

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 12 月 17 日 (17.12.2020)



(10) 国际公布号
WO 2020/248657 A1

(51) 国际专利分类号:
G06Q 20/38 (2012.01)

中国浙江省杭州市余杭区文一西路969号3号楼5楼
阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(21) 国际申请号: PCT/CN2020/082427

(22) 国际申请日: 2020 年 3 月 31 日 (31.03.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910507879.1 2019年6月12日 (12.06.2019) CN

(71) 申请人: 创新先进技术有限公司 (ADVANCED NEW TECHNOLOGIES CO., LTD.) [—/CN]; 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心, Grand Cayman KY1-9008 (KY)。

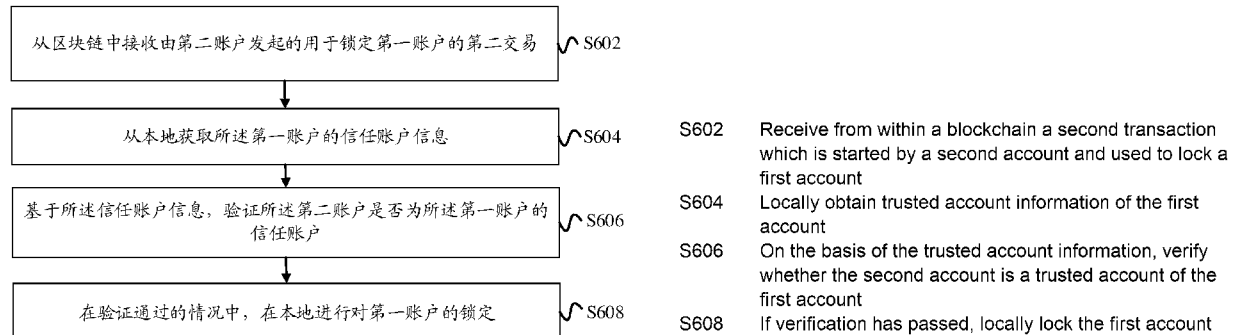
(72) 发明人: 方思羽 (FANG, Siyu); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 左军 (ZUO, Jun);

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街9号嘉华大厦B座409, Beijing 100085 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: METHOD AND APPARATUS FOR LOCKING ACCOUNT IN BLOCKCHAIN

(54) 发明名称: 一种在区块链中锁定账户的方法和装置



(57) Abstract: A method and apparatus for locking an account in a blockchain, the blockchain comprising a plurality of full nodes, the full nodes locally pre-storing trusted account information of a first account, the trusted account information at least comprising a second account that acts as a trusted account of the first account, and the method being performed by the full nodes in the blockchain, and comprising: receiving from within a blockchain a second transaction which is started by the second account and used to lock the first account (S602); locally obtaining the trusted account information of the first account (S604); on the basis of the trusted account information, verifying whether the second account is a trusted account of the first account (S606); and if verification has passed, locally locking the first account (S608).

(57) 摘要: 一种在区块链中锁定账户的方法和装置, 所述区块链中包括多个全节点, 所述全节点本地预先存储有第一账户的信任账户信息, 所述信任账户信息中至少包括作为第一账户的信任账户的第二账户, 所述方法由区块链中的全节点执行, 包括: 从区块链中接收由第二账户发起的用于锁定第一账户的第二交易 (S602); 从本地获取所述第一账户的信任账户信息 (S604); 基于所述信任账户信息, 验证所述第二账户是否为所述第一账户的信任账户 (S606); 以及在验证通过的情况下, 在本地进行对第一账户的锁定 (S608)。

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, WS, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告 (条约第21条(3))。

一种在区块链中锁定账户的方法和装置

技术领域

[01] 本说明书实施例涉及区块链技术领域，更具体地，涉及一种在区块链中锁定账户的方法和装置。

5 背景技术

[02] 区块链技术是构建在点对点(P2P)网络上，利用链式数据结构来验证与存储数据，利用分布式节点共识算法来生成和更新数据，利用密码学的方式保证数据传输和访问的安全，利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。所述区块链例如为以太坊区块链。在以太坊中，新增了账户的概念，其中，由用户创建的账户为以太坊中的外部账户。通常，每个外部账户拥有一对公私钥，其中，私钥用于进行数字签名，公钥用于验证签名。另外，在各个全节点中，在节点本地的数据库中以状态树的形式维持区块链中全部账户的数据表，该状态树为账户地址与账户内容之间的映射，所述账户内容包括，账户余额、账户密钥信息(哈希值)等。然而，在目前已有的区块链中，当用户发现区块链账户的密钥丢失或被盗后，一般无法进行账户锁定操作，很有可能导致用户损失进一步扩大。

[03] 因此，需要一种更有效的在区块链中锁定账户的方案。

发明内容

[04] 本说明书实施例旨在提供一种更有效的在区块链中锁定账户的方法和装置。

[05] 为实现上述目的，本说明书一个方面提供一种在区块链中存入账户的信任账户信息的方法，所述方法由第一用户在区块链中的第一账户客户端执行，包括：获取第二用户在区块链中的第二账户，所述第二用户为所述第一用户的信任用户；以及发起第一交易，所述第一交易用于在区块链中存入第一账户的信任账户信息，所述第一交易中至少包括作为第一账户的信任账户的所述第二账户，以使得所述信任账户信息中至少包括所述第二账户，其中，所述信任账户具有锁定第一账户的权限。

[06] 在一个实施例中，所述第一交易为调用第一智能合约的交易，所述第一智能合约

为区块链中预先部署的用于存入账户的信任账户信息的智能合约，所述第一交易的数据

字段中至少包括所述第二账户。

[07] 在一个实施例中，获取第二用户在区块链中的第二账户包括，获取第二用户在区块链中的第二账户及其公钥，其中，所述第一交易的数据字段中还包括第二账户的公钥，以使得所述信任账户信息中还包括第二账户的公钥。

- 5 [08] 本说明书另一方面提供一种在区块链中存入账户的信任账户信息的方法，所述方法由区块链中的全节点执行，包括：从区块链中接收由第一账户发起的第一交易，所述第一交易用于在区块链中存入第一账户的信任账户信息，所述第一交易中至少包括作为第一账户的信任账户的第二账户，所述信任账户具有锁定第一账户的权限；以及基于所述第一交易，在本地存入所述第一账户的信任账户信息，其中，所述信任账户信息中至少包括所述第二账户。

[09] 在一个实施例中，所述第一交易为调用第一智能合约的交易，所述第一智能合约

为区块链中预先部署的用于存入账户的信任账户信息的智能合约，其中，基于所述第一交易，在本地存入所述第一账户的信任账户信息包括，通过在本地执行所述第一智能合约而将所述信任账户信息存入本地的状态树中的第一账户下。

- 15 [10] 在一个实施例中，基于所述第一交易，在本地存入所述第一账户的信任账户信息包括，基于所述第一交易，在本地的新的区块中存入第一账户的信任账户信息，其中，所述第一交易中包括预定标志，用于指示该第一交易为用于向区块链中存入信任账户信息的交易。

- [11] 本说明书另一方面提供一种在区块链中锁定账户的方法，所述区块链中包括多个全节点，所述全节点本地预先存储有第一账户的信任账户信息，所述信任账户信息中至少包括作为第一账户的信任账户的第二账户，所述方法由第二账户客户端执行，包括：

[12] 发起第二交易，所述第二交易用于在区块链中锁定所述第一账户。

- [13] 在一个实施例中，所述第二交易为调用第二智能合约的交易，所述第二智能合约
- 为区块链中预先部署的用于锁定账户的智能合约，所述第二交易的数据字段中包括所述
- 25 第一账户。

[14] 本说明书另一方面提供一种在区块链中锁定账户的方法，所述区块链中包括多个全节点，所述全节点本地预先存储有第一账户的信任账户信息，所述信任账户信息中至少包括作为第一账户的信任账户的第二账户，所述方法由区块链中的全节点执行，包括：从区块链中接收由第二账户发起的用于锁定第一账户的第二交易；从本地获取所述第一

账户的信任账户信息；基于所述信任账户信息，验证所述第二账户是否为所述第一账户的信任账户；以及在验证通过的情况中，在本地进行对第一账户的锁定。

[15] 在一个实施例中，所述第二交易为调用第二智能合约的交易，所述第二智能合约
5 为区块链中预先部署的用于锁定账户的智能合约，其中，在本地进行对第一账户的锁定
包括，通过在本地执行所述第二智能合约而进行对第一账户的锁定。

[16] 在一个实施例中，所述信任账户信息被存储在所述全节点的本地状态树中，其中，
从本地获取所述第一账户的信任账户信息包括，从本地状态树中获取所述第一账户的信
任账户信息。

[17] 在一个实施例中，所述信任账户信息被存储在区块中，其中，从本地获取所述第
10 一账户的信任账户信息包括，从本地存储的多个区块中检索具有第一账户和预定标志的
交易，从而获取第一账户的信任账户信息。

[18] 本说明书另一方面提供一种在区块链中存入账户的信任账户信息的装置，所述装
置部署于第一用户在区块链中的第一账户客户端，包括：获取单元，配置为，获取第二
15 用户在区块链中的第二账户，所述第二用户为所述第一用户的信任用户；以及交易发起
单元，配置为，发起第一交易，所述第一交易用于在区块链中存入第一账户的信任账户
信息，所述第一交易中至少包括作为第一账户的信任账户的所述第二账户，以使得所述
信任账户信息中至少包括所述第二账户，其中，所述信任账户具有锁定第一账户的权限。

[19] 在一个实施例中，所述第一交易为调用第一智能合约的交易，所述第一智能合约
20 为区块链中预先部署的用于存入账户的信任账户信息的智能合约，所述第一交易的数据
字段中至少包括所述第二账户。

[20] 在一个实施例中，所述获取单元还配置为，获取第二用户在区块链中的第二账户
及其公钥，其中，所述第一交易的数据字段中还包括第二账户的公钥，以使得所述信任
账户信息中还包括第二账户的公钥。

[21] 本说明书另一方面提供一种在区块链中存入账户的信任账户信息的装置，所述装
25 置部署于区块链中的全节点，包括：接收单元，配置为，从区块链中接收由第一账户发
起的第一交易，所述第一交易用于在区块链中存入第一账户的信任账户信息，所述第一
交易中至少包括作为第一账户的信任账户的第二账户，所述信任账户具有锁定第一账户
的权限；以及存入单元，配置为，基于所述第一交易，在本地存入所述第一账户的信任
账户信息，其中，所述信任账户信息中至少包括所述第二账户。

[22] 在一个实施例中，所述第一交易为调用第一智能合约的交易，所述第一智能合约为区块链中预先部署的用于存入账户的信任账户信息的智能合约，其中，所述存入单元还配置为，通过在本地执行所述第一智能合约而将所述信任账户信息存入本地的状态树中的第一账户下。

- 5 [23] 在一个实施例中，所述存入单元还配置为，基于所述第一交易，在本地的新的区块中存入第一账户的信任账户信息，其中，所述第一交易中包括预定标志，用于指示该第一交易为用于向区块链中存入信任账户信息的交易。

[24] 本说明书另一方面提供一种在区块链中锁定账户的装置，所述区块链中包括多个全节点，所述全节点本地预先存储有第一账户的信任账户信息，所述信任账户信息中至少包括作为第一账户的信任账户的第二账户，所述装置部署于第二账户客户端，包括：

10

[25] 交易发起单元，配置为，发起第二交易，所述第二交易用于在区块链中锁定所述第一账户。

[26] 在一个实施例中，所述第二交易为调用第二智能合约的交易，所述第二智能合约为区块链中预先部署的用于锁定账户的智能合约，所述第二交易的数据字段中包括所述

15 第一账户。

[27] 本说明书另一方面提供一种在区块链中锁定账户的装置，所述区块链中包括多个全节点，所述全节点本地预先存储有第一账户的信任账户信息，所述信任账户信息中至少包括作为第一账户的信任账户的第二账户，所述装置部署于区块链中的全节点，包括：

20 接收单元，配置为，从区块链中接收由第二账户发起的用于锁定第一账户的第二交易；获取单元，配置为，从本地获取所述第一账户的信任账户信息；验证单元，配置为，基于所述信任账户信息，验证所述第二账户是否为所述第一账户的信任账户；以及锁定单元，配置为，在验证通过的情况中，在本地进行对第一账户的锁定。

[28] 在一个实施例中，所述第二交易为调用第二智能合约的交易，所述第二智能合约为区块链中预先部署的用于锁定账户的智能合约，其中，所述锁定单元还配置为，通过

25 在本地执行所述第二智能合约而进行对第一账户的锁定。

[29] 在一个实施例中，所述信任账户信息被存储在所述全节点的本地状态树中，其中，所述获取单元还配置为，从本地状态树中获取所述第一账户的信任账户信息。

[30] 在一个实施例中，所述信任账户信息被存储在区块中，其中，所述获取单元还配置为，从本地存储的多个区块中检索具有第一账户和预定标志的交易，从而获取第一账

户的信任账户信息。

[31] 本说明书另一方面提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行上述任一项方法。

[32] 本说明书另一方面提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现上述任一项方法。

[33] 在根据本说明书实施例的方案中，通过采用信任账户机制，通过对信任的第三方授权锁定账户的权限，从而在账户私钥丢失或被盗的情况中，可通过第三方进行账户锁定，从而防止损失进一步扩大。

附图说明

10 [34] 通过结合附图描述本说明书实施例，可以使得本说明书实施例更加清楚：

[35] 图 1 示出根据本说明书实施例的区块链 100 的示意图；

[36] 图 2 示出根据本说明书实施例的一种在区块链中存入账户的信任账户信息的方法；

[37] 图 3 示出了第一交易的示意形式；

[38] 图 4 示出根据本说明书实施例的一种在区块链中存入账户的信任账户信息的方法；

15 [39] 图 5 示出根据本说明书实施例的一种在区块链中锁定账户的方法；

[40] 图 6 示出根据本说明书实施例的一种在区块链中锁定账户的方法；

[41] 图 7 示出根据本说明书实施例的一种在区块链中存入账户的信任账户信息的装置 700；

20 [42] 图 8 示出根据本说明书实施例的一种在区块链中存入账户的信任账户信息的装置 800；

[43] 图 9 示出根据本说明书实施例的一种在区块链中锁定账户的装置 900；

[44] 图 10 示出根据本说明书实施例的一种在区块链中锁定账户的装置 1000。

具体实施方式

[45] 下面将结合附图描述本说明书实施例。

25 [46] 图 1 示出根据本说明书实施例的区块链 100 的示意图。如图 1 所示，假设区块链

100 为联盟链，其中包括图中 1、2、3、4 四个共识节点（全节点），另外，区块链中还包括多个通过客户端登录的用户，这些用户拥有自己的账户、私钥和公钥，其客户端可视为该区块链的轻节点，或者其客户端通过网关进行区块链中的操作。如图中所示，所述用户例如包括用户 A、用户 B 和用户 C。其中，用户 C 为恶意用户，其例如可能会盗取用户 A 的私钥，以进行非法交易活动。本说明书实施例为了应对例如用户 C 的恶意盗取用户私钥的情况，为用户设置信任用户机制，以便于用户在丢失私钥之后可通过其信任用户冻结（即锁定）其账户，以防止进一步的损失。例如，用户 B 为用户 A 的信任用户，用户 A 通过向区块链中发送第一交易而在区块链中存入用户 B 为信任用户的信息，而授予用户 B 冻结用户 A 账户的权限。从而，当用户 A 的私钥丢失时，用户 A 可通过线下通知用户 B，使得用户 B 向区块链发送第二交易，以使得在区块链中冻结用户 A 的账户。

[47] 可以理解，上文参考图 1 的描述仅是示意性的，并不用于限制本说明书实施例的范围，例如，所述区块链不限于为联盟链，其也可以为公链等，在区块链为公链的情况下，用户 A、B、C 对应的客户端也可为区块链中的全节点。下文中，将以联盟链为例进行具体描述。

[48] 下面将详细描述上述授权的过程和冻结账户的过程。

[49] 图 2 示出根据本说明书实施例的一种在区块链中存入账户的信任账户信息的方法，所述方法由第一用户在区块链中的第一账户客户端执行，包括：

[50] 步骤 S202，获取第二用户在区块链中的第二账户，所述第二用户为所述第一用户的信任用户；

[51] 步骤 S204，发起第一交易，所述第一交易用于在区块链中存入第一账户的信任账户信息，所述第一交易中至少包括作为第一账户的信任账户的所述第二账户，以使得所述信任账户信息中至少包括所述第二账户，其中，所述信任账户具有锁定第一账户的权限。

[52] 首先，在步骤 S202，获取第二用户在区块链中的第二账户，所述第二用户为所述第一用户的信任用户。

[53] 该方法由第一用户通过其在区块链中的第一账户客户端执行，用于设置其在区块链中的信任账户，所述信任账户具有锁定所述第一账户的权限。第一用户首先确定好可作为信任用户的用户，例如第二用户，例如，第一用户可在线下取得其信任的第二用户

的同意之后，将第二用户确定为信任用户。之后，第一账户客户端获取第二用户的第二账户，以用于发起下个步骤中的第一交易。第一账户客户端例如可从第一用户的输入获取第二用户的第二账户，或者，第一账户客户端可从第二账户客户端接收第二账户，等等。

- 5 [54] 在一个实施例中，在获取第二用户第二账户的同时，还可以获取第二账户的公钥，以提供给下个步骤中的第一交易。

[55] 可以理解，虽然在该步骤中仅描述了获取第一用户的一个信任用户的账户，在本说明书实施例中可通过该方法类似地设置第一用户的多个信任用户。

- 10 [56] 在步骤 S204，发起第一交易，所述第一交易用于在区块链中存入第一账户的信任账户信息，所述第一交易中至少包括作为第一账户的信任账户的所述第二账户，以使得所述信任账户信息中至少包括所述第二账户，其中，所述信任账户具有锁定第一账户的权限。

- 15 [57] 本领域技术人员可以理解，在区块链中，客户端可通过发起交易而向区块链中存入信息，该信息为经过共识的、各个节点一致的，因此具有更高的安全性、可信度。区块链中包括多种数据库，如区块、账户数据库（状态数据树）等，因此，向区块链中存入信息包括向区块、账户数据库等数据库中存入信息。

- 20 [58] 在一个实施例中，所述第一交易为调用第一智能合约的交易，所述第一智能合约
- 为区块链中预先部署的用于设置账户的信任账户的智能合约。所述第一智能合约中例如包括 set1()函数，用于在区块链中的状态树中设置账户的预置的信任账户字段。当第一
- 25 账户发起调用第一智能合约的第一交易时，第一交易例如如图 3 所示，图 3 示出了第一交易的示意形式，其中，第一交易中的发送字段（From）为第一账户，接收字段（To）为该第一智能合约的合约账户，数据字段（Data）为对第一智能合约中的 set1()函数的调用，例如{set1(strings),“第二账户”}，即，“第二账户”为 set1()函数的输入参数，另外，该第一交易包括通过第一账户的私钥生成的数字签名。第一账户例如向图 1 中的任一全
- 30 节点（例如节点 1）发送该第一交易，节点 1 在接收该第一交易之后，对该第一交易进行验证之后在共识节点中扩散该第一交易。在通过共识节点确定记账节点之后，在记账节点执行该第一智能合约，从而通过执行该第一智能合约将记账节点本地的状态树中的第一账户的信任账户字段设置为第二账户。可以理解，在状态树数据库中可设置不止一个信任账户字段，例如设置三个信任账户字段，从而第一账户客户端可首先获取三个信任账户，并在第一交易中通过三次调用 set1()函数，从而在状态树中分别设置三个信任

账户。记账节点在更新状态树之后，将该第一交易放入区块存入区块链中，并将该区块发送给其它共识节点，从而其它共识节点在接收到该区块之后也相同地更新本地状态树中第一账户的信任账户。

[59] 在一个实施例中，第一智能合约中除了包括 set1()函数，还包括 set2()函数，set2()函数用于在状态树中设置账户的信任账户的公钥。在该情况中，客户端在步骤 S202 中还获取第二账户的公钥，并在该步骤中类似地调用 set2()函数，例如，在第一交易的数据字段中还包括“set2(strings),“第二账户公钥””，从而通过第一智能合约设置状态树中第一账户的信任账户公钥字段，以便于后续的锁定账户过程。

[60] 可以理解，这里虽然通过智能合约自动在状态树中存入账户的信任账户信息，本说明书不限于此，例如，所述第一智能合约的函数包括的 Set 函数可以不进行任何操作，从而仅用于传递设置第二账户及其公钥的信息，使得将第二账户及其公钥与该智能合约的调用一起作为交易被存入区块中，以用于后续的信任账户信息的查找。或者可通过预定好的规则，使得区块链中的节点基于该交易中调用的智能合约账户，确定该交易为用于存入信任账户信息的交易，从而在本地状态树中更新第一账户的预置的信任账户信息字段。

[61] 在一个实施例中，所述第一交易例如为由第一账户发送给第二账户的普通交易（例如转账交易），在该交易的数据字段中，可设置预定标志，以用于标识该交易用于存入信任账户信息，例如，该交易的数据字段为“存入信任账户信息”，并约定好，第一账户的信任账户即为第一交易的接收账户。从而，第一账户通过对第二账户发送这样的第一交易，当第一交易在经过共识被存入区块中之后，也即，第一账户向区块链中存入了第一账户的信任账户信息，并将第一账户的信任账户设定为第二账户。另外，在该第一交易的数据字段中还可以包括第二账户的公钥，从而在第一账户的信任账户信息中还包括第二账户的公钥。可以理解，第一交易不限于为第一账户发送给第二账户的交易，而可以为第一账户发送给区块链中非第二账户的任一账户的交易，在该情况中，该交易的数据字段例如包括“将“第二账户”设置为信任账户”，从而向区块链中传播将第二账户设置为信任账户的信任账户信息。或者，可通过预定好的规则，使得区块链中的节点基于该第一交易中的预定标志，确定该第一交易为用于存入信任账户信息的交易，从而在本地状态树中更新第一账户的预置的信任账户信息字段。

[62] 图 4 示出根据本说明书实施例的一种在区块链中存入账户的信任账户信息的方法，所述方法由区块链中的全节点执行，包括：

[63] 步骤 S402, 从区块链中接收由第一账户发起的第一交易, 所述第一交易用于在区块链中存入第一账户的信任账户信息, 所述第一交易中至少包括作为第一账户的信任账户的第二账户, 所述信任账户具有锁定第一账户的权限; 以及

5 [64] 步骤 S404, 基于所述第一交易, 在本地存入所述第一账户的信任账户信息, 其中, 所述信任账户信息中至少包括所述第二账户。

[65] 该方法即为在第一账户客户端向区块链发出第一交易之后, 区块链中的各个全节点基于第一交易向区块链中存入第一账户的信任账户信息的过程。如上文所述, 此处, 向区块链中存入包括, 向状态树中存入, 或向区块中存入, 等等。

10 [66] 首先, 在步骤 S402, 从区块链中接收由第一账户发起的第一交易, 所述第一交易用于在区块链中存入第一账户的信任账户信息, 所述第一交易中至少包括作为第一账户的信任账户的第二账户, 所述信任账户具有锁定第一账户的权限。该全节点例如为通过共识确定的记账节点, 其可以为区块链中的任一全节点, 如图 1 中的节点 1、2、3、4, 因此, 参考上文对步骤 S202 中的描述, 该全节点可从第一账户客户端接收该第一交易, 或者可从其它任意全节点接收该第一交易。可以理解, 用于执行该方法的全节点不限于
15 为记账节点, 例如, 其可以为记账节点的共识节点, 其通过从记账节点接收新生成的区块中包含的第一交易, 从而接收该第一交易。参考上文对步骤 S204 中的描述, 该第一交易例如为调用第一智能合约的交易, 或者该第一交易的数据字段中包括预定标志, 以用于标识其为用于在区块链中存入第一账户的信任账户信息的交易。

20 [67] 在步骤 S404, 基于所述第一交易, 在本地存入所述第一账户的信任账户信息, 其中, 所述信任账户信息中至少包括所述第二账户。

[68] 参考上文中对步骤 S204 中的描述, 在一个实施例中, 所述第一交易为调用第一智能合约的交易, 所述第一智能合约区块链中预先部署的用于存入账户的信任账户信息的智能合约。从而, 该全节点通过在本地产地执行所述第一智能合约而自动将所述信任账户信息存入本地的状态树中的第一账户下。或者, 所述第一智能合约包括的 set 函数可不
25 进行任何操作, 仅用于传递信息, 从而, 该全节点通过在本地产地执行所述第一智能合约, 基于预定规则, 由全节点自身将所述信任账户信息存入本地的状态树中的第一账户下。

[69] 参考上文中对步骤 S204 中的描述, 在一个实施例中, 所述第一交易中包括预定标志 (例如第一智能合约的账户, 或者“存入信任账户信息”), 用于指示该第一交易为用于向区块链中存入信任账户信息的交易。例如记账节点基于所述第一交易生成新的区块

之后, 将该区块存入本地的区块数据库中, 并将该区块扩散给其它全节点, 从而其它全节点分别在本地的新的区块中存入第一账户的信任账户信息。

[70] 图 5 示出根据本说明书实施例的一种在区块链中锁定账户的方法, 所述区块链中包括多个全节点, 所述全节点本地预先存储有第一账户的信任账户信息, 所述信任账户信息中至少包括作为第一账户的信任账户的第二账户, 所述方法在第二账户客户端执行, 包括:

[71] 步骤 502, 发起第二交易, 所述第二交易用于在区块链中锁定所述第一账户。

[72] 在如上所述执行图 2 和图 4 所示方法之后, 区块链中已存入了第一账户的信任账户信息, 即, 所述信任账户信息中将第二账户设置为第一账户的信任账户。在该情况中, 第二账户具有发起锁定第一账户的权限。当第一用户在私钥丢失或被盗的情况中, 第一用户可例如通过电话、网络通信等通信方式告知第二用户, 并请求第二用户锁定第一账户。第二用户在接收到第一用户的请求之后, 可在通过第二账户客户端发出用于锁定第一账户的第二交易。

[73] 在一个实施例中, 所述第二交易为调用第二智能合约的交易, 所述第二智能合约为区块链中预先部署的用于锁定账户的智能合约。例如, 第二智能合约中包括“Lock()”函数, 其用于在确定满足预定条件的情况中, 即确定所述第二账户为第一账户的信任账户的情况中, 在区块链中的状态树中将指定账户的状态修改为锁定状态。第二账户发起的调用第二智能合约的第二交易的具体形式与第一交易的形式类似, 其也包括发送字段、接收字段和数据字段, 其中发送字段为第二账户, 接收字段为第二智能合约的合约账户, 数据字段为对“Lock()”函数的调用, 例如{Lock(strings), “第一账户”}。

[74] 可以理解, 同样地, 所述第二智能合约不限于包括上述 Lock 函数, 以通过执行该函数而在状态树中修改账户的状态, 在一个实施例中, 第二智能合约包括的 Lock 函数可以不进行任何操作, 仅用于传递锁定第一账户的信息, 从而使得在区块链各个节点在执行该智能合约时基于预定规则主动修改第一账户的状态。

[75] 在一个实施例中, 所述第二交易例如为由第二账户发送给第一账户的普通交易(例如转账交易), 在该交易的数据字段中, 可设置预定标志, 以用于标识该交易用于锁定账户, 例如, 该交易的数据字段为“锁定账户”, 并约定好, 第二交易的接收账户即为待锁定的账户。从而, 第二账户通过对第一账户发送这样的第二交易, 当第二交易在经过共识被存入区块中之后, 也即, 第二账户向区块链中传播了锁定第一账户的信息。区块

链中的各个节点在从第二交易中获取锁定第一账户的信息之后,可在本地将第一账户的状态修改为锁定状态。可以理解,第二交易不限于为第二账户发送给第一账户的交易,而可以为第二账户发送给区块链中非第一账户的任一账户的交易,在该情况中,该交易的数据字段例如包括“锁定“第一账户””,从而向区块链中传播锁定第一账户的信息。

5 [76] 图 6 示出根据本说明书实施例的一种在区块链中锁定账户的方法,所述区块链中包括多个全节点,所述全节点本地预先存储有第一账户的信任账户信息,所述信任账户信息中至少包括作为第一账户的信任账户的第二账户,所述方法由区块链中的全节点执行,包括:

[77] 步骤 S602,从区块链中接收由第二账户发起的用于锁定第一账户的第二交易;

10 [78] 步骤 S604,从本地获取所述第一账户的信任账户信息;

[79] 步骤 S606,基于所述信任账户信息,验证所述第二账户是否为所述第一账户的信任账户;

[80] 步骤 S608,在验证通过的情况下,在本地进行对第一账户的锁定。

[81] 在第二账户进行图 5 所示方法之后,即向区块链中发起第二交易之后,区块链中
15 通过共识节点的共识产生记账节点,从而记账节点及其共识节点可执行图 6 所示的方法,所述共识节点都应为区块链中的全节点,即,本地都包括全部区块和账户数据库,从而可基于数据库中的内容进行对交易的验证。

[82] 首先,在步骤 S602,从区块链中接收由第二账户发起的用于锁定第一账户的第二交易。

20 [83] 第二账户客户端在向区块链中发送第二交易时,即将该第二交易发送给区块链中的任一全节点,该任一全节点然后将该第二交易扩散给其它全节点。从而,例如记账节点可以从第二账户直接接收第二交易,或者可从区块中的其它全节点接收第二交易。

[84] 在步骤 S604,从本地获取所述第一账户的信任账户信息。

[85] 如上为所述,在一个实施例中,所述信任账户信息被存储在所述全节点的本地状态树中,其中,从本地获取所述第一账户的信任账户信息包括,从本地状态树中获取所述
25 所述第一账户的信任账户信息。

[86] 在一个实施例中,所述信任账户信息被存储在区块中,其中,从本地获取所述第一账户的信任账户信息包括,从本地存储的多个区块中检索具有第一账户和预定标志的

交易（即上述第一交易），从而获取第一账户的信任账户信息。

[87] 该全节点在接收到该第二交易并获取第一账户的信任账户信息之后，首先使用第二账户的公钥对该第二交易的数字签名进行验证，另外，在例如以太坊中，该全节点还对第一账户的剩余燃料进行验证等，在此不一一列出。

5 [88] 在信任账户信息中还包括第二账户公钥的情况中，记账节点可以从例如账户状态树中获取第二账户公钥，以用于验证第二交易的数字签名。当信任账户信息中不包括第二账户公钥的情况中，记账节点可通过其他方法获取第二账户公钥，如通过密钥管理方获取第二账户公钥等。

10 [89] 在进行上述常规的验证之后，在一个实施例中，所述第二交易为调用第二智能合约的交易，从而该全节点开始执行该智能合约中的上述 Lock()函数，从而通过执行该函数自动进行下述的步骤 S606-S608。在一个实施例中，如上文所述，所述第二交易中包括预定标志，用于指示该第二交易为用于锁定账户的交易，从而使得该全节点本地执行下述的步骤 S606-S608。

15 [90] 步骤 S606，基于所述信任账户信息，验证所述第二账户是否为所述第一账户的信任账户。

[91] 在获取信任账户信息之后，可基于该信息确定第二账户是否为第一账户的信任账户。在一个实施例中，该信任账户信息存储在状态树的第一账户下，从而，可确定状态树的第一账户下的信任账户字段中是否包括第二账户，从而验证第二账户是否为第一账户的信任账户。在一个实施例中，信任账户信息存储在区块的一个交易中，从而可基于
20 区块中该交易的信息，确定第二账户是否为第一账户的信任账户。

[92] 在步骤 S608，在验证通过的情况中，在本地进行对第一账户的锁定。

[93] 在一个实施例中，所述第二交易为调用第二智能合约的交易，如上文所述，所述第二智能合约区块链中预先部署的用于锁定账户的智能合约，从而，记账节点通过在本地执行所述第二智能合约而进行对第一账户的锁定，也即，通过执行上述“Lock()”函数，执行步骤 S606，在验证通过的情况中，自动将本地状态树中的第一账户的状态修改为锁定状态。
25

[94] 在一个实施例中，所述第二交易为普通交易，如上文所述，其向记账节点传递了锁定第一账户的信息，从而记账节点可在验证通过的情况中将本地状态树中的第一账户的状态修改为锁定状态。

30 [95] 记账节点在修改本地状态树之后，将第二交易打包到区块中并发送给其它全节点，

从而将该区块存入区块链中。其它节点在接收包括第二交易的区块之后，可同样地基于第二交易，修改本地状态树中第一账户的状态，从而达到各个全节点的数据一致性。

[96] 图 7 示出根据本说明书实施例的一种在区块链中存入账户的信任账户信息的装置 700，所述装置部署于第一用户在区块链中的第一账户客户端，包括：

5 [97] 获取单元 71，配置为，获取第二用户在区块链中的第二账户，所述第二用户为所述第一用户的信任用户；

[98] 交易发起单元 72，配置为，发起第一交易，所述第一交易用于在区块链中存入第一账户的信任账户信息，所述第一交易中至少包括作为第一账户的信任账户的所述第二账户，以使得所述信任账户信息中至少包括所述第二账户，其中，所述信任账户具有锁
10 定第一账户的权限。

[99] 在一个实施例中，所述第一交易为调用第一智能合约的交易，所述第一智能合约
为区块链中预先部署的用于存入账户的信任账户信息的智能合约，所述第一交易的数据
字段中至少包括所述第二账户。

[100] 在一个实施例中，所述获取单元 71 还配置为，获取第二用户在区块链中的第二账
15 户及其公钥，其中，所述第一交易的数据字段中还包括第二账户的公钥，以使得所述信
任账户信息中还包括第二账户的公钥。

[101] 图 8 示出根据本说明书实施例的一种在区块链中存入账户的信任账户信息的装置
800，所述装置部署于区块链中的全节点，包括：

[102] 接收单元 81，配置为，从区块链中接收由第一账户发起的第一交易，所述第一交
20 易用于在区块链中存入第一账户的信任账户信息，所述第一交易中至少包括作为第一账
户的信任账户的第二账户，所述信任账户具有锁定第一账户的权限；以及

[103] 存入单元 82，配置为，基于所述第一交易，在本地存入所述第一账户的信任账户
信息，其中，所述信任账户信息中至少包括所述第二账户。

[104] 在一个实施例中，所述第一交易为调用第一智能合约的交易，所述第一智能合约
25 为区块链中预先部署的用于存入账户的信任账户信息的智能合约，其中，所述存入单元
82 还配置为，通过在本地执行所述第一智能合约而将所述信任账户信息存入本地的状态
树中的第一账户下。

[105] 在一个实施例中，所述存入单元 82 还配置为，基于所述第一交易，在本地的新的
30 区块中存入第一账户的信任账户信息，其中，所述第一交易中包括预定标志，用于指示
该第一交易为用于向区块链中存入信任账户信息的交易。

[106] 图 9 示出根据本说明书实施例的一种在区块链中锁定账户的装置 900, 所述区块链中包括多个全节点, 所述全节点本地预先存储有第一账户的信任账户信息, 所述信任账户信息中至少包括作为第一账户的信任账户的第二账户, 所述装置部署于第二账户客户端, 包括:

5 [107] 交易发起单元 91, 配置为, 发起第二交易, 所述第二交易用于在区块链中锁定所述第一账户。

[108] 图 10 示出根据本说明书实施例的一种在区块链中锁定账户的装置 1000, 所述区块链中包括多个全节点, 所述全节点本地预先存储有第一账户的信任账户信息, 所述信任账户信息中至少包括作为第一账户的信任账户的第二账户, 所述装置部署于区块链中的
10 全节点, 包括:

[109] 接收单元 101, 配置为, 从区块链中接收由第二账户发起的用于锁定第一账户的第二交易;

[110] 获取单元 102, 配置为, 从本地获取所述第一账户的信任账户信息;

[111] 验证单元 103, 配置为, 基于所述信任账户信息, 验证所述第二账户是否为所述第
15 一账户的信任账户; 以及

[112] 锁定单元 104, 配置为, 在验证通过的情况中, 在本地进行对第一账户的锁定。

[113] 在一个实施例中, 所述第二交易为调用第二智能合约的交易, 所述第二智能合约
为区块链中预先部署的用于锁定账户的智能合约, 其中, 所述锁定单元 104 还配置为,
通过在本本地执行所述第二智能合约而进行对第一账户的锁定。

20 [114] 在一个实施例中, 所述信任账户信息被存储在所述全节点的本地状态树中, 其中,
所述获取单元 102 还配置为, 从本地状态树中获取所述第一账户的信任账户信息。

[115] 在一个实施例中, 所述信任账户信息被存储在区块中, 其中, 所述获取单元 102
还配置为, 从本地存储的多个区块中检索具有第一账户和预定标志的交易, 从而获取第
一账户的信任账户信息。

25 [116] 本说明书另一方面提供一种计算机可读存储介质, 其上存储有计算机程序, 当所
述计算机程序在计算机中执行时, 令计算机执行上述任一项方法。

[117] 本说明书另一方面提供一种计算设备, 包括存储器和处理器, 所述存储器中存储
有可执行代码, 所述处理器执行所述可执行代码时, 实现上述任一项方法。

[118] 在根据本说明书实施例的方案中, 通过采用信任账户机制, 通过对信任的第三方
30 授权锁定账户的权限, 从而在账户私钥丢失或被盗的情况中, 可通过第三方进行账户锁

定，从而防止损失进一步扩大。

[119] 需要理解，本文中的“第一”，“第二”等描述，仅仅为了描述的简单而对相似概念进行区分，并不具有其他限定作用。

5 [120] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

10 [121] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

15 [122] 本领域普通技术人员应该还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执轨道，取决于技术方案的特定应用和设计约束条件。本领域普通技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

20 [123] 结合本文中所公开的实施例描述的方法或算法的步骤可以用硬件、处理器执轨道的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器（RAM）、内存、只读存储器（ROM）、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

25 [124] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

1、一种在区块链中存入账户的信任账户信息的方法，所述方法由第一用户在区块链中的第一账户客户端执行，包括：

获取第二用户在区块链中的第二账户，所述第二用户为所述第一用户的信任用户；

5 以及

发起第一交易，所述第一交易用于在区块链中存入第一账户的信任账户信息，所述第一交易中至少包括作为第一账户的信任账户的所述第二账户，以使得所述信任账户信息中至少包括所述第二账户，其中，所述信任账户具有锁定第一账户的权限。

2、根据权利要求1所述的方法，其中，所述第一交易为调用第一智能合约的交易，
10 所述第一智能合约为区块链中预先部署的用于存入账户的信任账户信息的智能合约，所述
所述第一交易的数据字段中至少包括所述第二账户。

3、根据权利要求2所述的方法，其中，获取第二用户在区块链中的第二账户包括，
获取第二用户在区块链中的第二账户及其公钥，其中，所述第一交易的数据字段中还包
括第二账户的公钥，以使得所述信任账户信息中还包括第二账户的公钥。

15 4、一种在区块链中存入账户的信任账户信息的方法，所述方法由区块链中的全节
点执行，包括：

从区块链中接收由第一账户发起的第一交易，所述第一交易用于在区块链中存入第
一账户的信任账户信息，所述第一交易中至少包括作为第一账户的信任账户的第二账户，
所述信任账户具有锁定第一账户的权限；以及

20 基于所述第一交易，在本地存入所述第一账户的信任账户信息，其中，所述信任账
户信息中至少包括所述第二账户。

5、根据权利要求4所述的方法，其中，所述第一交易为调用第一智能合约的交易，
所述第一智能合约为区块链中预先部署的用于存入账户的信任账户信息的智能合约，其
中，基于所述第一交易，在本地存入所述第一账户的信任账户信息包括，通过在本
地执
25 行所述第一智能合约而将所述信任账户信息存入本地的状态树中的第一账户下。

6、根据权利要求4所述的方法，其中，基于所述第一交易，在本地存入所述第一
账户的信任账户信息包括，基于所述第一交易，在本地的新的区块中存入第一账户的信
任账户信息，其中，所述第一交易中包括预定标志，用于指示该第一交易为用于向区块
链中存入信任账户信息的交易。

30 7、一种在区块链中锁定账户的方法，所述区块链中包括多个全节点，所述全节点
本地预先存储有第一账户的信任账户信息，所述信任账户信息中至少包括作为第一账户

的信任账户的第二账户，所述方法由第二账户客户端执行，包括：

发起第二交易，所述第二交易用于在区块链中锁定所述第一账户。

8、根据权利要求7所述的方法，其中，所述第二交易为调用第二智能合约的交易，所述第二智能合约为区块链中预先部署的用于锁定账户的智能合约，所述第二交易的数据

5 据字段中包括所述第一账户。

9、一种在区块链中锁定账户的方法，所述区块链中包括多个全节点，所述全节点本地预先存储有第一账户的信任账户信息，所述信任账户信息中至少包括作为第一账户的信任账户的第二账户，所述方法由区块链中的全节点执行，包括：

从区块链中接收由第二账户发起的用于锁定第一账户的第二交易；

10 从本地获取所述第一账户的信任账户信息；

基于所述信任账户信息，验证所述第二账户是否为所述第一账户的信任账户；以及在验证通过的情况中，在本地进行对第一账户的锁定。

10、根据权利要求9所述的方法，其中，所述第二交易为调用第二智能合约的交易，所述第二智能合约为区块链中预先部署的用于锁定账户的智能合约，其中，在本地进行
15 对第一账户的锁定包括，通过在本地执行所述第二智能合约而进行对第一账户的锁定。

11、根据权利要求9所述的方法，其中，所述信任账户信息被存储在所述全节点的本地状态树中，其中，从本地获取所述第一账户的信任账户信息包括，从本地状态树中获取所述第一账户的信任账户信息。

12、根据权利要求9所述的方法，其中，所述信任账户信息被存储在区块中，其中，
20 从本地获取所述第一账户的信任账户信息包括，从本地存储的多个区块中检索具有第一账户和预定标志的交易，从而获取第一账户的信任账户信息。

13、一种在区块链中存入账户的信任账户信息的装置，所述装置部署于第一用户在区块链中的第一账户客户端，包括：

获取单元，配置为，获取第二用户在区块链中的第二账户，所述第二用户为所述第
25 一用户的信任用户；以及

交易发起单元，配置为，发起第一交易，所述第一交易用于在区块链中存入第一账户的信任账户信息，所述第一交易中至少包括作为第一账户的信任账户的所述第二账户，以使得所述信任账户信息中至少包括所述第二账户，其中，所述信任账户具有锁定第一账户的权限。

30 14、根据权利要求13所述的装置，其中，所述第一交易为调用第一智能合约的交易，所述第一智能合约为区块链中预先部署的用于存入账户的信任账户信息的智能合约，

所述第一交易的数据字段中至少包括所述第二账户。

15、根据权利要求 14 所述的装置，其中，所述获取单元还配置为，获取第二用户在区块链中的第二账户及其公钥，其中，所述第一交易的数据字段中还包括第二账户的公钥，以使得所述信任账户信息中还包括第二账户的公钥。

5 16、一种在区块链中存入账户的信任账户信息的装置，所述装置部署于区块链中的全节点，包括：

接收单元，配置为，从区块链中接收由第一账户发起的第一交易，所述第一交易用于在区块链中存入第一账户的信任账户信息，所述第一交易中至少包括作为第一账户的信任账户的第二账户，所述信任账户具有锁定第一账户的权限；以及

10 存入单元，配置为，基于所述第一交易，在本地存入所述第一账户的信任账户信息，其中，所述信任账户信息中至少包括所述第二账户。

17、根据权利要求 16 所述的装置，其中，所述第一交易为调用第一智能合约的交易，所述第一智能合约区块链中预先部署的用于存入账户的信任账户信息的智能合约，其中，所述存入单元还配置为，通过在本本地执行所述第一智能合约而将所述信任账户信息存入本地的状态树中的第一账户下。

18、根据权利要求 16 所述的装置，其中，所述存入单元还配置为，基于所述第一交易，在本地的新的区块中存入第一账户的信任账户信息，其中，所述第一交易中包括预定标志，用于指示该第一交易为用于向区块链中存入信任账户信息的交易。

19、一种在区块链中锁定账户的装置，所述区块链中包括多个全节点，所述全节点本地预先存储有第一账户的信任账户信息，所述信任账户信息中至少包括作为第一账户的信任账户的第二账户，所述装置部署于第二账户客户端，包括：

交易发起单元，配置为，发起第二交易，所述第二交易用于在区块链中锁定所述第一账户。

20、根据权利要求 19 所述的装置，其中，所述第二交易为调用第二智能合约的交易，所述第二智能合约区块链中预先部署的用于锁定账户的智能合约，所述第二交易的数据字段中包括所述第一账户。

21、一种在区块链中锁定账户的装置，所述区块链中包括多个全节点，所述全节点本地预先存储有第一账户的信任账户信息，所述信任账户信息中至少包括作为第一账户的信任账户的第二账户，所述装置部署于区块链中的全节点，包括：

30 接收单元，配置为，从区块链中接收由第二账户发起的用于锁定第一账户的第二交易；

获取单元，配置为，从本地获取所述第一账户的信任账户信息；

验证单元，配置为，基于所述信任账户信息，验证所述第二账户是否为所述第一账户的信任账户；以及

锁定单元，配置为，在验证通过的情况中，在本地进行对第一账户的锁定。

5 22、根据权利要求 21 所述的装置，其中，所述第二交易为调用第二智能合约的交易，所述第二智能合约为区块链中预先部署的用于锁定账户的智能合约，其中，所述锁定单元还配置为，通过在本本地执行所述第二智能合约而进行对第一账户的锁定。

10 23、根据权利要求 21 所述的装置，其中，所述信任账户信息被存储在所述全节点的本地状态树中，其中，所述获取单元还配置为，从本地状态树中获取所述第一账户的信任账户信息。

24、根据权利要求 21 所述的装置，其中，所述信任账户信息被存储在区块中，其中，所述获取单元还配置为，从本地存储的多个区块中检索具有第一账户和预定标志的交易，从而获取第一账户的信任账户信息。

15 25、一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行权利要求 1-12 中任一项的所述的方法。

26、一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-12 中任一项所述的方法。

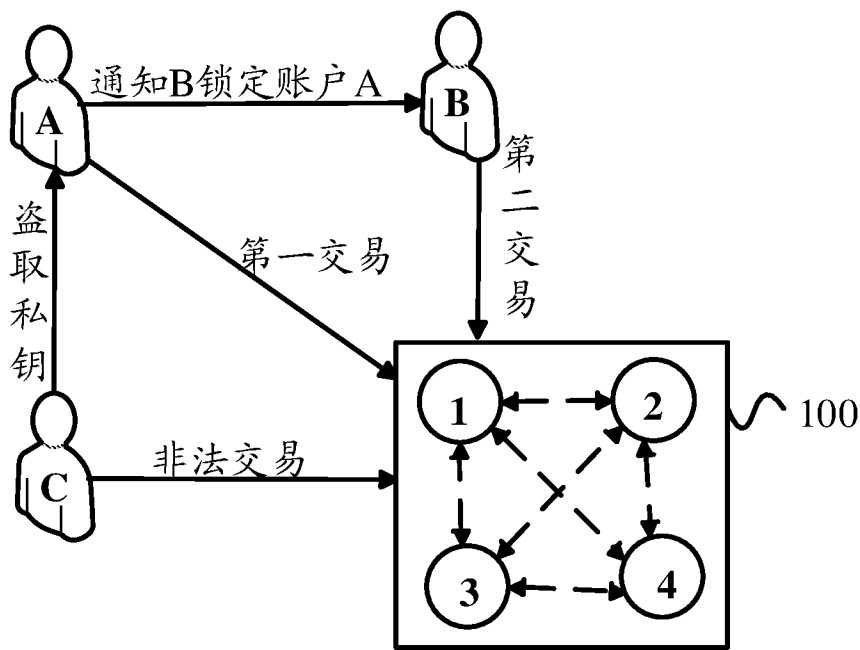


图 1

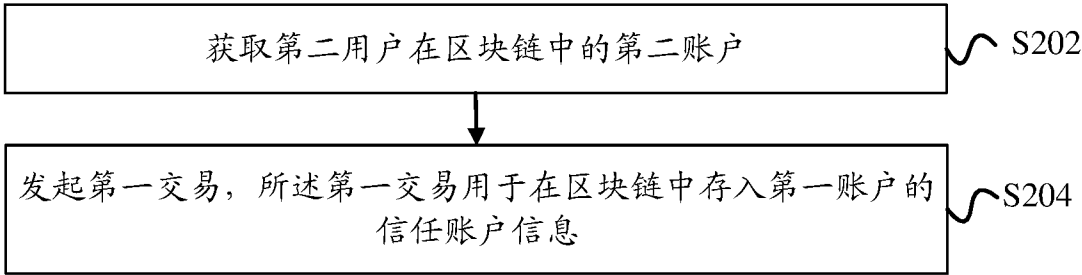


图 2

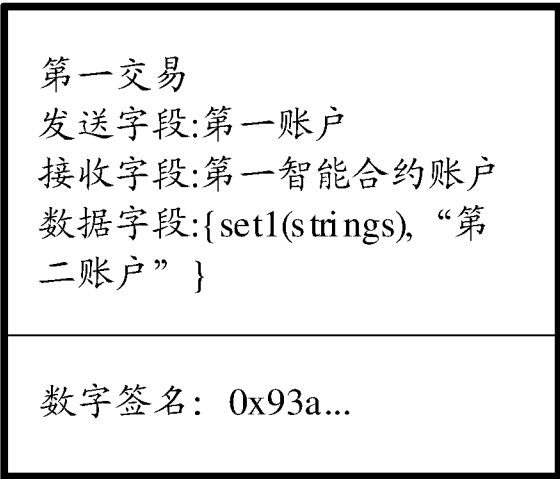


图 3

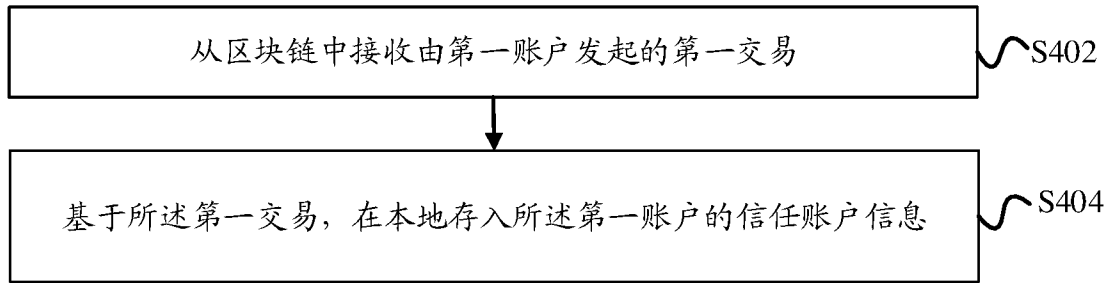


图 4

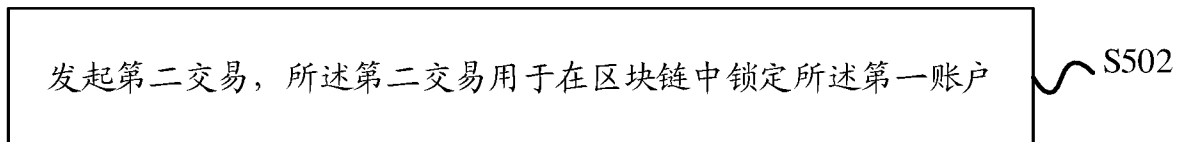


图 5

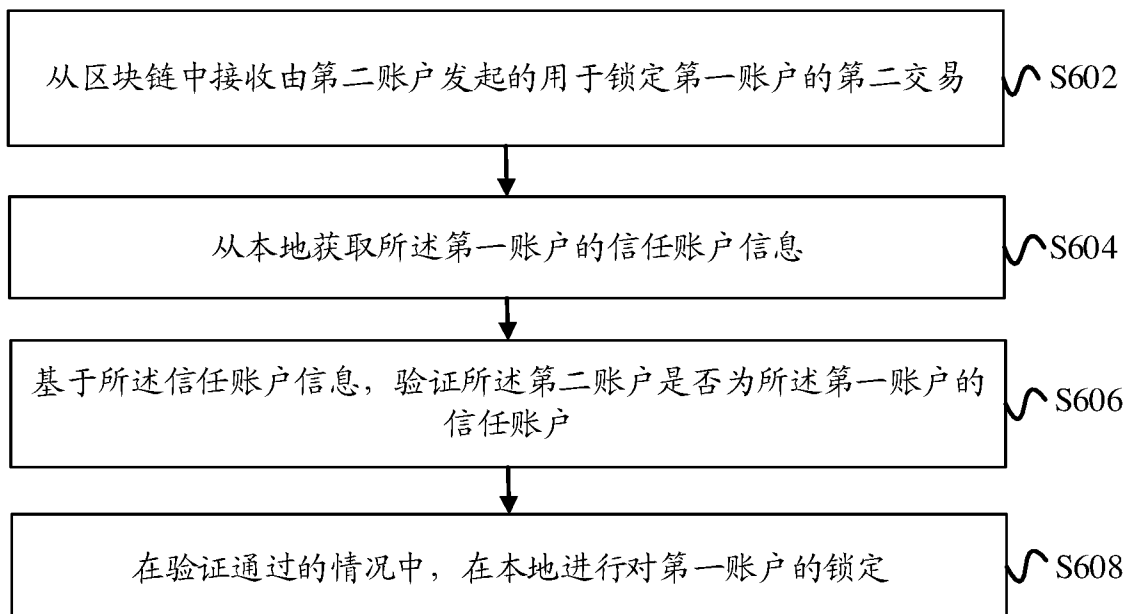


图 6



图 7

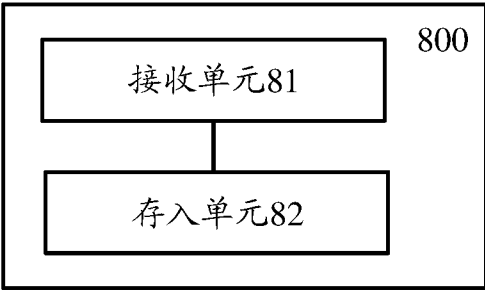


图 8

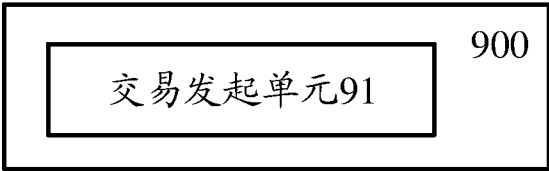


图 9

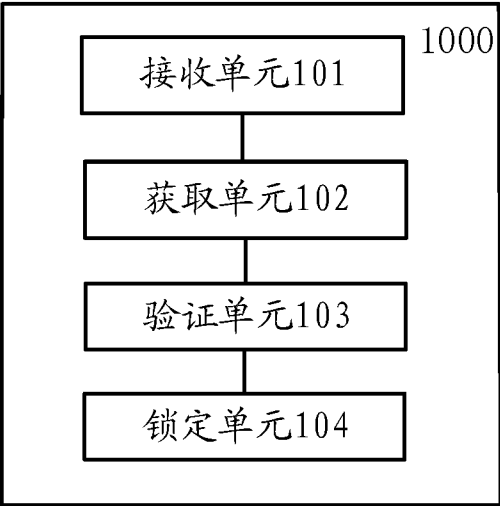


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/082427

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, IEEE: 区块链, 账户, 交易, 锁定, 公钥, 节点, 智能合约, block, chain, blockchain, account, transaction, lock, public, key, node, intelligent, contract

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110414977 A (ALIBABA GROUP HOLDING LIMITED) 05 November 2019 (2019-11-05) claims 1-26	1-26
X	CN 108830577 A (BEIJING LIANQI TECHNOLOGY CO., LTD.) 16 November 2018 (2018-11-16) description paragraphs [0053]-[0124]	1-26
A	CN 107609876 A (BEIJING YUNZIC TECHNOLOGY CO., LTD.) 19 January 2018 (2018-01-19) entire document	1-26
A	CN 109064327 A (ULTRAIN TECHNOLOGY LTD.) 21 December 2018 (2018-12-21) entire document	1-26
A	CN 109146448 A (HANGZHOU FUZAMEI TECHNOLOGY CO., LTD.) 04 January 2019 (2019-01-04) entire document	1-26
A	US 2019026450 A1 (DELL PRODUCTS, LP) 24 January 2019 (2019-01-24) entire document	1-26



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

16 June 2020

Date of mailing of the international search report

30 June 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/082427

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110414977	A	05 November 2019	None			
CN	108830577	A	16 November 2018	None			
CN	107609876	A	19 January 2018	None			
CN	109064327	A	21 December 2018	None			
CN	109146448	A	04 January 2019	None			
US	2019026450	A1	24 January 2019	US	2020050747	A1	13 February 2020

国际检索报告

国际申请号

PCT/CN2020/082427

A. 主题的分类 G06Q 20/38 (2012.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) G06Q 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNPAT, WPI, EPDOC, CNKI, IEEE: 区块链, 账户, 交易, 锁定, 公钥, 节点, 智能合约, block, chain, blockchain, account, transaction, lock, public, key, node, intelligent, contract		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 110414977 A (阿里巴巴集团控股有限公司) 2019年 11月 5日 (2019 - 11 - 05) 权利要求1-26	1-26
X	CN 108830577 A (北京连琪科技有限公司) 2018年 11月 16日 (2018 - 11 - 16) 说明书第[0053]-[0124]]段	1-26
A	CN 107609876 A (北京云知科技有限公司) 2018年 1月 19日 (2018 - 01 - 19) 全文	1-26
A	CN 109064327 A (浙江超脑时空科技有限公司) 2018年 12月 21日 (2018 - 12 - 21) 全文	1-26
A	CN 109146448 A (杭州复杂美科技有限公司) 2019年 1月 4日 (2019 - 01 - 04) 全文	1-26
A	US 2019026450 A1 (DELL PRODUCTS, LP) 2019年 1月 24日 (2019 - 01 - 24) 全文	1-26
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2020年 6月 16日		国际检索报告邮寄日期 2020年 6月 30日
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 王莹 电话号码 86-(10)-53961411

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/082427

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	110414977	A	2019年 11月 5日	无	
CN	108830577	A	2018年 11月 16日	无	
CN	107609876	A	2018年 1月 19日	无	
CN	109064327	A	2018年 12月 21日	无	
CN	109146448	A	2019年 1月 4日	无	
US	2019026450	A1	2019年 1月 24日	US 2020050747 A1	2020年 2月 13日