(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110291756 B
(45)授权公告日 2023.07.14

(21)申请号 201880011031.3
(22)申请日 2018.11.07
(65)同一申请的已公布的文献号
申请公布号 CN 110291756 A
(43)申请公布日 2019.09.27
(85)PCT国际申请进入国家阶段日
2019.08.08
(86)PCT国际申请的申请数据
PCT/CN2018/114322 2018.11.07
(87)PCT国际申请的公布数据
WO2019/072262 EN 2019.04.18
(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 刘正 李漓春 殷山
(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.
H04L 9/14(2006.01)
审查员 朱华慧

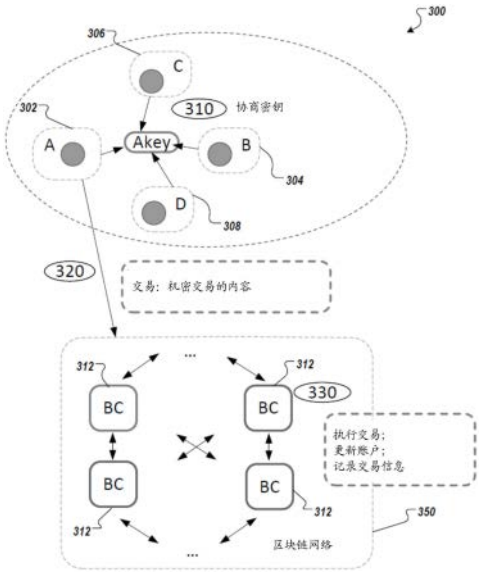
权利要求书3页 说明书12页 附图5页

(54)发明名称

在区块链机密交易中恢复加密交易信息

(57)摘要

本公开的实施方式包括:由客户端节点根据多个客户端节点同意的阈值秘密共享方案来获得密钥;通过将加密承诺方案应用于交易数据,生成所述客户端节点的机密交易的一个或多个承诺值;通过使用所述密钥加密所述交易数据来生成所述机密交易的加密交易信息;以及将所述机密交易的内容发送至区块链网络中的共识节点以供执行,其中,所述机密交易的所述内容包括:所述一个或多个承诺值;所述加密交易信息;以及所述交易数据的一个或多个零知识证明。



CN 110291756 B

1.一种计算机实现的客户端节点参与区块链机密交易的方法,所述方法包括:

由客户端节点根据经多个客户端节点同意的阈值秘密共享方案来获得密钥;

通过将加密承诺方案应用于交易数据,生成所述客户端节点的机密交易的一个或多个承诺值;

通过使用所述密钥加密所述交易数据来生成所述机密交易的加密交易信息;以及

将所述机密交易的内容发送至区块链网络中的共识节点以由所述区块链网络中的所述共识节点基于所述机密交易的所述内容验证所述机密交易有效,并将所述加密交易信息存储在所述区块链网络的区块链上,其中,所述机密交易的所述内容包括:

所述一个或多个承诺值;

所述加密交易信息;以及

所述交易数据的一个或多个零知识证明。

2.如权利要求1所述的方法,其中,所述机密交易的所述交易数据包括:所述客户端节点在所述机密交易之前的账户余额和/或所述机密交易的交易金额。

3.如权利要求1所述的方法,其中,所述交易数据的所述一个或多个零知识证明包括:关于所述交易数据的值在相应的范围内的一个或多个零知识范围证明。

4.如权利要求1所述的方法,

其中,所述加密承诺方案包括佩德森承诺方案;

其中,通过将加密承诺方案应用于交易数据来生成所述客户端节点的机密交易的一个或多个承诺值,包括:基于所述交易数据和对应于所述交易数据的随机数生成所述客户端节点的所述机密交易的所述一个或多个承诺值;以及

其中,生成所述机密交易的加密交易信息,包括:通过使用所述密钥加密所述交易数据和对应于所述交易数据的随机数来生成所述机密交易的加密交易信息。

5.如权利要求1所述的方法,其中,所述阈值秘密共享方案包括夏米尔的秘密共享方案。

6.一种计算机实现的区块链网络的共识节点参与区块链机密交易的方法,所述方法包括:

由区块链网络中的共识节点接收客户端节点的机密交易的内容,其中,所述机密交易的所述内容包括:

由所述客户端节点通过将加密承诺方案应用于所述机密交易的交易数据生成的所述机密交易的一个或多个承诺值;

通过使用所述客户端节点的密钥加密所述交易数据生成的加密交易信息,其中,所述客户端节点根据与多个客户端节点的阈值秘密共享方案获得密钥;以及

所述交易数据的一个或多个零知识证明;

由所述区块链网络中的所述共识节点基于所述机密交易的所述内容验证所述机密交易有效;以及

由所述区块链网络中的所述共识节点将所述加密交易信息存储在所述区块链网络的区块链上。

7.如权利要求6所述的方法,其中,所述机密交易的所述交易数据包括:所述客户端节点在所述机密交易之前的账户余额和/或所述机密交易的交易金额。

8.如权利要求6所述的方法,其中,所述交易数据的所述一个或多个零知识证明包括:关于所述交易数据的值在相应范围内的一个或多个零知识范围证明。

9.如权利要求6所述的方法,其中,基于所述机密交易的所述内容验证所述机密交易有效,包括:

基于所述承诺方案确定所述一个或多个承诺值正确;以及

验证所述交易数据的所述一个或多个零知识证明。

10.如权利要求9所述的方法,其中,验证所述交易数据的所述一个或多个零知识证明,包括:

确定所述客户端节点在所述机密交易之前的账户余额大于零;以及

确定所述机密交易的交易金额小于或等于所述客户端节点在所述机密交易之前的账户余额。

11.如权利要求6所述的方法,其中,

所述加密承诺方案是同态的,并且

所述方法进一步包括:基于所述承诺方案的同态性在所述机密交易之后更新所述客户端节点的账户余额。

12.如权利要求6所述的方法,其中,所述阈值秘密共享方案包括夏米尔的秘密共享方案。

13.一种计算机实现的用于在区块链机密交易中恢复加密交易信息的方法,所述方法包括:

由特定客户端节点从区块链网络中的共识节点接收所述特定客户端节点的机密交易的加密交易信息,其中,所述加密交易信息被存储在所述区块链网络中的至少一个区块链中,所述特定客户端节点不能访问配置为解密所述加密交易信息的密钥,并且所述特定客户端节点先前被发布了所述密钥;

由所述特定客户端节点根据由所述区块链网络上的多个客户端节点同意的阈值秘密共享方案,从所述多个客户端节点中的至少阈值数量的客户端节点恢复所述密钥;以及

由所述特定客户端节点使用所述恢复的密钥从所述加密交易信息解密出所述特定客户端节点的所述机密交易的交易数据。

14.如权利要求13所述的方法,其中,所述阈值秘密共享方案包括夏米尔的秘密共享方案。

15.如权利要求13所述的方法,其中,使用所述密钥从所述加密交易信息解密出所述特定客户端节点的所述机密交易的交易数据,包括:使用所述密钥恢复所述机密交易的转移金额。

16.如权利要求11所述的方法,其中,使用所述密钥从所述加密交易信息解密出所述特定客户端节点的所述机密交易的交易数据,包括:使用所述密钥恢复所述机密交易的转移金额和对应于所述转移金额的随机数,其中,所述转移金额和所述随机数使用在用于隐藏所述特定客户端节点的所述机密交易的交易信息的佩德森承诺方案中。

17.一种耦接到一个或多个处理器且其上存储有指令的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,促使所述一个或多个处理器根据权利要求1-16中任一项所述的方法执行操作。

18.一种计算系统,包括:

一种计算设备;以及

一种耦接到所述计算设备且其上存储有指令的计算机可读存储介质,当所述指令由所述计算设备执行时,促使所述计算设备根据权利要求1-16中任一项所述的方法执行操作。

在区块链机密交易中恢复加密交易信息

技术领域

[0001] 本公开涉及区块链技术领域。

背景技术

[0002] 分布式账本(DLS),也可被称为共识网络和/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(例如加密货币)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。公有区块链网络向所有实体开放使用DLS,并开放参与共识处理。为特定实体提供私有区块链网络,该实体集中控制读写权限。为选择的实体组提供联盟区块链网络,该实体组控制共识处理,并包含访问控制层。

[0003] 区块链用于加密货币网络,加密货币网络使得参与者能够使用加密货币进行交易以买卖商品和/或买卖服务。在加密货币网络中,记账模型用于记录用户之间的交易。示例性记账模型包括未消费交易输出(UTXO)模型,以及账户模型(也称为基于账户的模型或账户/余额模型)。

[0004] 在UTXO模型中,链上的资产以交易的形式存在。每笔交易消费来自先前交易的输出并生成可以在后续交易中消费的新输出。跟踪用户的未消费交易,并且计算未消费交易的总和作为该用户拥有的用于消费的余额。每笔交易可使用一个或多个未消费输出(且只有未消费输出)作为输入并且可以具有一个或多个输出。为了防止双花和欺诈,有必要要求在进一步的交易中仅使用未消费的输出。该UTXO模型支持交易验证和证明功能,但对智能合约的支持较弱。

[0005] 以太坊采用账户模型。账户模型像传统银行一样进行记账并管理账户余额。在此模型下,账户可以拥有地址和相应的账户余额。链上的资产被表示为账户的余额。每笔转移交易可以具有转移资产的账户地址以及接收资产的账户地址。交易金额直接在账户余额上更新。该账户模型是高效的,原因在于每笔交易可以仅需要验证发送账户具有足够的余额来支付交易。除了支持交易验证和证明功能外,账户模型还可以完全支持智能合约,特别是那些需要状态信息或涉及多方的合约。

发明内容

[0006] 本公开的实施方式包括计算机实现的用于基于区块链技术的机密交易的方法(称为区块链机密交易或简称为机密交易)。更具体地,本公开的实施方式涉及在区块链机密交易中恢复加密的交易信息。

[0007] 在一些实施方式中,动作包括:由客户端节点根据多个客户端节点同意的阈值秘密共享方案来获得密钥;通过将加密承诺方案应用于交易数据,生成所述客户端节点的机密交易的一个或多个承诺值;通过使用所述密钥加密所述交易数据来生成所述机密交易的加密交易信息;并且将所述机密交易的内容发送至区块链网络中的共识节点以供执行,其中,所述机密交易的所述内容包括:所述一个或多个承诺值;所述加密交易信息;以及所述

交易数据的一个或多个零知识证明。

[0008] 在一些实施方式中，动作包括：由区块链网络中的共识节点接收客户端节点的机密交易的内容，其中，所述机密交易的所述内容包括：所述客户端节点通过将加密承诺方案应用于所述机密交易的交易数据生成的所述机密交易的一个或多个承诺值；通过使用所述客户端节点的密钥加密所述交易数据生成的加密交易信息，其中，所述客户端节点根据与多个客户端节点的阈值秘密共享方案获得密钥；以及所述交易数据的一个或多个零知识证明；由所述区块链网络中的所述共识节点基于所述机密交易的所述内容验证所述机密交易有效；以及由所述区块链网络中的所述共识节点将所述加密交易信息存储在所述区块链网络的区块链上。

[0009] 在一些实施方式中，动作包括：由特定客户端节点从区块链网络中的共识节点接收所述特定客户端节点的机密交易的加密交易信息，其中，所述加密交易信息被存储在所述区块链网络中的至少一个区块链中，其中，所述特定客户端节点不能访问配置为解密所述加密交易信息的密钥，且其中所述特定客户端节点先前被发布了所述密钥；由所述区块链网络上的所述特定客户端节点根据由多个客户端节点同意的阈值秘密共享方案，从所述多个客户端节点中的至少阈值数量的客户端节点恢复所述密钥；以及由所述特定客户端节点使用所述恢复的密钥从所述加密交易信息中解密出所述特定客户端节点的所述机密交易的交易数据。

[0010] 其他实施方式包括相应系统、装置以及配置为执行所述方法的动作、编码在计算机存储设备上的计算机程序。

[0011] 这些及其他实施方式可以各自可选地包括如下一个或多个特征：

[0012] 第一特征，可与以下任一特征组合，其中，所述机密交易的所述交易数据包括：所述客户端节点在所述机密交易之前的账户余额和/或所述机密交易的交易金额。

[0013] 第二特征，可与先前或以下任一特征组合，其中，所述交易数据的一个或多个零知识证明包括所述交易数据的值在相应的范围内的一个或多个零知识范围证明。

[0014] 第三特征，可与先前或以下任一特征组合，其中，所述加密承诺方案包括佩德森(Pedersen)承诺方案，其中，通过将加密承诺方案应用于交易数据来生成所述客户端节点的机密交易的一个或多个承诺值包括：基于所述交易数据以及对应于所述交易数据的随机数生成所述客户端节点的所述机密交易的一个或多个承诺值；并且其中，生成所述机密交易的加密交易信息包括：通过使用所述密钥加密所述交易数据和对应于所述交易数据的随机数来生成所述机密交易的加密交易信息。

[0015] 第四特征，可与先前或以下任一特征组合，其中，所述阈值秘密共享方案包括夏米尔(Shamir)的秘密共享方案。

[0016] 第五特征，可与先前或以下任一特征组合，其中，基于所述机密交易的所述内容验证所述机密交易有效包括：基于所述承诺方案确定所述一个或多个承诺值正确；并验证所述交易数据的所述一个或多个零知识证明。

[0017] 第六特征，可与先前或以下任一特征组合，其中，验证所述交易数据的所述一个或多个零知识证明包括：确定所述客户端节点在所述机密交易之前的账户余额大于零；并且确定所述机密交易的交易金额小于或等于所述客户端节点在所述机密交易之前的账户余额。

[0018] 第七特征，可与先前或以下任一特征组合，其中，所述加密承诺方案是同态的，且所述方法进一步包括基于所述承诺方案的同态性在所述机密交易之后更新所述客户端节点的账户余额。

[0019] 第八特征，可与先前或以下任一特征组合，其中，使用所述密钥从所述加密交易信息解密出所述特定客户端节点的所述机密交易的交易数据，包括：使用所述密钥恢复所述机密交易的转移金额。

[0020] 第九特征，可与先前或以下任一特征组合，其中，使用所述密钥从所述加密交易信息解密出所述特定客户端节点的所述机密交易的交易数据，包括：使用所述密钥恢复所述机密交易的转移金额和对应于所述转移金额的随机数，其中，所述转移金额和所述随机数使用在用于隐藏所述特定客户端节点的所述机密交易的交易信息的佩德森承诺方案中。

[0021] 本公开还提供了耦接到一个或多个处理器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，所述指令将促使所述一个或多个处理器按照本文提供的所述方法的实施方式执行操作。

[0022] 本公开还提供了用于实现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；以及耦接到所述一个或多个处理器其上存储有指令的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，所述指令将促使所述一个或多个处理器按照本文提供的所述方法的实施方式执行操作。

[0023] 应理解，根据本公开的方法可包括本文所述的各方面和特征的任意组合。也就是说，根据本公开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。

[0024] 在附图和以下描述中阐述了本公开的一个或多个实施方式的细节。根据说明书和附图以及权利要求，本公开的其他特征和优点将显而易见。

附图说明

[0025] 图1描绘了可用于执行本公开的实施方式的示例性环境。

[0026] 图2描绘了根据本公开的实施方式的示例性概念架构。

[0027] 图3描绘了根据本公开的实施方式的用于准备机密交易的示例性处理300。

[0028] 图4描绘了根据本公开的实施方式的机密交易的交易信息的示例性恢复处理400。

[0029] 图5描绘了可以根据本公开的实施方式执行的示例性处理。

[0030] 各附图中相同的附图标记表示相同元件。

实施方式

[0031] 本公开的实施方式包括计算机实现的用于基于区块链技术的机密交易的方法。更具体地，本公开的实施方式涉及在区块链机密交易中恢复加密的交易信息。

[0032] 在一些实施方式中，动作包括：由客户端节点根据多个客户端节点同意的阈值秘密共享方案来获得密钥；通过将加密承诺方案应用于交易数据，生成所述客户端节点的机密交易的一个或多个承诺值；通过使用所述密钥加密所述交易数据来生成所述机密交易的加密交易信息；并且将所述机密交易的内容发送至区块链网络中的共识节点以供执行，其中，所述机密交易的所述内容包括：所述一个或多个承诺值；所述加密交易信息；以及所述

交易数据的一个或多个零知识证明。

[0033] 在一些实施方式中，动作包括：通过区块链网络中的共识节点接收客户端节点的机密交易的内容，其中，所述机密交易的所述内容包括：由所述客户端节点通过将加密承诺方案应用于所述机密交易的交易数据生成的所述机密交易的一个或多个承诺值；通过使用所述客户端节点的密钥加密所述交易数据生成的加密交易信息，其中，所述客户端节点根据与多个客户端节点的阈值秘密共享方案获得密钥；以及所述交易数据的一个或多个零知识证明；由所述区块链网络中的所述共识节点基于所述机密交易的所述内容验证机密交易有效；以及通过所述区块链网络中的所述共识节点将所述加密交易信息存储在所述区块链网络的区块链上。

[0034] 在一些实施方式中，动作包括：由特定客户端节点从区块链网络中的共识节点接收所述特定客户端节点的机密交易的加密交易信息，其中，所述加密交易信息被存储在所述区块链网络中的至少一个区块链中，其中，所述特定客户端节点不能访问配置为解密所述加密交易信息的密钥，且其中所述特定客户端节点先前被发布了所述密钥；由所述特定客户端节点根据由多个客户端节点同意的阈值秘密共享方案，从所述区块链网络上的所述多个客户端节点中的至少阈值数量的客户端节点恢复所述密钥；以及由所述特定客户端节点使用所述恢复的密钥从所述加密交易信息中解密出所述特定客户端节点的所述机密交易的交易数据。

[0035] 为本公开的实施方式提供进一步的背景，并且如上所述，分布式账本系统(DLS)也可称为共识网络(例如，由点对点(Peer-to-Peer)节点组成)和区块链网络，使参与实体能够安全地、不可篡改地进行交易和存储数据。尽管术语“区块链”通常和加密货币网络相关联，但在不参考任何特定用例的情况下，本文使用区块链一般指DLS。如上所述，区块链网络可以被提供为公有区块链网络、私有区块链网络以及联盟区块链网络。

[0036] 在公有区块链网络中，共识处理由共识网络的节点控制。例如，数百、数千甚至数百万个实体可以协同运作公有区块链网络，每个实体操作该公有区块链网络中的至少一个节点。因此，公有区块链网络可被认为是关于参与实体的公有网络。在一些示例中，大多数实体(节点)必须对每个区块签名以使该区块有效，并且被添加到区块链网络的区块链(分布式账本)中。示例性公有区块链网络包括点对点支付网络。该网络利用被称为区块链的分布式账本。然而，如上所述，术语“区块链”通常用于指代分布式账本。

[0037] 通常，公有区块链网络支持公开交易。公开交易被公有区块链网络中的所有节点共享，并存储在全局区块链中。全局区块链是跨所有节点复制的区块链。也即，所有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，同意将向区块链添加区块)，在公有区块链网络内实施共识协议。示例性共识协议包括但不限于工作量证明(POW)。

[0038] 通常，为特定实体提供私有区块链网络，该特定实体集中控制读写权限。该实体控制哪些节点能参与到该区块链网络中。因此，私有区块链网络通常被称为许可网络，其限制允许谁参与网络，以及它们的参与级别(例如，仅在某些交易中)。各种类型的访问控制机制可被使用(例如，现有参与者投票添加新实体，监管机构可以控制许可)。

[0039] 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，共识处理由授权的节点集控制，一个或多个节点由相应实体(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，其中每

个实体可以操作联盟区块链网络中的至少一个节点。因此，联盟区块链网络可被认为是与参与实体相关的私有网络。在一些示例中，每个实体(节点)必须对每个区块签名，以使该区块有效并被添加到该区块链中。在一些示例中，至少实体(节点)的子集(例如至少7个实体)必须对每个区块签名，以使区块有效并被添加至区块链中。

[0040] 本文参考联盟区块链网络进一步详细描述本公开的实施方式。然而，可以预期，本公开的实施方式可以在任何适当类型的区块链网络中实现。

[0041] 鉴于以上背景，本文进一步详细描述了本公开的实施方式。更具体地，且如上所述，本公开的实施方式涉及在区块链机密交易中恢复加密交易信息。

[0042] 区块链是一种防篡改的共享数字账本，其记录公有或私有点对点网络中的交易。账本被分发至网络中的所有成员节点，并且在网络中发生的资产交易历史被永久地记录在区块中。由于账本对参与的实体完全公开，因此区块链账本自身没有隐私保护功能，并且需要额外的技术以保护资产交易的内容的隐私。

[0043] 用于区块链的隐私保护技术可以包括用于实现机密交易以保护交易内容的隐私的技术。在机密交易中，交易的内容只能由交易的参与者访问或知晓，而不是任何其他外人。例如，机密交易只允许参与交易的双方私下知道正在进行交易的金额，并且防止外部观察者知道该信息。

[0044] 用于区块链的隐私保护技术还可以包括例如可以使用隐形地址或环签名机制来实现的用于保护交易方的身份的技术。

[0045] 通过向区块链添加隐私保护(例如，在机密交易的背景下)，可以使用诸如佩德森(Pedersen)承诺方案的承诺方案来隐藏或加密客户端节点的特定交易信息。该交易信息可以包括，例如交易之前的用户账户余额、交易金额和/或其他信息。例如，客户端节点(也称为客户端、用户、当事人或交易的参与者)可以根据Pedersen承诺方案许诺或承诺交易前账户余额a和相应的随机数r。客户端节点可以保存值a和随机数r。一旦与承诺相对应的a或r丢失，账户中的余额就不能被客户端节点使用。例如，在a和r都丢失的情况下，客户端节点既不知道余额a也不知道与该余额对应的随机数r。在仅丢失r但不丢失a的情况下，客户端节点可以知道余额t，但是不能使用其自己的余额，因为余额的使用涉及r的运算。在丢失a的情况下，客户端不知道他或她自己的余额。如果客户端节点的计算能力有限，则客户端节点不能修复或恢复明文金额a。

[0046] 描述了当承诺方案(例如，Pedersen承诺)被用于隐藏或加密交易的信息时的示例性技术以解决上述问题。所描述的技术可以使客户端节点在这种交易信息丢失的情况下恢复原始明文交易信息(例如，被承诺值a和/或随机数r)成为可能并且更容易。

[0047] 所描述的技术包括用于恢复区块链机密交易中隐藏的交易信息(例如，已经丢失的被承诺交易值a)的恢复方案。在一些实施方式中，所描述的技术包括在区块链网络中的一个或多个区块链中存储隐藏的交易信息。在一些实施方式中，存储在区块链中的机密交易的隐藏的交易信息可被加密。加密前的信息可以称为明文信息。加密后得到的信息可以称为加密或密文信息。

[0048] 在一些实施方式中，客户端节点可以使用密钥将特定交易数据(即，明文交易数据)加密成加密或密文交易数据。例如，客户端节点可以使用密钥，根据Pedersen承诺来加密明文值(例如，账户信息)和与明文值对应的随机数。所得到的机密交易的加密的交易信

息(例如,加密的随机数和加密的明文值)可以被包括为交易内容的一部分并且被提交以供区块链网络执行。一个或多个区块链节点可以在例如区块链网络中的一个或多个区块链中存储加密的交易信息。客户端节点可以从一个或多个区块链节点检索与客户端节点相对应的加密的交易信息,并使用密钥从加密的交易信息中解密出明文交易数据。

[0049] 在一些实施方式中,客户端节点可能丢失明文交易数据和/或密钥。例如,如果客户端节点在客户端节点的数据存储设备上本地保存了明文交易数据和/或密钥,则当数据存储设备被压缩或损坏时,客户端节点可能丢失明文交易数据和/或密钥。所描述的技术可以帮助恢复明文交易数据和/或密钥。

[0050] 在一些实施方式中,可以根据用于安全多方计算(MPC)的阈值秘密共享方案(例如,夏米尔(Shamir)的秘密共享方案)来生成客户端节点的密钥。例如,对应于客户端节点的加密承诺的私钥可以在Shamir的秘密共享方案的全部参与者(例如,n个参与者)之间被协商和生成。密钥可以分成多个部分并分别由全部参与者存储,从而避免客户端节点的密钥的泄漏。在客户端节点丢失密钥的情况下,客户端节点可以根据Shamir的秘密共享方案通过从n个参与者中的至少k个参与者接收密钥的至少阈值数量的部分(例如,k个部分)来恢复密钥。因此,客户端节点可以恢复密钥并使用该密钥从使用该密钥加密的交易信息中解密出明文交易数据。

[0051] 所描述的技术可以帮助恢复机密交易的密钥和明文交易数据。所描述的技术不依赖于基于硬件的备份方案,其中客户端节点使用其硬件来备份其密钥(例如,在基于硬件的钱包中)。当交易数据存储在区块链网络中的一个或多个区块链上时,所描述的技术可以为交易数据提供增强的安全性和鲁棒性。不管基于硬件的钱包或基于软件的钱包的实施方式,所描述的技术可以为客户端节点提供对其密钥的访问。所描述的技术可以实现额外的或不同的优点。

[0052] 图1描绘了可用于执行本公开实施方式的示例性环境100。在一些示例中,示例性环境100使得实体能够参与联盟区块链网络102。示例性环境100包括计算设备或系统106、108和网络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,并连接网络站点、客户端设备(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。

[0053] 在所描绘的示例中,计算系统106、108可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。示例性计算设备包括但不限于服务器、台式计算机、膝上型计算机、平板计算设备和智能电话。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交互。例如,计算系统106可承载第一实体(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,例如,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,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。

[0054] 图2描绘了根据本公开实施方式的示例性概念架构200。示例性概念架构200包括实体层202、承载服务层204以及区块链网络层206。在描绘的示例中,实体层202包括三个实

体,实体_1(E1)、实体_2(E2)、实体_3(E3),每个实体具有对应的交易管理系统208。

[0055] 在所描绘的示例中,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,相应的交易管理系统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提供相应的交易管理系统208和区块链网络层206之间的通信连接。更具体地,接口210与区块链网络层206中的区块链网络212通信。在一些示例中,利用远程过程调用(RPCs)来进行接口210与区块链网络层206间的通信。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)。

[0056] 如本文所述,区块链网络212提供为点对点网络,其包括在区块链216中不可篡改地记录信息的多个节点214。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存储区块链的副本。在一些实施方式中,区块链216存储与参与在联盟区块链网络中的两个或更多实体之间进行的交易相关联的信息。

[0057] 图3描绘了根据本公开的实施方式的用于准备机密交易的示例性处理300。客户端节点A 302、B 304、C 306和D 308表示阈值秘密共享方案(也称为阈值密钥共享方案)的参与者。阈值秘密共享方案解决了由多方进行密钥安全管理的问题。作为示例性秘密共享方案,Shamir的秘密共享方案(标记为Shamir(k, n))将密钥划分为n个部分并且将n个部分分别分配给n个参与者。每个参与者具有密钥的唯一份额。为重建原始密钥,需要最小或阈值数量的部分。在阈值方案中,该最小数量k小于部分的总数n。换句话说,如果收集了密钥的至少k个部分,则原始密钥可被恢复。Shamir算法可以使用例如拉格朗日差分算法(Lagrangian difference algorithm)或其他方法来恢复密钥。

[0058] 这里,Shamir(k, n)意味着明文m被加密并被划分成n个部分,并且需要至少k个部分来恢复明文m。如图3所示,客户端节点A 302可以生成密钥Akey,并将Akey分解为四个部分。客户端节点A 302可以保留一个部分并且分给每个客户端节点B 304、C 306和D 308相应的部分。

[0059] 在一些实施方式中,从客户端节点A 302的角度来看,在310,客户端节点A 302可以根据标记为Shamir(k, n)的Shamir的秘密共享方案协商并获得密钥Akey,如上所述。例如,可以基于安全性和复杂性的考虑由客户端节点A 302或另一方确定k和n的值。在图3所示的示例中,n可以是4,使得客户端节点A 302、B 304、C 306和D 308都是Shamir的秘密共享方案的参与者。在这种情况下,k可以是2或3,使得客户端节点A 302可以从所有参与者,即,客户端节点A 302、B 304、C 306和D 308,中的至少2个或3个参与者中恢复密钥Akey。作为另一示例,k可以是4并且n可以大于4,使得客户端节点A 302可以从Shamir的秘密共享方案的所有参与者中的至少4个参与者恢复密钥Akey。

[0060] 在一些实施方式中,客户端节点A 302是对应于如图1和图2中所描述的第一客户端或实体的计算系统106、108的示例。客户端节点A 302具有用于区块链网络350上的交易的对应账户(例如,公共账户或私有账户)。区块链网络350可以包括多个共识节点(例如图3中的区块链节点312)。在一些实施方式中,客户端节点B 304、C 306和D 308可以是或可以不是区块链网络350中的客户端节点。换句话说,客户端节点A 302可以独立于区块链网络350来获得密钥。例如,客户端节点A 302可以通过区块链网络350之外的通信从客户端节点

B 304、C 306和D 308获得密钥。

[0061] 在一些实施方式中，客户端节点A 302可以与另一客户端节点(例如，客户端节点B 304)进行机密交易，使得交易信息仅可由客户端节点A 302和客户端节点B 304而不是其他方(例如，客户端节点C 306或D 308、或区块链网络350中的区块链节点312)查看或以其他方式知悉。

[0062] 在320，客户端节点A 302创建机密交易以将金额t转移至客户端节点B 304。在一些实施方式中，客户端节点A 302可以本地构建机密交易的内容并向区块链网络350(例如，在区块链网络350中的一个或多个区块链节点312)提交机密交易的内容。

[0063] 在一些实施方式中，可以基于承诺方案来构建机密交易以隐藏交易数据(例如，交易之前的账户余额和交易金额)。示例性承诺方案包括但不限于Pedersen承诺(PC)。例如，客户端节点A 302使用PC基于交易金额t和随机数r生成承诺值。例如，承诺值包括可以根据PC(t)= rG + tH获得的密文，其中G和H可以是椭圆曲线的生成元，PC(t)是曲线点的标量乘法，t是被承诺的值。PC承诺方案具有同态性，即$PC(t_1)+ PC(t_2)= PC(t_1 + t_2)$。密文PC(t)的持有者可以通过使用随机数r来验证交易金额t。尽管本文参考PC进一步详细描述了本公开的实施方式，但是可以预期，可以使用任何适当的承诺方案来实现本公开的实施方式。

[0064] 在示例性机密交易中，客户端节点A 302可以对交易前的账户余额a和转移金额t承诺。在一些实施方式中，客户端节点A 302可以基于交易前的账户余额a和对应的随机数ra使用PC生成承诺值PC(a)。类似地，客户端节点A 302可以基于转移金额t和相应的随机数rt使用PC生成承诺值PC(t)。在一些实施方式中，客户端节点A 302还可以承诺它具有足够的资金，使得交易后的余额a-t大于或等于0。例如，考虑到PC的同态属性，客户端节点A 302可以例如基于承诺值PC(a)和PC(t)生成承诺值PC(a-t)。承诺值可以被包含在机密交易的内容中。

[0065] 在一些实施方式中，机密交易的内容可以包括一个或多个零知识证明，以使接收方能够确认发送方正在发送的信息是有效的。零知识证明使得接收方能够在实际上不知道被确认的信息的情况下这样做。零知识证明可以包括范围证明，例如证明(a-t> 0)、证明(t> 0)和证明(a> 0)，或其他类型的证明。在不知道用于转移金额的余额a，甚至转移金额t的情况下，零知识证明使得接收方(例如，客户端节点B)能够确认发送方(例如，客户端节点A)具有足够的资金来转移(即，a-t> 0)，并且转移金额大于零。

[0066] 在一些实施方式中，对于每个Pedersen承诺，可以使用密钥Akey来加密随机数r和金额t，以获得加密的交易信息，M = Akey(r,t)。加密的交易信息M可以作为机密交易的内容的一部分被包括。

[0067] 在一些实施方式中，示例性机密交易的内容可以包括例如A对交易的数字签名的其他交易相关信息。

[0068] 在生成交易内容之后，客户端节点A 302可以将机密交易的内容提交至区块链网络350(例如，区块链网络350中的一个或多个区块链节点312)。在330，区块链网络350可以执行机密交易。在一些实施方式中，机密交易可以由区块链网络350中的每个区块链节点312执行。例如，每个区块链节点312可以例如通过验证包含在机密交易的内容中的一个或多个承诺值及零知识证明，来确定机密交易的内容是否合法。例如，每个区块链节点312可以通过验证PC(a)= PC(t)+ PC(a-t)，即，输入交易值等于输出交易值来验证承诺值。每个

区块链节点312可以例如基于防弹证明(Bulletproof)、RingCT算法或任何其他合适的算法来验证零知识证明。

[0069] 在一些实施方式中,在承诺值和零知识证明已经被验证后,每个区块链节点312可以记录交易并更新客户端节点A 302和客户端节点B 304的账户。例如,在交易之后,客户端节点A 302具有账户余额a-t,客户端节点B 304具有账户余额b+t。在一些实施方式中,由于承诺方案的同态性,可以通过对承诺值的直接运算来反映客户端节点A 302和客户端节点B 304的交易后余额。例如,客户端节点A 302现在可以具有交易后账户余额的承诺值PC(a-t) = PC(a)-PC(t)。客户端节点B 304现在可以具有交易后账户余额的承诺值PC(b + t)= PC(b)+ PC(t)。

[0070] 在一些实施方式中,每个区块链节点312可以记录或存储加密的交易信息。例如,对应于承诺PC(a)的加密的交易信息Ma = Akey(ra,a)和对应于承诺PC(t)的加密的交易信息Mt = Akey(rt,t)可以由每个区块链节点312记录在区块链中,其中,ra和rt分别代表对应于金额a和t的随机数。

[0071] 图4描绘了根据本公开的实施方式的机密交易的交易信息的示例性恢复处理400。例如,在客户端节点A 302丢失其密钥Akey的情况下,因此不知道其对应的区块链账户上的金额。客户端节点A302可以使用示例性恢复处理400来恢复客户端节点A 302的账户金额。

[0072] 在410,客户端节点A 302例如通过从区块链节点312下载或与区块链节点312同步来获得根据Pedersen承诺加密的交易信息(例如,Ma = Akey(ra,a)和Mt = Akey(rt,t))。在一些实施方式中,客户端节点A302可以保存根据Pedersen承诺加密的交易信息的本地副本。

[0073] 在420,客户端节点A 302可以与客户端节点B 304、C 306和D 308通信,以例如,根据例如区块链网络350的Shamir秘密共享方案来恢复密钥Akey。

[0074] 具有了恢复的密钥Akey,在430,客户端节点A 302可以解密与客户端节点302的账户的每个Pedersen承诺相对应的加密的交易信息(例如,Ma = Akey(ra,a)和Mt. = Akey(rt,t))。然后,客户端节点A 302可以使用恢复的密钥Akey来解密加密的交易信息(例如,Ma = Akey(ra,a)和Mt = Akey(rt,t))并获得明文交易信息ra、a、rt、和t。

[0075] 图5描绘了可以根据本公开的实施方式执行的示例性处理500。在一些实施方式中,可以使用利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示例性处理500。为了清楚地呈现,以下描述结合本说明书中其他附图的上下文一般地描述了方法500。例如,如图3和图4所描述的,客户端节点510可以包括客户端节点C 306和客户端节点D 308;区块链节点520可以是区块链节点312;客户端节点A 530可以是客户端节点A 302;客户端节点B 540可以是客户端节点B 304。然而,应当理解,方法500可以例如通过任何合适的系统、环境、软件和硬件,或系统、环境、软件和硬件的组合来合理执行。在一些实施方式中,方法500的各个步骤可以并行、组合、循环或以任何顺序运行。

[0076] 在512,多个(例如,n个)客户端节点510生成区块链网络中的客户端节点(例如,客户端节点A 530)的密钥。在一些实施方式中,可以根据全部客户端节点510所同意的阈值秘密共享方案,由全部(例如,n个)客户端节点510协商或以其他方式生成密钥。在一些实施方法中,阈值秘密共享方案包括Shamir的秘密共享方案。

[0077] 在514,多个客户端节点510可以向客户端节点A 530发布密钥。客户端节点A 530

可以使用密钥来加密和解密客户端节点A 530的机密交易的交易信息。

[0078] 在532,客户端节点A 530根据全部客户端节点510(例如,秘密共享方案的全部参与者)所同意的阈值秘密共享方案来获得密钥。客户端节点A 530可以使用客户端节点A 530的密钥来加密客户端节点A 530的机密交易的交易数据。例如,客户端节点A 530的机密交易可以是例如将一定数量的资金从客户端节点A 530的账户转移到客户端节点B 540的账户的机密交易535。客户端节点A 530可以构建机密交易的内容以保护交易数据的隐私并隐藏交易数据防止除了交易的参与者(即,在该示例中为客户端节点A 530和客户端节点B 540)之外的其他实体查看交易数据。在一些实施方式中,客户端节点A 530可以基于承诺方案并使用根据阈值秘密共享方案获得的密钥来隐藏机密交易的交易数据。

[0079] 在一些实施方式中,机密交易的交易数据包括客户端节点A 530在机密交易之前的账户余额和/或机密交易的交易金额。在一些实施方式中,机密交易的交易数据可以包括附加交易信息(例如,交易时间、交易资产类型(例如,股票证券或其他类型)的各方)。

[0080] 在534,客户端节点A 530通过将加密承诺方案应用于机密交易的交易数据来生成客户端节点A 530的机密交易的一个或多个承诺值。在一些实施方式中,加密承诺方案包括同态加密承诺方案,例如Pedersen承诺方案,或另一类型的承诺方案。

[0081] 在536,客户端节点A 530通过使用客户端节点A 530的密钥加密交易数据来生成机密交易的加密的交易信息,其中,加密的交易信息被配置为允许客户端节点A 530使用密钥解密。

[0082] 在一些实施方式中,加密承诺方案包括Pedersen承诺方案。在这种情况下,通过将加密承诺方案应用于交易数据来生成客户端节点的机密交易的一个或多个承诺值,包括基于交易数据和对应于交易数据的随机数生成客户端节点的机密交易的一个或多个承诺值,并且生成机密交易的加密的交易信息包括,通过使用客户端节点A 530的密钥加密交易数据和与交易数据相对应的随机数来生成机密交易的加密的交易信息。

[0083] 在538,客户端节点A 530将机密交易的内容提交给区块链网络以供执行,例如,通过将机密交易的内容发送到区块链节点520(例如,区块链网络中的共识节点)。在一些实施方式中,机密交易的内容可以包括由客户端节点A 530通过将加密承诺方案应用于机密交易的交易数据而生成的机密交易的一个或多个承诺值、由客户端节点A 530通过使用密钥来加密交易数据而生成的加密的交易信息、及交易数据的一个或多个零知识证明。

[0084] 在一些实施方式中,交易数据的一个或多个零知识证明包括交易数据的值在相应的范围内的一个或多个零知识范围证明。例如,一个或多个零知识范围证明可以包括客户端节点A 530在机密交易之前的账户余额大于零的零知识范围证明、机密交易的交易金额大于零的零知识范围证明、以及交易金额小于或等于客户端节点A 530在机密交易之前的账户余额的零知识范围证明。

[0085] 在一些实施方式中,机密交易的内容还包括客户端节点A 530的数字签名。在一些实施方式中,机密交易的内容可以包括附加或不同的信息。

[0086] 在522,在接收到机密交易的内容时,区块链节点520可以执行机密交易,例如,通过基于机密交易的内容验证机密交易有效。在一些实施方式中,基于机密交易的内容验证机密交易有效可以包括以下中的一个或多个:基于承诺方案和/或一个或多个零知识证明确定一个或多个承诺值是正确的;或者,例如根据关于图3所描述的算法验证交易数据的一

个或多个零知识证明。

[0087] 在524,在验证机密交易有效之后,区块链节点520可以更新受机密交易影响的账户信息(例如,客户端节点A 530和客户端节点B 540的账户余额)。在一些实施方式中,加密承诺方案是同态的,并且例如根据关于图3描述的技术或其他技术,区块链节点520可以基于承诺方案的同态性来更新账户信息。

[0088] 在526,区块链节点520可以将加密的交易信息存储在区块链网络的区块链上。在一些实施方式中,加密的交易信息可以被存储在区块链网络中的多于一个/所有共识节点中,从而提供客户端节点A 530的加密的交易信息的鲁棒备份以防客户端节点A 530丢失密钥。此外,在区块链网络的区块链中存储加密的交易信息可以减少或消除客户端节点A 530对本地或单点存储方案的依赖,从而提高客户端节点A 530对加密的交易信息的访问的安全性和可靠性。

[0089] 在528,客户端节点A 530可以从区块链节点520(例如,区块链网络中的共识节点)检索或以其他方式获得加密的交易信息。加密的交易信息存储在区块链网络中的至少一个区块链中。客户端节点A 530可以使用密钥从加密的交易信息中解密出明文交易信息。

[0090] 在542,客户端节点A 530确定其丢失或以其他方式不能访问被配置为解密加密的交易信息的密钥,并且该密钥先前被发布到客户端节点A 530。

[0091] 在516和544,在一些实施方式中,响应于这样的确定,客户端节点A 530根据多个客户端节点同意的阈值秘密共享方案(例如,Shamir的秘密共享方案),从区块链网络中的全部(例如,n个)客户端节点中的至少阈值数量(例如,k个)的客户端节点恢复密钥,例如,通过从区块链网络中的全部客户端节点中的至少阈值数量的客户端节点中接收密钥的至少阈值数量的部分。

[0092] 在546,客户端节点A 530使用恢复的密钥从加密的交易信息中解密出客户端节点A 530的机密交易的交易数据(例如,明文交易数据)。在一些实施方式中,从使用密钥加密的交易信息中解密出特定客户端节点的机密交易的交易数据,包括:使用密钥恢复机密交易的转移金额。在一些实施方式中,从使用密钥加密的交易信息中解密出特定客户端节点的机密交易的交易数据,包括:使用密钥恢复机密交易的转移金额、以及对应于该转移金额的随机数,其中,将转移金额和随机数用在Pedersen承诺方案中,以用于隐藏特定客户端节点的机密交易的交易信息。

[0093] 所描述的特征可以在数字电子电路中实现,或在计算机硬件、固件、软件或他们的组合中实现。该装置可以在有形地体现在信息载体中(例如,在机器可读存储设备中)的计算机程序产品中实现,以被可编程处理器执行;方法步骤可以由执行指令程序的可编程处理器执行,以通过对输入数据进行操作并生成输出来执行所描述的实施方式的功能。所描述的特征可有利地在可编程系统上执行的一个或多个计算机程序中实现,所述可编程系统包括至少一个可编程处理器,其被耦接以从数据存储系统、至少一个输入设备和至少一个输出设备接收数据和指令,并向其发送数据和指令。计算机程序是可以直接或间接地在计算机中使用以执行特定活动或带来特定结果的一组指令。计算机程序可以用任何形式的编程语言编写,包括编译或演绎性语言,并且可以配置为任何形式,包括作为独立程序或作为模块、组件、子程序或适合在计算环境中使用的其他单元。

[0094] 用于执行指令程序的合适处理器包括,例如,通用和专用微处理器,以及任何类型

的计算机的唯一处理器或多个处理器之一。通常，处理器将从只读存储器和/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处理器和用于存储指令和数据的一个或多个存储器。通常，计算机还可以包括或可操作地耦合以与一个或多个大容量存储设备通信以存储数据文件；这些设备包括磁盘，例如内部硬盘和可移动磁盘；磁光盘；和光盘。适合于有形地体现计算机程序指令和数据的存储设备包括所有形式的非易失性存储器，包括例如半导体存储器设备，诸如EPROM、EEPROM和闪存设备；磁盘，诸如内部硬盘和可移动磁盘；磁光盘；和CD-ROM以及DVD-ROM磁盘。处理器和存储器可以补充有专用集成电路(ASIC)或集成在专用集成电路中。

[0095] 为了提供与客户端的交互，这些特征可以在计算机上实现，该计算机具有例如阴极射线管(CRT)或液晶显示器(LCD)监视器的、用于向客户端节点A 302显示信息的显示设备，以及客户端可以用来向计算机提供输入的键盘和诸如鼠标或轨迹球的指针设备。

[0096] 这些特征可以在包括例如数据服务器的后端组件、或者包括例如应用服务器或因特网服务器的中间件组件、或包括例如具有图形客户端接口或因特网浏览器的客户端计算机的前端组件，或它们的任何组合的计算机系统中实现。系统的组件可以通过诸如通信网络的任何形式或介质的数字数据通信连接。通信网络的示例包括例如局域网(LAN)、广域网(WAN)以及形成因特网的计算机和网络。

[0097] 计算机系统可以包括客户端和服务器。客户端节点A 302和服务器通常彼此远离并且通常通过例如所描述的网络进行交互。客户端节点A 302和服务器的关系通过借助于在各个计算机上运行的并且彼此具有客户端-服务器关系的计算机程序产生。

[0098] 另外，图中描绘的逻辑流程不需要按所示的特定顺序或次序来实现期望的结果。另外，可以从所描述的流程中提供其他步骤，或者可以从所描述的流程中消除步骤，并且可以将其他组件添加到所描述的系统或从所述系统中移除。因此，其他实施方式在以下权利要求的范围内。

[0099] 已经描述了本公开的许多实施方式。然而，应该理解，在不脱离本公开的精神和范围的情况下，可以进行各种修改。因此，其他实施方式在以下权利要求的范围内。

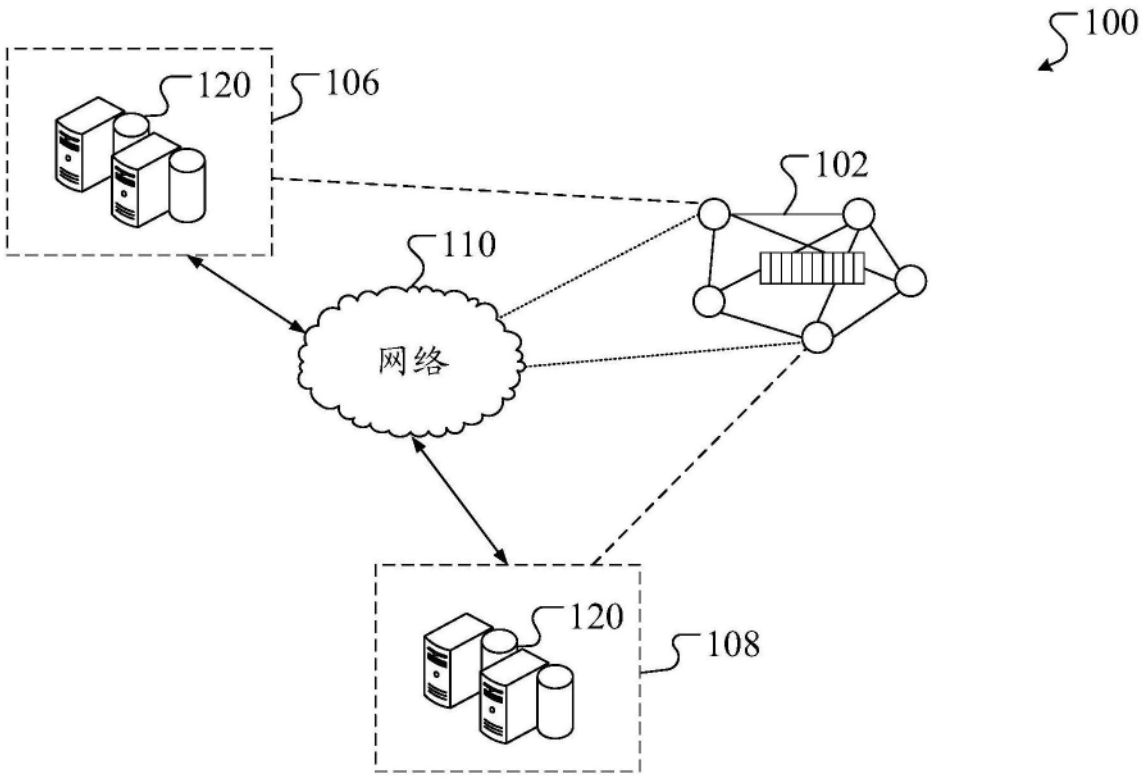


图1

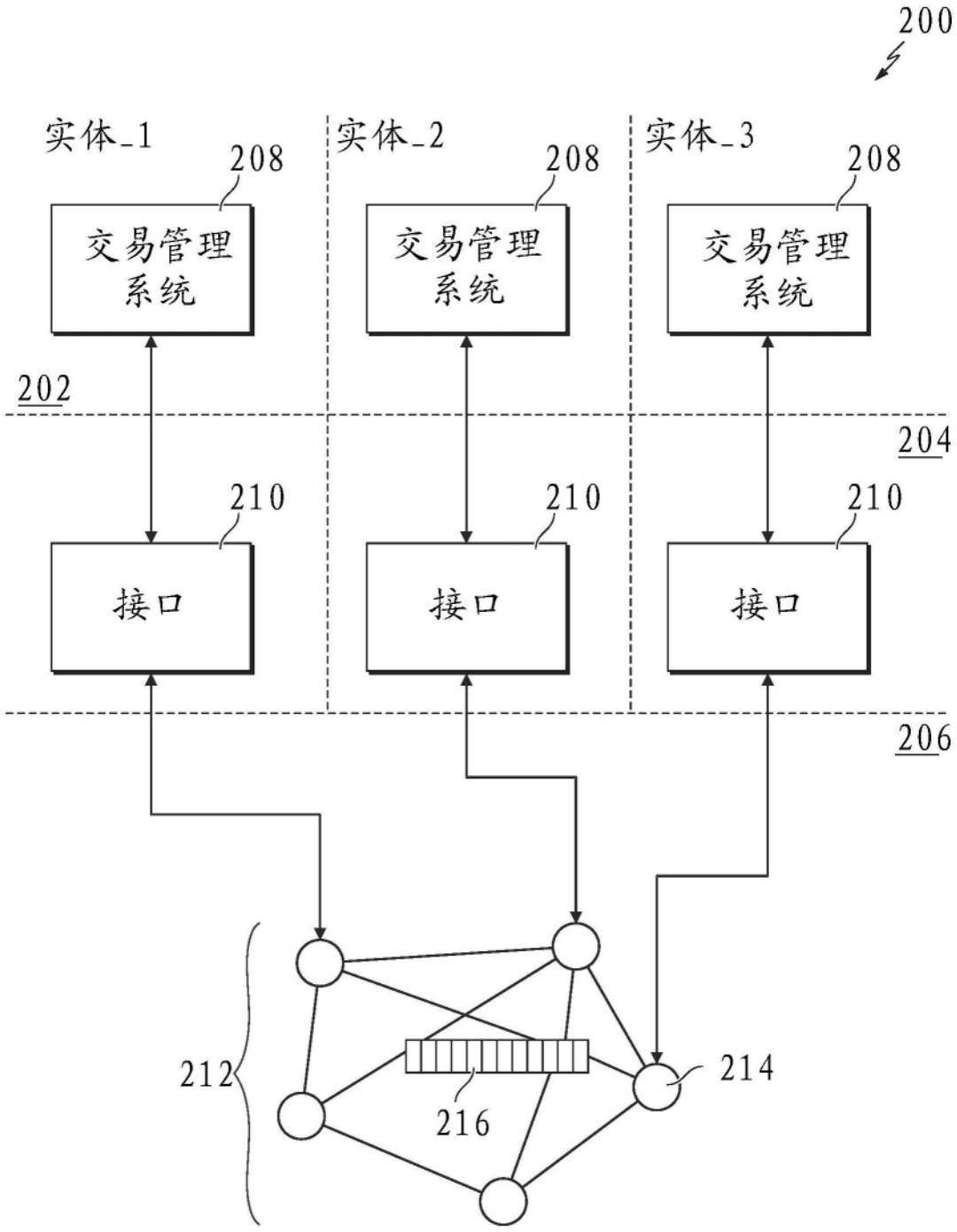

200
实体_1
实体_2
实体_3
208
208
208
交易管理系统
交易管理系统
交易管理系统
202
204
210
210
210
接口
接口
接口
206
212
214
216

图2

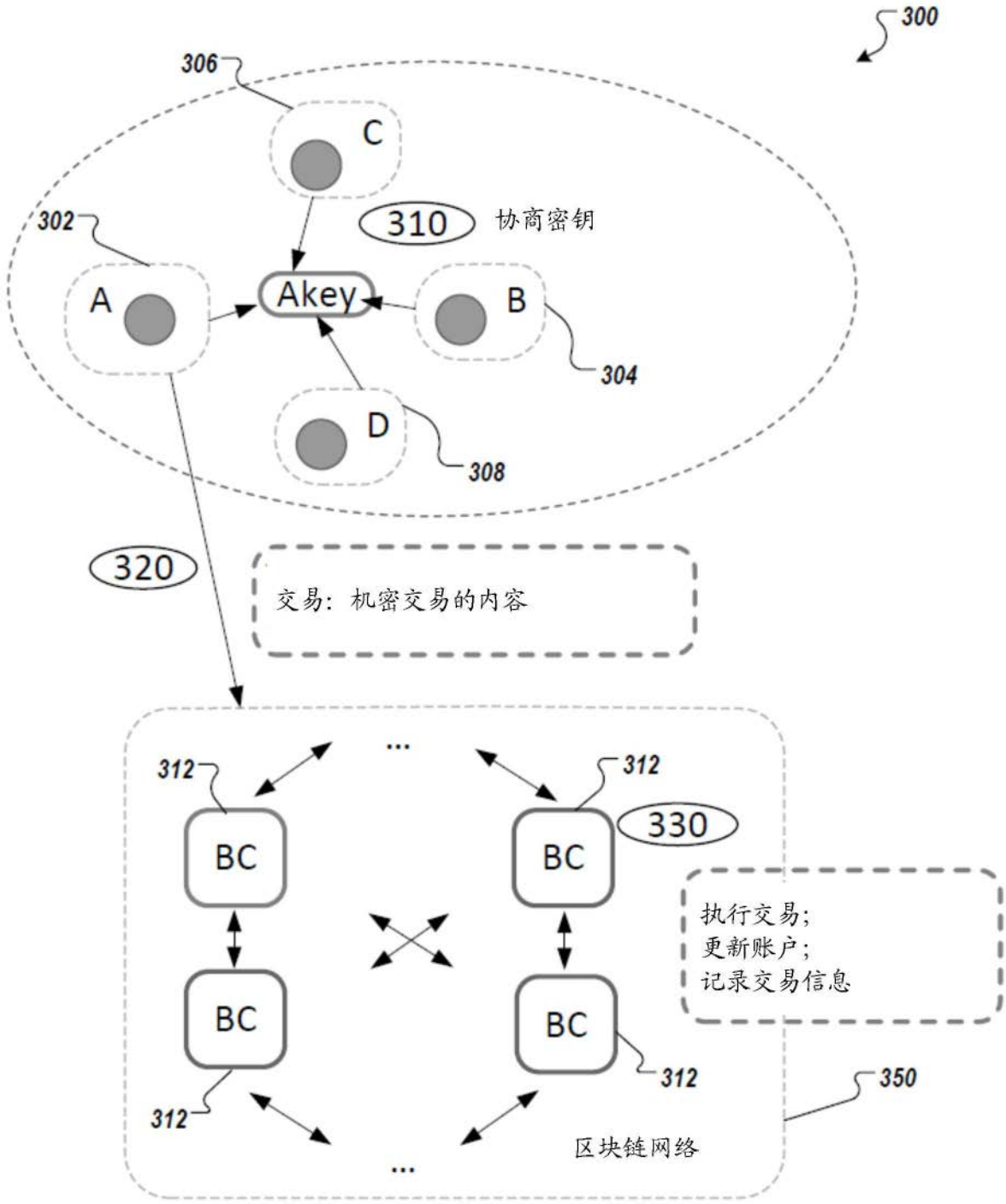

300
306
C
310
协商密钥
302
A
Akey
B
304
D
308
320
交易：机密交易的内容
312
BC
330
执行交易；
更新账户；
记录交易信息
350
区块链网络

图3

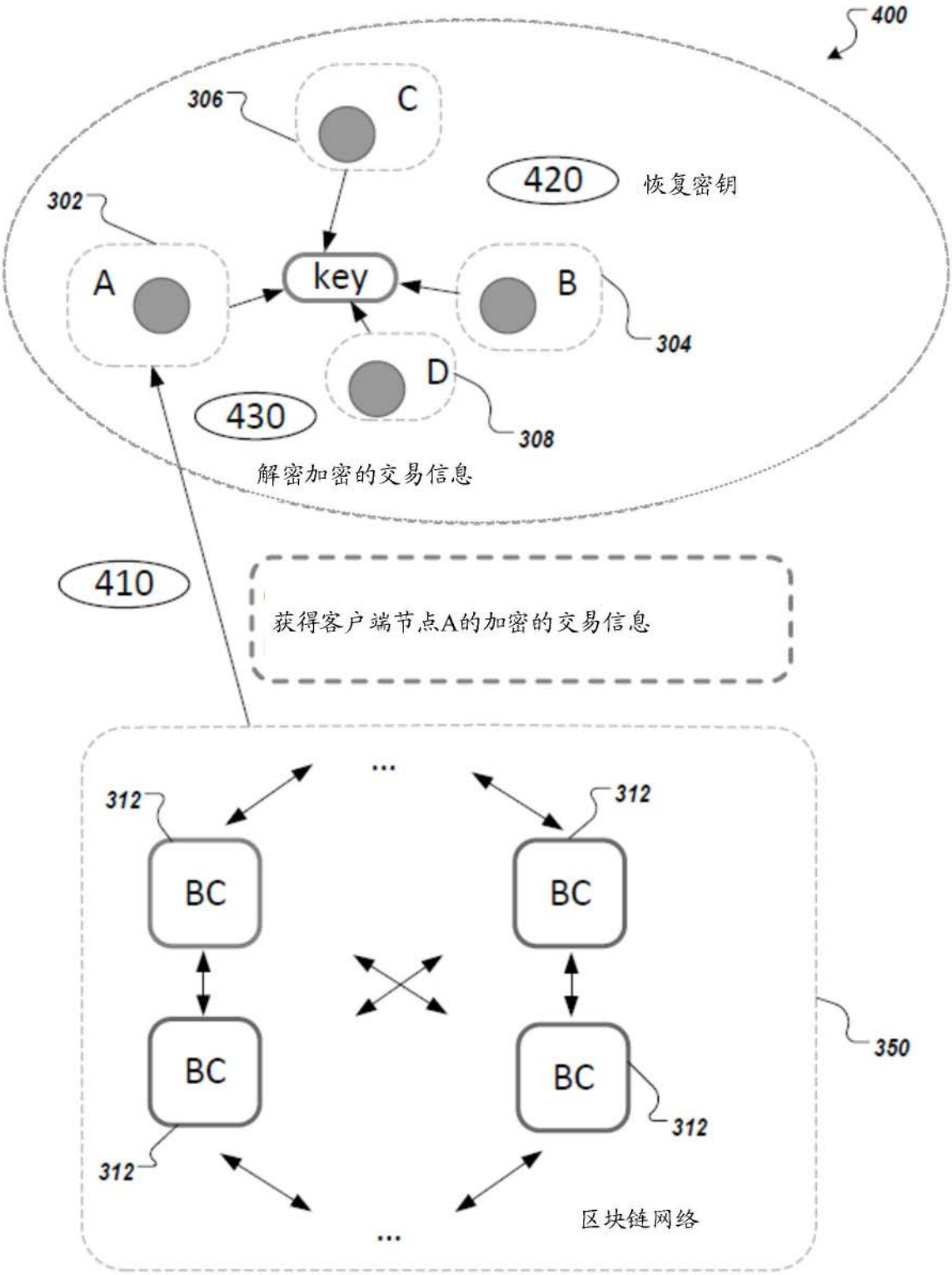

400
306
C
420
恢复密钥
302
A
key
B
304
D
308
430
解密加密的交易信息
410
获得客户端节点A的加密的交易信息
312
BC
BC
BC
BC
312
312
312
350
区块链网络

图4

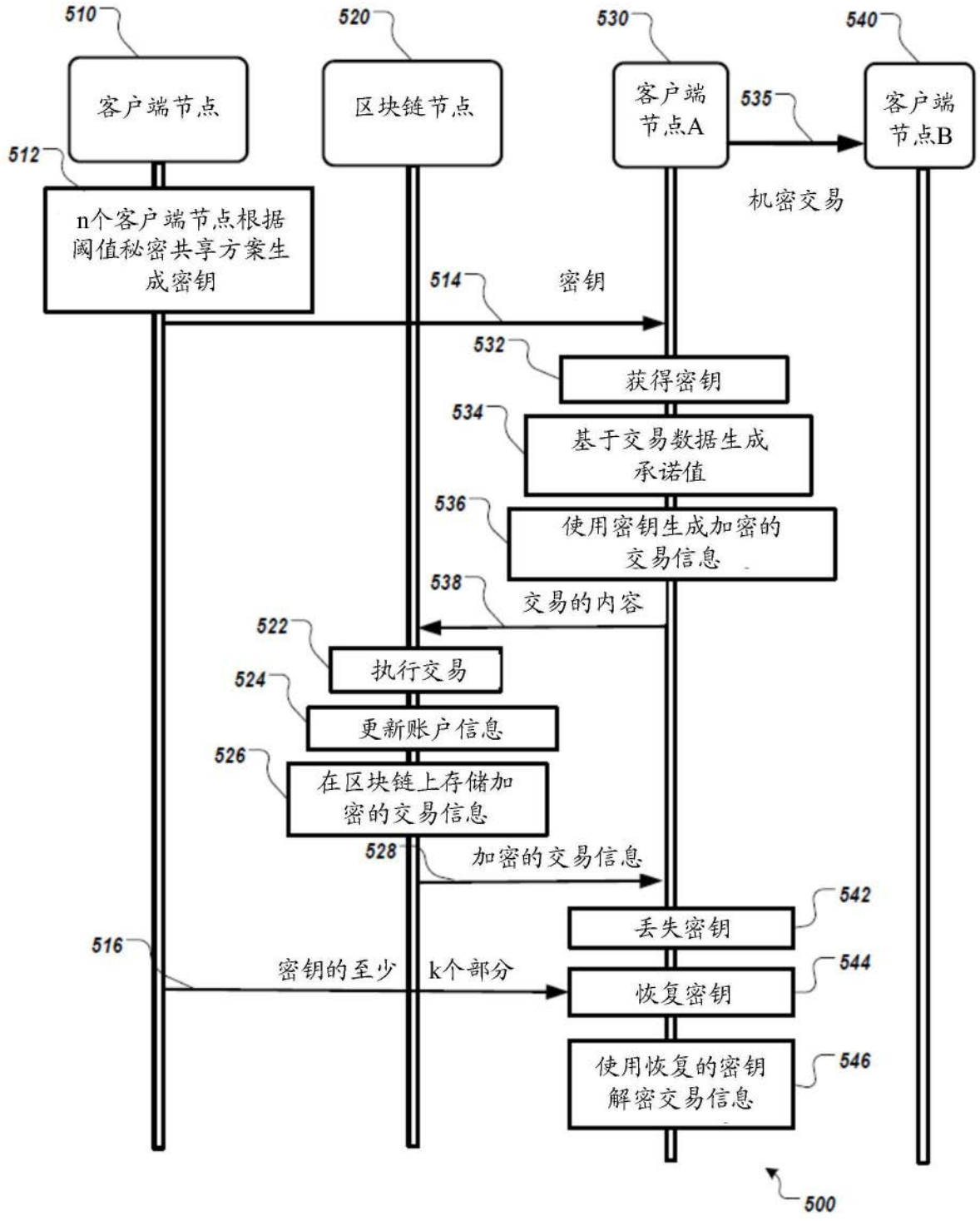

510
客户端节点
520
区块链节点
530
客户端节点A
535
540
客户端节点B
机密交易
512
n个客户端节点根据阈值秘密共享方案生成密钥
514
密钥
532
获得密钥
534
基于交易数据生成承诺值
536
使用密钥生成加密的交易信息
538
交易的内容
522
执行交易
524
更新账户信息
526
在区块链上存储加密的交易信息
528
加密的交易信息
542
丢失密钥
516
密钥的至少
k个部分
544
恢复密钥
使用恢复的密钥解密交易信息
546
500

图5