变。如上所述，阈值签名方案可以是各种类型的，包括椭圆曲线数字签名算法或基于Schnorr方案的阈值方案。

[0091] 私钥份额可以在TEE 250(图2)内生成，并且可以安全地存储在节点102。例如，私钥份额可以存储在TEE 250中。

[0092] 在由各个节点生成私钥份额之后，可将先前会议公钥控制下的资金、例如转移到与原始会议公钥相关联的公共群组地址的资金(通过足以在阈值签名方案下生成有效签名的多个群组节点的合作)转移到与新私钥份额相关联的新会议公钥。

[0093] 在操作408生成私钥份额之后，可以在方法400的操作410下使用它。私钥份额可用于从可以由成员广播的公共群组地址合作生成用于交易的有效签名。也就是说，私钥份额可用于阈值签名方案中帮助签名生成。在阈值签名方案下，会议的阈值数量的私钥份额需要被各个成员使用以产生有效签名，签名允许将数字资产转出会议。进行方法400的节点102可以从存储中检索私钥份额并使用私钥份额从而帮助签名生成。如果足够数量的其他会议成员也使用他们各自的私钥来帮助签名生成，则签名生成并且可以广播有效的向外交易。当区块链网络100的矿工104(图1)将交易添加到通过区块链网络100中的节点102的共识而添加到区块链的被开采区块并且该区块被确认时，向外交易完成。此时，交易中所代表的数字资产可以不再受会议的控制。也就是说，这种数字资产可以不再受会议公钥的阻碍。

[0094] 在操作408使用私钥份额可以在节点102的TEE内执行。TEE保护私钥份额，使得系统的其他部分或成员本身不能访问存储在飞地中的任何数据，例如私钥份额。此外，TEE保护私钥，因为如果成员想要回他们的存款并撤回他们的存款，它就不能保留私钥的副本，因为它必须在证明返回成员存款之前删除私钥。

[0095] 图4的方法400可以在初始设置阶段期间或之后进行。也就是说，方法400可以在分配初始密钥份额之前(例如，在图3的方法300的操作308期间)或之后(例如，在下面将更详细讨论的再平衡期间)进行。

[0096] 在操作410处交易可将数字资产转移回最初将这些数字资产存入会议池的一方。也就是说，转移可将数字资产返回存款人。转移也可将数字资产转移到其他地方。例如，可将数字资产转移到第三方或不可耗用的地址。

[0097] 没收数字资产

[0098] 下面参考图5,示出没收数字资产的示例性方法500。图5的方法500可由节点102进行,节点102可以是与进行图4的方法400的节点相同的节点。可以在图4的方法400的操作408之后进行方法500,从而在进行图5的方法500时,该节点102已经可以访问私钥份额。

[0099] 在操作502,节点102检测恶意方的恶意活动。恶意方可以是会议的另一个成员。当节点102确定会议的成员违反预定协议或准则时,检测到恶意活动。例如,当作为会议成员的节点向会议的其他成员报告错误信息(即,错误、不一致或其他不可接受的信息)时,可将该成员视为恶意成员。

[0100] 在操作503,响应于检测到恶意活动,节点102与会议中的其他节点合作,可以将作为恶意方的成员挂起。也就是说,会议可以排除恶意方进一步参与会议。

[0101] 为了确保所有节点102都按照预定协议或准则进行操作,可以对进入会议池的成员存款进行没收。没收意味着永久阻止被视为没收的成员存款的返回。构成由于恶意活动而未返回的成员存款的(一个或多个)数字资产可以留在会议池中但不返回(响应于应当采取该行动的共识),立即或在将来被转移到另一个不可耗用的地址,或以其他方式没收,并且没收的性质可以取决于会议是否充当用于侧链的担保验证者集合。例如,在操作504,响应于检测到恶意方的恶意活动,进行方法500的节点102可以使用私钥份额来提供在没收交易(其是这样一种交易:将数字资产转移到不可耗用的地址或作为揭发恶意活动的奖励的另一个节点)上的部分签名。也就是说,该节点与会议的其他节点合作,以没收先前由恶意方转移到公共群组地址(即,转移到会议池)的数字资产的至少一部分。也就是说,响应于观察到群组成员违反预定协议或准则,将私钥份额用于帮助与该群组成员相关联的、且在会议池中持有的一个或多个数字资产的交易的授权。

[0102] 因为阈值签名方案与会议公钥一起使用,所以单独行动的个别节点不能将另一个会议成员的数字资产的存款转出离开会议池(例如,转移到不可耗用的地址)。相反,当阈值数量的私钥份额被它们各自的成员用于生成有效签名以将数字资产(多个)转移到另一个地址时,或者当至少具有阈值数量的私钥份额的成员群组达成共识以将成员挂起时(在操作503),数字资产只能通过转移而被没收,这导致来自被挂起成员的任何撤回请求都被自动忽略。当通过转移没收数字资产时,(一个或多个)数字资产可以被转移至其的其他地址可以与不可耗用的地址相关联。例如,另一个地址可以是不存在私钥的地址,因此任何一方都不能访问由该地址的公钥绑定的数字资产。当确认将数字资产转移到不可耗用的地址的交易时或者当在侧链上达成共识应该没收数字资产时,数字资产可能视为已经被烧毁,因为它们不再可以被会议的任何成员或者实际上被区块链网络100中的任何节点耗用。

[0103] 因此,在操作504,节点可通过与会议的其他成员合作地使用私钥份额来没收数字资产,以生成用于交易至不可耗用的地址的有效签名,并且在一些实施方式中可以涉及在第二区块链上达成共识,即应当永久剥夺成员的全部或部分存款。

[0104] 此外,在一些实施方式中,会议可以充当担保验证者集合,用以确保权益证明侧链,并且该侧链可以用作广播信道。例如,会议成员可以在侧链上达成共识,即成员已经恶意行动。这种共识可以与包含恶意活动的控告证据的、对侧链交易的确认相对应。达成共识后,恶意成员提出的任何撤回成员存款的请求将被拒绝,并且存款将被视为没收。没收的数字资产可能在将来的某个时间被烧毁。也就是说,在以后的某个时间,阈值数量的成员(不包括恶意成员)可以合作,以授权将没收的数字资产转移到不可耗用的地址。

[0105] 因为会议是可通过存储数字资产而由区块链网络100的任何节点102加入的开放群组，所以群组成员资格可以周期性地改变。在发生这种改变时，可以更新私钥份额分配。下面参考图6，示出更新私钥份额分配的示例性方法600。方法600可通过区块链网络100的节点102与区块链网络100的其他节点合作进行。

[0106] 使用新公共地址更新私钥份额分配

[0107] 在方法600的操作602，节点102检测到重新分配请求，重新分配请求是一种其实现牵涉到重新分配密钥份额的请求。例如，节点102可以检测到潜在的新成员已经将数字资产转移到公共群组地址中或者现有成员已经请求撤回成员存款。

[0108] 数字资产可以通过如下节点转移到公共群组地址：请求加入会议或者增加他们在会议中的参与度的节点以及并未请求加入会议但是因为其他目的将数字资产转移到会议的其他节点(例如将数字资产转移到侧链，如下所述)。在操作602，节点102可以使用包括在数字资产到公共群组地址的至少一部分交易中的一个或多个属性来识别会议成员(即，将数字资产转移到会议公钥以加入会议而不是处于其他目的的各方)。例如，可以使用交易中的属性将某些交易标记为特殊交易。这些属性(不管存在还是不存在)可以指示进行转移的目的。例如，当转移者未请求加入会议时，可以在交易中包括标记。

[0109] 响应于在操作602检测到其实现牵涉到重新分配密钥份额的请求，在操作604，节点102以类似于在图4的方法400的操作408生成私钥份额的方式，生成新的私钥份额。会议的其他成员节点也生成相应的私钥份额。这些私钥份额可以与用于新会议公钥的阈值签名方案一起使用。将在此时离开会议的成员在操作604期间不生成新的私钥份额并且因为他们不会被分配以与新的会议公钥一起使用的私钥份额，所以他们失去参加会议的能力并且不再被视为会议成员。

[0110] 此外，响应于检测到重新分配请求(重新分配请求是其实现牵涉到重新分配密钥份额的请求)，在操作606，节点102与其他会议成员合作，将公共群组地址中的所有数字资产转移到与新公钥(以后会成为新的会议公钥)相关联的新公共地址。

[0111] 因此，根据图6的方法600，当存款的分配改变时或当从成员接收到撤回存款的请求时，可以重新生成私钥份额，并且可将所有在会议控制下的数字资产移动到新的公钥。会议成员资格可被更新的频率受到区块链网络100的区块时间限制。很多应用程序可能只需要在低频率下重新平衡。

[0112] 在保留现有公共群组地址的同时更新私钥份额分配

[0113] 下面参考图7，示出更新私钥份额分配的另一个示例性方法700。方法700可通过区块链网络100的节点102与区块链网络100的其他节点合作进行。

[0114] 在图7的方法700中，每次成员存款的分配改变时，会议公钥不改变。当检测到用以分配新密钥份额的请求时(在操作702，其可通过将数字资产存放到公共群组地址而发生)，节点102与会议的其他成员合作，以(在操作704)向群组的新成员发布用于相同公钥的新的私钥份额。合作的节点数量至少是在阈值签名方案下生成数字签名所需的节点的阈值数量。在操作704，可以分配额外的密钥份额，而其他密钥份额保持不变。这可能牵涉到(阈值签名方案)的阈值改变，但是实际上改变可能很小。或者，在操作704，可以分配额外的密钥份额，同时更新其他密钥份额。这种更新需要伴随着对删除任何上一代密钥份额的证明。在这种情况下，可以在保持相同阈值的同时分配新份额(在SSS的背景下，这涉及共享更高阶

的新的多项式)。

[0115] 在操作702,节点102可以使用包括在数字资产到公共群组地址的至少一部分交易中的一个或多个属性来识别会议成员(即,将数字资产转移到会议公钥以加入会议而不是因为其他目的的各方)。例如,某些交易可以使用交易中的属性标记为特殊交易。这些属性(不管存在还是不存在)可以指示进行转移的目的。例如,当转移者未请求加入会议时,可以在交易中包括标记。

[0116] 当成员离开使用方法700的会议时,他们可以安全地删除他们的私钥份额。为了确保旧成员的私钥份额不可用,可以要求会议的成员使用具有特殊TEE的节点102。TEE是在硬件级别实现的体系结构,它保证在其中执行的指令和数据免受来自系统其余部分的访问和操作。TEE可以采用硬件机制来响应远程证明询问,其可用于向外部方(例如,会议中的其他节点)验证系统的完整性。

[0117] 每个成员节点可以使用经证明的TEE,该经证明的TEE被配置为生成一个或多个随机秘密值,该随机秘密值保持对于主机系统的不可访问而不会损害集成电路级别的硬件。通过这种方式生成的秘密值将用于私钥份额的分布式生成(例如,在图4的方法400的操作410中)。该秘密值还可用于在会议的设立阶段建立共享公钥。与设立协议相关联的计算在TEE飞地内进行,使得任何成员或前成员都不能根据成员间通信或任何其他方法得出关于他们自己或其他私钥份额的任何信息。TEE内的飞地使得能够进行远程证明协议,其可用于向其他节点证明TEE飞地是可信的并且它正在运行经批准的计算机可读指令。

[0118] 与群组改变相关联的计算在TEE飞地内进行。例如,在TEE飞地中进行新安全随机秘密的生成,该新安全随机秘密可用于处于SSS目的计算新多项式的。

[0119] 此外,TEE飞地的目的是确保在返回成员存款之前,安全删除不再使用的先前密钥份额和先前秘密。更具体而言,为了将成员存款返回,证明协议可能要求TEE飞地证明密钥份额的删除。通过远程证明协议,每个节点102可将这种证明解释为对在其他节点上已经发生所需删除的确认。因此,方法700还可包括确认先前在离开会议的成员的TEE内持有的私钥份额已经从与该成员相关联的节点中删除。可通过接收对私钥份额的删除的证明来进行该确认。因此,远程证明协议可用于获得对先前在离开会议的成员的TEE中持有的私钥份额的删除的证明。

[0120] 图6的方法600和图7的方法700都提供各种好处。例如,图6的方法600不依赖于安全删除,也不需要依赖可信的硬件。但是,图6的方法600可以得益于这种硬件,因为在某些情况下,这种硬件可以使得密钥份额的恶意汇集更加不可能。

[0121] 图7的方法700避免每次成员资格变更时必须在新的会议公钥下重新锁定数字资产。此外在一些情况下,方法700与图6的方法600相比可以更快地更新成员资格,因为在图7的方法700下,不需要将交易添加到区块链中以将所有数字资产移动到新的公钥,这是因为数字资产并未移动到新的公钥。也就是说,可以使用图7的方法700来更新成员资格而无需等候生成若干区块来确认将数字资产转移到新公钥,因为公钥并未改变。

[0122] 从会议注销

[0123] 如上所述,群组成员有时候可以请求离开会议,并且当群组成员从会议注销时,他们存放到会议池的数字资产可能会被返回给他们。下面参考图8,以流程图的形式示出返回存款的示例性方法800。该方法可通过节点102与会议的其他节点102合作进行。

[0124] 在方法800的操作802，节点102从作为会议成员的请求者接收撤回请求。撤回请求也可称为注销请求。撤回请求是撤回由请求者先前存放并且当前由会议控制的数字资产的请求。请求可能已由请求者向所有会议成员广播。

[0125] 响应于接收请求，节点102在操作804针对确定的准则评估请求。这些准则可以是预定准则。如果会议根据其中每次群组成员资格改变时会议公钥未改变的会议协议进行操作，则在操作804，节点102可以确认请求者已经删除私钥份额。可以使用与TEE相关联的远程证明协议来获得这种确认。

[0126] 如果会议协议是在成员资格改变时会议公钥被改变的协议，则节点102可以不确认私钥份额的删除，因为私钥份额不再有效。相反，可以使用新的会议密钥，并且可将会议控制下的其他数字资产转移到新的会议密钥。

[0127] 如果节点102基于评估批准撤回请求，则在操作806，节点帮助撤回数字资产。也就是说，节点102使用其私钥份额来合作生成数字签名并使用数字签名将请求者先前存放的数字资产转移回请求者。例如，可将数字资产发送回先前从其接收到该数字资产的地址。根据阈值签名方案进行操作806，使得仅在至少阈值数量的会议成员授权撤回时才进行撤回。在希望注销的成员被挂起而不进行活动一段时间之后进行操作806。这个等待时段阻止了成员在进行用于其成员存款返回的协议时从事不当行为。

[0128] 用于智能合约的不可信代理

[0129] 会议提供用于执行各种功能的安全机制，并且会议协议可以用于多种不同的目的。通常，会议不可信地操作并且提供对于数字资产的所有权的控制。

[0130] 例如，该会议协议可以用于为智能合约提供不可信代理。更具体地，该会议协议可以用于激活脚本比如智能合约。智能合约的激活可能“触碰(poke)”智能合约，以使智能合约的一个或更多个功能被执行，或者智能合约的激活可以向智能合约提供外部数据。也就是说，通过使用会议协议，可以安全地获得区块链网络(在该区块链网络上智能合约被执行)之外的数据，并且该数据可以与智能合约结合使用。因此，该会议协议可以用于提供与智能合约相关联的区块链脚本的自主激活(即“触碰”这样的区块链脚本)或者向这样的区块链脚本提供对外部数据(即，先前在区块链上不可用的数据)的访问。如下面将更详细描述的，可以使用会议协议来为区块链网络上的智能合约提供触碰(poker)和数据馈送。

[0131] 现在参照图9，以框图形式示出了用于激活区块链网络900上的脚本的系统。该系统包括多个节点102a、102b、102c，这些节点可以是区块链网络(诸如图1的区块链网络)的节点。节点102包括多个会议节点102a。会议节点是区块链网络900的已经加入到群组中(在此称为会议110)的节点。会议节点可能已经以上面参照图4描述的方式加入了该群组。

[0132] 图9的系统中的节点中的至少一个节点是请求者节点102b。请求者节点102b是发布用于激活脚本的请求的节点。这种请求可能伴随有充当奖金的数字资产的存放。更具体地，可以持有数字资产用于在促进该请求的实现的节点之间分配。例如，奖金可以在帮助实现请求的信息提供系统中以及在其参与为协议提供安全性和可靠性的会议成员中分配。

[0133] 该请求可以是用以获得外部数据(即，在区块链网络上尚不可用的数据)并且将这样的数据提供给诸如智能合约之类的脚本的请求，或者该请求可以是其他的激活这样的脚本的请求。例如，该请求可以是当满足指定条件时(例如，以在特定时间激活智能合约，或当外部数据满足指定条件时等)触碰智能合约的请求。

[0134] 区块链网络900的节点还包括多个信息提供系统，其也被称为信息提供节点102c。这些信息提供节点102c是声称实现或帮助实现由请求者节点102b发布的请求的电子设备。例如，信息提供节点102c可以操作成从外部数据源比如从web服务器检索数据。

[0135] 如下面将更详细地说明的，虽然信息提供节点通常用于实现由请求者节点发布的请求，但是会议节点合作提供安全性和可靠性。例如，会议节点可以操作成提高由声称实现该请求的信息提供节点执行或提供的信息或动作的准确性。

[0136] 因此，区块链网络100(图1)中的节点102(图1)可以实施不可信代理协议，以激活或促进诸如智能合约之类的脚本的激活。这样的节点102可以包括存储在存储器220(图2)中的计算机可执行指令，该计算机可执行指令实施这样的协议。这样的指令在被处理器210(图2)执行时使节点102(比如参照图2所描述的类型的电子设备200)执行协议的一个或更多个方法。这些方法可以包括图3至图8、图10和图11的方法300、方法400、方法500、方法600、方法700、方法800、方法1000或方法1100中的任何一个方法或方法的组合。

[0137] 现在将参照图10，其示出了可以由请求者节点102b(图9)执行的方法。图10的方法可以被称为请求者方法1000。请求者节点102b可以是与脚本相关联的节点，比如区块链网络上的智能合约的一方。

[0138] 在请求者方法1000(图10)的操作1002中，请求者节点102b发布请求。该请求是激活诸如智能合约之类的脚本的请求。该请求以与区块链网络100相关联的数字资产的形式提供了奖金，以换取安全和可靠地激活脚本。该请求可以包括各种信息，所述信息包括以下各项中的一者或更多者：与请求相关联的脚本的标识，比如与脚本状态相关联的公钥；最小参与者信息，其可以指定要用于激活脚本的信息提供系统的最小数量；诸如挖掘费用的费用信息，其将被提供给会议以促进脚本的激活；和/或阈值指示符，其定义相对于共识数据和/或关于将在脚本的激活中使用的外部数据的信息的可接受变化量。代替上述数据或除上述数据之外，其他数据也可以包括在请求中。

[0139] 该请求可以从区块链外发出(即，“链下”)。例如，可以在可经由因特网访问的web服务器上发布请求。例如，可以在交换机上发布请求。该交换机可以是下述服务器：来自多个请求者节点的多个请求被发布在该服务器上。

[0140] 在请求者方法1000的操作1004中，请求者节点102b确定一个或更多个会议已经接受了该请求。也就是说，请求者节点102b确定会议(其包括多个会议节点102a)已经提供了依照该请求激活脚本。

[0141] 请求者节点102b可以在操作1006中选择接受该请求的一个或更多个会议。请求者节点102b可以例如针对一个或更多个阈值评估每个会议的信誉数据。信誉数据可以例如基于由先前参与相关联的会议以促进请求的完成的其他请求者节点102b提供的评级或其他度量。

[0142] 请求者节点102b可以选择接受该请求的会议中的单个会议，或者请求者节点102b可以选择多个这样的会议。请求者节点102b可以选择接受该请求的所有会议或这些会议的子集。通过选择多个会议，可以使所选择的会议有效地相互竞争。

[0143] 在请求者方法的操作1008中，请求者节点广播可支付给与所选择的会议相关联的会议池的交易(其可以被称为区块链交易)。交易包括呈数字资产形式的奖金，该数字资产可支付给与接受请求并在操作1006中选择的会议相关联的公共组地址。交易可以包括到与

请求相关联的数据的链接。例如，链接可以是到存储关于请求的信息的服务器的链接。这种信息可以包括：例如与请求相关联的脚本的标识、比如与脚本状态相关联的公钥；最小参与者信息，其可以指定要用于激活脚本的信息提供系统的最小数量；诸如挖掘费用的费用信息，其将被提供给会议以促进脚本的激活；阈值指示符，其定义相对于共识数据和/或关于将在脚本的激活中使用的外部数据的信息的可接受变化量、或其他信息、条件或要求。

[0144] 包括奖金的交易可以是时间锁定的，使得交易仅在将来的指定时间变得有效。时间锁定可以防止交易直到指定时间以后还被添加在区块链上。

[0145] 在选择(在操作1006中)多个会议以促进请求的完成的情况下，交易可以锁定奖金，使得仅可以允许完成请求最快的会议要求获得该奖金。

[0146] 现在参照图11，示出了会议方法1100。该会议方法1100可以由该会议的节点与该会议的其他节点合作来执行。也就是说，会议的节点可以配置有用于与会议的其他节点合作来执行方法1100的计算机可执行指令。也就是说，该会议方法1100可以由已经加入会议以成为会议节点的一个或更多个节点来执行。更具体地，区块链网络中的节点可以通过向会议池广播交易来加入由会议节点群组形成的会议。交易将一个或更多个数字资产的控制转移至会议。这种数字资产充当(用于成员进行存放的)成员存款，并且这种数字资产如以上参照图5所述那样被没收。在上面特别地参照图4更详细地描述了用于加入会议的技术。

[0147] 在节点加入会议成为会议节点之后，图11的方法1100可以由该会议节点与同一会议的其他会议节点合作来执行。

[0148] 在操作1102中，该会议节点识别请求。该请求可以是在图10的请求者方法1000的操作1002中发布的请求。

[0149] 在操作1104中，会议节点与该会议的其他节点合作接受该请求。对请求的接受可以被传送至发布请求的请求者节点。会议节点可以被配置成在接受请求之前彼此合作，以确定是否接受请求。例如，会议节点可以对于是否接受请求达成共识。例如，可以通过使用私钥份额达成共识。也就是说，会议成员可以使用其私钥份额来有效地投票决定是否接受该请求。如果至少阈值数量的私钥份额被用于有效地投票以接受该请求，则该请求将被会议接受。例如，该投票程序可以发生在侧链上(即，在不是主区块链的区块链上)。

[0150] 在该会议已经接受来自请求者的激活脚本的请求之后，在操作1106中，该会议节点可以检测来自请求者的交易，该交易包括与该请求相关联的奖金。也就是说，会议节点可以确定在请求者方法1000的操作1008中广播的交易已经被添加到区块链。如前所述，在操作1008中广播的交易可以被时间锁定，使得直到指定时间才将该交易添加到区块链。在这种情况下，操作1106在该时间之后执行。

[0151] 一旦操作1008中广播的交易(其可以称为“第一交易”)被会议节点确定为已经被确认(这可以于在该第一交易之上已经创建了至少阈值数量的块之后发生)，节点可以准备(在操作1108中)并发布可支付到会议池(即，与会议相关联的公共组地址)的交易(其可以称为“第二交易”)。

[0152] 第二交易可以被配置成允许多个信息提供系统(例如，图9的信息提供节点102c)向交易添加输入。例如，第二交易可以被签署SIGHASH_ALL|SIGHASH_ANYONECANPAY。SIGHASH_ALL是默认的签名散列类型，其对除了任何签名脚本之外的整个交易进行签署，从而防止对签署部分的修改。SIGHASH_ANYONECANPAY是仅对当前输入进行签署的签名散列类

型。

[0153] 诸如信息提供节点102c的信息提供系统可以随后提交以完成该请求。为此，信息提供系统添加到第二交易。例如，信息提供系统将由信息提供系统持有的数字资产作为输入添加到第二交易。这样的数字资产由信息提供系统作为保证提供(即，这样的数字资产将作为保证金来持有)，以确保信息提供系统根据该请求以及根据协议来操作。

[0154] 信息提供系统还将解决方案数据证明作为元数据添加到第二交易。例如，基于对请求的解决方案的散列可被添加到第二交易。该解决方案可以是例如外部数据，比如因特网上可用的数据或者来自脚本操作所需的另一数据源的数据。在这样的情况下，解决方案数据证明可以是基于外部数据的散列。散列还可以基于用于信息提供系统的公钥和/或出于安全性的盐值(salt)。盐值是用作散列函数的附加输入的随机数据。通过示例的方式，第二交易可以由信息提供系统更新，以包括被确定为HASH(q+PK+s)的元数据，其中q是解决方案，PK是信息提供系统的公钥，s是盐值。

[0155] 该会议可以将参与第二交易保持开放，直到满足一个或更多个预定条件为止。预定条件可以是例如基于时间的条件。例如，当在公布第二交易之后已经过去至少阈值时间量时，预定条件可以关闭参与。也就是说，信息提供系统可以被提供有其可以参与的一定量的时间。在该时间段期满之后，信息提供系统可能不再被允许参与。

[0156] 预定条件可能需要至少阈值数量的信息提供系统的参与。也就是说，可以保持对第二交易的参与开放，直到至少阈值数量的信息提供系统已经通过将相应的存款作为输入添加到第二交易而提交完成请求为止。

[0157] 用于将参与保持开放的预定条件可以由会议定义或者可以由请求者定义。例如，请求者可以将预定条件包括在请求中。

[0158] 在操作1110中，在确定已经满足预定条件之后(例如，在已经由信息提供系统向交易添加输入之后)，会议锁定信息提供系统的参与。也就是说，执行方法1100的会议节点可以与其他会议节点合作，以防止进一步的提交被添加到第二交易。该会议节点可以通过与其他会议节点合作耗用第二交易(即，解锁第二交易)来完成此操作。更具体地，会议节点可以使用该节点持有的私钥份额与其他这样的会议节点合作，以为该交易生成有效的加密签名以耗用该交易。这样的会议节点可以通过添加基于相应的私钥份额而生成的部分签名来合作，直到根据阈值签名方案生成有效签名为止。一旦挖掘了第二交易，并且在其上添加了足够数量的块以便确认第二交易，则认为该交易已被耗用。

[0159] 第二交易用作已经提交以完成请求的信息提供系统的寄存器。也就是说，第二交易充当如下信息提供系统的寄存器，该信息提供系统已经指示其具有对该请求的解决方案并且已经提交以提供该解决方案。第二交易还用于从参与的每个信息提供系统收集存款，并且第二交易用于提供信息提供系统打算提交的解决方案证明以使值不能在稍后的时间改变且使得值不能从其他参与者复制。

[0160] 在第二交易已经被耗用之后，在操作1112中，数据可以由会议节点从向第二交易添加输入的多个信息提供系统接收。例如，现在由信息提供系统向会议节点提供由每个信息提供系统提出的解决方案。该解决方案q可以与散列中使用的其他信息一起发送，其中该散列由信息提供系统添加到第二交易。例如，可以与用于信息提供系统的公钥PK和盐值s一起提供解决方案q。

[0161] 在操作1112中接收数据之后，会议节点可以确认该解决方案q对应于提交的解决方案(即，对应于由第二交易中的解决方案数据证明所识别的解决方案)。例如，会议节点可以对解决方案q、公钥PK和盐值s执行散列(即，HASH(q+PK+s))。该散列可与第二交易中的散列进行比较以确定该解决方案是否对应于提交的解决方案。如果解决方案不对应于提交的解决方案(例如，如果生成的散列不对应于第二交易中的散列)，则可以丢弃该解决方案(即，表示该解决方案的数据)，使得该解决方案不在方法1000的后续操作中使用。

[0162] 在操作1114中，会议节点与其他会议节点合作识别用于该请求的正确数据(例如，正确的解决方案)。例如，会议节点可以确定从所述多个信息提供系统接收到的数据的中心点。例如，在数据表示数值的情况下，中心点可以是在操作1112中从信息提供系统接收到的所有值的平均值(即，中心点可以被确定为接收到的所有值的平均值)。通过另一示例的方式，在一些实施方式中，中心点可以是从信息提供系统接收到的最常见的值或解决方案(即，中心点可以被确定为所接收到的所有值的模式)。通过又一示例的方式，在一些实施方式中，中心点可以是从信息提供系统接收到的中间值(即，中心点可以被确定为接收到的所有值的中值)。中心点可以基于从请求者接收的数据来确定。例如，请求者可以指定用于识别中心点的技术，并且在操作1114中会议可以使用指定的技术。

[0163] 中心点可以由会议节点的共识来选择。通过示例的方式，可以在侧链上确定中心点，并且会议节点可以使用相应的私钥份额来合作地为代表中心点的交易生成有效签名。当生成有效签名时，这是会议对于中心点达成共识的指示。

[0164] 在操作1116中，会议节点与该会议的其他节点合作识别提供正确数据的信息提供系统。也就是说，会议节点可以识别以声称请求的实现的方式提供数据的信息提供系统的子集。该子集由提供与在操作1114中识别的正确数据足够相似的数据的信息提供系统构成。例如，节点可以将提供在操作1114中识别的中心点附近的数据的信息提供系统识别为子集。将理解的是，在一些情况下，提供数据的所有信息提供系统可能已经提供了正确数据，而在其他情况下，仅一部分这样的信息提供系统可能已经提供了正确数据。

[0165] 为了识别提供与正确数据足够相似的数据的信息提供系统，可以使用阈值。阈值可以由请求者指定。例如，由请求者发出的请求可以包括阈值指示符。阈值指示符可以被包括在请求本身中，或者阈值指示符可以被链接到请求中。也就是说，该请求可以链接到对阈值指示符进行定义的数据，比如服务器上的数据。阈值指示符定义了所请求的精度并且可以用于对被认为已经提交了正确信息的信息提供者的子集进行识别。例如，阈值指示符可以指定用于确定给定数据是否与要被确定为正确的正确数据足够相似的百分比或其他度量。在操作1116提供了来自正确数据的阈值量内的数据的信息提供系统被确定为已经提供了足够正确数据，并且被识别为已经提供了正确数据。

[0166] 在一些情况下，仅与正确数据匹配的数据将被认为是正确的。也就是说，在一些情况下，阈值指示符可以被设置为零，使得仅与正确数据匹配的数据被认为是与要被确定为正确的正确数据足够相似。也就是说，如果阈值指示符被设置为零，则数据必须与被认为有效的正确数据相同。

[0167] 在操作1118中，会议节点与其他会议节点合作激活与该请求相关联的脚本。该会议节点可以基于正确数据激活脚本。例如，会议节点可以基于如在操作1114中确定的数据的中心点来激活脚本。会议节点合作以在区块链网络上发送对与所述请求相关联的脚本进

行解锁的交易。交易可以包括正确数据，并且可以根据脚本中的代码来利用该数据。

[0168] 在操作1120中，会议节点与会议的其他节点合作，以分配在操作1106检测到的交易中所接收到的奖金。更具体地，可以广播交易，从而将奖金的一部分转移到被确定为已经提供了足够正确数据的每个信息提供系统(其可以是响应于请求而提供数据的所有信息提供系统的子集，或者可以是当所有这样的系统响应于请求而提供正确数据时的所有信息提供系统)。例如，会议节点可以与形成该会议的一组节点中的其他会议节点合作以授权将数字资产转移到该子集中的每个信息提供系统。交易将受会议公钥阻碍的数字资产转移到与提交足够正确数据的信息提供系统相关联的公钥。为了签署交易，会议节点使用其私钥份额以与其他会议节点(其使用足以根据阈值签名方案生成有效签名的相应私钥份额)合作生成有效签名。交易还可以将奖金的一部分分配给一个或更多个会议成员。

[0169] 会议节点与会议的其他节点合作也可以返还由信息提供系统提供的存款中的至少一些存款。例如，会议节点可以广播交易，该交易包括根据阈值签名方案与其他会议节点合作产生的有效签名。该请求可以将存款返还给提供足够正确数据的任何信息提供系统。可以没收没有提供足够正确数据的任何信息提供系统的存款。也就是说，这样的存款可能不被返还。例如，可以在确实提供了足够正确值的节点之间分配没有提供足够正确数据的节点的存款。

[0170] 上面描述的方法一般被描述为在节点处执行，但是该方法的特征依赖于与其他节点的合作并且可以在其他地方执行。

[0171] 应当指出的是，上述实施方式说明而不是限制本发明，并且本领域技术人员将能够在不脱离由所附权利要求限定的本发明的范围的情况下设计许多替代实施方式。在权利要求中，置于括号中的任何附图标记不应被解释为限制权利要求。用语“包括”和“包含”等不排除除了在任何权利要求或说明书中作为整体列出的元件或步骤之外的元件或步骤的存在。在本说明书中，“包括”表示“包括或由.....构成”，并且“包含”表示“包含或由.....构成”。元件的单数引用不排除这些元件的复数引用，反之亦然。本发明可以借助于包括若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的设备权利要求中，这些装置中的若干个装置可以由同一个硬件项实现。在相互不同的从属权利要求中陈述某些手段的仅有事实并不表示这些手段的组合不能用于获益。

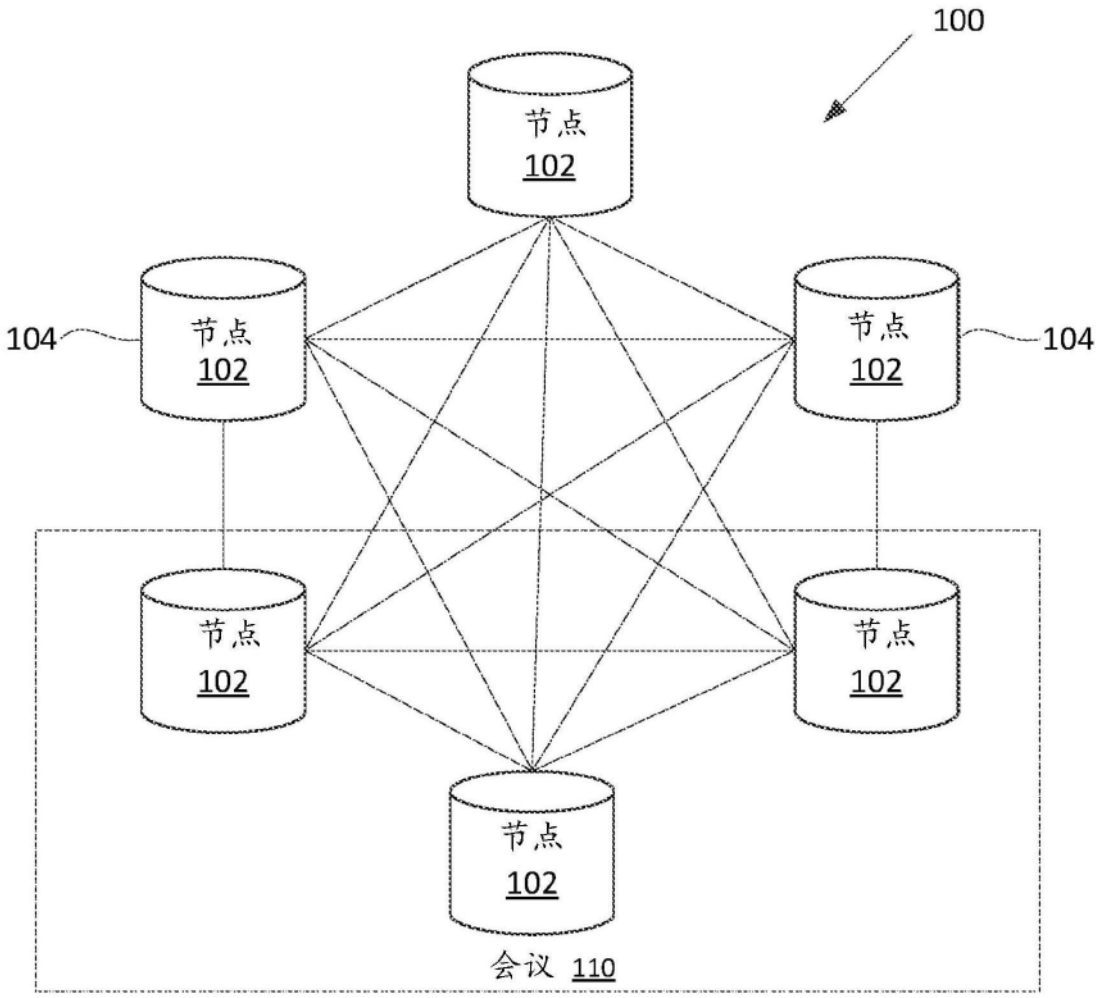


图1

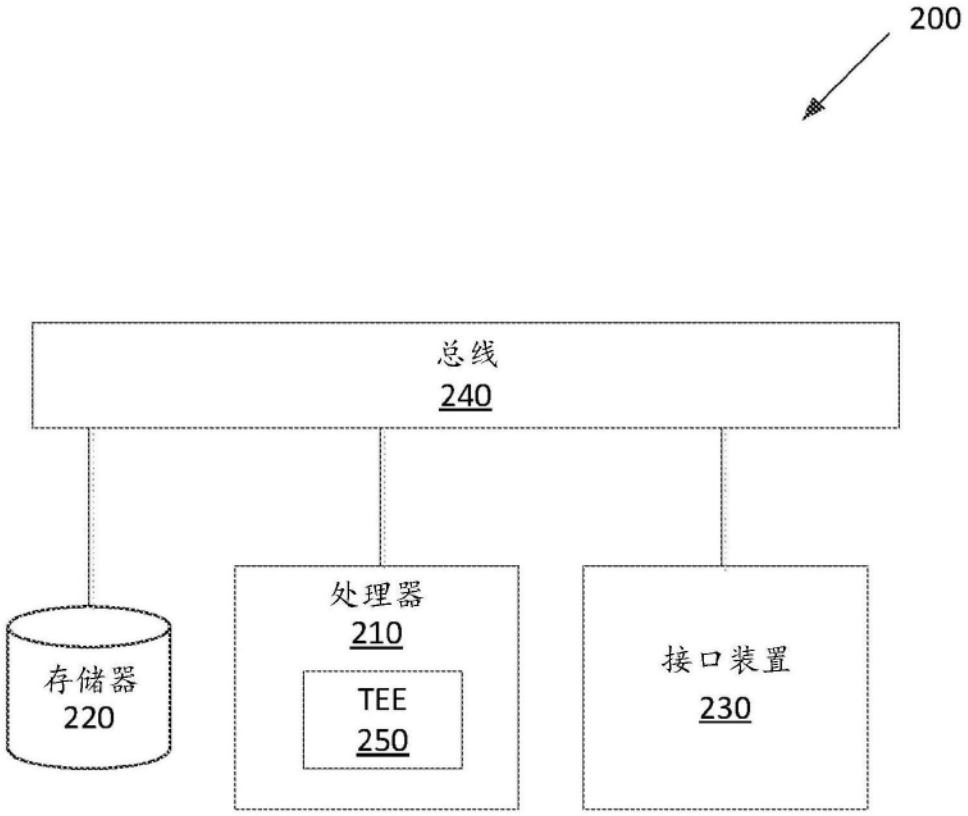


图2

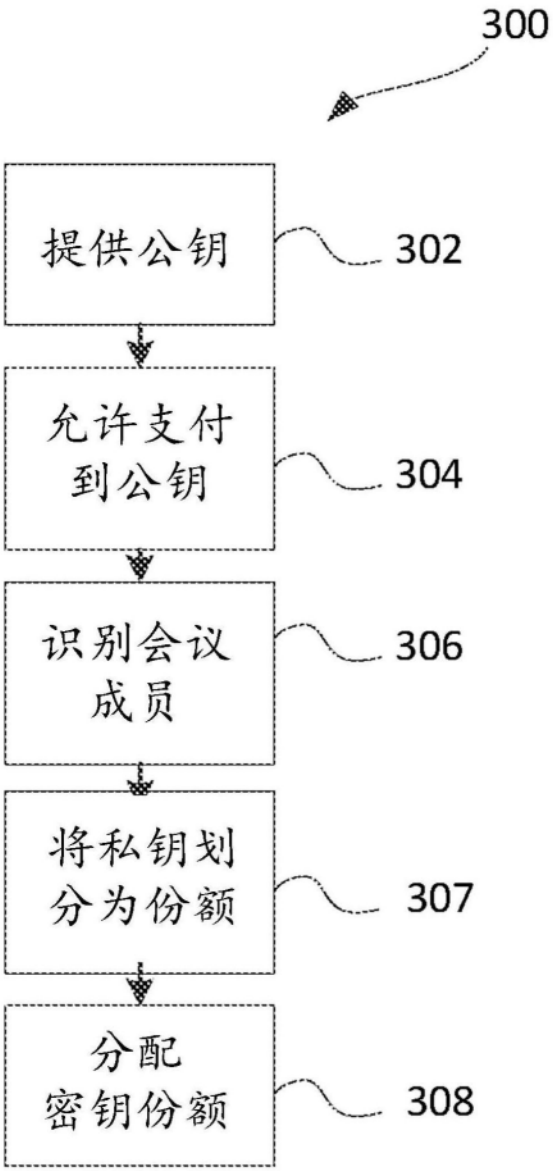


图3

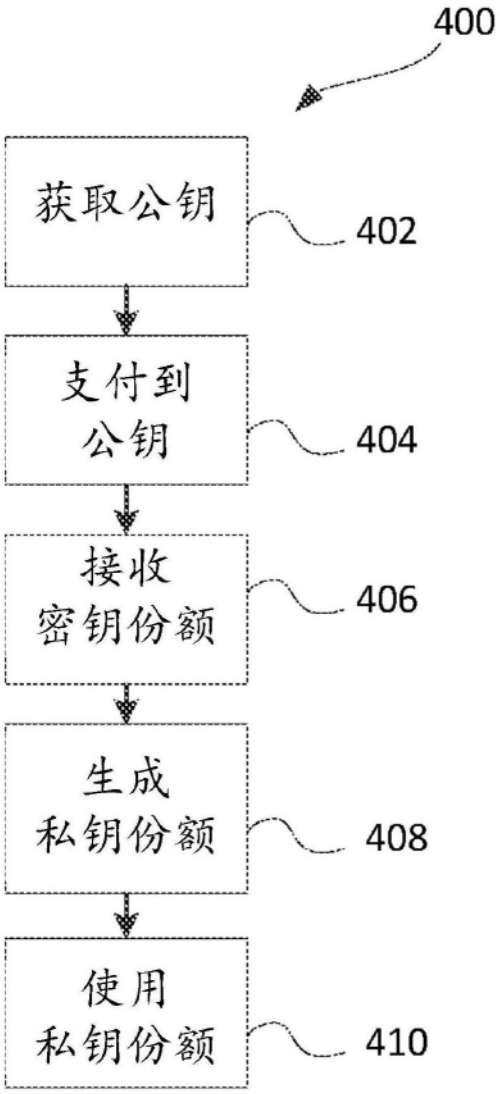


图4

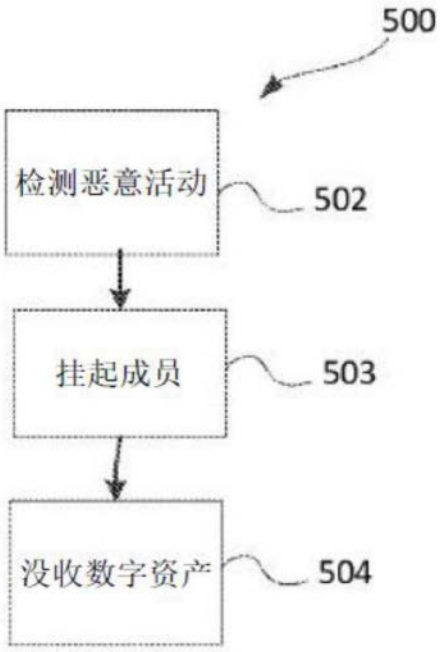

500
检测恶意活动
502
挂起成员
503
没收数字资产
504

图5

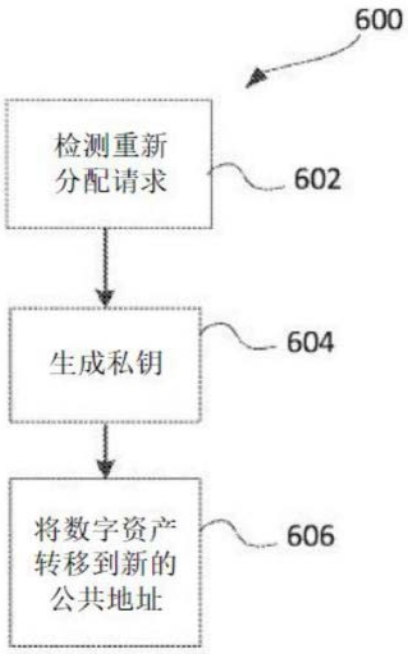

600
检测重新
分配请求
602
生成私钥
604
将数字资产
转移到新的
公共地址
606

图6

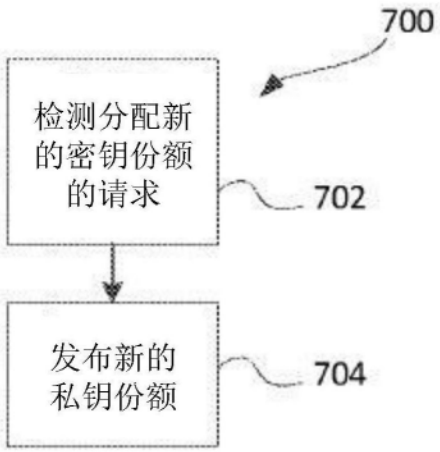

700
检测分配新的密钥份额的请求
702
发布新的私钥份额
704

图7

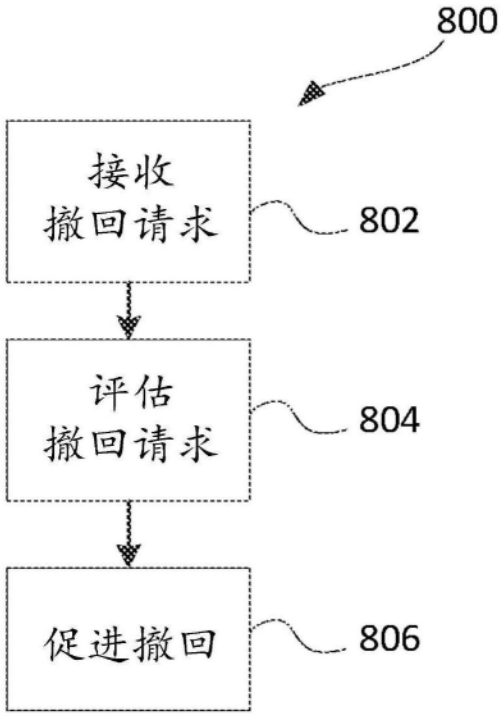

800
接收撤回请求
802
评估撤回请求
804
促进撤回
806

图8

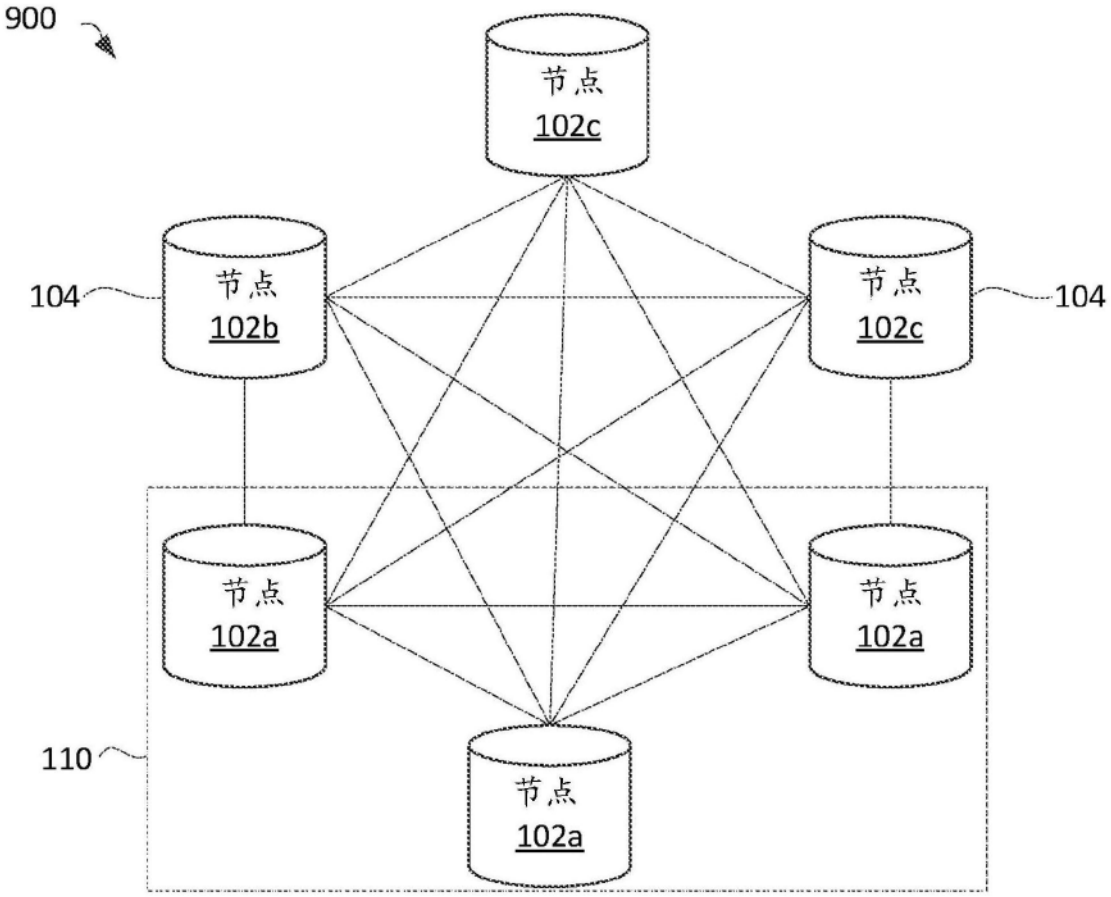


图9

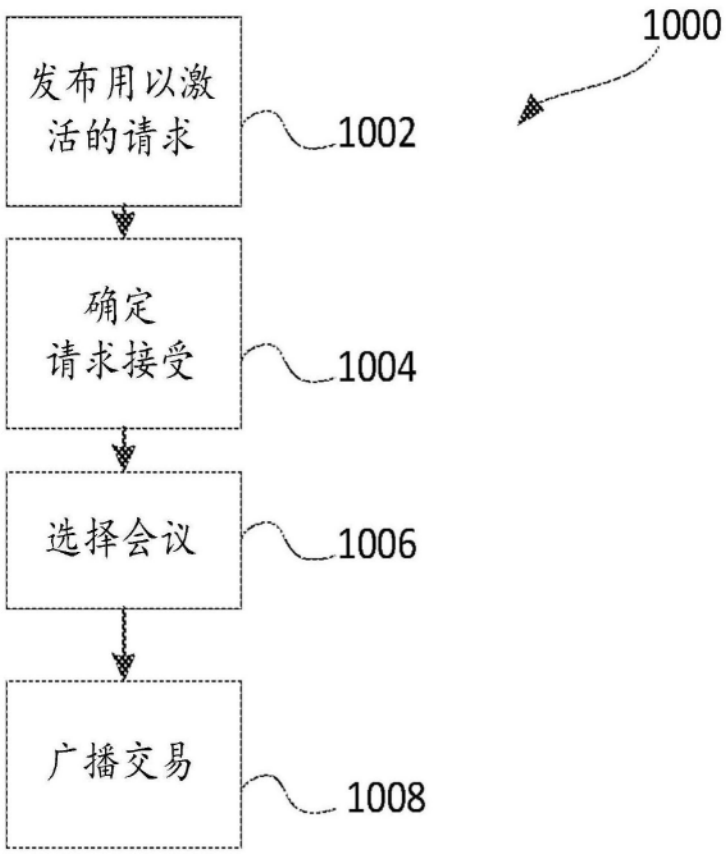


图10

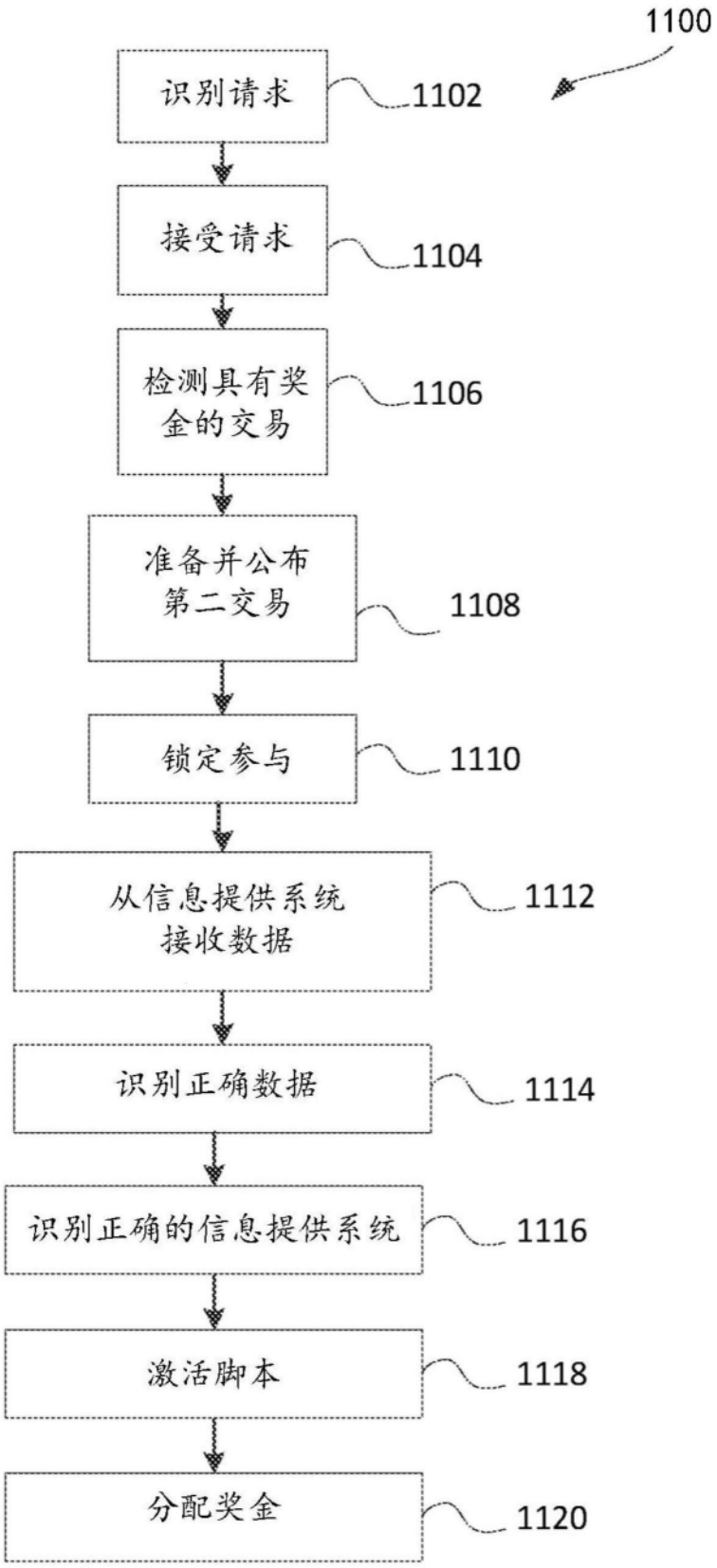

1100
识别请求
1102
接受请求
1104
检测具有奖金的交易
1106
准备并公布第二交易
1108
锁定参与
1110
从信息提供系统接收数据
1112
识别正确数据
1114
识别正确的信息提供系统
1116
激活脚本
1118
分配奖金
1120

图11