(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110998633 B
(45)授权公告日 2023.11.21

(21)申请号 201980003849.5

(22)申请日 2019.04.30

(65)同一申请的已公布的文献号
申请公布号 CN 110998633 A

(43)申请公布日 2020.04.10

(85)PCT国际申请进入国家阶段日
2020.02.12

(86)PCT国际申请的申请数据
PCT/CN2019/085212 2019.04.30

(87)PCT国际申请的公布数据
WO2019/137567 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 冯志远

(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
CN 109508968 A,2019.03.22
CN 108846659 A,2018.11.20
CN 108921559 A,2018.11.30
CN 109087204 A,2018.12.25
CN 109271245 A,2019.01.25
US 2017140408 A1,2017.05.18
US 2019114182 A1,2019.04.18
WO 2018120057 A1,2018.07.05
ANKUR SHARMA 等.How to Databasify a Blockchain: the Case of Hyperledger Fabric.《arxiv preprint arxiv: 1810.13177》.2018,第5-8页.
王德文;柳智权.基于智能合约的区域能源交易模型与实验测试.《电网技术》.2019,(第06期),全文.
王锡亮;刘学枫;赵淦森;王欣明;周子衡;莫泽枫.区块链综述:技术与挑战.《无线电通信技术》.2018,(第06期),全文.

审查员 吴单单

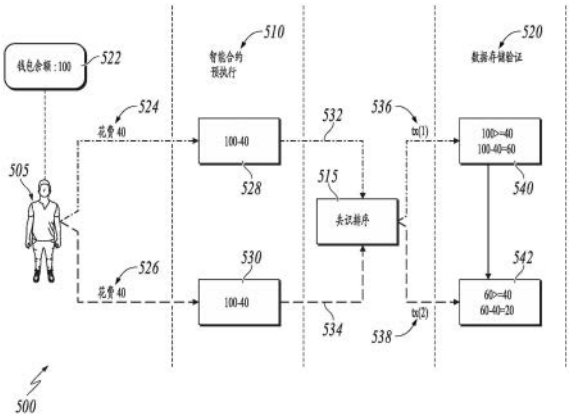
权利要求书1页 说明书16页 附图7页

(54)发明名称

在区块链技术中避免双花问题的方法和设备

(57)摘要

本文公开了用于在基于读写集模型的区块链技术中避免双花问题的方法、系统和装置,包括编码在计算机存储介质上的计算机程序。方法之一包括:接收指令以在一条数据上执行两个或更多个区块链交易,其中所述两个或更多个区块链交易中的所有区块链交易修改该条数据的值;以及针对所述两个或更多个区块链交易中的每个区块链交易:预执行与所述区块链交易相关联的智能合约,以生成指示所述区块链交易的特殊指令,其中所述特殊指令用于在执行所述智能合约以将所述区块链交易写入区块链时,验证该条数据的当前值支持所述区块链交易。



CN 110998633 B

1.一种计算机实现的用于避免区块链交易中的双花问题的方法,包括:

接收指令以在一条数据上执行两个或更多个区块链交易,其中所述两个或更多个区块链交易中的所有区块链交易修改该条数据的值,且所述两个或更多个区块链交易在该条数据上并行执行;以及

针对所述两个或更多个区块链交易中的每个区块链交易:

预执行与所述区块链交易相关联的智能合约,以生成指示所述区块链交易的特殊指令而不是读写集,其中,所述特殊指令用于在执行所述智能合约以将所述区块链交易写入区块链时,验证该条数据的当前值支持所述区块链交易,所述区块链基于读写集模型。

2.如权利要求1所述的方法,其中,

所述两个或更多个区块链交易中的所述区块链交易从该条数据中扣除一金额,以及

验证该条数据的所述当前值支持所述区块链交易包括,验证该条数据的所述当前值大于或等于所述金额。

3.如权利要求2所述的方法,还包括:

提交所述区块链交易以进行共识排序;以及

响应于验证该条数据的所述当前值大于或等于所述金额,执行与所述区块链交易相关联的所述智能合约以将所述区块链交易写入所述区块链。

4.如权利要求3所述的方法,其中,验证该条数据的所述当前值大于或等于所述金额不包括:

验证该条数据的所述当前值与由指示所述区块链交易的所述特殊指令指示的该条数据的值相等。

5.如权利要求3所述的方法,其中,执行与所述区块链交易相关联的所述智能合约以将所述区块链交易写入所述区块链,包括:

生成与所述区块链交易相关联的数据区块;以及

将所述数据区块发布至所述区块链。

6.如权利要求1所述的方法,其中,针对所述两个或更多个区块链交易中的每个区块链交易,预执行与所述区块链交易相关联的所述智能合约,以生成指示所述区块链交易的所述特殊指令,包括:

对该条数据进行余额检查;以及

如果对该条数据进行的所述余额检查支持所述区块链交易,则生成指示所述区块链交易的所述特殊指令。

7.如权利要求1所述的方法,其中,所述特殊指令指示在执行所述智能合约时对该条数据执行比较操作。

8.一种用于避免区块链交易中的双花问题的系统,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且其上存储有指令的一个或多个计算机可读存储器,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7中任一项所述的方法。

9.一种用于避免区块链交易中的双花问题的装置,所述装置包括用于执行权利要求1至7中任一项所述的方法的多个模块。

在区块链技术中避免双花问题的方法和设备

技术领域

[0001] 本文涉及区块链技术领域，具体涉及用于在基于读写集模型的区块链技术中避免双花问题的方法和设备。

背景技术

[0002] 分布式账本系统(DLS)，也可称为共识网络和/或区块链网络，使得参与的实体能够安全地且不可篡改地进行交易以及存储数据。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处理，并且联盟区块链网络包含访问控制层。

[0003] 在区块链网络中，由于数据的可重复性，数字资产可能被再利用。例如，可以在同一数字资产上执行多个并行区块链交易(称为双花)。在一些情况下，如果多个并行区块链交易在同一数据上读取，则一旦第一并行区块链交易修改数据，其他并行区块链交易可能由于数据修改而失败(称为双花问题)。

[0004] 目前，有两种主要的区块链处理类型。一种是由以太坊主导，首先达成共识，然后执行智能合约，并最后修改数据状态。另一种是由Hyperledger Fabric主导，首先预执行智能合约以用于逻辑验证，然后针对所生成的读写集执行共识排序，最后针对每个生成的读写集执行数据验证。因为以太坊按顺序执行交易，因此可能没有双花问题。然而Hyperledger Fabric实现了基于读写集的预执行智能合约方案，并且可能遇到双花问题。

[0005] 期望提供一种针对基于读写集模型的区块链技术(例如，Hyperledger Fabric)中的双花问题的解决方案。

发明内容

[0006] 本文描述了用于在区块链技术中避免双花问题的技术。这些技术一般涉及接收指令以在一条数据上执行两个或更多个区块链交易，其中，两个或更多个区块链交易中的所有区块链交易修改该条数据的值；以及针对两个或更多个区块链交易中的每个区块链交易：预执行与区块链交易相关联的智能合约，以生成指示区块链交易的特殊指令，其中，特殊指令用于在执行智能合约以将区块链交易写入区块链时，验证该条数据的当前值支持区块链交易。

[0007] 本文还提供了耦接到一个或多个处理器并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，当所述指令由所述一个或多个处理器执行时，所述指令促使所述一个或多个处理器按照本文提供的方法的实施例执行操作。

[0008] 本文还提供了用于实施本文提供的所述方法的系统。所述系统包括一个或多个处理器及计算机可读存储介质，所述计算机可读存储介质耦接至所述一个或多个处理器且其上存储有指令，当所述指令被所述一个或多个处理器执行时，所述指令促使所述一个或多个处理器根据本文所提供的方法的实施例中方式执行操作。

[0009] 应了解，依据本文的方法可以包括本文描述的方面和特征的任意组合。也就是说，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，还可以包括所提供的方面和特征的任意组合。

[0010] 以下在附图和描述中阐述了本文的一个或多个实施例中的细节。根据文和附图以及权利要求，本文的其他特征和优点将显现。

附图说明

[0011] 图1是示出可用于执行本文实施例的环境的示例的图。

[0012] 图2是示出根据本文实施例的概念性架构的示例的图。

[0013] 图3是示出根据本文实施例的区块链交易执行场景的示例的框图。

[0014] 图4是示出根据本文实施例的用于两个并行区块链交易的传统执行场景的示例的框图。

[0015] 图5是示出根据本文实施例的用于两个并行区块链交易的执行场景的示例的框图。

[0016] 图6是示出根据本文实施例的用于避免区块链交易中的双花问题的方法的示例的流程图。

[0017] 图7描绘了根据本文实施例的装置的模块的示例。

[0018] 各附图中相同的附图标记和名称表示相同的元件。

具体实施方式

[0019] 以下具体实施方式描述了用于在基于读写集模型的区块链技术中避免双花问题，并被呈现以使得本领域技术人员能够在一个或多个特定实施例的上下文中实现或使用所公开的主题。接收用以在一条数据上执行两个或更多个区块链交易的指令。对于每个区块链交易，预执行对应的智能合约以生成特殊指令，而不是读写集。该特殊指令用于在执行对应的智能合约以将区块链交易写入区块链时，验证该条数据的当前值支持该区块链交易。

[0020] 可以对所公开的实施例进行各种修改、变更和置换，并且对于本领域普通技术人员来说是明显的，并且在不脱离本文的范围的情况下，所定义的一般原理可以应用于其他实施例和应用。在一些情况下，可以省略对于获得对所描述的主题的理解不必要并且在本领域普通技术人员的技术范围内的一个或多个技术细节，以免使一个或多个所描述的实施例不清楚。本文不意图限于所描述或说明的实施例，而是与符合所述原理和特征的最宽范围相一致。

[0021] 为本文实施例提供进一步的背景，并且如上所述，分布式账本系统(DLS)，又可称为共识网络(例如，由点对点节点组成)和区块链网络，使参与的实体能够安全地、不可篡改地进行交易和存储数据。尽管术语区块链通常与特定网络和/或用例关联，但是在不参考任何特殊用例的情况下，本文中所使用的区块链主要指DLS。

[0022] 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之前的前一区块的加密哈希值(cryptographic hash)链接到该前一区块。每个区块还包括时间戳、自身的加密哈希值以及一个或多个交易。已经被区块链网络中的节点验证的交易

经哈希处理并编入默克尔(Merkle)树中。Merkle树是一种数据结构,在该树的叶节点处的数据经哈希处理,并且在该树的每个分支中的所有哈希值在该分支的根处级联。沿着树持续该处理一直到整个树的根,在整个树的根处存储了代表树中所有数据的哈希值。通过确定哈希值是否与该树的结构一致而可快速验证该哈希值是否为存储在该树中的交易的哈希值。

[0023] 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,区块链网络可作为公有区块链网络、私有区块链网络或联盟区块链网络被提供。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。

[0024] 通常,联盟区块链网络在参与的实体中是私有的。在联盟区块链网络中,共识处理由被授权的可被称为共识节点的节点集控制,一个或多个共识节点由对应的实体(例如,金融机构、保险公司)操作。例如具有十(10)个实体(例如,金融机构、保险公司)的联盟可以操作联盟区块链网络,其中每个实体可以操作该联盟区块链网络中的至少一个节点。

[0025] 在一些示例中,在联盟区块链网络内,提供全局区块链作为跨所有节点复制的区块链。也即,所有共识节点相对于全局区块链都处于完全共识状态。为达成共识(例如,同意将区块添加至区块链),在联盟区块链网络中实施共识协议。例如,联盟区块链网络可以实现实用拜占庭容错(PBFT)共识,下面将进一步详细描述。

[0026] 图1是示出可用于执行本文实施例的环境100的示例的图。在一些示例中,环境100使实体能够参与到联盟区块链网络102中。环境100包括计算系统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)、互联网或其组合,并连接网络站点、用户设备(例如,计算设备)和后端系统。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。在一些示例中,网络110使得与联盟区块链网络102通信以及在联盟区块链网络102内部进行通信成为可能。通常,网络110表示一个或多个通信网络。在一些情况下,计算系统106、108可以是云计算系统(未示出)的节点,或者每个计算系统106、108可以是单独的云计算系统,所述云计算系统包括由网络互连并且用作分布式处理系统的多个计算机。

[0027] 在所描绘的示例中,计算系统106、108可以各自包括能够作为节点参与至联盟区块链网络102中的任何适当的计算设备。计算设备的示例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施的服务,用于与联盟区块链网络102进行交互。例如,计算系统106可以承载第一实体(例如,用户A)的由计算机实施的、例如交易管理系统的服务,第一实体使用该交易管理系统管理其与一个或多个其他实体(例如,其他用户)的交易。计算系统108可以承载第二实体(例如,用户B)的由计算机实施的、例如交易管理系统的服务,第二实体使用该交易管理系统管理其与一个或多个其他实体(例如,其他用户)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),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。

[0028] 图2是示出根据本文实施例的概念性架构200的示例的图。示例性概念架构200包括分别对应于参与者A、参与者B、参与者C的参与者系统202、204、206。每个参与者(例如,用

户、企业)参与到作为点对点网络提供的区块链网络212中,该点对点网络包括多个节点214,至少一些节点将信息不可篡改地记录在区块链216中。如图中进一步详述,尽管在区块链网络212中示意性地描述了单个区块链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。

[0029] 在所描绘的示例中,每个参与者系统202、204、206分别由参与者A、参与者B和参与者C提供或代表参与者A、参与者B和参与者C,并且在区块链网络中作为各自的节点214发挥作用。如这里所使用的,节点通常是指连接到区块链网络212且使相应的参与者能够参与到区块链网络中的个体系统(例如,计算机、服务器)。在图2的示例中,参与者对应于每个节点214。然而,可以预期,一个参与者可以操作区块链网络212内的多个节点214,和/或多个参与者可以共享一个节点214。在一些示例中,参与者系统202、204、206使用协议(例如,超文本传输协议安全(HTTPS))和/或使用远程过程调用(RPC)与区块链网络212通信或通过区块链网络212进行通信。

[0030] 节点214可以在区块链网络212内具有不同的参与程度。例如,一些节点214可以参与共识处理(例如,作为将区块添加到区块链216的监视节点),而其他节点214不参与此共识处理。作为另一示例,一些节点214存储区块链216的完整的副本,而其他节点214仅存储区块链216的一部分的副本。例如,数据访问特权可以限制相应的参与者在其相应系统内存储的区块链数据。在图2的示例中,参与者系统202、204、206存储区块链216的相应的完整副本216’、216’’、216’’’。

[0031] 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。数据的示例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存储在区块链中(例如,文档、图像、视频、音频)。交易的示例可以包括但不限于有价物的交换(例如,资产、产品、服务、货币)。交易数据不可篡改地存储在区块链中。也就是说,交易数据不能改变。

[0032] 在将交易数据存储在区块中之前,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。哈希处理可确保即使交易数据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。哈希函数的示例包括但不限于输出256位哈希值的安全哈希算法(SHA)-256。

[0033] 多个交易的交易数据被哈希处理并存储在区块中。例如,提供两个交易的哈希值,并对它们本身进行哈希处理以提供另一个哈希值。重复此处理,直到针对所有要存储在区块中的交易提供单个哈希值为止。该哈希值被称为Merkle根哈希值,并存储在区块的头中。任何交易中的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。

[0034] 通过共识协议将区块添加到区块链。区块链网络中的多个节点参与共识协议,执行工作以将区块添加到区块链中。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性示例。共识节点执行共识协议以将交易添加到区块链,并更新区块链网络的整体状态。

[0035] 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,并将所得的

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)。将此哈希值添加到区块头中。共识节点还确定区块链中最近的区块的哈希值(即，添加到区块链中的最后一个区块)。共识节点还向区块头添加随机数(nonce)和时间戳。

[0036] 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)。这通过假设将发生故障(例如，假设存在独立节点故障和/或由共识节点发送的操纵消息)在PBFT中实现。在PBFT中，以包括主要共识节点和备共识节点的顺序提供共识节点。主共识节点定期更换。区块链网络内的所有共识节点将交易添加到区块链，就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消息是从指定的点节点接收的，并验证在传输期间消息未被篡改。

[0037] 在PBFT中，共识协议以多个阶段提供，所有共识节点以相同状态开始。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)。响应于接收到请求，主共识节点将请求组播到备共识节点。备共识节点执行请求，并且每个节点都向客户端发送回复。客户端等待直到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，并且记录被接受或拒绝。

[0038] 在一些区块链网络中，用密码学来维护交易的隐私。例如，如果两个节点期望保持交易隐私，以使得区块链网络中的其他节点不能看出交易的细节，则这两个节点可以对交易数据进行加密处理。加密处理的示例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(即，从明文生成密文)又进行解密(即，从密文生成明文)的加密处理。在对称加密中，同一密钥可用于多个节点，使得每个节点都可以对交易数据进行加密/解密。

[0039] 非对称加密使用密钥对，其中每个密钥对包括私钥和公钥。私钥仅对特定节点是已知的，并且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可以使用其私钥来解密该加密数据(例如，密文)并提取原始数据(例如，明文)。使用节点的公钥加密的消息只能使用该节点的私钥解密。

[0040] 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的该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将向参与者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，参与者B可以确认该消息确实来自参与者A，且未被篡改。

[0041] 图3是示出根据本文实施例的区块链交易执行场景300的示例的框图。区块链交易执行场景300包括一区块链交易，其中用户305意图花费40元(¥ 40)。区块链交易包括智能合约预执行阶段310和数据存储验证阶段315。为方便起见，区块链交易执行场景300将被描

述为由位于一个或多个位置并且根据本文适当地编程的一个或多个计算机的系统(例如,图1的计算系统106和/或108或者图2的参与者系统202、204和/或206)执行。

[0042] 如图3中所示,用户305具有钱包余额为100元的数字钱包320。用户意图花费40元(322)。例如通过用于智能合约的软件开发工具包(SDK)调用324,提交用于花费40元的区块链交易326以供执行。为了执行区块链交易326,智能合约可以首先被预执行以对区块链交易326执行逻辑验证,从而生成读写集。在共识排序后,基于读写集对区块链交易326执行数据验证,以确定区块链交易326是否可以被成功执行。

[0043] 在智能合约预执行阶段310,在328处,接收用于花费40元的区块链交易。流程从328进行到330。

[0044] 在330,读取用户的账户余额(即,余额=100)。在智能合约预执行阶段310,用户的账户余额未被修改(即,余额保持在100元)。流程从330进行到332。

[0045] 在332,确定用户的账户中是否有足够(即充足的)的余额用于花费40元的区块链交易。如果确定用户的账户中没有足够的余额用于花费40元的区块链交易,则流程进行到334,其中向用户305发送指示没有足够金额的通知。换句话说,在没有足够余额的情况下,智能合约预执行阶段310失败,并且花费40元的区块链交易失败。否则,如果确定用户的账户中有足够的余额用于花费40元的区块链交易,则流程进行到336,其中生成读写集。例如,生成读写集(100->60)。读写集(100->60)指示从用户的具有100元余额的账户中扣除40元,用户的账户在花费40元的区块链交易成功后具有60元余额(例如,用户的账户余额从100元变为60元)。在336之后,在数据存储验证阶段315结束之前,提交具有生成的读写集的区块链交易以进行共识排序(338)。

[0046] 在数据存储验证阶段315,在340,接收具有读写集的区块链交易。流程从340进行到342。

[0047] 在342,读取用户的账户余额(即,余额=100)。流程从342进行到344。

[0048] 在344,确定用户的账户余额是否等于读写集(100->60)中指示的账户余额(即,读写集账户余额=100)。如果确定用户的账户余额不等于读写集(100->60)中指示的账户余额,则流程进行到346,其中发送指示数据不匹配的消息以通知用户305。换句话说,数据存储验证阶段315失败,并因此花费40元的区块链交易失败。否则,如果确定用户的账户余额等于读写集(100->60)中指示的账户余额,则流程进行到348,其中根据读写集(100->60)修改数据库(例如,用户的账户余额从100元被修改为60元)。例如,花费40元的区块链交易存储在区块链的数据区块中。流程从348进行到350,其中发送指示花费的金额的消息以通知用户305。换句话说,花费40元的区块链交易成功。

[0049] 图3中示出的区块链交易执行场景300使用了基于读写集模型的区块链技术(例如,Hyperledger Fabric)。与传统的智能合约调用逻辑(例如,以太坊)不同,基于读写集模型的区块链技术将逻辑验证和数据验证分开。智能合约预执行阶段310(例如,逻辑验证)的执行不修改数据,并且可以获得区块链网络中的一个或多个节点的背书。在共识排序之后以及在数据存储验证阶段315(例如数据验证)的交易可以修改数据。通过这样做可以改善区块链技术的性能。

[0050] 图4是示出根据本文实施例的用于两个并行区块链交易的传统执行场景400的示例的框图。传统执行场景400包括两个并行区块链交易,其中用户405意图在两个并行区块

链交易中的每个区块链交易中花费40元(¥ 40)。每个区块链交易包括智能合约预执行阶段410、共识排序阶段415和数据存储验证阶段420。在一些实施例中,传统执行场景400可以包括两个以上的并行区块链交易。为方便起见,传统执行场景400将被描述为由位于一个或多个位置并根据本文适当地编程的一个或多个计算机的系统执行。(例如,图1的计算系统106和/或108或者图2的参与者系统202、204和/或206)。

[0051] 如图4所示,用户405具有钱包余额为100元的数字钱包422。用户405意图在两个并行区块链交易424和426中总共花费80元。每个区块链交易将要花费40元。在一些实施例中,可以在每个区块链交易上花费不同的金额。为了执行两个并行区块链交易424和426,首先预执行智能合约以对每个区块链交易执行逻辑验证从而生成相应的读写集。在共识排序之后,基于相应的读写集对每个区块链交易执行数据验证,以确定每个区块链交易是否可以成功执行。

[0052] 在智能合约预执行阶段410(类似于图3中的智能合约预执行阶段310),针对区块链交易424生成读写集428(即(100->60))。读写集428指示从用户的具有100元余额的账户中扣除40元,并且在区块链交易424成功后用户的账户具有余额60元(例如,用户的账户余额从100元变为60元)。此外,针对区块链交易426生成读写集430(即(100->60))。

[0053] 如果用户的账户没有其他消费,则在智能合约预执行阶段410,两个并行区块链交易424和426读取存储在数据库中的同一用户的账户余额。因此,读写集430还指示从用户的具有100元余额的账户中扣除40元,并且在区块链交易430成功后,用户的账户具有余额60元(例如,用户的账户余额从100元变为60元)。

[0054] 在智能合约预执行阶段410之后,提交具有读写集428的区块链交易(432)以进行共识排序,并且还提交具有读写集430的区块链交易(434)以进行共识排序。

[0055] 在共识排序阶段415,为了方便起见,假设具有读写集428的区块链交易被视为将要在数据存储验证阶段420执行的第一交易436,并且具有读写集430的区块链交易被视为将要在数据存储验证阶段420执行的第二交易438。

[0056] 在数据存储验证阶段420(类似于图3中的数字存储验证阶段315),具有读写集428的区块链交易首先被执行(440)。在440,读取用户的账户余额(即,余额=100)。确定用户的账户余额等于读写集428中指示的账户余额(即100==100)。根据读写集428修改数据库(例如,将用户的账户余额从100元修改为60元)。换句话说,用于具有读写集428的区块链交易的数据存储验证阶段420成功,并因此区块链交易424成功。在具有读写集428的区块链交易成功后,流程进行到442,其中具有读写集430的区块链交易被执行。在442,读取用户的账户余额(即,余额=60)。确定用户的账户余额不等于读写集430中指示的账户余额(即,60!=100)。换句话说,用于具有读写集430的区块链交易的数据存储验证阶段420失败,并且因此区块链交易426失败。

[0057] 如图4所示,当对一条数据(例如,账户余额)执行两个或更多个并行区块链交易时,在逻辑验证期间(例如,智能合约预执行阶段410)针对每个区块链交易读取相同的数据。在共识排序之后和数据验证期间(例如,数据存储验证阶段420),在两个或更多个区块链交易之中第一个执行的区块链交易(例如,区块链交易424)在数据验证中成功,并修改一条数据。结果,在第一个执行的区块链交易之后执行的后续区块链交易将在数据验证中失败。换句话说,即使有足够的余额支持后续区块链交易(例如,区块链交易426),后续区块链

交易也会在数据验证中失败，这是因为该条数据已经被第一个执行的区块链交易修改。例如，除了第一个执行的区块链交易之外，所有并行区块链交易都会失败。因此，当对于该条数据进行频繁的并行交易时，传统执行场景400是低效的且消耗更多的资源。

[0058] 图5是示出根据本文实施例的用于两个并行区块链交易的执行场景500的示例的框图。执行场景500包括两个并行的区块链交易，其中用户505意图在两个并行区块链交易中的每个区块链交易花费40元(¥ 40)。每个区块链交易包括智能合约预执行阶段510、共识排序阶段515以及数据存储验证阶段520。在一些实施例中，执行场景500可以包括两个以上的并行区块链交易。为方便起见，执行场景500将被描述为由位于一个或多个位置并根据本文适当地编程的一个或多个计算机的系统执行。例如，适当编程的计算系统(例如，图1的计算系统106和/或108，图2的参与者系统202、204和/或206)可以实现执行场景500。

[0059] 如图5中所示，用户505具有钱包余额为100元的数字钱包522。用户505意图在两个并行区块链交易524和526中总共花费80元。每个区块链交易要花费40元。在一些实施例中，可以在每个区块链交易上花费不同的金额。为了执行两个并行区块链交易524和526，首先预执行智能合约以对每个区块链交易执行逻辑验证从而生成相应的读写集。在共识排序之后，基于相应的读写集对每个区块链交易执行数据验证，以确定每个区块链交易是否可以成功执行。

[0060] 在智能合约预执行阶段510，针对区块链交易524生成特殊指令528(例如，(100-40))而不是图4中的读写集428。特殊指令528指示从用户的账户中扣除40元。在一些实施例中，特殊指令528用于确定智能合约中的余额变化。另外，针对区块链交易526生成特殊指令530(例如，(100-40))，而不是图4中的读写集430。特殊指令530还指示从用户的账户中扣除40元。

[0061] 在智能合约预执行阶段510之后，提交具有特殊指令528的区块链交易(532)以进行共识排序，并且还提交具有特殊指令530的区块链交易(534)以进行共识排序。

[0062] 在共识排序阶段515，为方便起见，假设具有特殊指令528的区块链交易被视为将要在数据存储验证阶段520执行的第一交易536，并且具有特殊指令530的区块链交易被视为将要在数据存储验证阶段520执行的第二交易538。

[0063] 在数据存储验证阶段520，首先执行具有特殊指令528的区块链交易(540)。在540，读取用户的账户余额(即，余额=100)。确定用户的账户余额是否大于或等于特殊指令528中指示的花费金额(即，40)。在这种情况下，确定用户的账户余额大于或等于特殊指令528中指示的花费金额(即，100>=40)。然后，根据特殊指令528修改数据库(例如，从用户的账户中扣除40元)。换句话说，用于具有特殊指令528的区块链交易的数据存储验证阶段520成功，因此区块链交易524成功。在具有特殊指令528的区块链交易成功之后，流程进行到542，其中执行具有特殊指令530的区块链交易。在542，读取用户的账户余额(即，余额=60)。确定用户的账户余额是否大于或等于特殊指令530中指示的花费金额(即40)。在这种情况下，确定用户的账户余额大于或等于特殊指令530中指示的花费金额(即，60>=40)。然后，根据特殊指令530修改数据库(例如，从用户的账户中扣除40元)。换句话说，用于具有特殊指令530的区块链交易的数据存储阶段520成功，因此区块链交易526成功。

[0064] 与图4中的传统执行场景400不同，图5中的执行场景500在逻辑验证期间(例如，智能合约预执行阶段510)生成特殊指令。例如，特殊指令可以用于在数据验证期间验证账户

余额支持相应的区块链交易，而不是验证账户余额。因此，如果有足够的余额，所有并行区块链交易都可以成功执行。在一些实施例中，执行场景500可以用作现有基于读写集模型的区块链技术（例如，图4中的传统执行场景400）的扩展，以处理在一条数据上的多个并行区块链交易。例如，基于特殊指令的区块链技术（例如，执行场景500）可以用于具有频繁并发交易的账户，并且基于读写集模型的区块链技术可以用于具有较少或没有并发交易的账户。在一些实施例中，可以将简单逻辑命令嵌入到特殊指令中。然后可以使用特殊指令在数据存储验证阶段执行相应的逻辑验证，以确定相应的数据交易是否可以成功执行。

[0065] 优点可包括以下一个或多个。首先，可以解决从账户中并行扣除导致的双花问题。只要账户中有足够的余额（例如，根据特殊指令在逻辑上合理），就可以成功执行账户上的多个并行区块链交易。其次，引入了特殊指令作为现有的基于读写集模型的区块链技术的扩展。在智能合约中，确定余额变化的逻辑由特殊指令调用。当节点执行数据状态检查时，特殊指令用于检查余额以确定数据状态的有效性。另外，特殊指令方案可适用于对基于读写集模型的区块链技术中的一条数据应用单一策略修改的各种情况。该条数据可以具有包括数字型、状态型、和数据型中的至少一个的数据类型。

[0066] 图6是示出根据本文实施例的用于避免区块链交易中的双花问题的方法600的示例的流程图。为方便起见，方法600将被描述为由位于一个或多个位置并根据本文适当地编程的一个或多个计算机的系统执行。例如，适当编程的计算系统（例如，图1的计算系统106和/或108，图2的参与者系统202、204和/或206）可以执行方法600。

[0067] 在602处，接收指令以对一条数据执行两个或更多个区块链交易。两个或更多个区块链交易中的所有区块链交易修改（例如，增加，扣除）该条数据的值。在一些实施例中，该条数据可以是在区块链处理中使用（例如，修改的）数据。例如，该条数据可以是用户可以从中花费或向其中存款的用户账户。在一些实施例中，该条数据可以具有包括数字型、状态型、和数据型中的至少一个的数据类型。在一些实施例中，两个或更多个区块链交易是双花交易并在该条数据上并行执行。在一些实施例中，区块链是基于读写集模型的。

[0068] 在604，针对两个或更多个区块链交易中的每个区块链交易，与区块链交易相关联的智能合约被预执行以生成指示区块链交易的特殊指令。该特殊指令被用于当执行智能合约以将区块链交易写入区块链时，验证该条数据的当前值支持区块链交易。在一些实施例中，当预执行与区块链交易相关联的智能合约时，生成特殊指令而不是读写集。换句话说，当预执行与区块链交易相关联的智能合约时，没有生成读写集。例如，当执行从具有100元余额的账户中花费40元的区块链交易时，生成特殊指令（100-40）（例如，图5的528和/或530）而不生成读写集（100->60）（例如，图4的428和/或430）。

[0069] 在一些实施例中，区块链交易将从该条数据中扣除金额。在这种情况下，验证该条数据的当前值支持区块链交易包括：验证该条数据的当前值大于或等于该金额。在一些实施例中，区块链交易是将金额存入该条数据。在这种情况下，可以不执行验证该条数据的当前值支持区块链交易。例如，可以执行智能合约以将区块链交易写入区块链而不验证该条数据的当前值。在一些实施例中，针对每个区块链交易，预执行与区块链交易相关联的智能合约以生成指示区块链交易的特殊指令包括：对该条数据进行余额检查，以及如果对该条数据进行的余额检查支持区块链交易，则生成指示区块链交易的特殊指令。在一些实施例中，特殊指令指示要对该条数据执行的比较操作。例如，比较操作将该条数据的当前值与要

从该条数据中扣除的金额进行比较。

[0070] 可以修改或重新配置图6中所示的方法600以包括附加的、更少的或不同的动作(图6中未示出),其可以以所示的顺序或以不同的顺序执行。例如,在604之后,提交区块链交易以进行共识排序。响应于验证该条数据的当前值大于或等于该金额,执行与区块链交易相关联的智能合约以将区块链交易写入区块链。在一些实施例中,验证该条数据的当前值大于或等于该金额不包括:验证该条数据的当前值与指示区块链交易的特殊指令所指示的该条数据的值相同。在一些实施例中,执行与区块链交易相关联的智能合约以将区块链交易写入区块链包括:生成与区块链交易相关联的数据区块并将该数据区块发布至区块链。在一些实施例中,可以重复或迭代图6中示出的一个或多个动作,直到达到终止条件。在一些实施例中,图6中所示的一个或多个单独动作可以作为多个单独的动作来执行,或者图6中所示的动作的一个或多个子集可以被组合并作为单个动作来执行。在一些实施例中,也可以从方法600中省略图6中所示的一个或多个单独动作。

[0071] 图7描绘了根据本文实施例的装置700的模块的示例。

[0072] 装置700可以是被配置为避免区块链网络中的双花问题的区块链节点的实施例的示例,其中,区块链网络是联盟区块链网络。装置700可以对应于上述实施例,并且装置700包括以下内容:接收模块702,其接收用以在一条数据上执行两个或更多个区块链交易的指令;预执行模块704,其预执行与两个或更多个区块链交易中的区块链交易相关联的智能合约,以生成指示区块链交易的特殊指令;发送模块706,发送区块链交易以进行共识排序。

[0073] 在可选实施例中,两个或更多个区块链交易中的所有区块链交易修改该条数据的值,并且特殊指令用于在执行智能合约以将区块链交易写入区块链时验证该条数据的当前值支持区块链交易。

[0074] 在可选实施例中,在该条数据上并行执行两个或更多个区块链交易。

[0075] 在可选实施例中,区块链是基于读写集模型的。

[0076] 在可选实施例中,针对每个区块链交易,当预执行与区块链交易相关联的智能合约时,生成特殊指令而不是读写集。

[0077] 在可选实施例中,装置700还包括确定模块,用于确定该条数据的当前值大于或等于将要通过区块链交易从该条数据中扣除的金额,从而执行智能合约以将区块链交易写入区块链中。

[0078] 在可选实施例中,验证该条数据的当前值支持区块链交易不包括:验证该条数据的当前值与指示区块链交易的特殊指令所指示的该条数据的值相同。

[0079] 在可选实施例中,装置700还包括生成模块,用于生成与区块链交易相关联的数据区块,以及发布模块,用于将数据区块发布至区块链。

[0080] 在可选实施例中,装置700还包括余额检查模块,用于对该条数据进行余额检查,以及生成模块,用于如果对该条数据进行的余额检查支持区块链交易,则生成指示区块链交易的特殊指令。

[0081] 在先前实施例中示出的系统、装置、模块或单元可以通过使用计算机芯片或实体来实现,或者可以通过使用具有特定功能的产品来实现。典型的实施例设备是计算机,计算机可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板电脑、可穿戴设备或这些设备的任

意组合。

[0082] 对于装置中各个单元的功能和模块的实施例过程，可以参考前一方法中相应步骤的实施过程。为简单起见，这里省略了细节。

[0083] 由于装置实施方式基本上对应于方法实施例，对于相关部分，可参考本方法实施例中的相关描述。先前描述的装置实施例仅是示例。被描述为单独部分的模块可以或可以不是物理上分离的，并且显示为模块的部分可以是或可以不是物理模块，可以位于一个位置，或者可以分布在多个网络模块上。可以基于实际需求来选择一些或所有模块，以实现本文方案的目标。对本领域普通技术人员来讲，在不付出创造性劳动的前提下，可以理解并实现本申请的实施例。

[0084] 再次参考图7，它可以被解释为示出了区块链数据预执行装置的内部功能模块和结构。区块链数据预执行装置可以是被配置为避免区块链网络中的双花问题的区块链节点的示例。本质上，执行主体可以是电子设备，电子设备包括：一个或多个处理器；被配置为存储一个或多个处理器的可执行指令存储器。

[0085] 本文中描述的技术可以产生一种或多种技术效果。在一些实施例中，引入特殊指令作为现有的基于读写集模型的区块链技术的扩展，以处理双花问题(例如，在一条数据上执行多个并行区块链交易)。在其他实施例中，当在一条数据上执行多个并行区块链交易时，针对每个区块链交易生成特殊指令而不是读写集。在其他实施例中，特殊指令用于在执行智能合约以将相应的区块链交易写入区块链时验证该条数据的当前值支持相应的区块链交易。

[0086] 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。

[0087] 例如，在第一实施例中，计算机实现的用于避免区块链交易中的双花问题的方法，包括：接收指令以对一条数据执行两个或更多个区块链交易，其中两个或更多个区块链交易中的所有区块链交易修改该条数据的值；并且针对对两个或更多个区块链交易中的每个区块链交易：预执行与区块链交易相关联的智能合约以生成指示区块链交易的特殊指令，其中该特殊指令用于在执行智能合约以将区块链交易写入区块链时，验证该条数据的当前值是否支持区块链交易。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：

[0088] 第一特征，可与以下任意特征组合，指定两个或更多个区块链交易在该条数据上并行执行。

[0089] 第二特征，可与任何先前或以下特征组合，指定区块链基于读写集模型。

[0090] 第三特征，可与任何先前或以下特征组合，指定在预执行与区块链交易相关联的智能合约时，针对来自两个或更多个区块链交易的每个区块链交易生成特殊指令，而不是读写集。

[0091] 第四特征，可与任何先前或以下特征组合，指定针对两个或更多个区块链交易中的区块链交易从该条数据中扣除一金额，并且其中验证该条数据的当前值支持区块链交易包括验证该条数据的当前值大于或等于该金额。

[0092] 第五特征，可与任何先前或以下特征组合，所述方法包括：提交区块链交易以进行共识排序；以及响应于验证该条数据的当前值大于或等于该金额，执行与区块链交易相关联的智能合约以将区块链交易写入区块链。

[0093] 第六特征，可与任何先前或以下特征组合，指定验证该条数据的当前值大于或等于该金额不包括：验证该条数据的当前值与由指示区块链交易的特殊指令指示的该条数据的值相等。

[0094] 第七特征，可与任何先前或以下特征组合，指定执行与区块链交易相关联的智能合约以将区块链交易写入区块链包括：生成与区块链交易相关联的数据区块；以及将数据区块发布至区块链。

[0095] 第八特征，可与任何先前或以下特征组合，指定针对两个或更多个区块链交易中的每个区块链交易，预执行与区块链交易相关联的智能合约，以生成指示区块链交易的特殊指令，包括：对该条数据进行余额检查；以及如果对该条数据进行的余额检查支持区块链交易，则生成指示区块链交易的特殊指令。

[0096] 第九特征，可与任何先前或以下特征组合，指定该特殊指令指示在执行智能合约时对该条数据执行比较操作。

[0097] 在第二实施例中，一种用于避免区块链交易中的双花问题的系统，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一个或多个计算机可读存储器，所述指令可由所述一个或多个处理器执行以执行包括以下的操作：接收指令以在一条数据上执行两个或更多个区块链交易，其中，两个或更多个区块链交易中的所有区块链交易修改该条数据的值；以及针对两个或更多个区块链交易中的每个区块链交易：预执行与区块链交易相关联的智能合约，以生成指示区块链交易的特殊指令，其中，特殊指令用于在执行智能合约以将区块链交易写入区块链时，验证该条数据的当前值支持区块链交易。前述和其他所描述的实施例可以各自可选地包括一个或多个以下特征：

[0098] 第一特征，可与以下任何特征组合，指定两个或更多个区块链交易在该条数据上并行执行。

[0099] 第二特征，可与任何先前或以下特征组合，指定区块链基于读写集模型。

[0100] 第三特征，可与任何先前或以下特征组合，指定针对两个或更多个区块链交易中的每个区块链交易，在预执行与区块链交易相关联的智能合约时，生成特殊指令，而不是读写集。

[0101] 第四特征，可与任何先前或以下特征组合，指定两个或更多个区块链交易中的区块链交易从该条数据中扣除一金额，并且验证该条数据的当前值支持区块链交易包括，验证该条数据的当前值大于或等于该金额。

[0102] 第五特征，可与任何先前或以下特征组合，所述方法包括：提交区块链交易以进行共识排序；以及响应于验证该条数据的当前值大于或等于该金额，执行与区块链交易相关联的智能合约以将区块链交易写入区块链。

[0103] 第六特征，可与任何先前或以下特征组合，指定验证该条数据的当前值大于或等于该金额不包括：验证该条数据的当前值与由指示区块链交易的特殊指令指示的该条数据的值相等。

[0104] 第七特征，可与任何先前或以下特征组合，指定执行与区块链交易相关联的智能合约以将区块链交易写入区块链包括：生成与区块链交易相关联的数据区块；以及将数据区块发布至区块链。

[0105] 第八特征，可与任何先前或以下特征组合，指定针对两个或更多个区块链交易中

的每个区块链交易，预执行与区块链交易相关联的智能合约，以生成指示区块链交易的特殊指令包括：对该条数据进行余额检查；以及如果对该条数据进行的余额检查支持区块链交易，则生成指示区块链交易的特殊指令。

[0106] 第九特征，可与任何先前或以下特征组合，指定该特殊指令指示在执行智能合约时对该条数据执行比较操作。

[0107] 在第三实施例中，一种用于避免区块链交易中的双花问题的装置，所述装置包括多个模块用于执行包括以下的操作：接收指令以在一条数据上执行两个或更多个区块链交易，其中，两个或更多个区块链交易中的所有区块链交易修改该条数据的值；以及针对两个或更多个区块链交易中的每个区块链交易：预执行与区块链交易相关联的智能合约，以生成指示区块链交易的特殊指令，其中，特殊指令用于在执行智能合约以将区块链交易写入区块链时，验证该条数据的当前值支持区块链交易。前述和其他所描述的实施例可以各自可选地包括一个或多个以下特征：

[0108] 第一特征，可与以下任何特征组合，指定两个或更多个区块链交易在该条数据上并行执行。

[0109] 第二特征，可与任何先前或以下特征组合，指定区块链基于读写集模型。

[0110] 第三特征，可与任何先前或以下特征组合，指定针对两个或更多个区块链交易中的每个区块链交易，在预执行与区块链交易相关联的智能合约时，生成特殊指令，而不是读写集。

[0111] 第四特征，可与任何先前或以下特征组合，指定两个或更多个区块链交易中的区块链交易从该条数据中扣除一金额，并且验证该条数据的当前值支持区块链交易包括，验证该条数据集的当前值大于或等于该金额。

[0112] 第五特征，可与任何先前或以下特征组合，所述操作还包括：提交区块链交易以进行共识排序；以及响应于验证该条数据的当前值大于或等于该金额，执行与区块链交易相关联的智能合约以将区块链交易写入区块链。

[0113] 第六特征，可与任何先前或以下特征组合，指定验证该条数据的当前值大于或等于该金额不包括：验证该条数据的当前值与由指示区块链交易的特殊指令指示的该条数据的值相等。

[0114] 第七特征，可与任何先前或以下特征组合，指定执行与区块链交易相关联的智能合约以将区块链交易写入区块链包括：生成与区块链交易相关联的数据区块；以及将数据区块发布至区块链。

[0115] 第八特征，可与任何先前或以下特征组合，指定针对两个或更多个区块链交易中的每个区块链交易，预执行与区块链交易相关联的智能合约，以生成指示区块链交易的特殊指令，包括：对该条数据进行余额检查；以及如果对该条数据进行的余额检查支持区块链交易，则生成指示区块链交易的特殊指令。

[0116] 第九特征，可与任何先前或以下特征组合，指定该特殊指令指示在执行智能合约时对该条数据执行比较操作。

[0117] 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例可以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,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,其具有编码或存储在其上的指令。载体可以是有形的非暂态计算机存储介质,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)或其他类型的媒体。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可以部分是可机读存储设备、可机读存储基板、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。

[0118] 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、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,包括编译或演绎语言、或说明或程序语言;它可以配置为任何形式,包括作为独立程序,或者作为模块、组件、引擎、子程序或适合在计算环境中执行的其他单元,该环境可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。

[0119] 计算机程序可以但非必须对应于文件系统中的文件。计算机程序可以存储在:保存其他程序或数据的文件的一部分中,例如,存储在标记语言文档中的一个或多个脚本;专用于所讨论的程序的单个文件;或者多个协调文件,例如,存储一个或多个模块、子程序或代码部分的多个文件。

[0120] 举例来说,用于执行计算机程序的处理器包括通用和专用微处理器,以及任何类型的数字计算机的任意一个或多个处理器。通常,处理器将接收用于执行的计算机程序的指令以及来自耦接到处理器的非暂时性计算机可读介质的数据。

[0121] 术语“数据处理装置”包括所有类型的用于处理数据的装置、设备和机器,包括例如可编程处理器、计算机或多个处理器或计算机。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一个或多个的组合的代码。

[0122] 本文中描述的处理和逻辑流程可由一台或多台计算机或处理器执行一个或多个计算机程序执行,以执行通过运行输入数据并生成输出的操作。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。

[0123] 适合于执行计算机程序的计算机可以基于通用和/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。

[0124] 通常,计算机将包括或可操作地耦接至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时性计算机可读介质。但是,计算机不需要这样的设备。因此,计算机可以耦接到一个或多个存储设备,例如,本地和/或远程的一个或多个存储器。例如,计算机可以包括作为计算机的集成组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)接收器或便携式存储设备，例如，通用串行总线(USB)闪存驱动器，这里仅举几例。

[0125] 组件可以通过可交换地彼此“耦接”，例如直接地或通过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，组件也可以彼此“耦接”。例如，存储组件集成到处理器(例如，L2高速缓存组件)中即“耦接到”处理器中。

[0126] 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施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；以及输入设备，用户可以通过该输入设备向该计算机提供输入，例如键盘和例如鼠标、轨迹球或触摸板等的指针设备。其他类型的设备也可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，通过向用户设备上的web浏览器发送web页面以响应从web浏览器收到的请求，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)轮流发送文本消息或其他形式的消息，并接收来自用户的响应消息来与用户交互。

[0127] 本文使用与系统、装置和计算机程序组件有关的术语“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。

[0128] 虽然本文包含许多具体实施例细节，但是这些不应被解释为由权利要求本身限定的对要求保护的范围的限制，而是作为对特定实施例中的具体特征的描述。在本文多个单独实施例的上下文中的描述的多个特定特征也可以在单个实施例的组合中实现。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描述为以某些组合起作用并且甚至最初如此要求保护，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，并且可以要求保护指向子组合或子组合的变体。

[0129] 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。在特定情况下，多任务和并行处理可能是有利的。此外，上述实施例中的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或者打包成多个软件产品。

[0130] 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的范围内。例如，权利要求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。

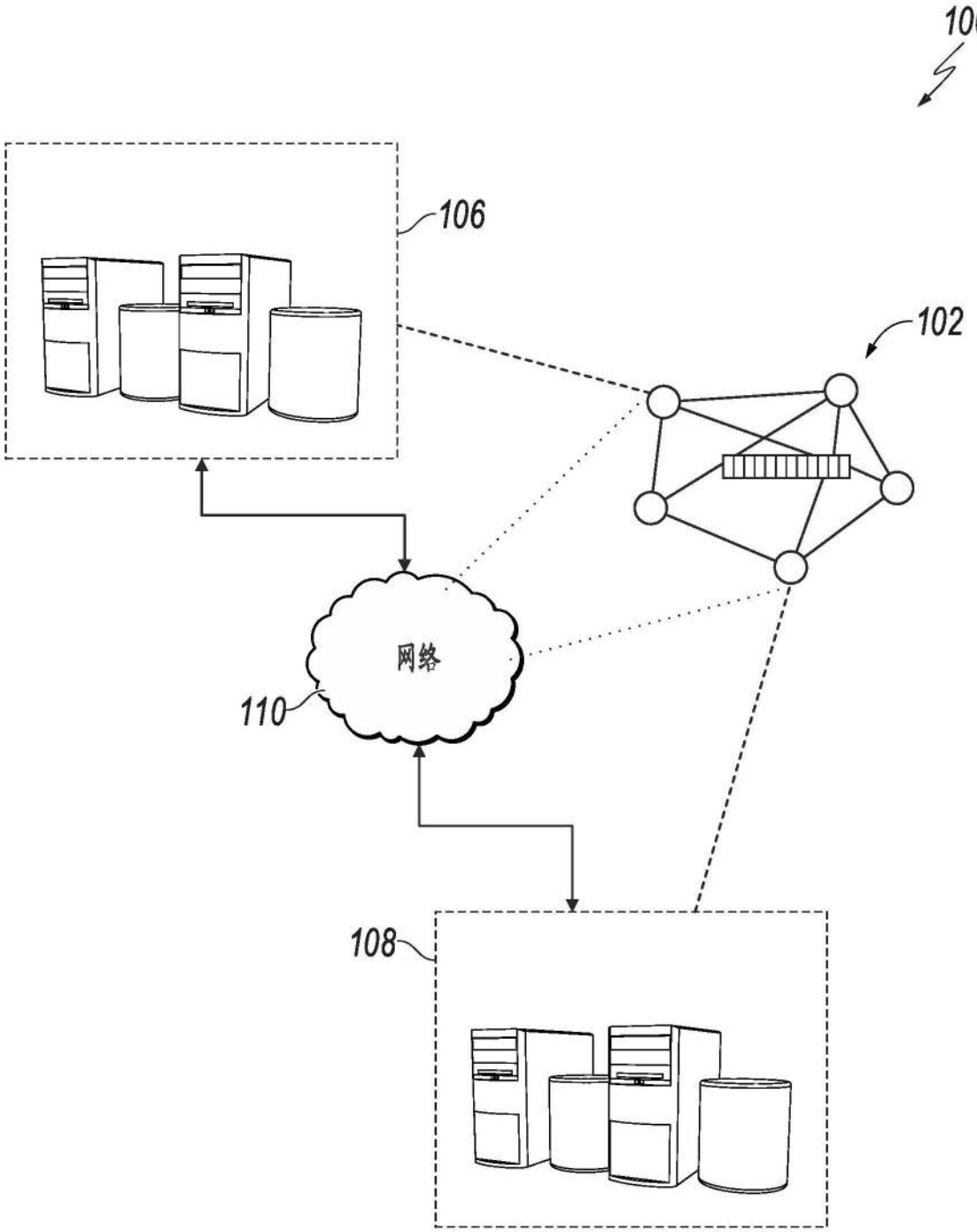


图1

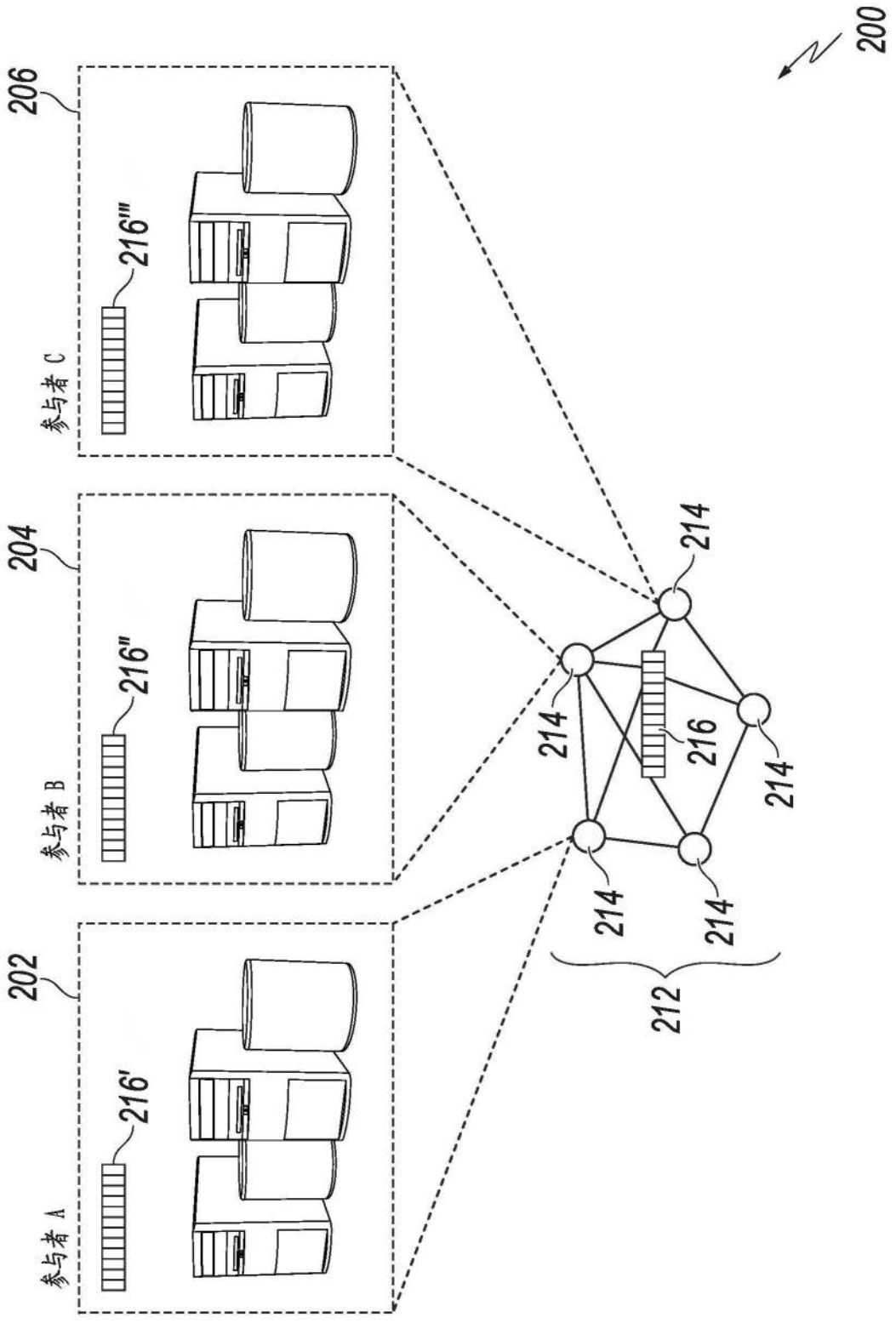

200
206
216'''
参与者 C
204
216''
参与者 B
202
216'
参与者 A
214
214
216
214
214
214
212

图2

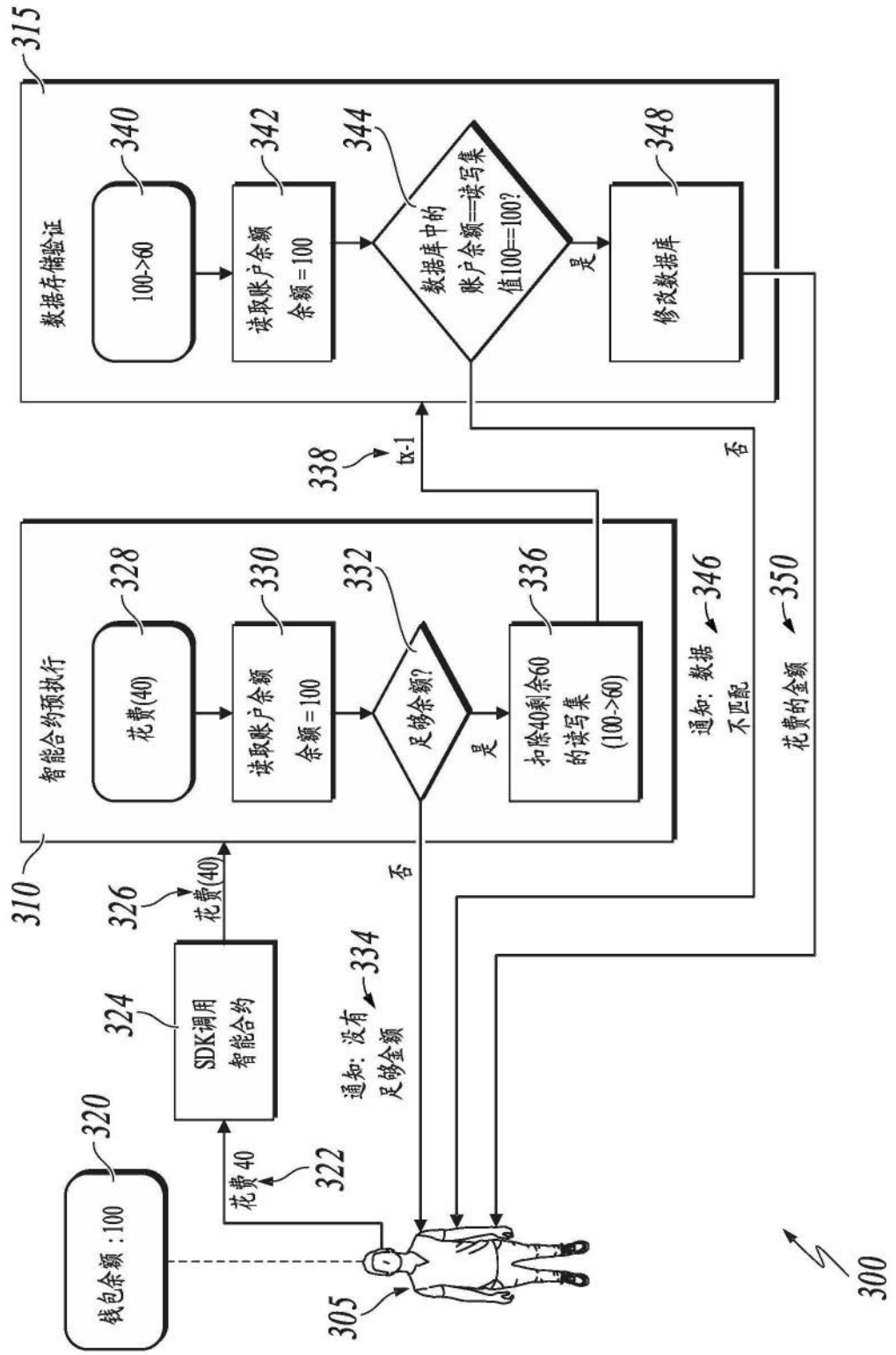

315
数据存储验证
340
100->60
342
读取账户余额
余额=100
344
数据库中的
账户余额==读写集
值100==100?
是
348
修改数据库
338
fx-1
否
310
智能合约预执行
328
花费(40)
330
读取账户余额
余额=100
332
足够余额?
是
336
扣除40剩余60
的读写集
(100->60)
通知: 数据
不匹配
346
花费的金额
350
326
花费(40)
324
SDK调用
智能合约
否
通知: 没有
足够金额
334
320
钱包余额 :100
花费40
322
305
300

图3

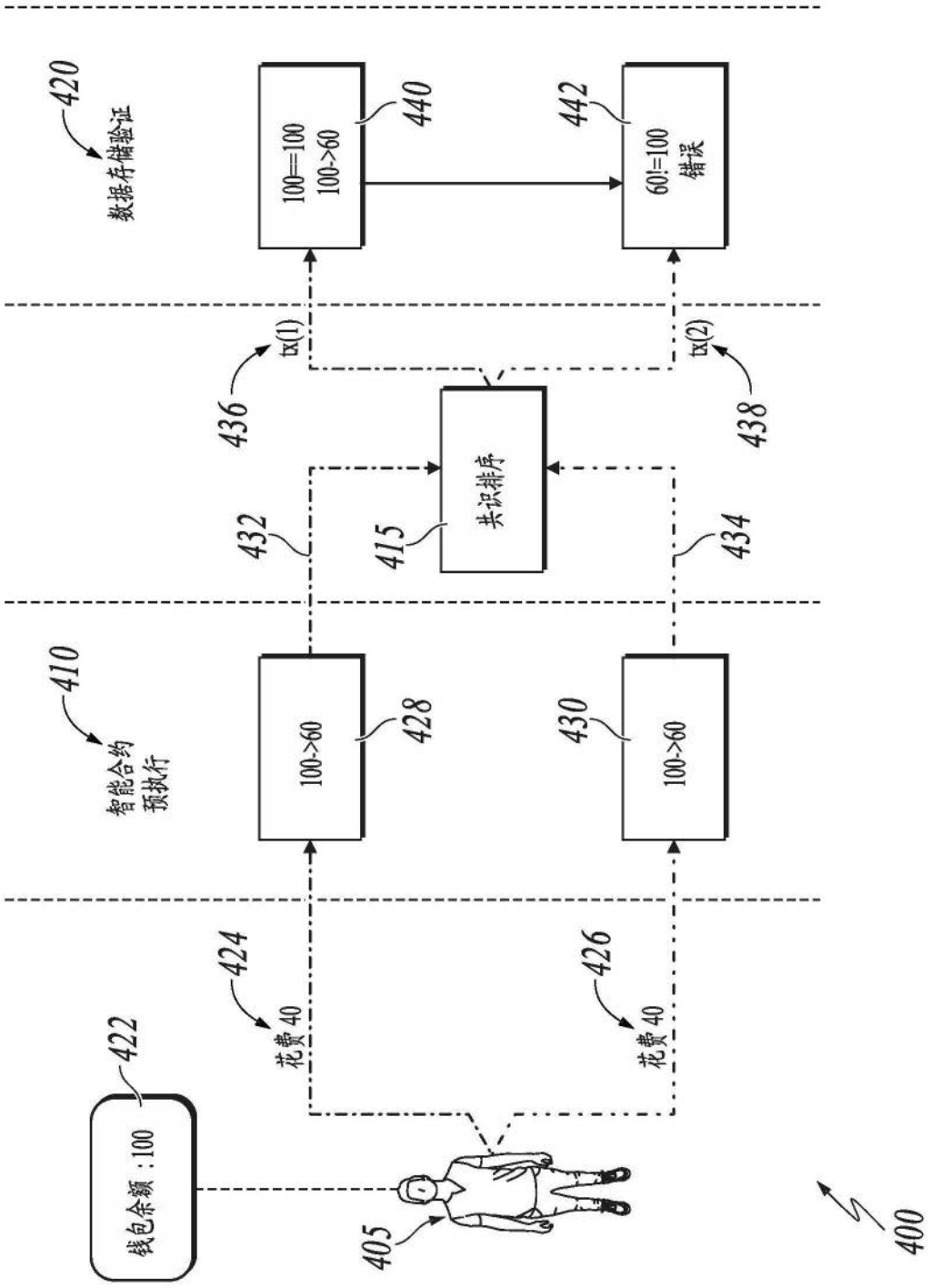

420
数据存储验证
100==100
100->60
440
442
60!=100
错误
tx(1)
tx(2)
436
438
共识排序
415
432
434
410
智能合约
预执行
100->60
428
100->60
430
424
花费40
426
花费40
422
钱包余额：100
405
400

图4

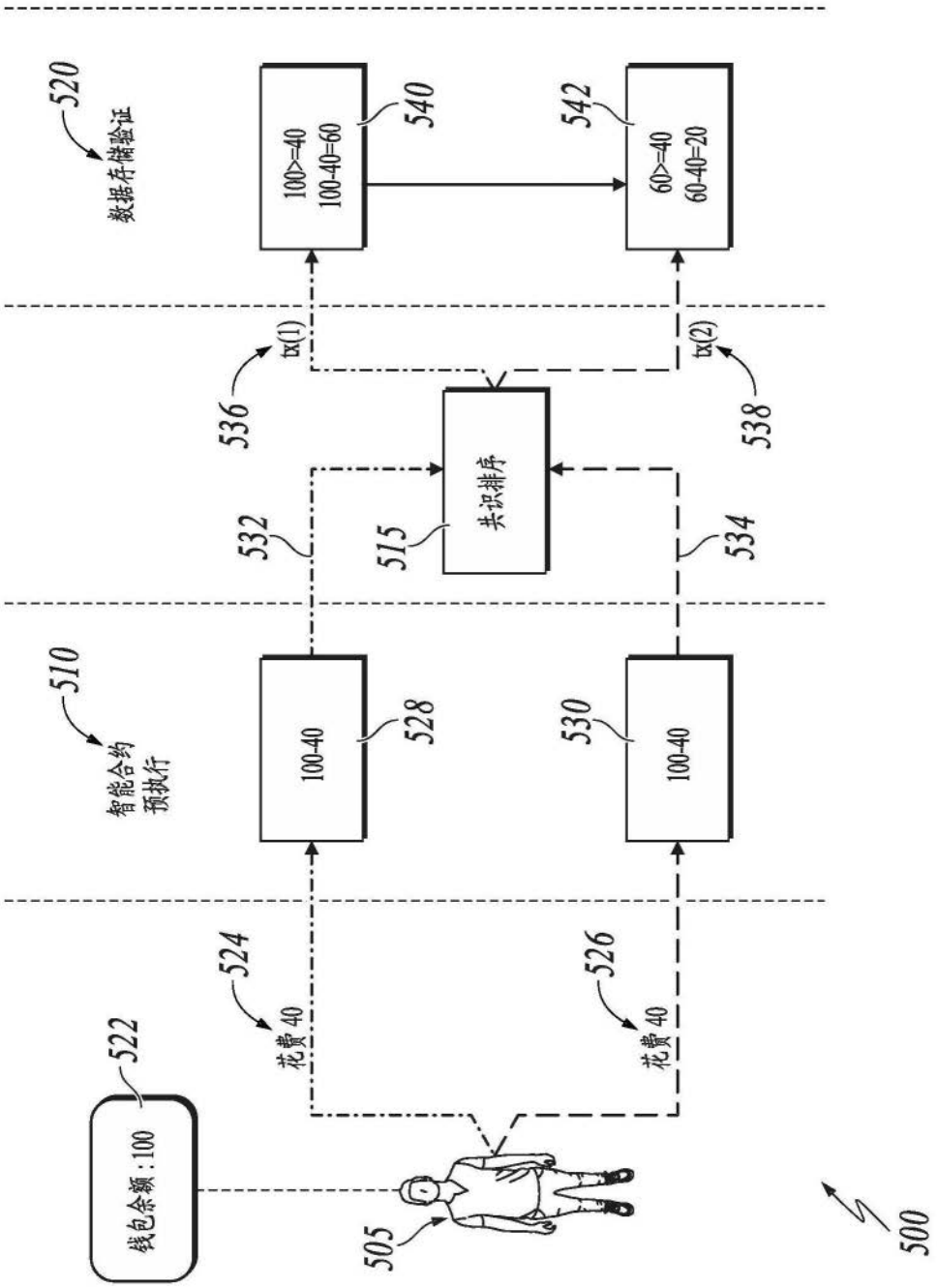

520
数据存储验证
100>=40
100-40=60
540
542
60>=40
60-40=20
tx(1)
tx(2)
536
538
共识排序
515
532
534
510
智能合约
预执行
100-40
528
530
100-40
524
花费40
526
花费40
522
钱包余额:100
505
500

图5

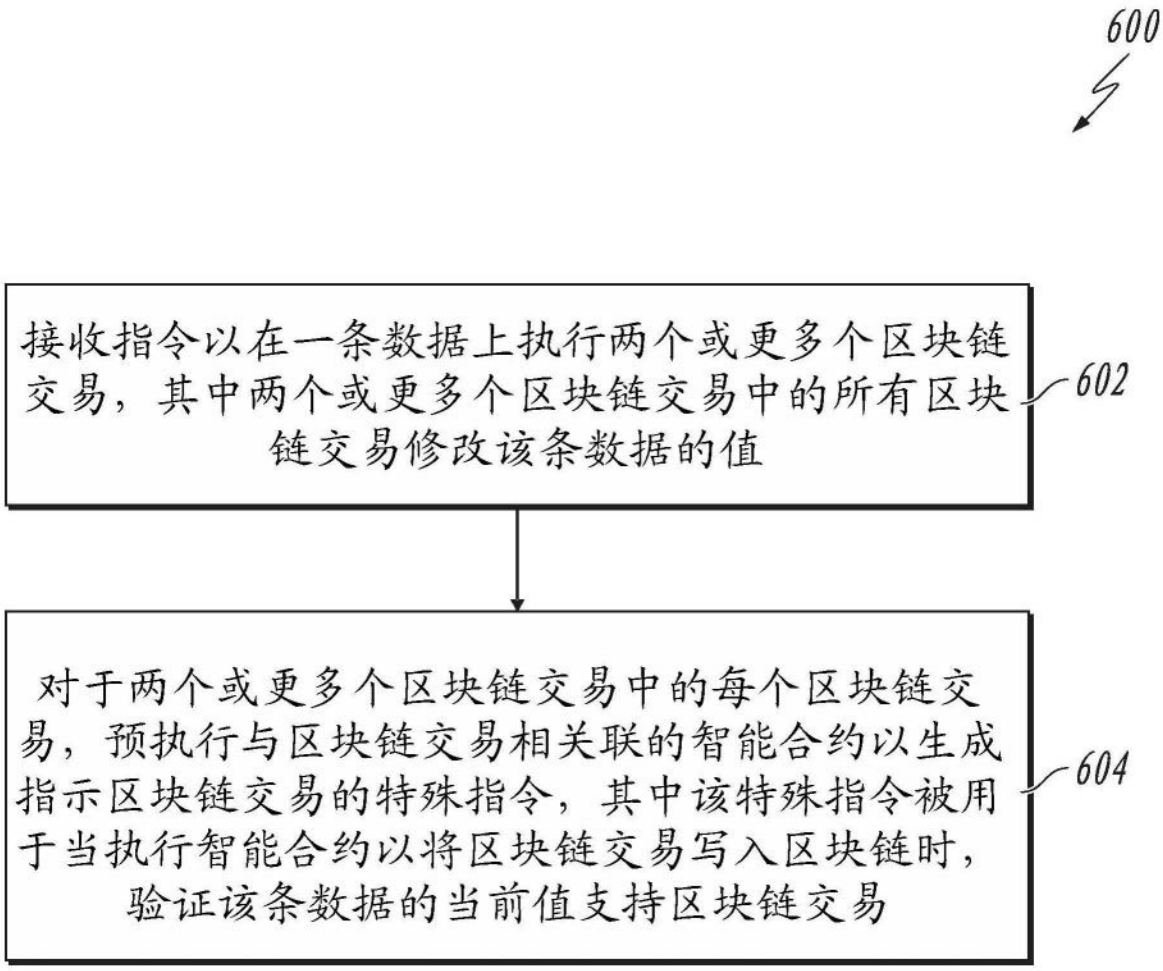

600
接收指令以在一条数据上执行两个或更多个区块链交易，其中两个或更多个区块链交易中的所有区块链交易修改该条数据的值
602
对于两个或更多个区块链交易中的每个区块链交易，预执行与区块链交易相关联的智能合约以生成指示区块链交易的特殊指令，其中该特殊指令被用于当执行智能合约以将区块链交易写入区块链时，验证该条数据的当前值支持区块链交易
604

图6

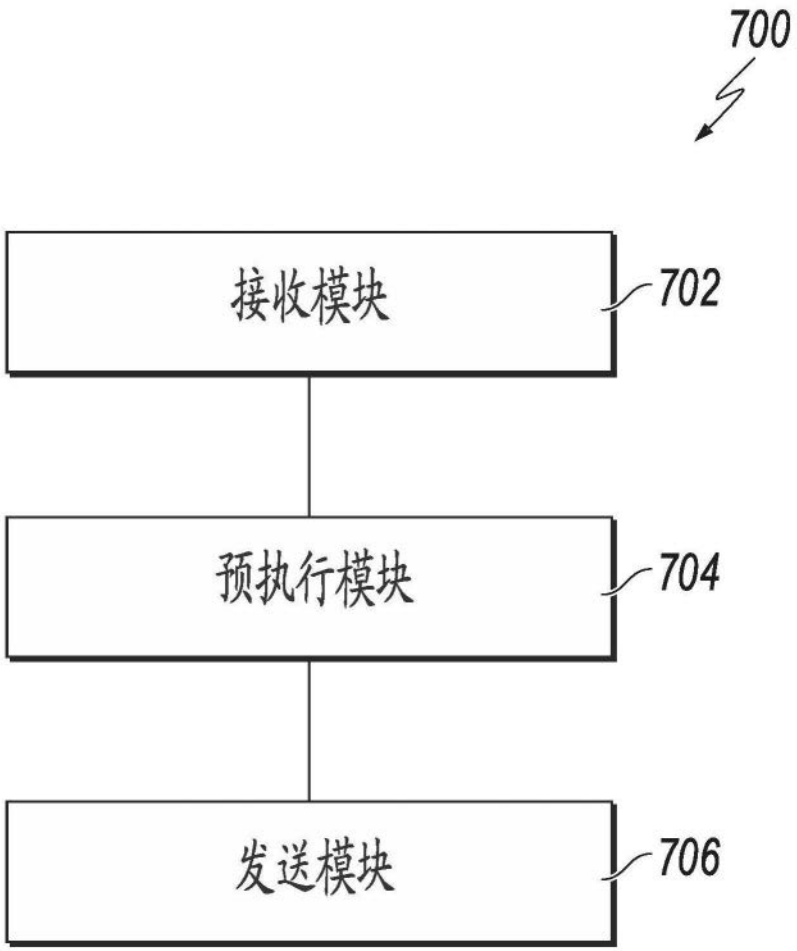


图7