(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 107683488 B
(45)授权公告日 2023.09.05

(21)申请号 201680032863.4
(22)申请日 2016.04.04
(65)同一申请的已公布的文献号
申请公布号 CN 107683488 A
(43)申请公布日 2018.02.09
(30)优先权数据
62/178,315 2015.04.05 US
(85)PCT国际申请进入国家阶段日
2017.12.05
(86)PCT国际申请的申请数据
PCT/US2016/025888 2016.04.04
(87)PCT国际申请的公布数据
WO2016/164310 EN 2016.10.13
(73)专利权人 数字资产(瑞士)股份有限公司
地址 瑞士苏黎世

(72)发明人 R·唐纳德·JR·威尔逊
苏尼尔·希拉尼
埃里克·W·萨拉尼奇
尤瓦尔·罗兹 绍尔·克弗尔

(74)专利代理机构 中科专利商标代理有限责任公司 11021
专利代理师 余婧娜
(51)Int.Cl.
G06Q 20/06(2006.01)
G06Q 20/38(2006.01)
G06Q 40/06(2006.01)

(56)对比文件
CN 101883100 A,2010.11.10
WO 2015024129 A1,2015.02.26
US 2013232023 A2,2013.09.05

审查员 余吉

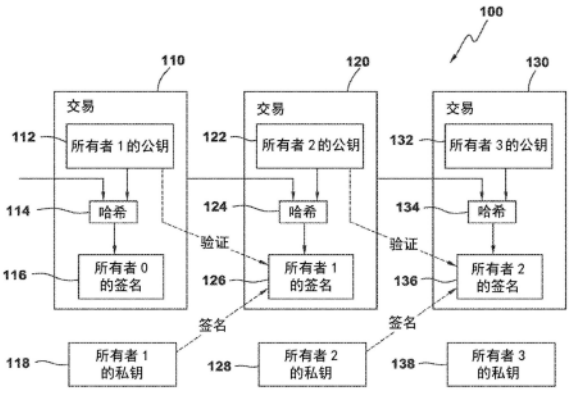
权利要求书5页 说明书16页 附图20页

(54)发明名称

数字资产中介电子结算平台

(57)摘要

一种数字资产结算方法,包括:从第一用户接收(1401)涉及已经在分布式账本上数字化的数字权利的有条件交易的授权,将来自第一用户的交易授权与来自至少一个其他用户的交易授权进行匹配(1413),如果满足条件,则结算(1416)至少第一用户和其他用户之间的交易,并且在分布式账本上记录(1508)已结算的交易。



CN 107683488 B

1.一种数字资产结算方法,包括:

从第一用户接收涉及所述第一用户对数字资产的权利的有条件交易的授权,所述数字资产已记录在分布式账本上,其中所述授权对数字资产从仅在所述第一用户的控制下的密钥存储库应用的控制转移到第一多密钥存储库应用的控制进行授权,其中所述第一多密钥存储库应用具有至少第一公钥和至少第二公钥,所述第一公钥的对应的第一私钥在所述第一用户的控制下,所述第二公钥的对应的第二私钥在中介电子结算平台的控制下,其中对所述第一私钥的控制指示对所对应的第一公钥持有的资产、权利或合同的控制,并且对所述第二私钥的控制指示对所对应的第二公钥持有的资产、权利或合同的控制;

将来自所述第一用户的交易授权与来自至少一个其他用户的涉及所述至少一个其他用户对至少一个数字资产的至少一个权利的交易授权进行匹配,所述至少一个数字资产已经记录在分布式账本上;

如果满足条件,则结算所述第一用户和所述至少一个其他用户之间的所述交易,其中,结算交易使得数字资产从所述第一多密钥存储库应用的控制转移到第二多密钥存储库应用的控制,所述第二多密钥存储库应用具有至少第三公钥,所述第三公钥的对应的第三私钥在所述至少一个其他用户的控制之下,其中对所述第三私钥的控制指示对所对应的第三公钥的持有的资产、权利或合同的控制;以及

在分布式账本上记录已结算的交易。

2.根据权利要求1所述的方法,其中,数字资产中的至少一个表示常规资产的数字化所有权。

3.根据权利要求1所述的方法,还包括将用于赎回的电子机制与第一用户对有条件交易的授权相关联,其中调用用于赎回的电子机制使得数字资产从所述第一多密钥存储库应用的控制转移回仅在所述第一用户控制下的密钥存储库应用的控制。

4.根据权利要求3所述的方法,其中,如果所述交易因不满足条件而未被结算,则调用用于赎回的电子机制。

5.根据权利要求3所述的方法,其中,在数字资产从仅在所述第一用户的控制下的密钥存储库应用的控制转移到第一多密钥存储库应用的控制之后,所述用于赎回的电子机制允许从第一多密钥存储库应用的控制回到仅在所述第一用户的控制下的密钥存储库应用的控制时所述第一用户在预设时间单方面撤回适用的资产、权利、资金或合同。

6.根据权利要求3所述的方法,其中,所述用于赎回的电子机制包括在赎回交易中使用的用于赎回的预签署授权,其中所述预签署授权由所述第一用户的密码密钥签署。

7.根据权利要求3所述的方法,其中,在数字资产从仅在所述第一用户的控制下的密钥存储库应用的控制转移到第一多密钥存储库应用的控制之后在预设时间自动调用用于赎回的电子机制。

8.一种程序存储设备,有形地包括处理器可执行的程序指令,以便:

从仅在第一用户的控制下的密钥存储库应用向在多方的控制下的第一多密钥存储库应用传输第一数字资产权利的所有权控制的数字表示,其中所述第一多密钥存储库应用包括至少第一公钥和至少第二公钥,所述第一公钥的对应的第一私钥在所述第一用户的控制下,所述第二公钥的对应的第二私钥在中介电子结算平台的控制下,其中对所述第一私钥的控制指示对所对应的第一公钥持有的资产、权利或合同的控制,并且对所述第二私钥的

控制指示对所对应的第二公钥持有的资产、权利或合同的控制；

从所述第一用户接收涉及已经在分布式账本上数字化的所述第一数字资产权利的交易的授权，所述分布式账本由计算机网络的多个节点来维护，其中所述交易的授权与绑定到第一赎回条件的、用于赎回第一数字资产权利的第一密码实施电子机制相关联，用于赎回的所述第一密码实施电子机制包括预签署授权，以允许所述第一用户在未来的预设时间从所述第一多密钥存储库应用单方面撤回所述第一数字资产权利，并且在满足所述第一赎回条件时是可执行的；

将来自所述第一用户的交易授权与来自至少一个其他用户的、涉及至少第二数字资产权利的交易授权进行匹配；以及

(i)如果不满足所述第一赎回条件，则：

a.对所述第一用户和所述至少一个其他用户的授权交易进行原子结算，以传输所述第一数字资产权利和所述第二数字资产权利的至少一部分的所有权控制的数字表示，其中，结算所述第一用户的授权交易使得对第一数字资产权利的所有权控制的数字表示从第一多密钥存储库应用传输到第二多密钥存储库应用，所述第二多密钥存储库应用具有至少第三公钥，所述第三公钥的对应的第三私钥在所述至少一个其他用户的控制之下，其中对所述第三私钥的控制指示对所对应的第三公钥的持有的资产、权利或合同的控制；以及

b.将所述第一数字资产权利和所述第二数字资产权利的所有权的数字表示记录在所述分布式账本的部分或完整副本中；

(ii)如果满足所述第一赎回条件，则：

a.执行用于赎回的所述第一密码实施电子机制，使得所述第一数字资产权利的所有权控制的数字表示从所述第一多密钥存储库应用传输回仅在所述第一用户的控制下的密钥存储库应用；以及

b.将执行后的赎回记录在所述分布式账本的部分或完全副本中。

9.根据权利要求8所述的程序存储设备，其中，所述第一数字资产权利和所述第二数字资产权利中的至少一个表示常规资产的数字化所有权。

10.根据权利要求8所述的程序存储设备，还包括所述处理器可执行的、用于刷新用于赎回的所述第一密码实施电子机制的程序指令。

11.根据权利要求8所述的程序存储设备，其中在步骤(i)(a)中，仅传输体现所述第一数字资产权利的一部分的所有权的数字表示，并且所述程序存储设备还包括所述处理器可执行的以下程序指令：

将绑定到第二赎回条件的、用于赎回的第二密码实施电子机制与所述第一数字资产权利未被传输的剩余部分相关联，用于赎回的所述第二密码实施电子机制包括预签署授权，以允许所述第一用户在未来的预设时间从所述第一多密钥存储库应用单方面撤回所述第一数字资产权利的剩余部分；以及

如果满足所述第二赎回条件，则：

a.执行用于赎回的所述第二密码实施电子机制，使得所述第一数字资产权利的所述剩余部分的所有权控制的数字表示从所述第一多密钥存储库应用传输回仅在所述第一用户的控制下的密钥存储库应用；以及

b.将执行后的赎回记录在所述分布式账本的部分或完全副本中。

12.根据权利要求8所述的程序存储设备，其中，所述第一数字资产权利包括数字合同。

13.根据权利要求8所述的程序存储设备，其中，所述第一赎回条件包括预定时间段的过期。

14.根据权利要求8所述的程序存储设备，还包括所述处理器可执行的、仅当满足某个定义的交换条件时才对所述第一用户和所述至少一个其他用户的授权交易进行密码签名的程序指令。

15.根据权利要求14所述的程序存储设备，其中，所述定义的交换条件包括所述第一用户的交易限制和匹配对手交易。

16.根据权利要求8所述的程序存储设备，其中，所述第一数字资产权利的所有权控制的数字表示从仅在所述第一用户的控制下的密钥存储库应用传输到所述第一多密钥存储库应用包括将所述第一数字资产权利储蓄在密钥库应用钱包中。

17.根据权利要求16所述的程序存储设备，其中，所述程序存储设备驻留在控制所述密钥库应用钱包中的至少一个私钥的中介电子结算平台服务器上。

18.根据权利要求8所述的程序存储设备，还包括所述处理器可执行的、刷新用于赎回的第一密码实施电子机制并改变第一赎回条件的程序指令。

19.根据权利要求8所述的程序存储设备，其中，用于赎回的第一密码实施电子机制包括时间锁定的交易。

20.根据权利要求8所述的程序存储设备，还包括所述处理器可执行的如下程序指令，其中如果满足所述第一赎回条件，则自动执行用于赎回的所述第一密码实施电子机制，并且将所述第一数字资产权利的所有权控制的数字表示从所述第一多密钥存储库应用传输到仅在所述第一用户的控制下的密钥存储库应用。

21.根据权利要求8所述的程序存储设备，其中，用于赎回的每个密码实施电子机制包括在赎回交易中使用的用于赎回的预签署授权。

22.根据权利要求8所述的程序存储设备，其中，所述第一数字资产权利与所述分布式账本中记录的唯一标识符相关联。

23.一种有形地体现处理器可执行的程序指令的程序存储设备，所述程序指令用于：

从第一用户接收涉及已经在分布式账本上数字化的第一数字资产权利的有条件交易的授权，其中所述有条件交易的授权对数字资产从仅在所述第一用户的控制下的密钥存储库应用的控制转移到第一多密钥存储库应用的控制进行授权以及所述有条件交易的授权与绑定到第一赎回条件的、用于赎回第一数字资产权利的第一密码实施电子机制相关联，用于赎回的所述第一密码实施电子机制包括预签署授权，以允许所述第一用户在未来的预设时间从所述第一多密钥存储库应用单方面撤回所述第一数字资产权利，其中所述第一多密钥存储库应用具有至少第一公钥和至少第二公钥，所述第一公钥的对应的第一私钥在所述第一用户的控制下，所述第二公钥的对应的第二私钥在中介电子结算平台的控制下，其中对所述第一私钥的控制指示对所对应的第一公钥持有的资产、权利或合同的控制，并且对所述第二私钥的控制指示对所对应的第二公钥持有的资产、权利或合同的控制；

将来自所述第一用户的交易授权与来自至少一个其他用户的涉及至少第二数字资产权利的交易授权进行匹配：

(i)如果不满足所述第一赎回条件，但满足了有条件交易的条件，则：

(a)结算所述第一用户和所述至少一个其他用户之间的交易,使得所述第一数字资产权利的控制从第一多密钥存储库应用转移到第二多密钥存储库应用,所述第二多密钥存储库应用具有至少第三公钥,所述第三公钥的对应的第三私钥在所述至少一个其他用户的控制之下,其中对所述第三私钥的控制指示对所对应的第三公钥的持有的资产、权利或合同的控制;以及

(b)将结算后的交易存储在所述分布式账本上;

(ii)如果满足所述第一赎回条件,则:

(a)执行用于赎回的所述第一密码实施电子机制,使得所述第一数字资产权利的控制从第一多密钥存储库应用被转移回仅在所述第一用户的控制下的密钥存储库应用;以及

(b)将执行后的赎回存储在所述分布式账本上。

24.根据权利要求23所述的程序存储设备,其中,所述第一数字资产权利和所述第二数字资产权利中的至少一个表示常规资产的数字化所有权。

25.根据权利要求23所述的程序存储设备,还包括所述处理器可执行的、用于刷新用于赎回的所述第一密码实施电子机制的程序指令。

26.根据权利要求23所述的程序存储设备,其中在步骤(i)(a)中,仅传输所述第一数字资产权利的一部分,并且所述程序存储设备还包括所述处理器可执行的以下程序指令:

将绑定到第二赎回条件的、用于赎回的第二密码实施电子机制与所述第一数字资产权利未被传输的剩余部分相关联,用于赎回的所述第二密码实施电子机制包括预签署授权,以允许所述第一用户在未来的预设时间从所述第一多密钥存储库应用单方面撤回所述第一数字资产权利的剩余部分;以及

如果满足所述第二赎回条件,则:

a.执行用于赎回的所述第二密码实施电子机制,使得所述第一数字资产权利的所述剩余部分的所有权控制的数字表示被传输回仅在所述第一用户的控制下的密钥存储库应用;以及

b.将执行后的赎回记录在所述分布式账本的部分或完全副本中。

27.根据权利要求23所述的程序存储设备,其中,所述第一数字资产权利包括数字合同。

28.根据权利要求23所述的程序存储设备,其中,所述第一赎回条件包括预定时间段的过期。

29.根据权利要求23所述的程序存储设备,还包括所述处理器可执行的、仅当满足某个定义的交换条件时才对所述第一用户和所述至少一个其他用户的授权交易进行密码签名的程序指令。

30.根据权利要求29所述的程序存储设备,其中,所述定义的交换条件包括所述第一用户的交易限制和匹配对手交易。

31.根据权利要求23所述的程序存储设备,还包括所述处理器可执行的、刷新用于赎回的第一密码实施电子机制并改变第一赎回条件的程序指令。

32.根据权利要求23所述的程序存储设备,其中,用于赎回的第一密码实施电子机制包括时间锁定的交易。

33.根据权利要求23所述的程序存储设备,还包括所述处理器可执行的如下程序指令,

其中如果满足所述第一赎回条件，则自动执行用于赎回的所述第一密码实施电子机制，并且将所述第一数字资产权利的控制传输给所述第一用户。

34.根据权利要求23所述的程序存储设备，其中，用于赎回的每个密码实施电子机制包括在赎回交易中使用的用于赎回的预签署授权。

35.根据权利要求23所述的程序存储设备，其中，所述第一数字资产权利与所述分布式账本中记录的唯一标识符相关联。

数字资产中介电子结算平台

[0001] 交叉引用

[0002] 本申请根据35 USC§119要求于2015年4月5日在美国专利商标局(USPTO)提交的美国临时专利申请No.62/178,315的优先权,其全部内容通过引用并入本文。

技术领域

[0003] 本公开涉及用于追踪和结算数字资产、债务和交易的电子结算平台。

背景技术

[0004] 现有的用于结算资产、债务和交易的封闭式中央管理账本被认为是不透明和易出错的。这使得监督繁琐,需要许多重复的过程和账本,并且容易造成欺诈。现有账本架构的第一个也是目前最大的替代方案以被称为比特币的分布式数字账本为代表,它使用“区块链”数据结构。比特币操作的一个基本原则是,该系统被设置为利用公私密钥密码技术的对等交易机制,没有中央中介存储库或中央存储库,并允许网络中的所有参与者持有并实时验证账本的完整副本的完整性。比特币区块链的设计是为了创建一种不可靠的本地资产,即比特币,其可以在全球范围内与假名方进行交换。

[0005] 目前用于支持类比特币或类区块链系统之上的数字资产而搭建的平台没有被结构化以提供对金融机构的全面保护,但这是法律对金融机构的许多现有交易业务所要求的。这些平台通常可能没有考虑金融机构和金融交易的监管制度。因此,机构投资者对进入数字资产市场犹豫不决,并且在他们的现有业务上避免使用分布式账本。

发明内容

[0006] 示例性实施例的数字资产结算方法包括:从第一用户接收涉及所述第一用户对数字资产的权利的有条件交易的授权,所述数字资产已记录在分布式账本上;将来自所述第一用户的交易授权与来自至少一个其他用户的涉及所述至少一个其他用户对至少一个数字资产的至少一个权利的交易授权进行匹配,所述至少一个数字资产已经记录在分布式账本上;如果满足条件,则结算所述第一用户和所述至少一个其他用户之间的所述交易;以及在分布式账本上记录已结算的交易。可选地,数字资产中的至少一个表示常规资产的数字化所有权。

[0007] 该方法还可以包括从第一用户接收用于赎回的电子机制。可选地,如果所述交易因不满足条件而未被结算,则调用用于赎回的电子机制。可选地,用于赎回的电子机制允许储蓄用户在未来的预设时间单方面撤回适用的资产、权利、资金或合同。可选地,用于赎回的电子机制包括在赎回交易中使用的用于赎回的预签署授权。可选地,自动调用用于赎回的电子机制。

[0008] 一个示例性实施例的数字资产电子结算平台包括节点,其中多个节点上存储有分布式账本的副本;与所述节点之一耦接进行信号通信的接口服务器;与接口服务器耦接进行信号通信的客户机;与所述客户机耦接进行信号通信的数据服务器;持久性单元,与所述

数据服务器耦接进行信号通信;与数据服务器耦接进行信号通信的高速缓存单元;以及协调单元,与所述数据服务器耦接进行信号通信。

[0009] 可选地,持久性单元、高速缓存单元或协调单元中的至少一个在数据服务器中实施。可选地,持久性单元、高速缓存单元或协调单元中的至少一个在另一数据服务器中实施。可选地,数据服务器提供数字资产和常规资产之间的联系。可选地,分布式区块链包括:来自包括至少一个数字资产和至少一个常规资产的交易的至少一个未使用的交易输出。可选地,数字资产包括数字合同。可选地,客户机被配置为基于来自数据服务器的信息来执行赎回交易,并且通过接口服务器将赎回交易记录在区块链中。可选地,数据服务器与接口服务器直接耦接进行信号通信。

[0010] 数字资产电子结算平台可以进一步包括时间戳服务器,该时间戳服务器被配置为对要加时间戳的项目区块进行哈希运算并且发布加时间戳的哈希。

[0011] 示例性实施例的程序存储设备有形地包括处理器可执行的指令程序,以从第一用户接收涉及已在分布式账本上数字化的数字资产权利的有条件交易的授权,将来自第一用户的交易授权与来自至少一个其他用户的交易授权进行匹配,如果满足条件,则结算至少第一用户和其他用户之间的交易,并且在分布式账本上记录已结算的交易。可选地,数字资产中的至少一个表示常规资产的数字化所有权。

[0012] 程序存储设备还可以包括从第一用户接收用于赎回的电子机制的程序指令。可选地,如果交易因不满足条件而未被结算,则调用用于赎回的电子机制。

附图说明

[0013] 从下面的详细描述中,特别是当结合附图时,可以更清楚地理解说明性的、非限制性的示例性实施例,其中:

[0014] 图1是所有权链的流程图,其中,通过数字批准(ratify)包括前一交易的哈希和接收者权利的记录,每个数字资产支付者将数字资产依次转移给每个后续的接收者;

[0015] 图2是数字资产时间戳服务器的混合图,该服务器获取要加时间戳的项目区块的哈希并广泛发布该哈希;

[0016] 图3是根据本发明构思的示例性实施例的用于与数字资产中介电子结算平台的结算服务进行分层交互的树形图;

[0017] 图4是根据本发明构思的示例性实施例的数字资产中介电子结算用户应用的示意图;

[0018] 图5是根据本发明构思的示例性实施例的数字资产中介电子结算平台的用户界面的图示;

[0019] 图6是图5的图形子部分;

[0020] 图7是图5的图形子部分;

[0021] 图8是图5的图形子部分;

[0022] 图9是图5的图形子部分;

[0023] 图10是图5的图形子部分;

[0024] 图11是示出根据本发明构思的示例性实施例的资金往来过程期间的交易相关性的相关性图;

[0025] 图12是示出根据本发明构思的示例性实施例的数字资产资金往来过程的序列图；

[0026] 图13是示出根据本发明构思的示例性实施例的赎回刷新过程的序列图；

[0027] 图14是示出根据本发明构思的示例性实施例的结算状态的状态图；

[0028] 图15是示出根据本发明构思的示例性实施例的用于成功结算处理的未使用的交易输出(utxos)的分阶段的序列图；

[0029] 图16是示出根据本发明构思的示例性实施例的成功匹配的对手数字资产/常规货币交易过程的序列图；

[0030] 图17是示出根据本发明构思的示例性实施例的过期结算过程的序列图；

[0031] 图18是示出根据本发明构思的示例性实施例的从数字资产中介电子结算多方批准应用撤回到数字资产中介电子结算用户应用过程的序列图；

[0032] 图19是示出了根据本发明构思的示例性实施例的数字资产中介电子结算用户的单方面赎回过程的序列图；以及

[0033] 图20是根据本发明构思的示例性实施例的可以用于实现数字资产中介电子结算平台的硬件架构的示意图。

具体实施方式

[0034] 将参考示出了示例性实施例的附图更充分地描述本发明构思。然而，本发明构思可以以许多不同的形式来实施，并且不应该被解释为限于本文阐述的实施例。贯穿本公开内容，相似的附图标记可以指代相似的元件。

[0035] 本发明构思提供了一种数字资产结算平台。示例性实施例的数字资产电子结算平台包括节点，一些节点上存储有分布式区块链和/或参考数据的副本；耦合到节点的接口服务器；耦合到接口服务器的客户机；耦合到客户机的数据服务器；耦合到数据服务器的持久性单元；耦合到数据服务器的高速缓存单元；以及耦合到数据服务器的协调单元。

[0036] 不受限制地，本发明构思的示例性实施例描述了利用“钱包”，该“钱包”是可以控制和包括私钥及其对应公钥的存储库的密钥存储库应用。这些密钥使得分布式账本上的交易、权利或合同能够批准(这里的签名)。控制私钥代表对由对应的公钥持有的资产、权利或合同的控制。

[0037] 根据本发明构思的示例性实施例的数字资产电子结算平台包括节点，其中一些节点维持所存储的分布式区块链的完整副本；耦合到节点的接口服务器；耦合到接口服务器的客户机；耦合到客户机的数据服务器；耦合到数据服务器的持久性单元；耦合到数据服务器的高速缓存单元；以及耦合到数据服务器的协调单元。例如，某些节点(例如签名服务器)可以可选地仅存储分布式区块链的部分副本。

[0038] 如图1所示，通用数字资产的所有权链一般由附图标记100表示。在第一交易110中，所有者0通过基于其私钥将其所有者0的数字签名116应用于将前一交易的输出与下一所有者1的公钥112进行组合的组合(例如而非限制，级联)的密码哈希114，将数字资产的所有权转移给下一个所有者1。在第二交易120中，所有者1通过基于其所有者1的私钥118将其所有者1的数字签名126应用于将前一交易110的输出与下一所有者2的公钥122进行组合的组合的密码哈希124，将同一数字资产的所有权转移给下一所有者2。在第三交易130中，所有者2通过基于其所有者2的私钥128将其所有者2的数字签名136应用于将前一交易120的

输出与下一所有者3的公钥132进行组合的组合的密码哈希134，将相同数字资产的所有权转移给下一所有者3。

[0039] 应该理解的是，公钥或签名的使用仅仅是为了便于在此描述的非限制性示例性实施例，其中该私有形式可以用于表示拥有数字资产的所有权或处置权的对应实体，该权利可以通过用相应的公钥进行签名来行使。本发明构思不限于此，并且可以可替代地以更广义的或更灵活的方式使用更一般的符号来定义权利，例如，指定权利的固定的持续时间，例如接下来的24小时，实体A拥有签署数字资产的所有权或处置权，并且此后实体B和C必须都签署。

[0040] 密码哈希是任意大量数据的固定长度“指纹”。相同的密码哈希将始终来自相同的数据，但是即使修改一个比特的数据也会显著改变密码哈希。交易输出和下一所有者的公钥的组合(例如，级联)的密码哈希被附加到所有权链的末尾。接收者可以验证该密码哈希和数字签名以验证所有权链。

[0041] 为了在没有可信第三方的情况下实现这一目标，交易是公开广播的，并且系统被参与者用于就订单的单个历史达成一致。接收者希望证明，在每次交易时，多个数字资产节点的所有功能正常的节点都同意它被接收并验证为有效。

[0042] 转到图2，提供这种证明的一个示例性解决方案是利用时间戳服务器。时间戳服务器实施过程200，该过程200获取将前一哈希与要加时间戳的包括一个或多个项目(在此包括作为图1的交易110的项目110)的区块210进行组合的所述组合(例如而非限制，级联)的密码哈希215，并广泛发布该密码哈希。这样的时间戳示出了区块210内的数据(包括交易项目110的记录)在区块210形成时已存在，以便进入密码哈希215。一旦所有者1授权图1的交易120，则该交易项目120可以被包括在随后的区块220中，该后续的区块220与前一哈希215的输出组合地进行密码哈希。因此，每个时间戳在其哈希中都包含前一时间戳以形成区块链，每个时间戳都加强了前一时间戳。

[0043] 数字资产电子结算平台可以包括时间戳服务器，该时间戳服务器被配置为对要加时间戳的每个项目区块进行哈希，并且通过将加时间戳的哈希以时间顺序附加到分布式账本来发布所述加时间戳的哈希，使得加时间戳的区块的顺序在不同功能正常的节点上维护的分布式账本的所有副本中是相同的。在优选实施例中，所述项目是交易。区块时间戳可以单独使用或与项目或交易时间戳一起使用。在替代实施例中，交易时间戳可以用来代替区块时间戳。当单独使用交易时间戳或与区块时间戳结合使用时，区块内交易的排序可以但不必是按时间顺序的。

[0044] 在本公开的示例性实施例中，这样的区块链由运行通用网络协议的通信节点的网络来维护。形式付款人A将数字资产Y转移给接收者B的交易被广播到网络。网络节点可以验证这些交易，将交易添加到该节点的账本副本，然后将这些账本新增内容广播到其他节点。

[0045] 为了独立验证所有权链和特定数字资产，网络节点存储区块链的副本。尽管可以在不同的分布式区块链网络中使用各种方法，包括工作证明、权证证明、实用拜占庭容错(PBFT)等，但工作证明方法(比如比特币)通常允许每个时间间隔产生一次新的区块，比如在比特币网络中大约每十分钟一次。每个新区块都包含一组可接受的交易，并被添加到区块链中，该区块链被立即发布到基本上所有节点。这允许这样的分布式区块链系统确定特定数字资产何时被转移或使用。确定何时使用特定的数字资产或其部分是必要的，以防止

在没有中央授权的环境中的双重使用或双重支出。

[0046] 本发明构思提供了支持对手交易以及数字资产和常规资产之间的联系的数字资产结算平台。具体地，在该平台上为受监管程度较高的金融机构和机构投资者提供了一种机制，通过这个机制，他们可以谨慎地进入数字资产市场，同时遵守所要求的透明度、风险管理和监管上的标准。

[0047] 根据本发明构思的原理，数字资产结算平台(例如具有信任应用层的数字资产中介结算平台)可以被配置为提供数字资产的结算服务，所述数字资产可以被定义为包括(而非限制)可替代资产、对资产所有权的引用、债务、信用和/或授权。这种结算平台可以电子方式作为数字资产中介电子结算平台运行。

[0048] 数字资产中介电子结算平台可以提供诸如密码货币的数字资产和诸如常规货币、证券等的其他既定资产类别之间的联系。这种数字资产中介电子结算平台支持赎回(redemption)交易

[0049] 为了说明的目的，本发明构思被示为应用于被称为比特币的示例性分布式对等交易网络。然而，应该理解的是，本发明构思的原理可以针对任何分布式的对等交易网络来实施。

[0050] 在一定程度上，世界上所有的交易都是以信任为基础的。例如，当顾客走进咖啡店时，商家和顾客互相信任以完成交易各方的职责；商家将提供咖啡，客户将付款。在一个更复杂的例子中，当一个国际企业将欧元收入转换成美元时，中介人介入交易以提供更高级别的安全性。

[0051] 通常，衡量信任的唯一途径是把活动集中到可信的、通常扩展到非常大的第三方。可信第三方具有积极和消极的外部效应。一方面，可信第三方具有很高的控制和可见性标准，但另一方面他们也代表集中的单点故障。在现代的网络犯罪世界中，这种风险已经变得更高。也产生了如下问题：由谁来衡量可信第三方的信任度。这已经落在了专门从事这些关系的政府或更大的可信第三方头上。对于世界上最大的交易来说，存在可信第三方和政府层面的交互来执行和结算交易。这是低效的，并且可能越来越难以保证安全。

[0052] 分布式的对等交易网络被设计为消除可信第三方的必要性。分布式网络协议被设计为允许交易对手直接执行交易；然而，在没有中介人代表其客户同意执行交易的情况下，分布式的对等交易网络中的交易可能缺乏控制。进而，这样的缺陷可能使用户面临交易对手风险，不可逆的错误交易，以及参与者超出风险限制。

[0053] 没有中介，任何规模的对等交易都可以从网络的任何成员流向任何其他成员。这意味着，例如，一个价值10亿美元的交易与0.000000001美元的交易在分布式网络中具有相同的交易要求和安全性。尽管分布式网络的底层协议对于最大交易来说需是健壮和安全的，但是提供对即使网络中的最小交易也能够进行扩展或加速的系统也是有益的。

[0054] 本发明构思通过在分布式对等交易网络之上引入信任层来创建规模、速度和安全性。本发明构思允许可信第三方以置信度和数字效率来验证、批准和认可交易。

[0055] 分布式账本可被视为完全可访问的归档系统或数据库，其中该上下文中的“完全”意味着网络中的参与者可以获得对数据库的完全访问。访问数据库中的信息可能会受到安全和隐私要求方面的限制，并在数据结构本身中执行。归档系统不受任何单一用户改变存储数据的单方面能力的影响至关重要。为了实现这一点，许多分布式的对等交易网络假设

交易是在一个真正的无中介的环境中进行的。但是，这忽略了系统中可信中介的好处。

[0056] 本发明构思的示例性实施例平台添加了信任层，其中数字资产成员实体必须知道用户并且用户必须根据其成员资格规则进行操作。程序上，平台不能单方面控制用户的资产。该平台可以确保用户按照意图并根据向其提供服务的数字资产成员所规定的规则来执行任何“交易”或账本输入。例如，通过这样做，平台为金融机构提供了验证数字资产交易(包括至少包含一个数字资产的对手交易)的工具，从而允许他们快速、高效且安全地进行结算。

[0057] 通过使用分布式账本，无论是公开的、半公开的、还是私人的，本发明构思的实施例提供附加的好处，即具有一种交易系统，其实时显示“交易”，并提供向任何监管机构或适当的管理机构显示交易的可能性。

[0058] 根据本发明构思的原理，数字资产中介电子结算平台支持数字资产的中介服务。数字资产中介电子结算平台提供数字资产和其他既定资产类别之间的综合方法。例如，数字资产电子结算平台提供了数字资产与受监管程度较高的(迄今为止避免进入数字资产市场的)金融机构和机构投资者之间缺失的联系。

[0059] 术语“数字资产”在此用于包括既定资产类别、债务、合同或明确授权的数字实施例。例如，用于股票的具有法律约束力的文件是纸质证书，并且根据本发明构思，可以创建包含数字形式的该股票证书的数字令牌。另外，本发明构思的数字资产中介电子结算平台的示例性实施例可以用作常规资产结算平台和账本的替代品。这种常规的资产结算平台和账本的示例包括但不限于电子资产，例如电子证券、电子合同等。

[0060] 任何常规的证券都可以在分布式账本上数字化，并且有资格作为电子证券被纳入数字资产中介电子结算平台。由此，这种加密的数字化证券可以被实时增扩、验证并从一个或多个合格且已知的用户电子转移到其他用户。这种常规证券的示例包括但不限于私人和公共股票、私人和公共债券、商业票据、衍生证券(远期契约、期货、期权或互换信贷)、债务、授权、合同或任何其他金融资产。

[0061] 任何合同都可以在分布式账本上数字化，并有资格作为电子合同被纳入数字资产中介电子结算平台。由此，这种加密的数字化合同可以被实时验证，并从一个或多个合格且已知的用户电子转移到其他用户。这些合同的示例包括但不限于衍生合同(远期契约、期货、期权或互换信贷)、买卖协议、贷款、回购(销售和回购)协议、反向回购(购买和转售)协议、遗嘱、保险单、担保债券、服务协议、合同债务或任何其他合同安排。

[0062] 可以被数字化且有资格被纳入数字资产中介电子结算平台中、并且因此可以被实时验证并从一个或者多个合格且已知的用户电子转移到其他用户的附加数字资产的示例包括但不限于：外汇(数字或常规)、矿权、航权、排污权、采矿权、产权(汽车、房屋等)、抵押、奖励积分或航空里程等。

[0063] 在示例性实施例中，任何数字资产(例如但不限于比特币的数量)可以与分布式账本上的唯一标识符或权利相关联，在一些账本实施方式(例如，使用未使用的交易输出或“utxo”的实施方式)中，分布式账本可以被称为令牌。本发明构思不限于示例性的utxo实施方式或令牌，并且与例如以太坊(Ethereum，不限于此)等替代分布式账本实施方式兼容。作为所有权证明的唯一权利或令牌与数字资产数据的哈希的组合可以通过本发明构思来传递，并被记录在公开、半公开或专有分布式账本网络上。本发明构思的数字资产中介电子结

算平台将帮助处理常规货币或以这种货币计值的相应的既定资产类别的数字资产交换。通过本发明构思的数字资产中介电子结算平台，成员或监管机构或两者可以有能力对发生在数字资产市场中的交易进行实时监视和反应。

[0064] 本发明构思的示例性实施例的数字资产中介电子结算平台帮助弥补了新创建的存在于相对无监管市场、受到相对有限监督的数字资产(例如比特币)与既定受监管的金融机构之间的空白。数字资产中介电子结算平台扩展到包括在分布式账本上数字化的新的和既定的资产类别。本发明构思的电子结算系统允许成员执行其用户的行为，同时允许用户成为他们的数字资产的管理者。结算系统允许交易的记录、追踪和结算，只要交易符合预设的限制。如果结算系统由于不符合预设的限制而未能结算交易，则可以使用已经预先签署的授权，以允许用户在未来的预设和已知的时间单方面从结算系统中撤回适用的权利。这个构思被称为“赎回交易”。数字资产中介电子结算系统不能单方面行使权利，也不能阻止用户退出系统。这是通过对权利控制的预先惩罚的几种可选机制之一来实现的，目前最简单的设想是，用户和结算系统预先签署交易，该交易在未来的预设时间内有效，并返还权利给在相应用户的独有控制下的应用或钱包。

[0065] 本发明构思的数字资产中介电子结算平台有助于向金融机构及其客户提供数字资产市场中的某些益处。具体而言，本发明构思的数字资产中介电子结算平台有助于防止欺诈交易，避免交易对手风险，验证权利和资金，并允许账户监督；这无需成员持有或处理数字资产，也无需将这些资产的所有权转让给结算系统。

[0066] 本发明构思的示例性实施例的数字资产中介电子结算平台包括用于加入仔细选择的参与者子集的过程。建立一个可信的成员(例如金融机构)网络。当利用本发明构思的数字资产中介电子结算平台时，避免了单点故障的风险，而不会使参与者必须面对处理完全未知或匿名对手方。结算可以被限制为只有已知的用户可用。由于在数字资产的管理处于用户控制下的情况下来完成结算，所以避免了交易所的管理要求，从而允许用户自己利用交易所的价格发现功能，而不会使自己面临未经授权的这些资产的所有权的损失。受监管的成员将是常规权利和资金的管理者，用户将是他们自己的数字资产的保管者。这将系统分配给许多管理者，并提供附加的安全层。

[0067] 本发明构思的数字资产中介电子结算平台的示例性实施例提供了数字资产的中介平台。利用数字资产中介电子结算平台允许多个当前的应用使用该平台，并提供适应未来尚未指定和未知的未来数字资产的基础。该系统允许针数字资产对常规资产或数字资产对其他数字资产的原子结算。在这种上下文中，“原子”意味着固有的联系，即转移的一个分支不能在没有另一分支的情况下发生。任何流经系统的交易都可以针对合规性、报告、评估、风险管理或其他目的进行审计。数字资产、交易、债务和协议可以被追踪。可以将风险部门的监视和控制工具应用于数字资产。可以施加后台监视工具和业务逻辑。电子结算系统在参与者和分布式账本之间添加了业务逻辑层。在该上下文中，“业务逻辑”是指为满足有关资产和/或交易的预期业务标准而必须满足的条件。一个示例就是强加一个预先商定的限制框架。业务逻辑的数字化提供了显著的规模经济的潜力。

[0068] 典型的多重签名或多方批准方案并非固有地对方案中的任何个体授权人施加限制，而本发明构思的数字资产中介电子结算平台的示例性实施例允许在例如由私钥签名实现的特定个体限制下共享应用或钱包中的资产。这种密钥存储库应用或“钱包”架构允许多

个用户共享超过任何单个参与者的限制的资源，这是对希望管理其授权雇员的活动(单个的和整体的)的机构的必要要求。例如，本发明构思的数字资产中介电子结算平台可以针对两个资产(其中至少一个资产是数字资产)之间的任何对手交易的结算施加相同的业务逻辑，并且可以扩展为包括单词交易中的许多资产和各方。

[0069] 本发明构思的数字资产中介电子结算平台的示例性实施例是彼此知晓假名的多重签名密钥存储库应用(“钱包”)的网络。用户钱包包含网络已知的公钥，而私钥只在用户的控制之下。本发明构思设想，用户将使用多个替代框架中的任何一个来保护这样的私钥。数字资产中介电子结算平台多重签名钱包包含与用户的一个或多个唯一私钥，以及与数字资产中介电子结算平台服务器的一个或多个唯一私钥。用户将数字资产转移到多重签名钱包的控制下，其中数字资产中介电子结算平台服务器控制至少一个私钥，以参与结算系统。系统中的交易发生在封闭网络内的多重签名钱包到多重签名钱包，并要求数字资产中介电子结算平台服务器以认可签名的形式批准。数字资产中介电子结算平台服务器不能单方面转移对数字资产的控制，因为数字资产存放在用户有足够控制的多重签名钱包中，以防止未经授权的转移。此外，数字资产中介电子结算平台服务器不得违背用户的意愿扣留数字资产，也不能用于扣留数字资产。数字资产中介电子结算平台服务器预先授权“赎回”交易，例如，在经过指定的时间段之后，授权将数字资产从多重签名钱包赎回返回到用户钱包。在指定的时间段过去之后，用户因此可以单方面地控制自己的资产，而无须数字资产中介电子结算平台所要求的进一步行动。

[0070] 通过利用根据本发明构思的原理的数字资产中介电子结算平台，可信第三方可以继续监视和行使数字资产的行为控制，而不必成为法定管理者。这使用户能够真正控制自己的资产，而可信第三方继续执行法律行为并提供结算效率。根据本发明构思的原理的数字资产中介电子结算平台在更大的网络内提供已知实体的闭环。为了参与，用户必须使用数字资产中介电子结算平台和钱包，按照程序进入和退出循环，并坚持系统的行为规则。

[0071] 参考图3，提供了与本发明构思的数字资产中介电子结算平台310交互的示例性各方的一般示意性概述。可以看到一组成员312。成员312能够执行金融行业标准尽职调查，例如遵守反贿赂和腐败法规的反洗钱(AML)，包括“银行保密法”(BSA)、“反海外腐败法”(FCPA)以及“了解您的客户”(KYC)和“客户信息计划”(CIP)等关键AML任务。

[0072] 成员312能够开设和管理账户，分析和设置限制，并提供战略咨询。数字资产中介电子结算平台的成员312管理与常规货币转移有关的实施，而数字资产中介电子结算平台则作为贸易结算期间数字资产转移的促进者。数字资产中介电子结算平台310的成员避免了交易对手风险，将价格发现从权利和资金的保管中分离出来。

[0073] 成员312可以利用数字资产中介电子结算平台310来加入成员的客户端，并且让这些成员的客户端在控制风险的同时在他们之间进行数字资产交易，而不需要任何直接保管数字资产。虽然没有正式要求，但成员312可以是金融机构。

[0074] 在成员之下是成员的客户314。成员的客户314希望结算交易和管理风险。同样，虽然没有正式要求，但通常成员客户314将是成员312的客户，例如通常使用其成员提供的各种服务的跨国公司。

[0075] 部署了多个交易台单元316。交易台单元316可以被设置为结算数字资产。交易台单元316的示例可以包括资金管理、公司风险管理、部门风险管理、货币间风险管理、专有交

易团体等。每个交易台单元316可以但不一定需要包括多个授权交易商318。

[0076] 用户由若干硬件和软件组件支持，这些组件可以包括例如前端、用户密钥存储库应用或“钱包”以及数字资产中介电子结算平台服务器。前端用户界面级可包括面向用户的屏幕，该屏幕包括系统概览、仪表板、风险控制台和日志控制台。仪表板屏幕将每个阶段发生的事情可视化。此外，交互式屏幕让参与者加入交易并查看实时结果和/或通知(例如，与交易无效有关)。

[0077] 参考图4，在本发明构思的一个示例性实施例中，提供了数字资产中介电子结算钱包410。数字资产中介电子结算钱包410包括多重签名用户钱包414和多重签名结算钱包416。在多重签名用户钱包414中，只有用户控制了私钥。私钥与多重签名用户钱包414在本地存储。多重签名结算钱包416以本领域已知的方式与其他数字钱包412交互。

[0078] 在本发明构思的一个示例性实施例中，根据用户的指示，本发明构思验证并启用多重签名用户钱包414与多重签名结算钱包416之间的资产交易。多重签名用户钱包416包括用户私钥和数字资产中介电子结算平台私钥。私钥(除了一个)与多重签名用户钱包416在本地存储。中介私钥是进行结算的最后一个也是强制性的签名。数字资产中介电子结算平台私钥驻留在数字资产中介电子结算平台服务器上，并且受到用户成员限制的严格制约，并匹配对手交易。

[0079] 通过利用根据本发明构思的原理的数字资产中介电子结算平台，成员可以参与现场情景，包括：平台对有效交易进行结算的成功结算；被称为“不良”交易的错误或无效的交易；以及成员客户加入，其中成员将新成员客户加入到数字资产中介电子结算平台而成为平台用户。交易可以通过各种方式发起，例如场外交易市场(例如通过电话)或交易所或两者。当某场景正在进行时，成员可以查看成员的仪表板、成员客户、成员风险管理功能、以及用于操作功能的数字资产中介电子结算平台日志屏幕。在成功的场外交易中，两位参与者坐在不同的计算机前，并使用交易进入工具向数字资产中介电子结算平台服务器独立地报告交易细节。在成功的交易所执行的交易中，交易所通知数字资产中介电子结算系统已经验证和执行的交易所发起的交易。

[0080] 以下总结了示例性结算请求过程。最初，交易者Ta打开交易进入工具。交易者Ta初始化交易进入工具，仪表板将交易者Ta识别为活跃的。该应用将针对交易者Ta的当前信用限额(如在风险控制台中设置的)通知给交易者Ta的交易进入工具。同时，交易者Tb也打开交易进入工具。交易者Tb初始化交易进入工具，仪表板将交易者Tb识别为活跃的。应用将交易者Tb的当前信用限额(如风险控制台中设置的)通知给交易者Tb。

[0081] 交易者Ta填写指定资产、数量、价格和交易对手的票据；并通过密码签名进行授权。分配新的交易号，从交易者Ta和/或交易者Ta成员中划拨结算资金，仪表板显示交易者Ta票据，指示该票据尚未填写。启动倒计时计时器，对交易时间进行倒计时(例如15分钟)。仪表板还显示交易者的信用限额。同时，交易者Tb还填写指定资产、数量、价格和交易对手的票据；并进行授权/使用/消费。交易者Tb提交针对交易对手方的票据。交易者Tb票据变得有效，出现积极的视觉效果，例如，票据变灰，交易者Ta和交易者Tb票据合并，票据被推送到可接受的交易箱。

[0082] 以下总结了示例性的成功交易结算过程。信用限额报价器闪烁并被更新。短时间(例如0.5秒)过去了。同时，签名视觉闪烁并变为有效，表示2/2或3/3或4/4(或需要结算系

统签名的任何数量的签名)使用/消费签名,以及常规货币(例如,美元)饼图闪烁和更新,表明系统正在指示交易者Tb的成员向交易者Ta的成员发送常规货币。市场数据馈送被更新,以包括成功结算的价格和数量细节。成功的结算细节也通过应用编程接口(API)同时发送给交易者Ta和交易者Tb的成员,允许这些成员提交适当的监管文件。

[0083] 例如,人为错误、达到限额、企图欺骗系统、潜在的漏洞等等可能导致不良交易情况。在交易者交易进入工具、风险仪表板和成员风险仪表板上报告错误。以下总结了由于"信用不良"情况而发生的示例性不良交易。交易者Ta试图向交易者Tb提交比如1000比特币的交易,交易者Tb只获得了500比特币交易的授权。如果交易是在场外发起的,则交易者Ta的交易进入工具通过例如变红并且使"提交"按钮变灰而指示不良交易。交易进入工具标题栏用消息表示这一问题,例如显示"交易者Tb没有足够的信用来完成此交易"。如果交易尝试在交易所进行,交易者Tb的限额是交易所已知的且由交易所执行。

[0084] 以下总结了由于"超出授权的夹子大小(clip size)"情况而导致的示例性不良交易。交易者Ta试图向交易者Tb提交例如1000比特币交易,但是不允许交易者Ta一次交易超过例如100比特币。交易者Ta的交易进入工具例如通过变红和使"提交"按钮变灰来指示不良交易。交易进入工具标题栏用消息表示这一情况,例如显示"交易者Ta已经超过了夹子限额大小"。如果交易尝试在交易所进行,则交易者Tb被阻止执行一次超过100比特币的订单。

[0085] 以下总结了由于"未经授权的交易者"情况而导致的示例性不良交易。未经授权的用户试图在交易者Ta的交易进入工具处提交交易。要激活"提交"按钮,需要用户提供交易者特定的密码。输入的密码不正确。交易进入工具例如通过变红并且使"提交"按钮变灰来指示不良交易。如果该过程重复给定的次数,例如三次,则交易进入工具不再有效,并且用户的钱包将被认为被破坏。数字资产中介电子结算平台服务器启动与成员客户和系统外成员的联系,作为建立从数字资产中介电子结算平台安全撤回或其他情形的纠正的手段。

[0086] 以下总结了由于"不正确的交易细节"或"错误的限额"情况而导致的示例性场外不良交易。交易者Ta提交与交易者Tb的例如1000比特币的交易;交易者Tb提交与交易者Ta的例如100比特币的交易。匹配引擎等待给定间隔(例如15分钟)以使两个票据都找到匹配。交易者交易进入工具显示尚未确认的待处理的交易队列。如果队列中的交易接近该间隔的结束,则排队的项目将进入"临界队列",该队列显示即将过期的未匹配的交易。系统显示未匹配的交易日志,包括匹配或过期的交易。交易所向系统报告的用于结算的交易已经由交易所进行匹配。存在很多潜在的、系统可以被设计成用来识别的不良交易场景的示例。

[0087] 图5-10给出了使用户能够与本发明构思的数字资产中介电子结算平台交互的示例性图形用户界面;这些示例仅是本发明构思所设想的若干替代方案中的一个,并且旨在是非限制性的。

[0088] 参考图5,示出了本发明构思的数字资产中介电子结算平台的示例性图形用户界面屏幕截图。在一个实施例中,屏幕被分成余额历史部分512、统计数据部分514、交易部分516和细节部分518。图6示出了余额历史部分512的更详细的描述;图7示出了统计数据部分514的更详细的描述;图8示出了交易部分516的更详细的描述;以及图9和图10示出了细节部分518的更详细的描述。

[0089] 参考图6,余额历史部分512包括成员的排在前面的常规货币余额线图612和成员的排在前面的数字资产余额连线图614。提供了成员标签616、机构标签618、交易台标签620

和交易账户标签622。成员标签包括成员姓名624、常规货币余额626、常规货币信用628、买入交易630和卖出交易632。同样，机构标签618包括成员的客户名称、常规货币余额、常规货币信用、买入交易和卖出交易。交易台标签620包括交易台名称、常规货币余额、常规货币信用、买入交易和卖出交易。交易账户标签622包括交易账户名称、常规货币余额、常规货币信用、买入交易和卖出交易。

[0090] 参考图7，统计数据部分514包括成员的排在前面的常规货币余额饼图712和成员的排在前面的数字资产余额饼图714。排在前面的常规货币信用图716列出排在前面的成员的常规货币信用。排在前面的数字资产余额图718列出排在前面的成员的数字资产余额。排在前面的账户余额值图721列出排在前面的成员的账户余额值。排在前面的买入量图723列出排在前面的成员买入量。排在前面的售出量图725列出排在前面的成员的售出量。排在前面的名义量图727列出排在前面的成员的名义量。排在前面的交易量图729列出排在前面的成员的交易量。

[0091] 参考图8，细节部分518还包括待处理的交易图812，其详细描述交易ID、价格、数字资产量、常规货币量、数字资产卖家、数字资产买家、创建时间以及待处理交易的交易状态。已结算的交易图814详述了交易ID、价格、数字资产量、常规货币量、数字资产卖家、数字资产买家、创建时间以及已结算交易的交易状态。未结算的交易图816详述了交易ID、价格、数字资产量、常规货币量、数字资产卖家、数字资产买家、创建时间以及未结算交易的交易状态。

[0092] 参考图9，交易部分516还包括数字资产图912，其列出了数字资产交易的哈希、数量、费用、输入和输出。参考图10，交易部分1012标识了交易ID、状态、创建时间、价格、数字资产量、常规货币量、买家和卖家。提供了添加数字资产签名按钮1014。添加交易部分标识了交易账户余额(数字和既定资产)。作为输入字段，交易部分1012包括交易类型(买入或卖出数字资产)、数字资产量下拉菜单、常规货币面值的数字资产价格和交易对手。提供了卖出数字资产按钮1016。

[0093] 数字资产中介电子结算平台服务器接收来自认证用户的交易，进行交易验证，配对和结算，同时为运营商和成员提供每个结算的状态以及每个账户的信用和余额。图11-19给出了实现本发明构思的数字资产中介电子结算平台的数字资产中介电子结算平台过程和状态的详细示例。在图11-19所示的示例中，示例性数字资产是比特币。数字资产中介电子结算平台过程包括交易相关性图、数字资产资金往来过程、赎回刷新过程、结算状态、成功结算的准备过程，成功匹配的常规货币交易的对手数字资产过程、过期结算过程、从多重签名钱包撤回到用户钱包，以及用户签名赎回过程的示例。

[0094] 以下描述数字资产被转移到多重签名钱包的控制的过程的示例性实施例。为了结算的目的，转移给多重签名钱包的数字资产权利只有符合正确的过程才能被认定为有效。如果通过任何其他方式将任何数字资产权利转移给多重签名钱包中的公钥，则数字资产中介电子结算平台服务器自动授权交易将数字资产从多重签名控制发回给用户控制。数字资产中介电子结算平台服务器也拒绝将错误转移的数字资产权利识别为多重签名钱包中可用余额的一部分。

[0095] 参考图11，示出了显示在转移过程期间的交易相关性示例的相关性图。最初，出于示范的目的，卖家具有如下权利，该权利由控制钱包中的多个数字资产(假设例如100)的未

使用的交易输出(或utxo)来表示,其中只有卖家控制私钥(用户钱包)(1101)。用户钱包(1102)生成输入为utxo0并且输出为utxo1的用于将数字资产权利(例如,100)从用户钱包转移到多重签名钱包的交易(tx1)(1102)。

[0096] 参考图12,示出了示例性比特币资金往来过程的序列图。再一次,卖家具有仅由卖家控制私钥(用户钱包)的应用所控制的数字资产的utxo(1201),并且用户应用生成输入为utxo0输出为utxo1的、用于将数字资产从用户控制移动到多重签名控制的交易(tx1)(1202)。

[0097] 用户应用对tx1(将数字资产从用户控制移动到多重签名控制的交易)的细节进行哈希运算变换为交易id(txid(tx1))(1203)。用户应用通过发送txid(tx1)通知数字资产中介电子结算平台服务器即将转移到多重签名控制(1204)。数字资产中介电子结算平台服务器使用txid(tx1)生成并签署未来(例如+24小时)有效的赎回交易(tx1.R),并且数字资产中介电子结算平台服务器将tx1.R发送给用户钱包(1205)。用户钱包确认tx1.R将在未来的时间范围(例如,24小时)中成为有效的交易(1206)。

[0098] 时间锁交易是在未来的预定时间之前在网络中不成为有效的交易。这种交易的细节可以被预先签署并由用户本地存储,以便将来向网络广播,当广播时这些细节将被添加到区块中。用户钱包广播将赎回交易直接广播到区块链,以避免给数字资产中介电子结算平台服务器拦截该消息的机会,从而进一步确立电子结算系统没有任何用户数字资产的所有权。

[0099] 在显示图11的示例性过程的相关性图中,卖家用户应用持有预先许可的赎回交易或"赎回"(1103)。返回参考图12,用户应用将tx1发送给数字资产中介电子结算平台服务器(1207)。数字资产中介电子结算平台服务器检查tx1是有效的交易,然后将其广播到区块链(1208)。在区块链中经过适当数量的确认后,卖家多重签名应用包含utxo1形式的数字资产的活跃余额,以用于该时间范围(例如24小时)的余额,其可用于结算对手交易(1209)。如果在该时间范围内(例如24小时)没有进行结算,则必须使用或刷新赎回。

[0100] 参考图13,示出了示出示例性赎回刷新过程的序列图。赎回交易tx1.R成为有效交易(1301)。卖家指示数字资产中介电子结算平台服务器刷新资金(1302)。数字资产中介电子结算平台服务器创建tx2(其中输入是utxo1并且输出是utxo2),授权tx2,并且向卖家多重签名应用发送tx2(1303)。卖家多重签名应用授权tx2(1304)。卖家多重签名应用生成tx2的哈希,并创建和发送txid(tx2)给数字资产中介电子结算平台服务器(1305)。

[0101] 数字资产中介电子结算平台服务器使用txid(tx2)来生成并签署在未来时间段(例如+24小时)内有效的赎回交易(tx2.R),并且数字资产中介电子结算平台服务器将tx2.R发送给卖家多重签名应用(1306)。卖家多重签名应用确认tx2.R将在该时间段(例如24小时)内成为有效的交易(1307)。卖家多重签名应用将tx2发送给数字资产中介电子结算平台服务器(1308)。数字资产中介电子结算平台服务器检查tx2是有效的交易并将其广播到区块链(1309)。在区块链中经过适当次数的确认之后,卖家多重签名应用控制utxo2形式的数字资产权利的活跃余额,用于所述时间段(例如24小时)的余额,其可用于结算对手交易(1310)。

[0102] 对于任何低于卖家多重签名控制的总余额的交易,必须引入余额的粒度,并且必须发出新的赎回。任何使用utxo作为输入的交易都会使使用该utxo作为输入的任何其他未

来的账本条目无效。因此，必须产生新的赎回以确保用户可以撤回权利。

[0103] 参考图14，示出了示例性结算状态的状态图。权利在卖家多重签名钱包中被分成两个utxo单元：一个utxo单元将用于结算潜在的交易；另一个utxo单元代表应用控制下的剩余余额。输入新的结算状态(1401)。电子结算平台信用管理者从卖家余额中进行划拨，并为即将到来的交易预留权利(1402)。如果资金划拨被拒绝(1403)，则进入被拒状态(1405)；如果权利被划拨，则卖家结算状态变成指示性的(1404)。

[0104] 参考图15，示出了用于成功结算过程的未使用的交易输出(“utxos”)的示例性分阶段。应当理解的是，本发明构思不限于示例性的utxo实施方式，并且与例如以太坊等替代分布式账本实施方式兼容，不限于此。这里，卖家通过使用指示性交易的交易进入工具来通知数字资产中介电子结算平台服务器(1501)。如图10所示，显示了买入/卖出切换、数字资产数量(在图10的例子中，BTC数量)、价格和交易对手。卖家向数字资产中介电子结算平台服务器报告数量、价格和交易对手。在图14所示的示例性权利状态中，卖家多重签名钱包被分阶段进行结算(1104)。

[0105] 在图15中，数字资产中介电子结算平台服务器创建并授权tx2，其中输入是utxo1，输出是utxo2.1和utxo2.2(1502)。utxo2.1和utxo2.2目的地都是在卖家多重签名应用中卖家所拥有的地址。卖家多重签名应用授权tx2(1503)。卖家多重签名应用生成tx2的哈希，从而创建txid(tx2)并将其发送给数字资产中介电子结算平台服务器(1504)。数字资产中介电子结算平台服务器使用txid(tx2)生成并签署两个赎回交易(统称为tx2.R)，这些赎回交易将在未来的时间范围内(例如+24小时)成为有效的，并且数字资产中介电子结算平台服务器将tx2.R发送给卖家多重签名钱包(1505)。卖家多重签名应用确认tx2.R将是在所述时间范围内(例如，24小时)的有效交易(1506)。卖家多重签名应用将tx2发送给数字资产中介电子结算平台服务器(1507)。数字资产中介电子结算平台服务器检查tx2是有效的交易并将其广播到区块链(1508)。

[0106] 卖家多重签名应用现在控制utxo2.1和utx2.2之间的数字资产权利余额(例如100)(1509)。在图11所示的示例权利状态中，示出了多重签名钱包中的utxos的状态(1105)。状态(1107)指的是在权利已被划拨后没有发生结算的情况下卖家对utxo2.1和utxo2.2的有效赎回。数字资产中介电子结算平台服务器创建输入为utxo2.1、输出为utxo3且包括目的地买家的tx3。在图15中，数字资产中介电子结算平台服务器将tx3发送给卖家多重签名应用(1510)。卖家多重签名应用授权tx3并将其发送给数字资产中介电子结算平台服务器(1511)。

[0107] 在图14中看到的示例性结算状态中，如果没有接收到包含卖家授权的消息，则发生被取消/过期(1407)，并且状态变为被取消(1412)。包含tx3的卖家多重签名应用签名的消息承诺卖家进行结算(1406)。此时，结算系统正在等待买方报告该交易的对手侧。结算状态变得实盘(1408)。状态(1409)是买家向数字资产中介电子结算平台交易进入工具报告交易的过程，但是从买家的角度来看可以在状态(1408)中找到。结算系统可以保持在这个结算状态一段时间(例如15分钟)；在该结算状态之后，实盘状态将变得“匹配”(1410)或“过期”(1411)。如果过期(1411)，则状态将变为被取消(1412)。如果匹配，状态就变为匹配(1413)。同样地，结算的买方可以首先发生，然后匹配引擎等待卖家进行如上所述的处理。

[0108] 买家必须有足够的购买力，并按照买家成员的规则行事，才有资格结算交易。足够

的购买力由买家成员来确定，并且可以代表成员发出的信用能力；然而，该成员在其结算系统结算账户中也必须具有足够的常规货币，以便将常规货币从买家成员移动到卖家成员。同样，卖家必须按照卖家的成员规则行事，而且成员客户必须具有足够的数字资产可供结算。

[0109] 参考图16，序列图示出了成功匹配的对手数字资产/常规货币交易过程的示例。买家拥有买家成员的常规货币信用(1601)。买家使用指示性结算的交易进入工具通知数字资产中介电子结算平台服务器。如图7所示，显示了买入/卖出切换、数字资产数量(在图7的例子中，BTC数量)、价格和交易对手。

[0110] 在图14所示的示例性结算状态中，数字资产信用管理者从买家信用中划拨资金并预留用于即将到来的交易(1402)。买家向数字资产中介电子结算平台的交易报告承诺买家进行结算(1406)。买家结算状态变得实盘(1408)。数字资产中介电子结算平台匹配引擎确认卖家实盘报价和买家实盘出价是匹配的对手交易(1410)。卖家实盘状态和买家实盘状态合并成匹配状态(1413)。

[0111] 返回参考图16，数字资产中介电子结算平台服务器授权包括输入utxo 2.1、目的买家多重签名应用、输出uxto3的tx3(1602)。这也在图15(1512)中看得到。数字资产中介电子结算平台服务器创建tx3的哈希，从而创建txid(tx3)并将其发送给买家多重签名应用(1603)。在数字资产中介电子结算平台服务器向区块链广播tx3(1604)的同时，数字资产中介电子结算平台服务器向成员发送将常规货币从买入成员的账户转移到卖出成员的账户的消息。权利和资金的移动受到成员的控制，并且通知成员权利和资金已被要求移动。在图14所示的示例性结算状态中，匹配状态结算成(1414)结算状态(1416)。“被拒”状态(1405)表明，结算已被识别为不良交易，并被数字资产中介电子结算平台拒绝，并且所尝试的结算不超出通过交易进入工具向系统报告的尝试。数字资产中介电子结算平台不能防止数字资产在有交易双方签名的情况下移动，但在手动过程状态(1417)中，如果交易因任何原因发生争议，则成员可以冻结交易双方的常规货币。

[0112] 在图11所示的示例性资金状态中，买家的多重签名权利被分阶段进行结算(1106)。回到图16，买家多重签名应用现在包含utxo3，其中tx3.R包含在时间范围内(例如24小时)的单个数字资产的活跃结算系统结算余额(1605)。卖家多重签名应用现在包含utxo2.2，其中tx2.R包含在时间范围(例如24小时)中的数字资产的活跃结算系统结算余额(例如99)(1606)。

[0113] 实盘结算状态只在指定的时间段内是活跃的(例如15分钟)。为了表明数字资产中介电子结算平台在结算状态过期后丧失了结算交易能力，数字资产中介电子结算平台使用针对该过期结算划拨的权利来创建将数字资产直接发送给卖家多重签名应用的交易。在不同的交易中使用utxo表示的权利会使未来在另一交易中重用该权利的任何尝试都是无效的。在指定的时间段过去之后，结算状态在图14中变为“过期”(1411)。

[0114] 参考图17，示出了示出示例性过期结算过程的序列图。数字资产中介电子结算平台服务器创建包括输入utxo2.1、目的卖家多重签名应用、输出utxo4的tx4，并且数字资产中介电子结算平台服务器授权并发送给卖家多重签名应用(1701)。卖家多重签名应用授权tx4(1702)。卖家多重签名应用创建tx4的哈希，从而创建txid(tx4)并将其发送到数字资产中介电子结算平台服务器(1703)。

[0115] 数字资产中介电子结算平台服务器使用txid(tx4)生成并签署将来(例如+24小时)有效的赎回交易(tx4.R),并且数字资产中介电子结算平台服务器将tx4.R发送给卖家多重签名应用(1704)。卖家多重签名应用确认tx4.R将在指定的时间段(例如24小时)内成为有效的交易(1705)。卖家多重签名应用将tx4发送给数字资产中介电子结算平台服务器(1706)。数字资产中介电子结算平台服务器检查tx4是有效的交易并将其广播到区块链(1707)。现在,在图14中结算状态是“被取消”(1412)。卖家多重签名应用现在控制utxo4和utx2.2之间的数字资产权利余额(例如100),其中包括有效赎回tx2.R和tx4.R(1708)。

[0116] 用户可以随时从结算系统转移数字资产权利。用户可以要求立即撤回,或者用户可以单方面签署活跃的赎回。撤回和赎回只能转移到数字资产中介电子结算平台服务器已知和授权的应用控制地址。这确保了离开网络的数字资产权利的接收者是权利的正确所有者。

[0117] 参考图18,示出了显示从多重签名应用撤回到用户应用过程的示例的序列图。用户多重签名应用具有对utxo1形式的数字资产权利的余额(例如100)的活跃控制(1801),其中赎回tx1.R将在一段时间(例如24小时)内激活。多重签名应用通过交易进入工具向数字资产中介电子结算平台服务器通知撤回(1802)。数字资产中介电子结算平台服务器创建包括输入utxo1、目的用户应用的tx2,并发送给多重签名应用(1803)。多重签名应用(1803)授权tx2并将其发送给数字资产中介电子结算平台服务器(1804)。数字资产中介电子结算平台服务器检查tx2是有效的交易并授权tx2(1805)。数字资产中介电子结算平台服务器将tx2广播到区块链(1806)。用户应用现在具有对数字资产权利的余额(例如100)的控制(1807)。

[0118] 参考图19,序列图示出了示例性的用户单方面赎回过程。多重签名应用具有对utxo1形式的数字资产权利的活跃余额(例如100)的控制,其中赎回tx1.R将在指定时间段(例如24小时)内激活(1901)。在指定时间段(例如,24小时)期间,不会创建新的未来有效的赎回日期,也不会结算交易(1902)。多重签名应用授权tx1.R并将其广播到区块链(1903,1103)。在图11所示的示例性资金状态中,卖家的单方面撤回状态(1103)是发起赎回的一种方式,或者数字资产中介电子结算平台已经承诺通过授权一个时间锁定的交易从数字资产中介电子结算平台发送权利,其结果是卖家可以“单方面”随意决定撤回。用户应用现在具有对数字资产权利的余额(例如100)的控制(1904)。

[0119] 参考图20,可以用来实现本发明构思的示例性实施例系统总体由附图标记2000表示。该示例仅是本发明构思所设想的若干替代方案中的一个,并且旨在是非限制性的。示出了具有基于web浏览器的用户界面的用户访问计算机2010。用户访问计算机与web服务器集群2020和数据API集群2030对接。取决于用户的角色,用户访问计算机可以替代地访问本地驻留在用户的基础设施内的数字资产中介电子结算平台服务器2040或由第三方托管的数字资产中介电子结算平台服务器,以及数字资产节点2044的关联集群2042。web服务器群集通过传输层安全性(TLS)上的超文本传输协议(HTTP)提供超文本标记语言(HTML)和基于JavaScript的用户界面。数据API集群与协调服务集群2050、缓存服务集群2060、持久性服务集群2070对接;并且与数字资产接口服务器2080和数字资产节点2084的相关集群2082对接。持久性服务器2070的持久性服务群集存储密钥值并将值保存在磁盘上以便长期存储。存储在持久性服务集群中的值是不可变的,允许缓存服务集群缓存这些值。协调服务器

2050的协调服务集群包含可变数据，即，持久性服务中的名称到根密钥的映射。数字资产接口群集2042和2082以及数字资产中介电子结算平台服务器2040和2080与数字资产对等网络交互并保存不可变的私钥。数字资产中介电子结算平台服务器可以可选地通过诸如但不限于短消息服务(SMS)、电子邮件或专用硬件设备的第二因素认证手段来连接到用户。

[0120] 用户访问计算机与web服务器集群、数据API集群基础设施以及数字资产中介电子结算平台服务器之间的接口应包括但不限于：广域网连接、局域网连接、适当的网络交换机和路由器、电力、备用电源、存储区域网络硬件、服务器级计算硬件、个人计算机、平板电脑、智能手机和操作系统。

[0121] 例如，数据API集群可以运行在例如使用多个处理器和/或多核处理器、RAM、高吞吐量网络控制器、热插拔SSD和SATA驱动器以及冗余电源的服务器集群上。

[0122] 虽然已经通过关于示例性实施例的示例描述了本发明的构思，但是对于相关领域的普通技术人员来说，其他替换、修改和变化将是显而易见的。因此，所附权利要求书的范围旨在包括在此阐述的示例性实施例的所有这样的替代、修改和变化以及落入本公开的范围和精神内的等价物。

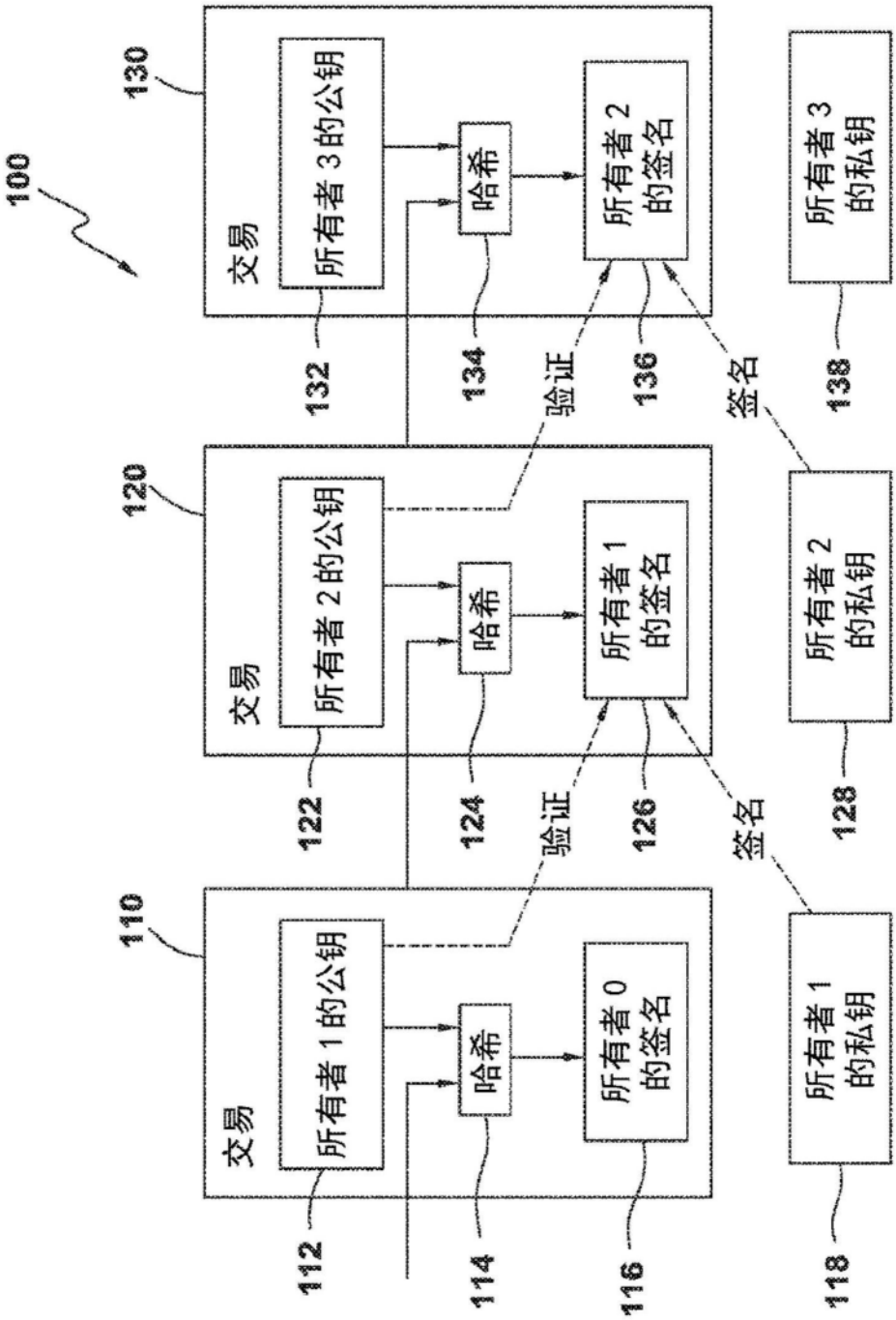

100
130
交易
所有者 3 的公钥
哈希
所有者 2
的签名
所有者 3
的私钥
132
134
验证
136
签名
138
120
交易
所有者 2 的公钥
哈希
所有者 1
的签名
所有者 2
的私钥
122
124
验证
126
签名
128
110
交易
所有者 1 的公钥
哈希
所有者 0
的签名
所有者 1
的私钥
112
114
116
118

图1

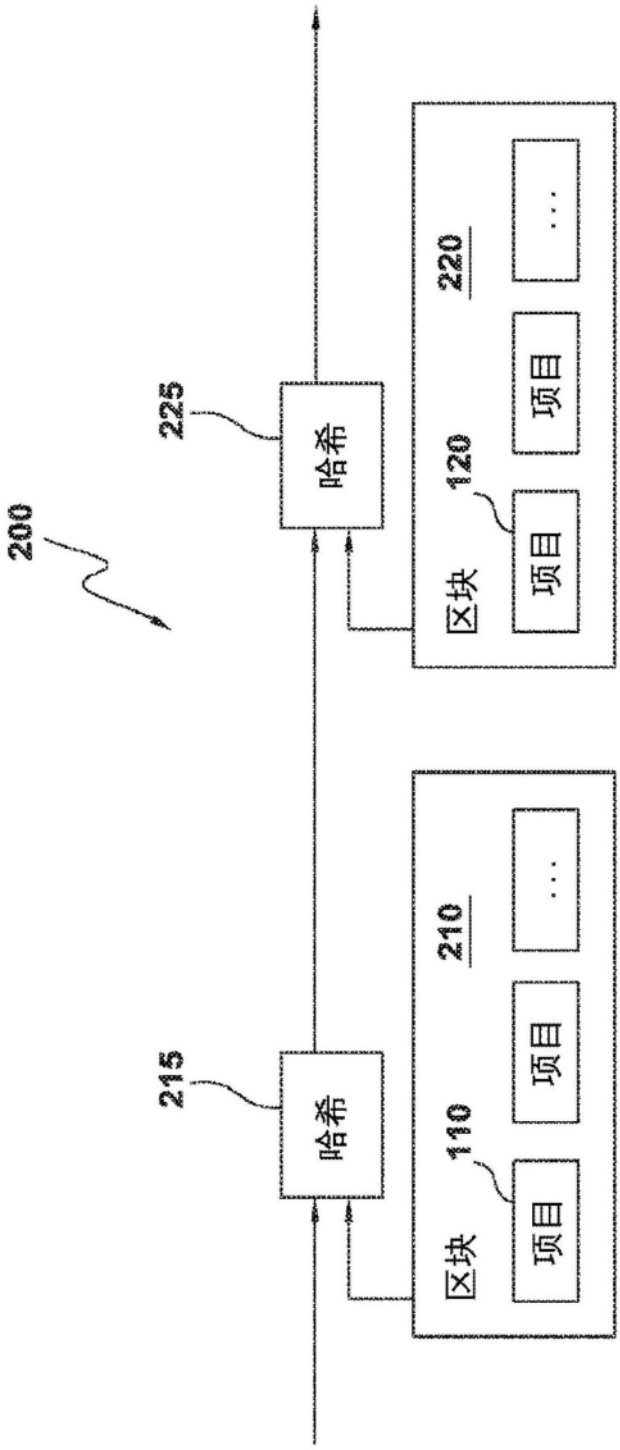


图2

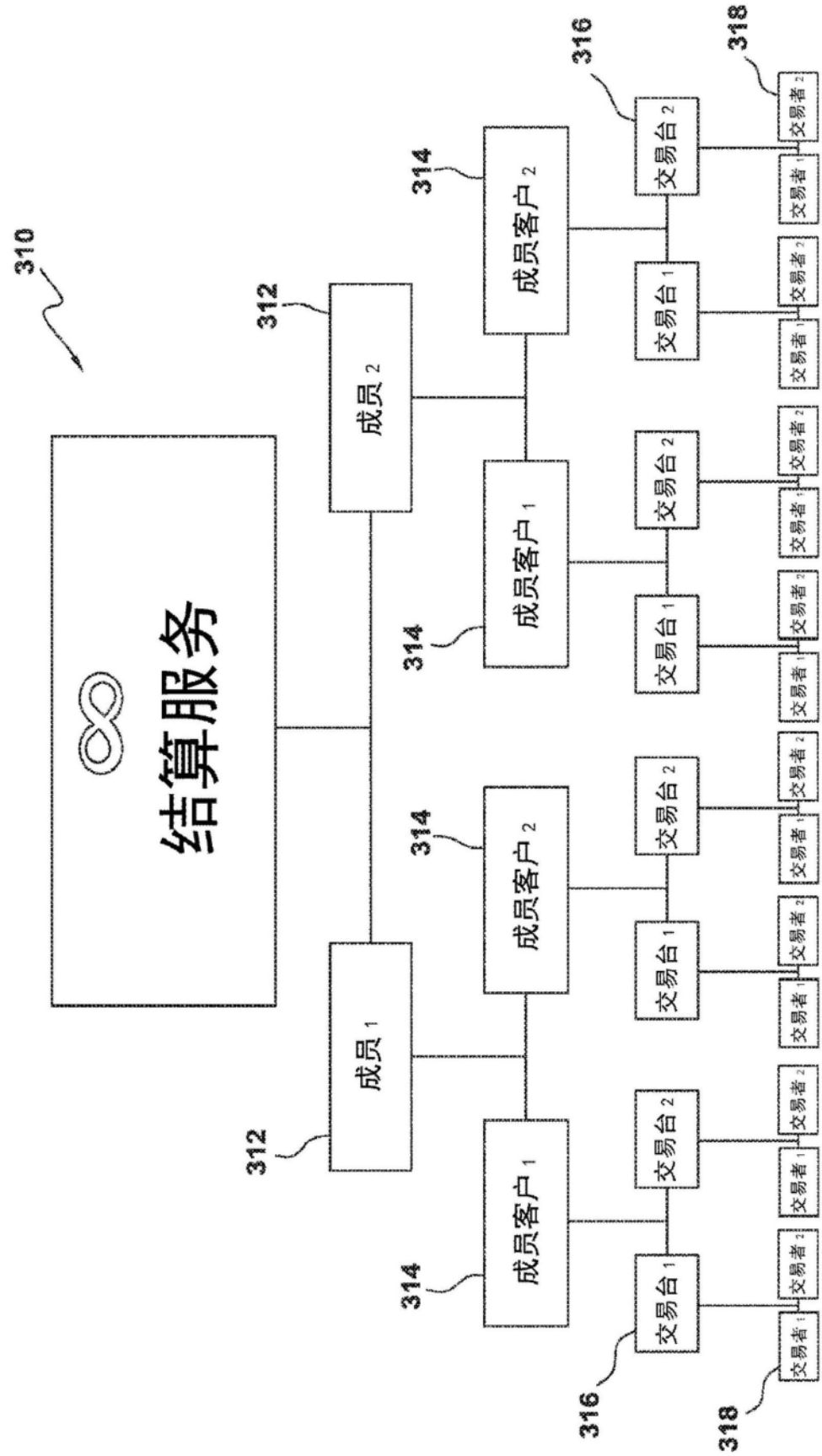

310
结算服务
312
成员 1
成员 2
314
成员客户 1
成员客户 2
316
交易台 1
交易台 2
318
交易者 1
交易者 2

图3

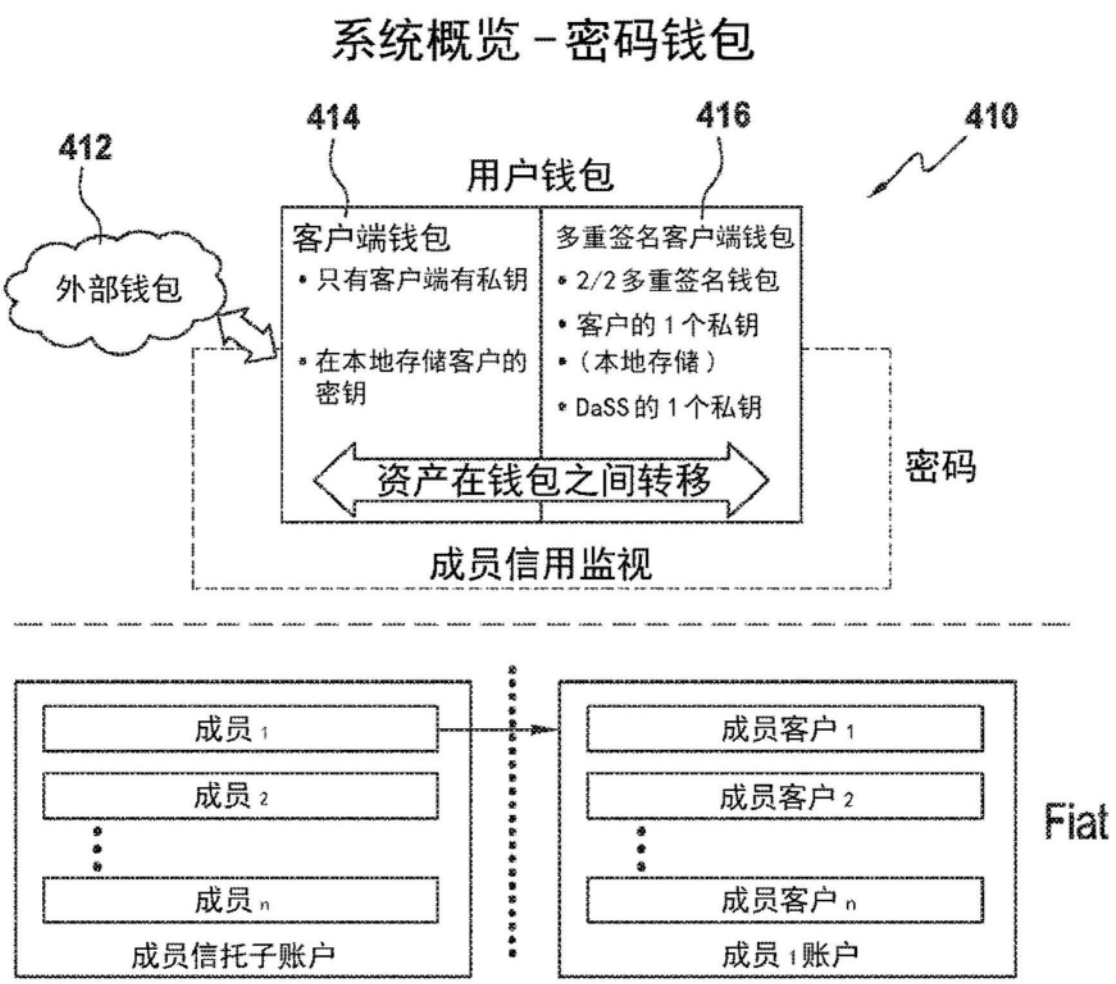

系统概览－密码钱包
412
414
416
410
用户钱包
外部钱包
客户端钱包
• 只有客户端有私钥
• 在本地存储客户的密钥
多重签名客户端钱包
• 2/2 多重签名钱包
• 客户的 1 个私钥
• （本地存储）
• DaSS 的 1 个私钥
资产在钱包之间转移
密码
成员信用监视
成员 1
成员 2
成员 n
成员信托子账户
成员客户 1
成员客户 2
成员客户 n
成员 1 账户
Fiat

图4

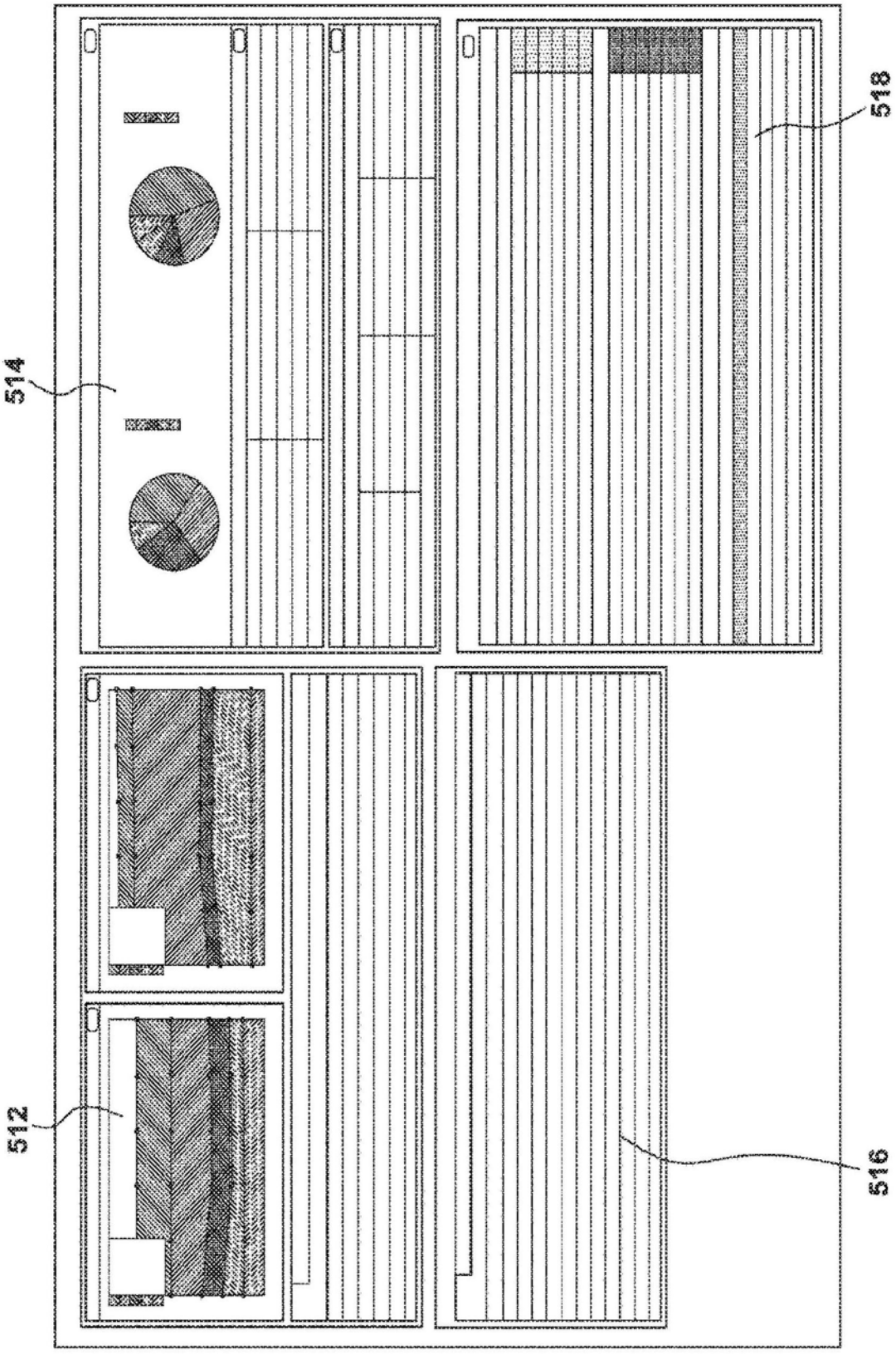


图5

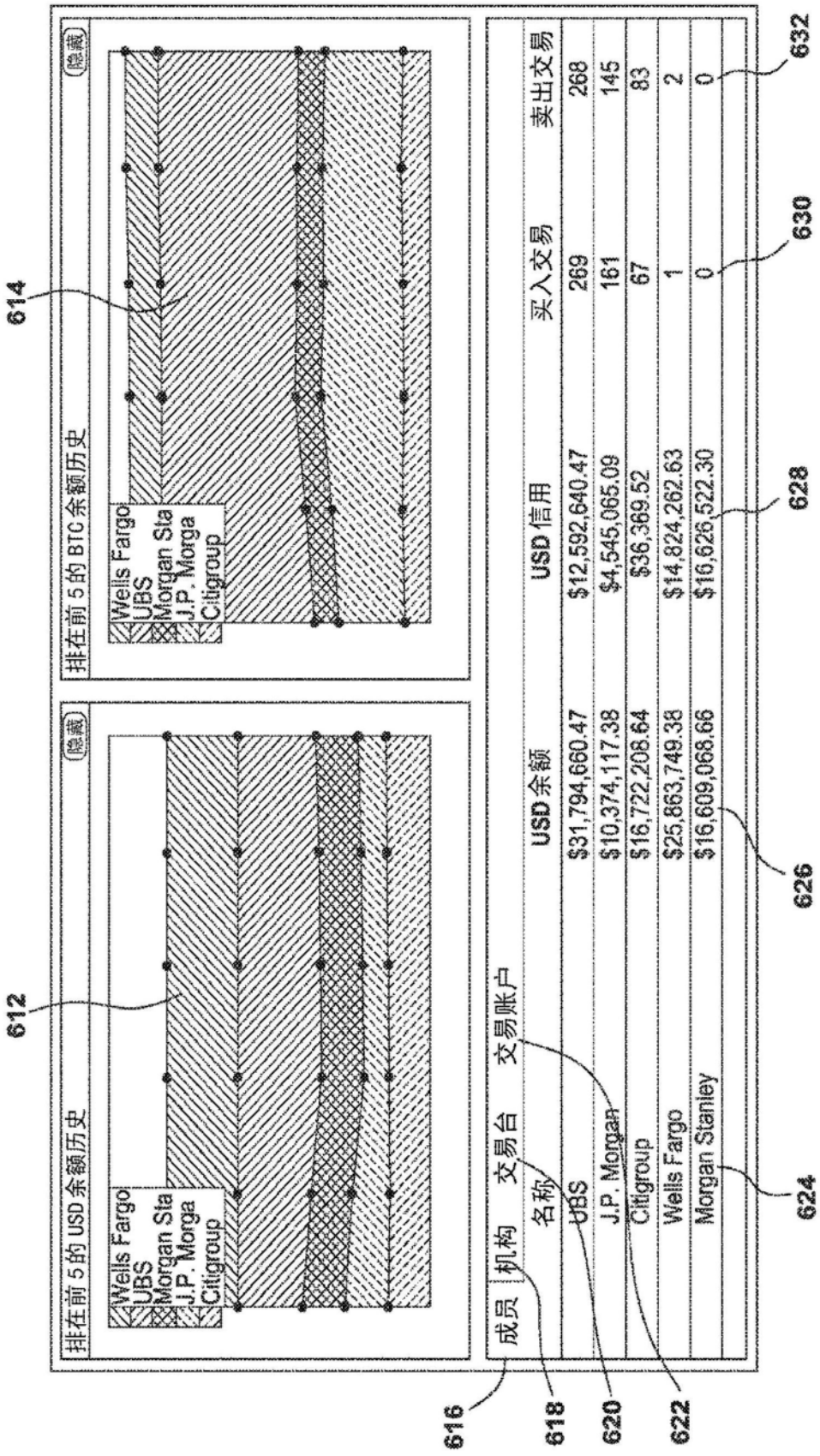

612
614
排在前 5 的 USD 余额历史
隐藏
Wells Fargo
UBS
Morgan Sta
J.P. Morga
Citigroup
排在前 5 的 BTC 余额历史
隐藏
Wells Fargo
UBS
Morgan Sta
J.P. Morga
Citigroup
成员
机构 交易台 交易账户
名称
USD 余额
USD 信用
买入交易
卖出交易
UBS
$31,794,660.47
$12,592,640.47
269
268
J.P. Morgan
$10,374,117.38
$4,545,065.09
161
145
Citigroup
$16,722,208.64
$36,369.52
67
83
Wells Fargo
$25,863,749.38
$14,824,262.63
1
2
Morgan Stanley
$16,609,068.66
$16,626,522.30
0
0
616
618
620
622
624
626
628
630
632

图6

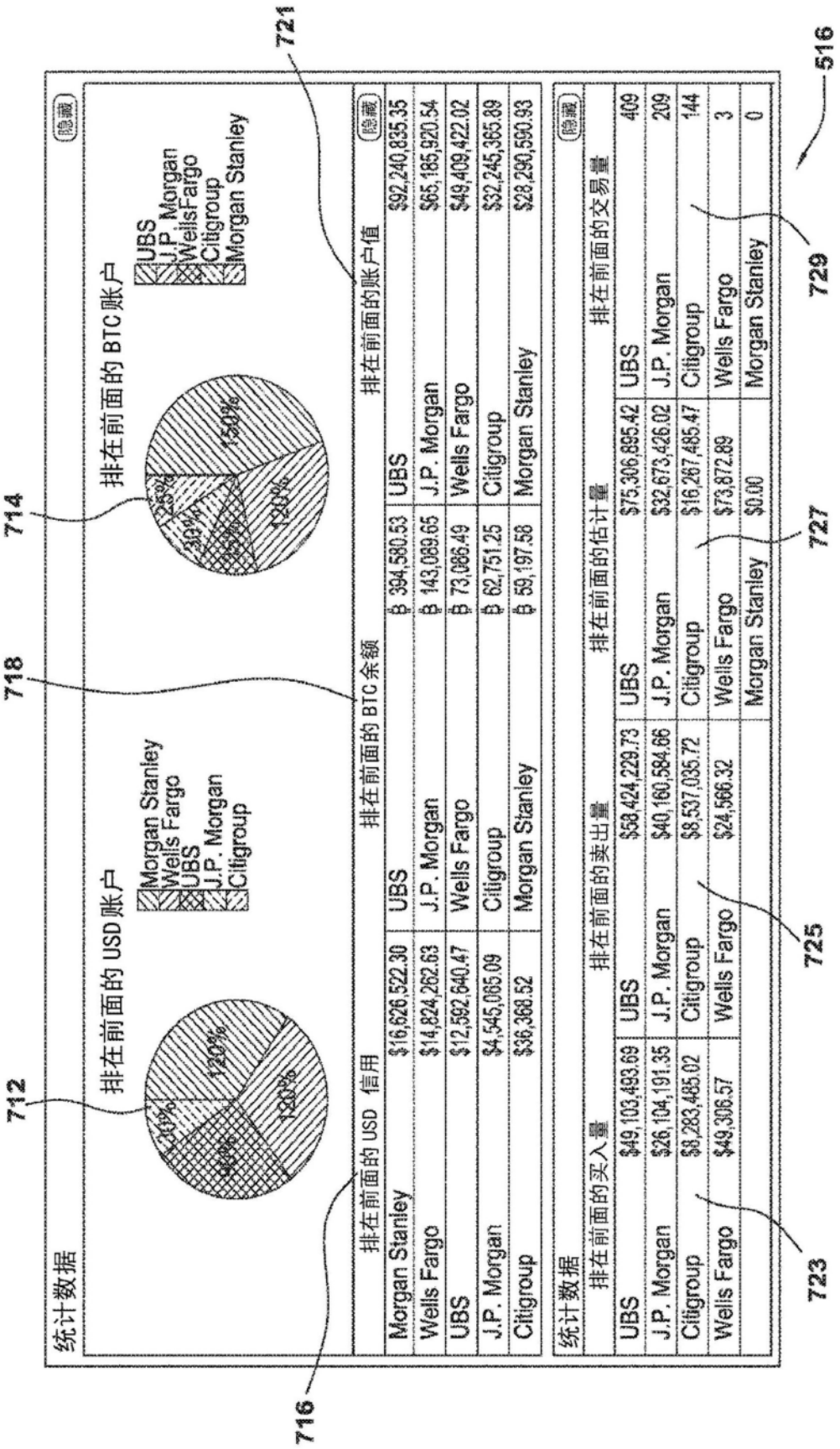

712
714
716
718
721
723
725
727
729
516
统计数据
隐藏
排在前面的 USD 账户
Morgan Stanley
Wells Fargo
UBS
J.P. Morgan
Citigroup
20%
120%
120%
排在前面的 BTC 账户
UBS
J.P. Morgan
WellsFargo
Citigroup
Morgan Stanley
25%
30%
150%
120%
排在前面的 USD 信用
排在前面的 BTC 余额
排在前面的账户值
Morgan Stanley $16,626,522.30 UBS ฿ 394,580.53 UBS $92,240,835.35
Wells Fargo $14,824,262.63 J.P. Morgan ฿ 143,089.65 J.P. Morgan $65,185,920.54
UBS $12,592,640.47 Wells Fargo ฿ 73,086.49 Wells Fargo $49,409,422.02
J.P. Morgan $4,545,065.09 Citigroup ฿ 62,751.25 Citigroup $32,245,365.89
Citigroup $36,368.52 Morgan Stanley ฿ 59,197.58 Morgan Stanley $28,290,590.93
统计数据
隐藏
排在前面的买入量
排在前面的卖出量
排在前面的估计量
排在前面的交易量
UBS $49,103,493.69 UBS $58,424,229.73 UBS $75,306,895.42 UBS 409
J.P. Morgan $26,104,191.35 J.P. Morgan $40,160,584.66 J.P. Morgan $32,673,426.02 J.P. Morgan 209
Citigroup $8,283,485.02 Citigroup $8,537,035.72 Citigroup $16,267,485.47 Citigroup 144
Wells Fargo $49,306.57 Wells Fargo $24,566.32 Wells Fargo $73,872.89 Wells Fargo 3
Morgan Stanley $0.00 Morgan Stanley 0

图7

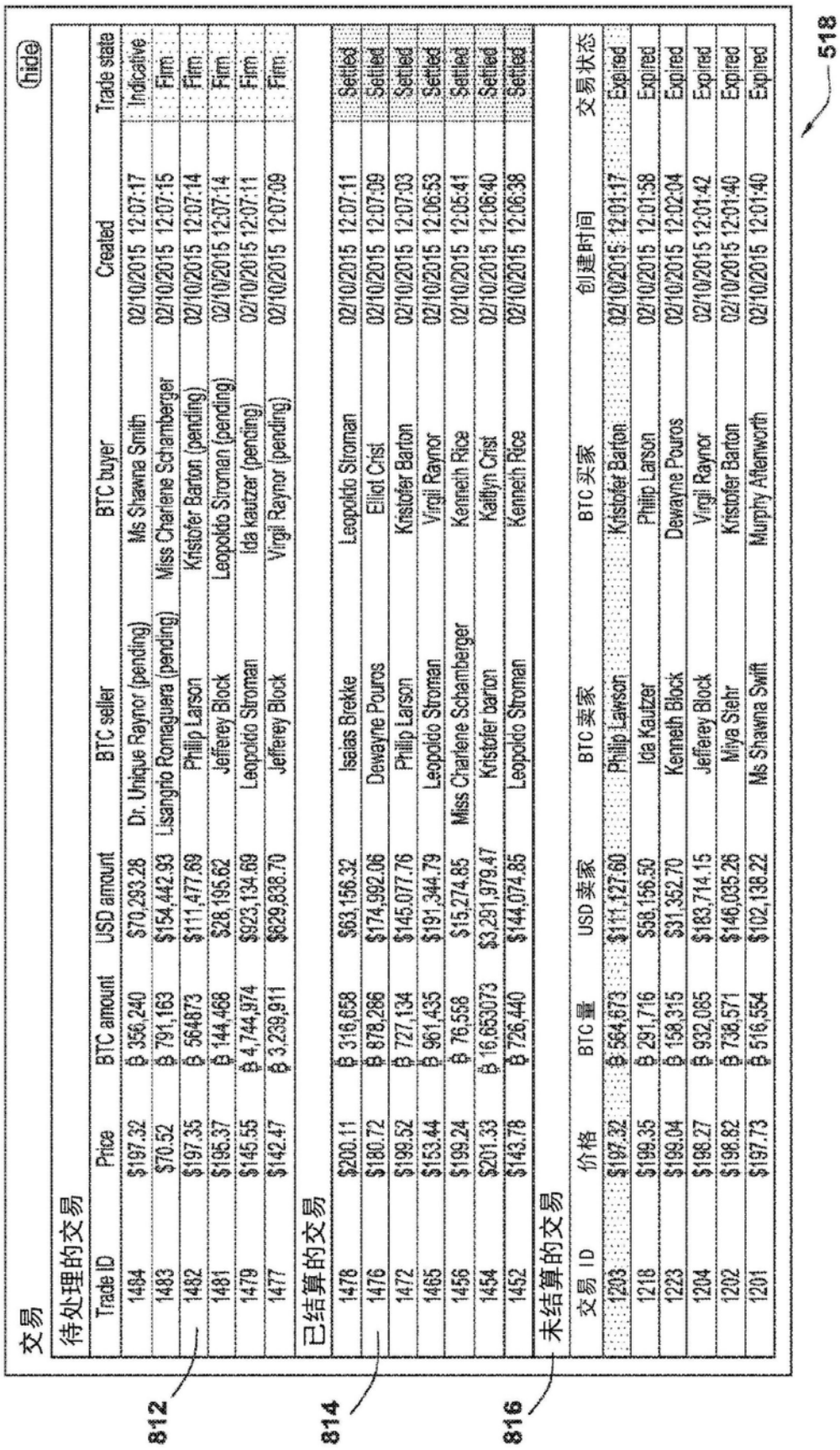

交易
(hide)
待处理的交易
Trade ID | Price | BTC amount | USD amount | BTC seller | BTC buyer | Created | Trade state
1484 | $197.32 | Ƀ 356.240 | $70,293.28 | Dr. Unique Raynor (pending) | Ms Shawna Smith | 02/10/2015 12:07:17 | Indicative
1483 | $70.52 | Ƀ 791.163 | $154,442.93 | Lisangrio Romaguera (pending) | Miss Charlene Schamberger | 02/10/2015 12:07:15 | Firm
1482 | $197.35 | Ƀ 564873 | $111,477.69 | Phillip Larson | Kristofer Barton (pending) | 02/10/2015 12:07:14 | Firm
1481 | $195.37 | Ƀ 144.468 | $28,195.62 | Jefferey Block | Leopoldo Stroman (pending) | 02/10/2015 12:07:14 | Firm
1479 | $145.55 | Ƀ 4,744.974 | $923,134.69 | Leopoldo Stroman | Ida kautzer (pending) | 02/10/2015 12:07:11 | Firm
1477 | $142.47 | Ƀ 3,239.911 | $829,838.70 | Jefferey Block | Virgil Raynor (pending) | 02/10/2015 12:07:09 | Firm
已结算的交易
1478 | $200.11 | Ƀ 316.658 | $63,156.32 | Isaias Brekke | Leopoldo Stroman | 02/10/2015 12:07:11 | Settled
1476 | $180.72 | Ƀ 878.286 | $174,992.06 | Dewayne Pouros | Elliot Crist | 02/10/2015 12:07:09 | Settled
1472 | $199.52 | Ƀ 727.134 | $145,077.76 | Phillip Larson | Kristofer Barton | 02/10/2015 12:07:03 | Settled
1465 | $153.44 | Ƀ 961.435 | $191,344.79 | Leopoldo Stroman | Virgil Raynor | 02/10/2015 12:06:53 | Settled
1456 | $199.24 | Ƀ 76.568 | $15,274.85 | Miss Charlene Schamberger | Kenneth Rice | 02/10/2015 12:05:41 | Settled
1454 | $201.33 | Ƀ 16.653073 | $3,291,979.47 | Kristofer barton | Kaitlyn Crist | 02/10/2015 12:06:40 | Settled
1452 | $143.78 | Ƀ 726.440 | $144,074.85 | Leopoldo Stroman | Kenneth Rice | 02/10/2015 12:06:38 | Settled
未结算的交易
交易 ID | 价格 | BTC 量 | USD 卖家 | BTC 卖家 | BTC 买家 | 创建时间 | 交易状态
1233 | $197.32 | Ƀ 564.673 | $111,427.60 | Phillip Lawson | Kristofer Barton | 02/10/2015 12:01:17 | Expired
1218 | $199.35 | Ƀ 291.716 | $58,156.50 | Ida Kautzer | Phillip Larson | 02/10/2015 12:01:58 | Expired
1223 | $199.04 | Ƀ 158.315 | $31,352.70 | Kenneth Block | Dewayne Pouros | 02/10/2015 12:02:04 | Expired
1204 | $198.27 | Ƀ 932.085 | $183,714.15 | Jefferey Block | Virgil Raynor | 02/10/2015 12:01:42 | Expired
1202 | $198.82 | Ƀ 738.571 | $146,035.26 | Miya Stehr | Kristofer Barton | 02/10/2015 12:01:40 | Expired
1201 | $197.73 | Ƀ 516.554 | $102,138.22 | Ms Shawna Swift | Murphy Aftenworth | 02/10/2015 12:01:40 | Expired
812
814
816
518

图8

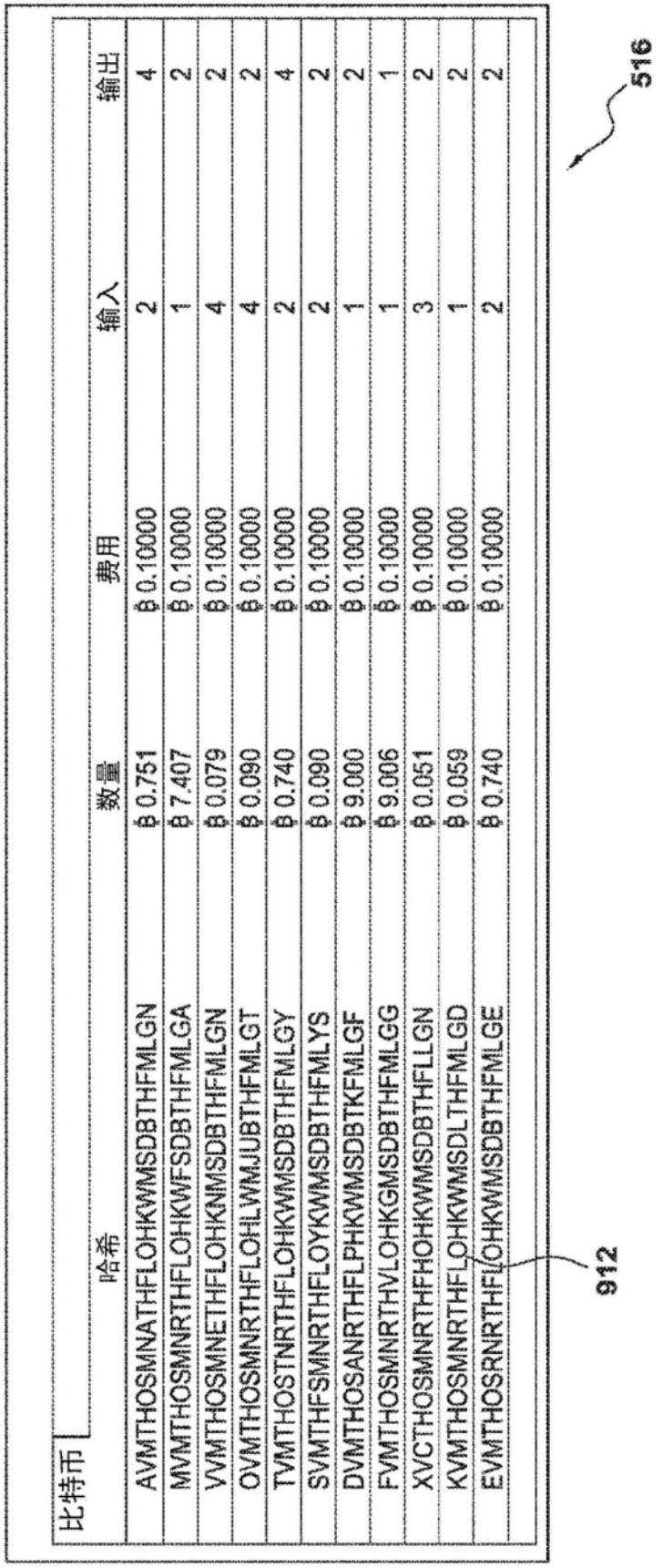

比特币
哈希
数量
费用
输入
输出
AVMTHOSMNATHFLOHKWMSDBTHFMLGN ฿0.751 ฿0.10000 2 4
MVMTHOSMNRTHFLOHKWFSDBTHFMLGA ฿7.407 ฿0.10000 1 2
VVMTHOSMNETHFLOHKNMSDBTHFMLGN ฿0.079 ฿0.10000 4 2
OVMTHOSMNRTHFLOHLWMJUBTHFMLGT ฿0.090 ฿0.10000 4 2
TVMTHOSTNRTHFLOHKWMSDBTHFMLGY ฿0.740 ฿0.10000 2 4
SVMTHFSMNRTHFLOYKWMSDBTHFMLYS ฿0.090 ฿0.10000 2 2
DVMTHOSANRTHFLPHKWMSDBTKFMLGF ฿9.000 ฿0.10000 1 2
FVMTHOSMNRTHVLOHKGMSDBTHFMLGG ฿9.006 ฿0.10000 1 1
XVCTHOSMNRTHFHOHKWMSDBTHFLLGN ฿0.051 ฿0.10000 3 2
KVMTHOSMNRTHFLOHKWMSDLTHFMLGD ฿0.059 ฿0.10000 1 2
EVMTHOSRNRTHFLOHKWMSDBTHFMLGE ฿0.740 ฿0.10000 2 2
912
516

图9

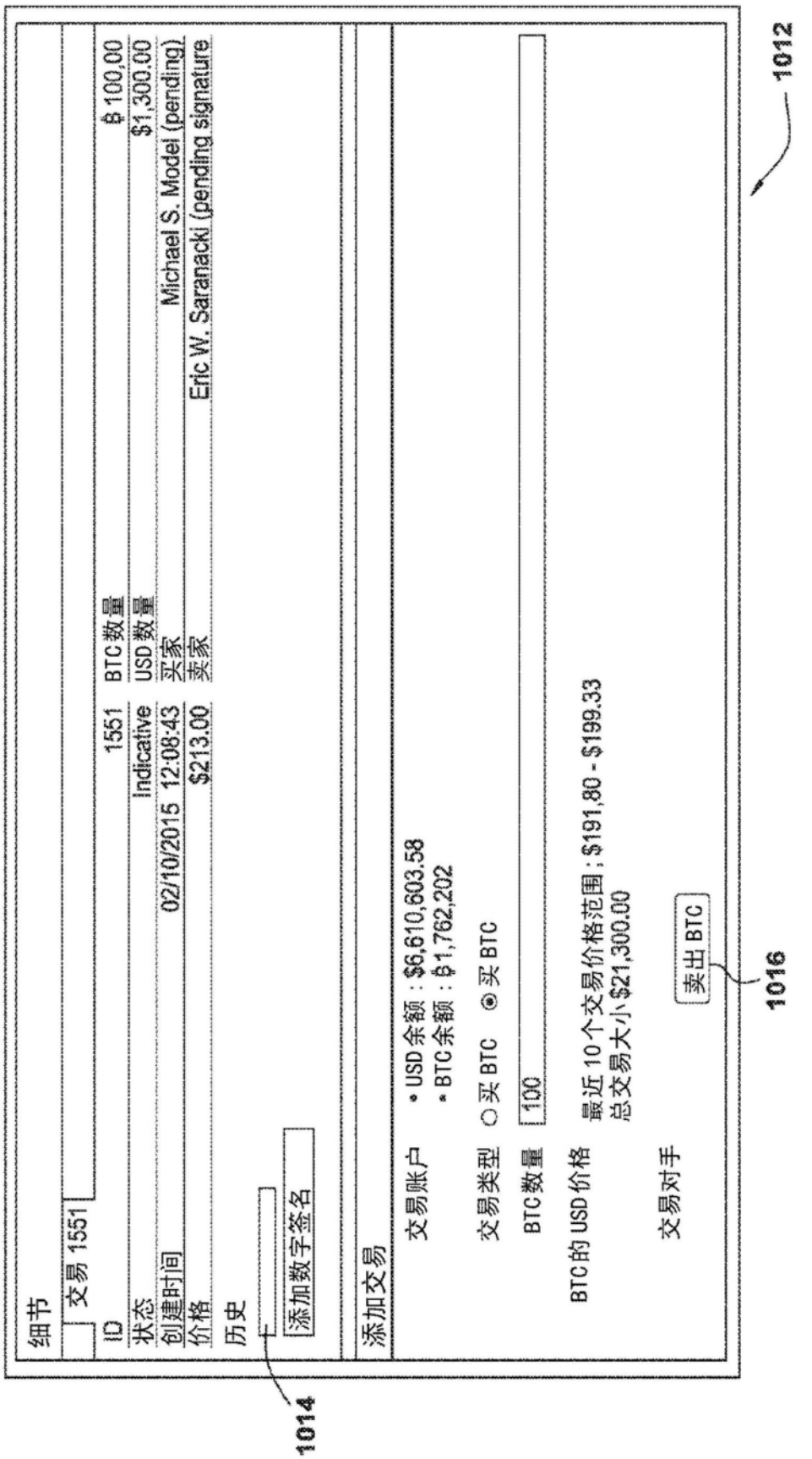

细节
交易 1551
ID 1551 BTC 数量 ฿100.00
状态 Indicative USD 数量 $1,300.00
创建时间 02/10/2015 12:08:43 买家 Michael S. Model (pending)
价格 $213.00 卖家 Eric W. Saranacki (pending signature
历史
添加数字签名
1014
添加交易
交易账户
• USD 余额：$6,610,603.58
• BTC 余额：฿1,762,202
交易类型 ○ 买 BTC ◉ 买 BTC
BTC 数量 100
BTC 的 USD 价格 最近 10 个交易价格范围：$191.80 - $199.33
总交易大小 $21,300.00
交易对手
卖出 BTC
1016
1012

图10

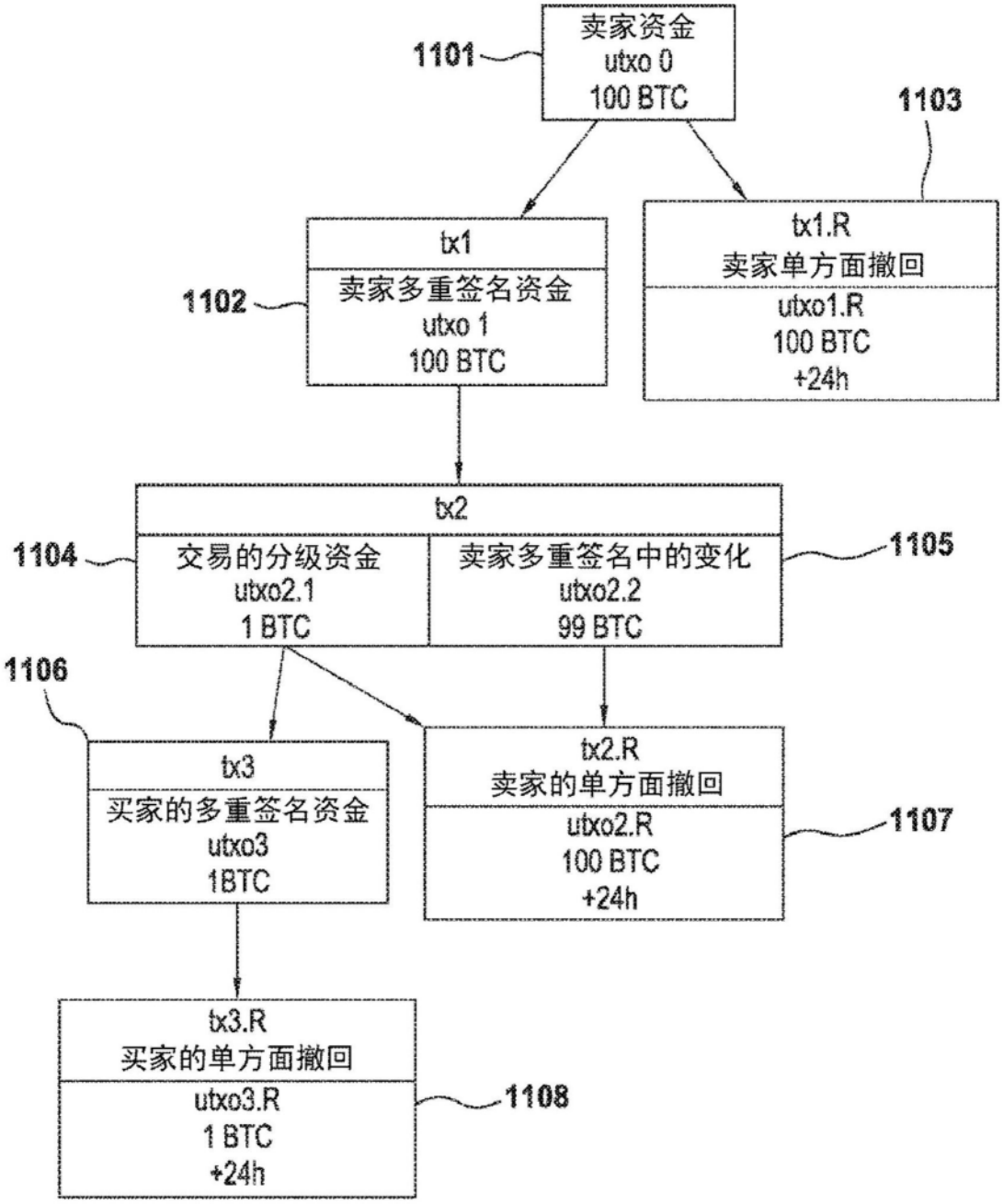

1101
卖家资金
utxo 0
100 BTC
1103
tx1
卖家多重签名资金
utxo 1
100 BTC
1102
tx1.R
卖家单方面撤回
utxo1.R
100 BTC
+24h
tx2
1104
交易的分级资金
utxo2.1
1 BTC
卖家多重签名中的变化
utxo2.2
99 BTC
1105
1106
tx3
买家的多重签名资金
utxo3
1BTC
tx2.R
卖家的单方面撤回
utxo2.R
100 BTC
+24h
1107
tx3.R
买家的单方面撤回
utxo3.R
1 BTC
+24h
1108

图11

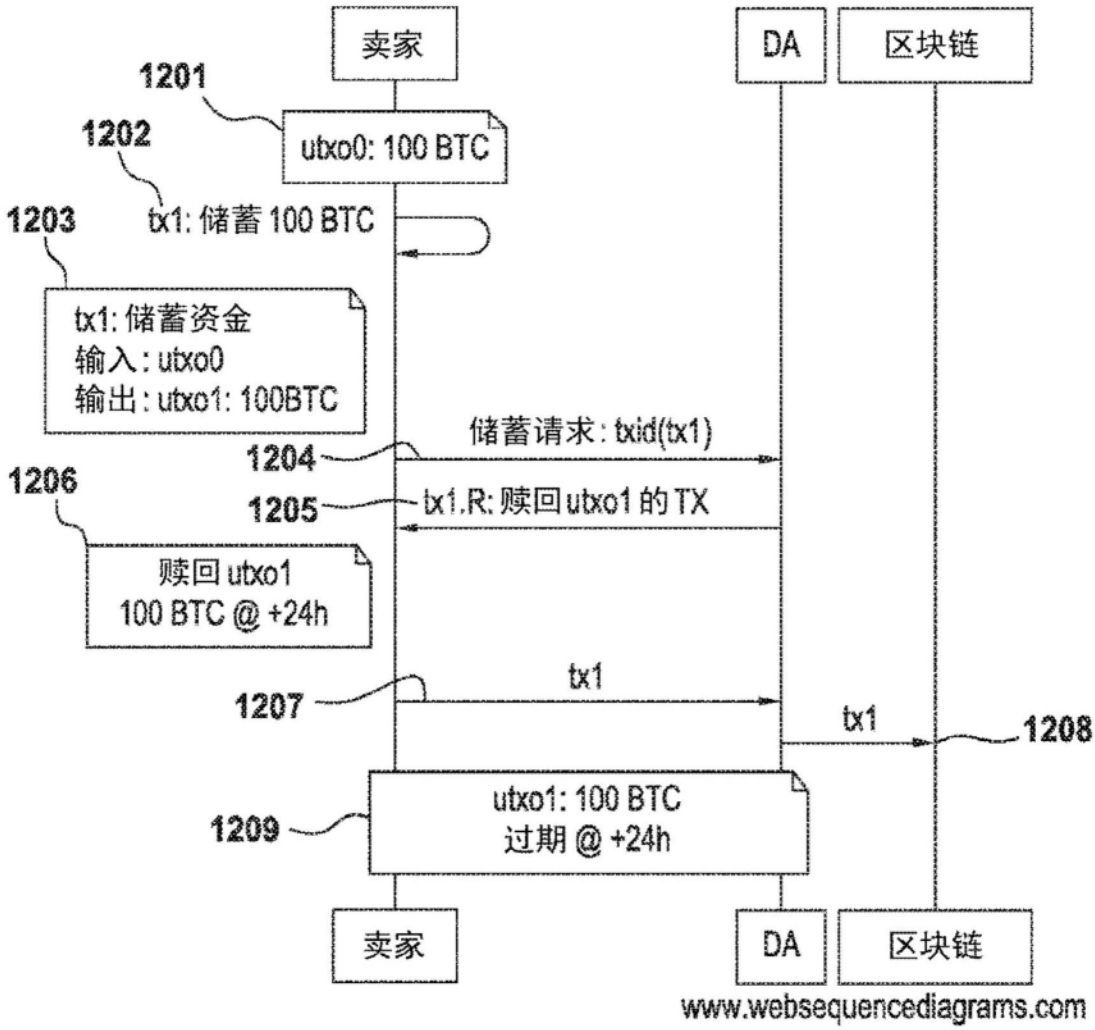

卖家
DA
区块链
1201
utxo0: 100 BTC
1202
tx1: 储蓄 100 BTC
1203
tx1: 储蓄资金
输入: utxo0
输出: utxo1: 100BTC
储蓄请求: txid(tx1)
1204
1206
1205
tx1.R: 赎回 utxo1 的 TX
赎回 utxo1
100 BTC @ +24h
tx1
1207
tx1
1208
utxo1: 100 BTC
过期 @ +24h
1209
卖家
DA
区块链
www.websequencediagrams.com

图12

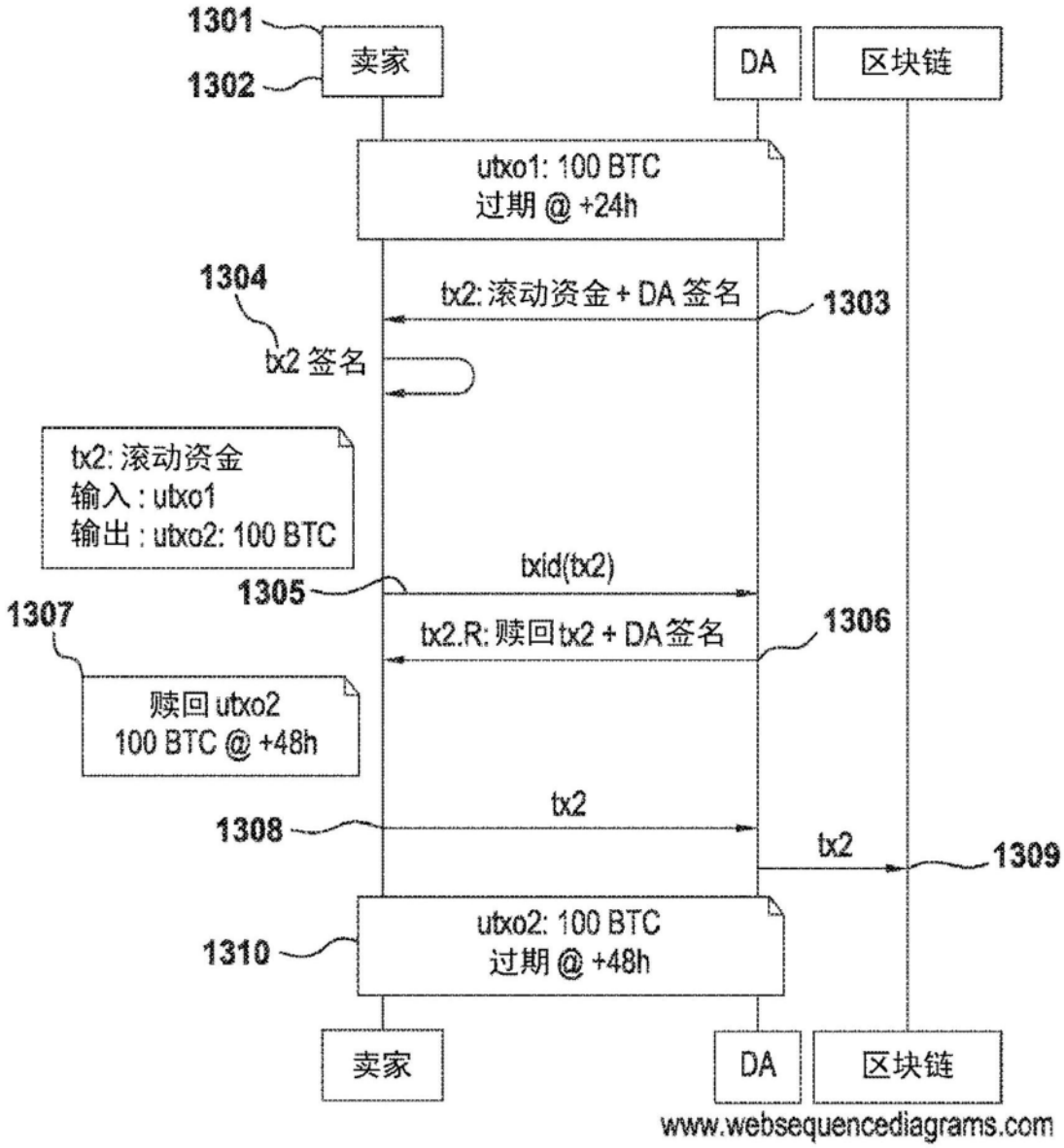

1301
卖家
1302
DA
区块链
utxo1: 100 BTC
过期 @ +24h
1304
tx2: 滚动资金 + DA 签名
1303
tx2 签名
tx2: 滚动资金
输入 : utxo1
输出 : utxo2: 100 BTC
txid(tx2)
1305
1307
tx2.R: 赎回tx2 + DA签名
1306
赎回 utxo2
100 BTC @ +48h
tx2
1308
tx2
1309
utxo2: 100 BTC
过期 @ +48h
1310
卖家
DA
区块链
www.websequencediagrams.com

图13

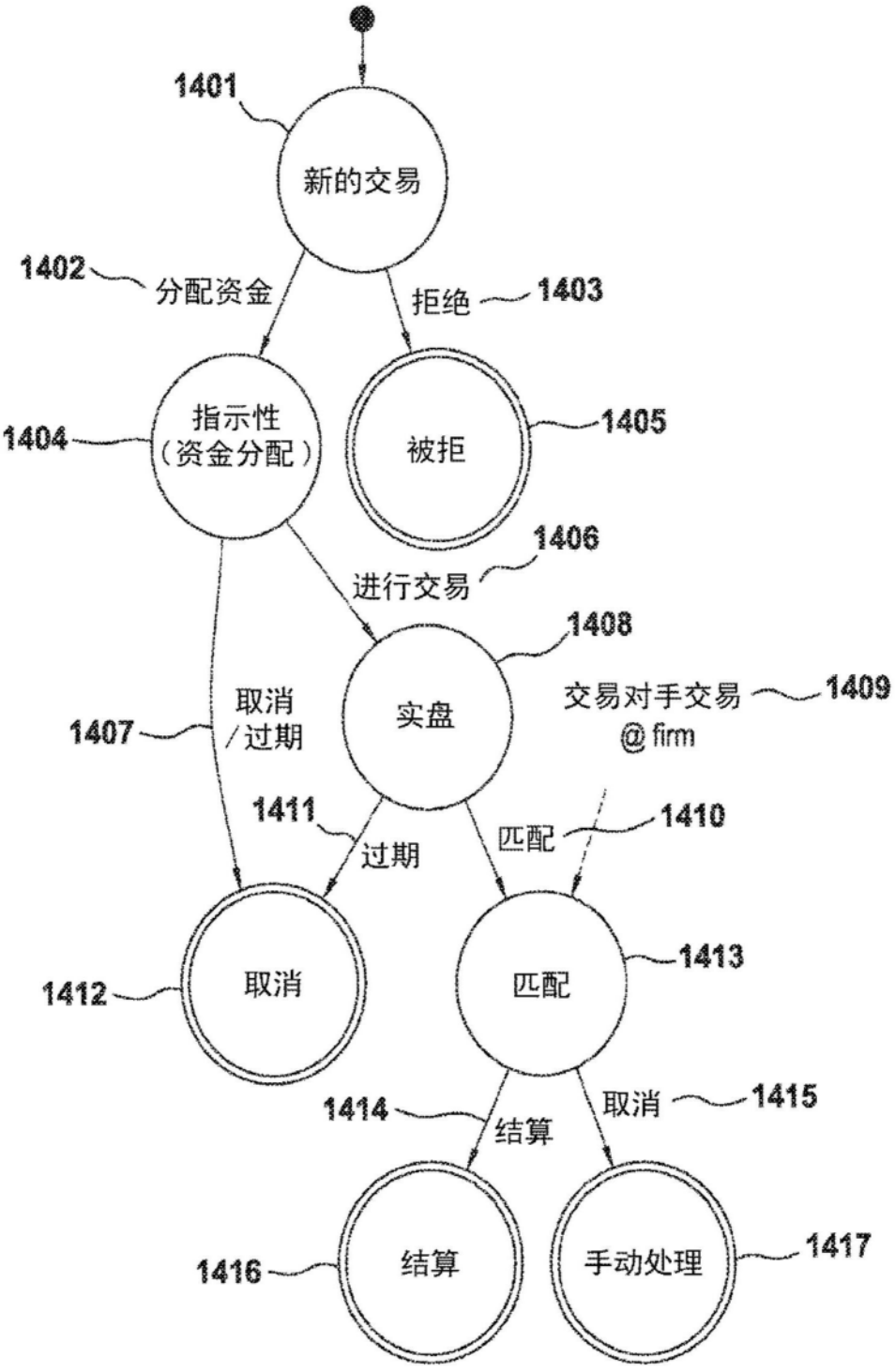

1401
新的交易
1402
分配资金
拒绝
1403
指示性
（资金分配）
1404
被拒
1405
1406
进行交易
1408
实盘
交易对手交易
@firm
1409
取消
/过期
1407
1411
过期
匹配
1410
取消
1412
匹配
1413
1414
结算
取消
1415
结算
1416
手动处理
1417

图14

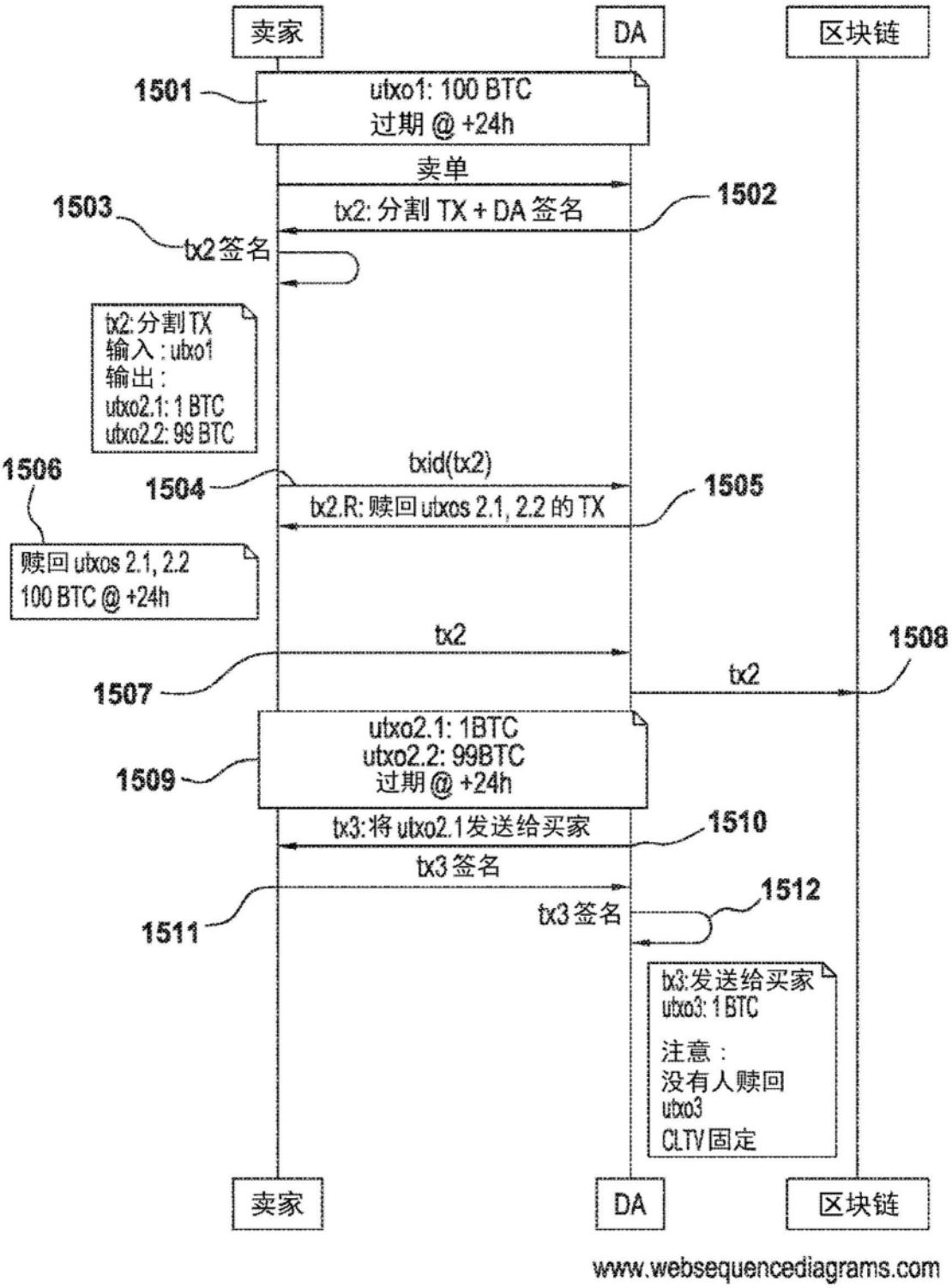

卖家
DA
区块链
1501
utxo1: 100 BTC
过期 @ +24h
卖单
1503
tx2: 分割 TX + DA 签名
1502
tx2签名
tx2: 分割TX
输入 : utxo1
输出 :
utxo2.1: 1 BTC
utxo2.2: 99 BTC
1506
txid(tx2)
1504
1505
tx2.R: 赎回 utxos 2.1, 2.2 的 TX
赎回 utxos 2.1, 2.2
100 BTC @ +24h
tx2
1508
1507
tx2
utxo2.1: 1BTC
utxo2.2: 99BTC
过期 @ +24h
1509
tx3: 将 utxo2.1 发送给买家
1510
tx3 签名
1512
1511
tx3 签名
tx3: 发送给买家
utxo3: 1 BTC
注意 :
没有人赎回
utxo3
CLTV 固定
卖家
DA
区块链
www.websequencediagrams.com

图15

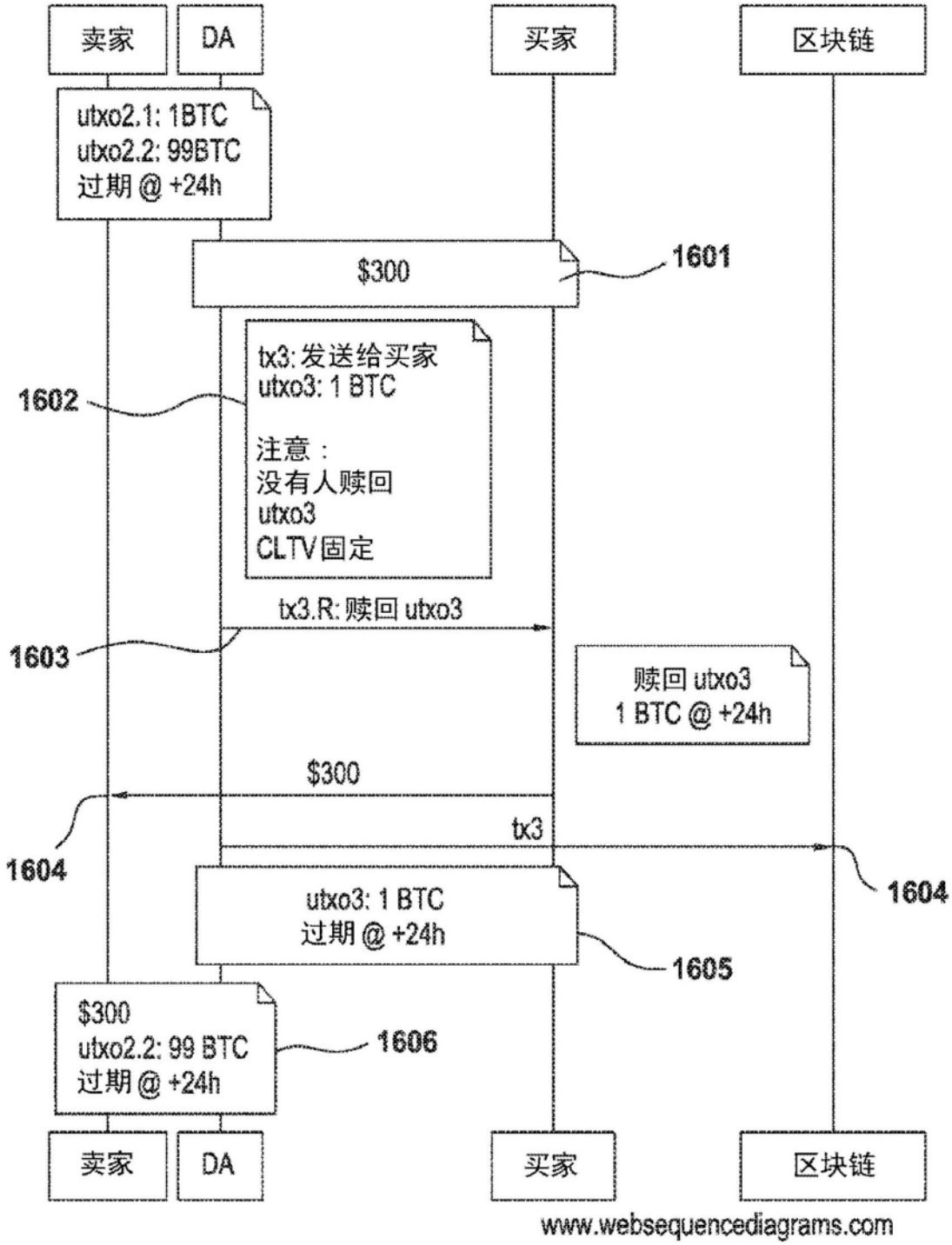

卖家
DA
买家
区块链
utxo2.1: 1BTC
utxo2.2: 99BTC
过期 @ +24h
$300
1601
tx3: 发送给买家
utxo3: 1 BTC
注意：
没有人赎回
utxo3
CLTV固定
1602
tx3.R: 赎回 utxo3
1603
赎回 utxo3
1 BTC @ +24h
$300
1604
tx3
1604
utxo3: 1 BTC
过期 @ +24h
1605
$300
utxo2.2: 99 BTC
过期 @ +24h
1606
卖家
DA
买家
区块链
www.websequencediagrams.com

图16

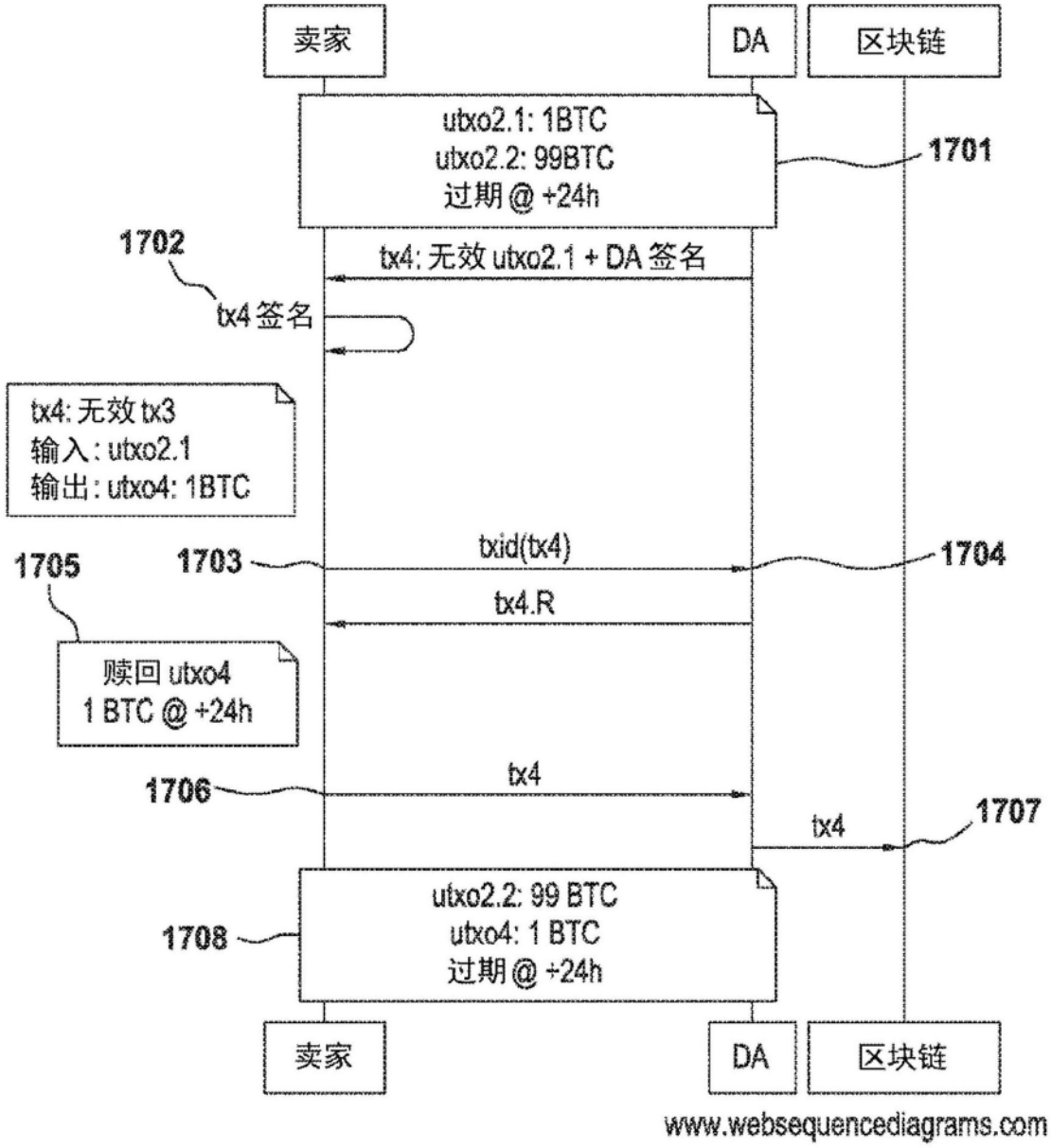

卖家
DA
区块链
utxo2.1: 1BTC
utxo2.2: 99BTC
过期@ +24h
1701
1702
tx4: 无效 utxo2.1 + DA 签名
tx4 签名
tx4: 无效 tx3
输入 : utxo2.1
输出 : utxo4: 1BTC
1705
1703
txid(tx4)
1704
tx4.R
赎回 utxo4
1 BTC @ +24h
1706
tx4
tx4
1707
utxo2.2: 99 BTC
utxo4: 1 BTC
过期@ +24h
1708
卖家
DA
区块链
www.websequencediagrams.com

图17

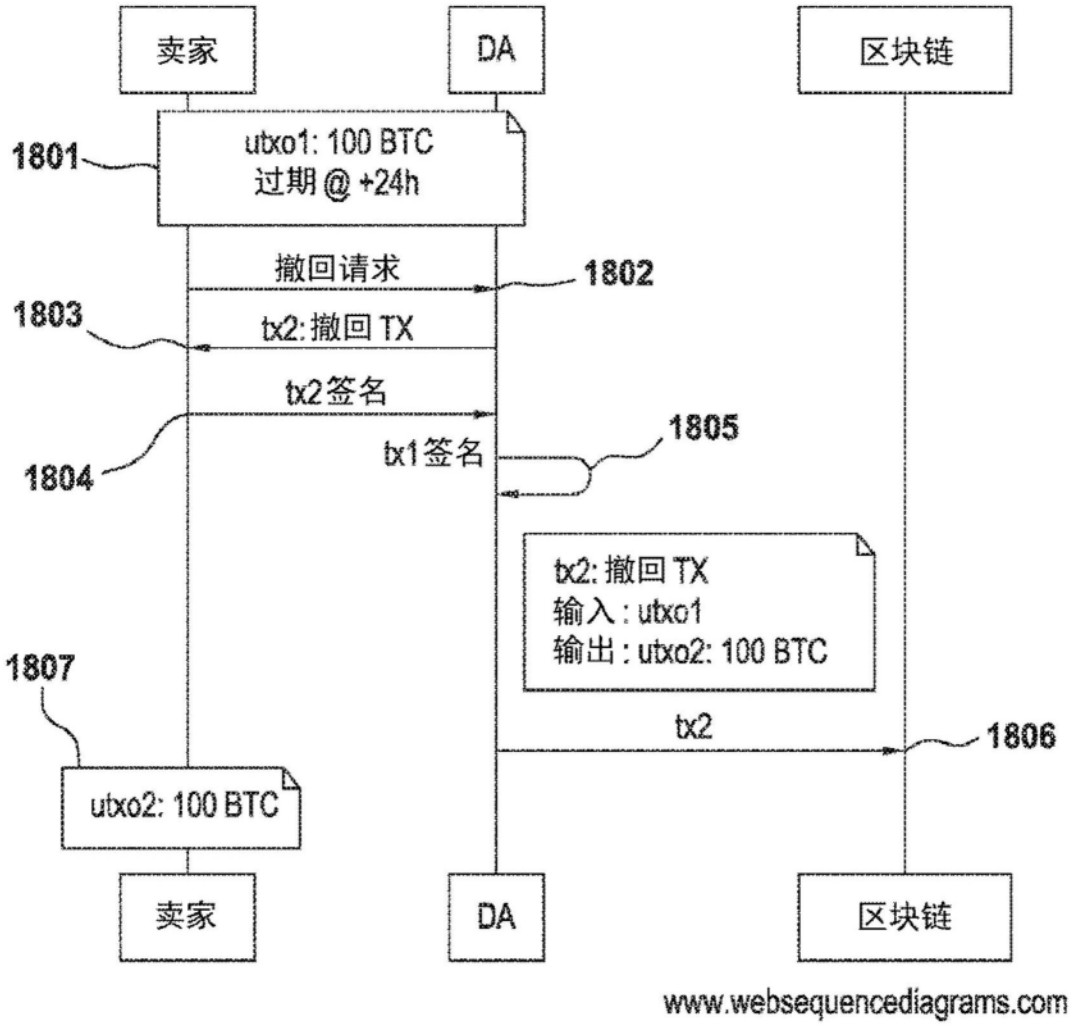

卖家
DA
区块链
1801
utxo1: 100 BTC
过期 @ +24h
撤回请求
1802
1803
tx2: 撤回 TX
tx2签名
1805
1804
tx1签名
tx2: 撤回 TX
输入 : utxo1
输出 : utxo2: 100 BTC
1807
tx2
1806
utxo2: 100 BTC
卖家
DA
区块链
www.websequencediagrams.com

图18

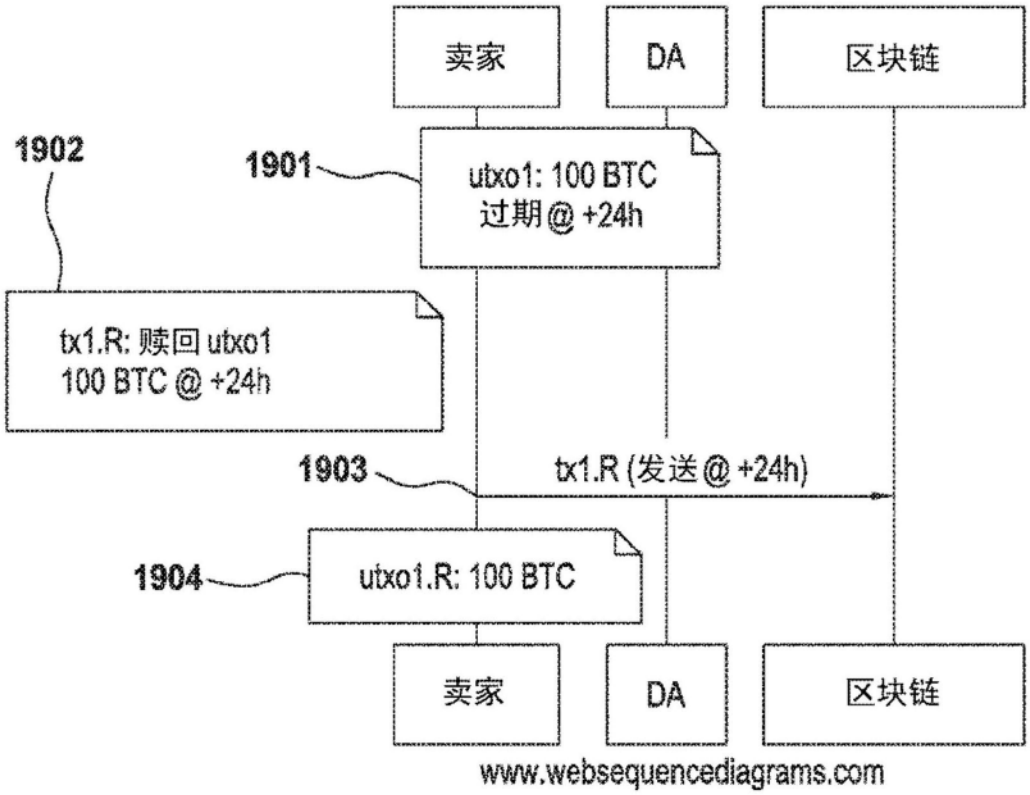

卖家
DA
区块链
1902
1901
utxo1: 100 BTC
过期@ +24h
tx1.R: 赎回 utxo1
100 BTC @ +24h
1903
tx1.R (发送@ +24h)
1904
utxo1.R: 100 BTC
卖家
DA
区块链
www.websequencediagrams.com

图19

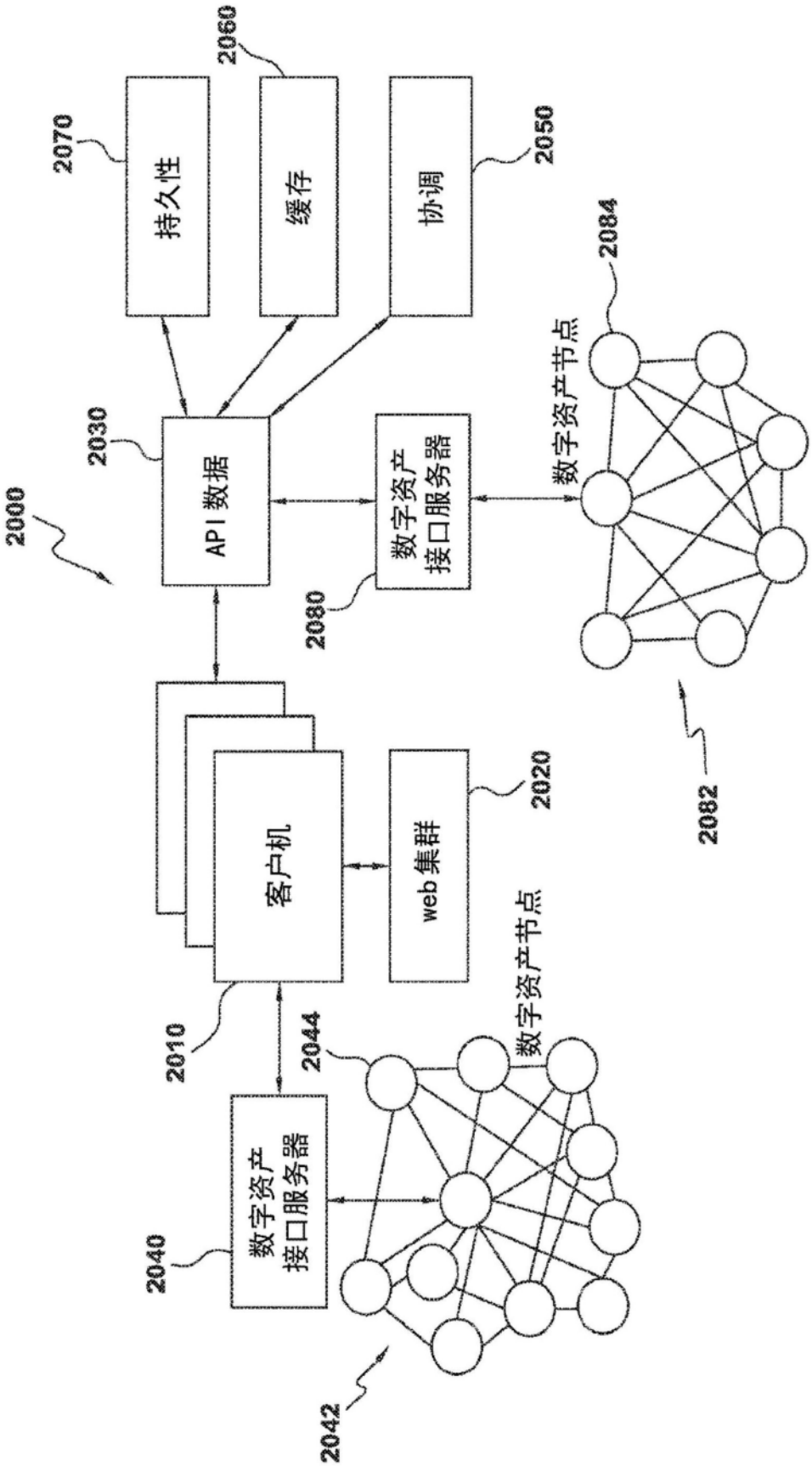

2000
2010
2020
2030
2040
2042
2044
2050
2060
2070
2080
2082
2084
API 数据
客户机
web 集群
持久性
缓存
协调
数字资产
接口服务器
数字资产节点
数字资产节点
数字资产
接口服务器

图20