(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109564660 B
(45)授权公告日 2024.08.13

(21)申请号 201780046102.9
(22)申请日 2017.01.06
(65)同一申请的已公布的文献号
申请公布号 CN 109564660 A
(43)申请公布日 2019.04.02
(30)优先权数据
62/366,119 2016.07.25 US
(85)PCT国际申请进入国家阶段日
2019.01.24
(86)PCT国际申请的申请数据
PCT/US2017/012613 2017.01.06
(87)PCT国际申请的公布数据
WO2018/022131 EN 2018.02.01
(73)专利权人 电信区块链联盟软件公司
地址 美国加利福尼亚州森尼维尔市沃尔夫北街440号
(72)发明人 吴陵
(74)专利代理机构 北京德恒律治知识产权代理有限公司 11409
专利代理师 章社杲 李伟
(51)Int.Cl.
G06Q 20/32(2006.01)
G06Q 20/38(2006.01)
G06Q 40/06(2006.01)
(56)对比文件
US 2016092988 A1,2016.03.31
US 2015262137 A1,2015.09.17
US 2015348017 A1,2015.12.03
US 2016125403 A1,2016.05.05
审查员 康茹

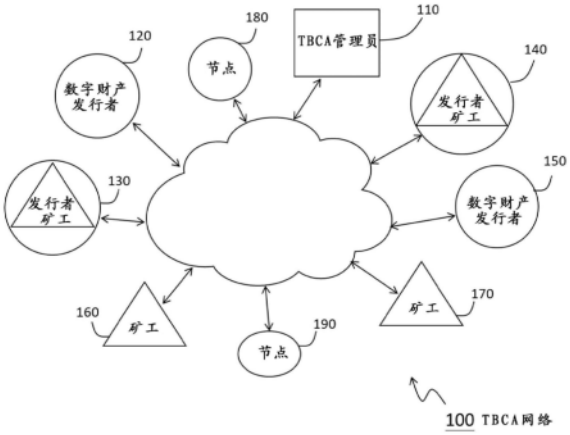
权利要求书6页 说明书8页 附图7页

(54)发明名称

分布式交易共识网络的数字财产管理

(57)摘要

一种管理数字财产的方法和系统,特别是基于分布式交易共识网络中的加密技术,即时清算和结算两个虚拟钱包之间的数字财产的交易,消除与传统结算过程相关的风险、复杂性和时间消耗。每个虚拟钱包只能存储由与虚拟钱包相关的数字财产发行者发行的数字财产。当完成交易时,虚拟钱包拥有者(发件人或收件人)与其相关的数字财产发行者之间的清算和结算不需要额外的操作。



CN 109564660 B

1.一种通过分布式交易共识网络的多个节点实施的方法,其中,所述多个节点包括彼此通信连接且不同的第一数字财产发行者和第二数字财产发行者,该第一数字财产发行者和该第二数字财产发行者均为非货币数字财产发行者,所述方法包括:

(a)通过所述分布式交易共识网络接收交易请求,以将由所述第一数字财产发行者发行的第一类型数字财产从与所述第一数字财产发行者相关的第一虚拟钱包转移至与所述第二数字财产发行者相关的第二虚拟钱包,其中所述第一类型数字财产为包含可辨识所述第一数字财产发行者的第一数据,可借由辨识所述第一数据要求所述第一类型数字财产仅可储存于与所述第一数字财产发行者相关的至少一虚拟钱包,包含所述第一虚拟钱包;

(b)使所述第二虚拟钱包接收由所述第二数字财产发行者发行的第二类型数字财产,其中所述第二类型数字财产包含可辨识所述第二数字财产发行者的第二数据,可借由辨识所述第二数据要求所述第二类型数字财产仅可储存于与所述第二数字财产发行者相关的至少一虚拟钱包,包含所述第二虚拟钱包;以及

(c)在分布式分户账中记录所请求的交易。

2.根据权利要求1所述的方法,其中,所述第一类型数字财产是数字证券、数字债券、数字期货和数字贵金属中的一种,并且所述第二类型数字财产是数字证券、数字债券、数字期货和数字贵金属中的一种。

3.根据权利要求1所述的方法,其中,所述第一类型数字财产与所述第二类型数字财产相同。

4.根据权利要求1所述的方法,其中,所述步骤(b)包括:

(b1)所述第一数字财产发行者将由所述第一数字财产发行者发行的所述第一类型数字财产从第一订户拥有的所述第一虚拟钱包转移至所述第一数字财产发行者拥有的第一虚拟资金库;

(b2)所述第一数字财产发行者将由所述第一数字财产发行者或所述第二数字财产发行者发行的一种或多种选定类型的数字财产从所述第一虚拟资金库转移至由所述第二数字财产发行者拥有的第二虚拟资金库,其中,从所述第一虚拟资金库包含的任何类型的数字财产中选择所述一种或多种选定类型的数字财产;

(b3)所述第二数字财产发行者将由所述第二数字财产发行者发行的所述第二类型数字财产从所述第二虚拟资金库转移至第二订户拥有的所述第二虚拟钱包。

5.根据权利要求1所述的方法,其中,所述步骤(b)包括:

(b1)所述第一数字财产发行者将由所述第一数字财产发行者发行的所述第一类型数字财产从第一订户拥有的所述第一虚拟钱包转移至所述第一数字财产发行者拥有的第一虚拟资金库;

(b2)所述第一数字财产发行者将由所述第一数字财产发行者或所述第二数字财产发行者发行的所述第一类型数字财产从所述第一虚拟资金库转移至所述第二数字财产发行者拥有的第二虚拟资金库;

(b3)所述第二数字财产发行者将由所述第二数字财产发行者发行的所述第二类型数字财产从所述第二虚拟资金库转移至第二订户拥有的所述第二虚拟钱包,其中,所述第二类型数字财产与所述第一类型数字财产相同。

6.根据权利要求5所述的方法,其中,在步骤(b2)中,当所述第一虚拟资金库包含由所

述第二数字财产发行者发行的所述第一类型数字财产时,所述第一数字财产发行者优先从所述第一虚拟资金库将由所述第二数字财产发行者发行的所述第一类型数字财产转移至所述第二虚拟资金库;并且当所述第一虚拟资金库不包含由所述第二数字财产发行者发行的所述第一类型数字财产的请求金额时,所述第一数字财产发行者从所述第一虚拟资金库将由所述第一数字财产发行者发行的所述第一类型数字财产的剩余金额转移至所述第二虚拟资金库。

7.根据权利要求5所述的方法,其中,所述第二数字财产发行者设置持有由所述第一数字财产发行者发行的所述第一类型数字财产的风险限额。

8.根据权利要求7所述的方法,其中,当所述交易使所述第二数字财产发行者持有由所述第一数字财产发行者发行的所述第一类型数字财产比由所述第二数字财产发行者设置的所述风险限额更多的金额时,拒绝所述交易请求。

9.根据权利要求7所述的方法,其中,当用于转移由所述第一数字财产发行者发行的第一类数字财产的私钥被盗或丢失时,将所述第二数字财产发行者的持有由所述第一数字财产发行者发行的所述第一类型数字财产的风险限额设置为零。

10.根据权利要求1所述的方法,其中,所述第一虚拟钱包能够存储由所述第一数字财产发行者发行的一种或多种类型的数字财产,但不存储由所述第二数字财产发行者发行的任何类型的数字财产;并且所述第二虚拟钱包能够存储由所述第二数字财产发行者发行的一种或多种类型的数字财产,但不存储由所述第一数字财产发行者发行的任何类型的数字财产。

11.根据权利要求1所述的方法,还包括:

(d)由所述第一数字财产发行者向所述第一虚拟钱包收取第一交易费用;以及

(e)由所述第二数字财产发行者向所述第二虚拟钱包收取第二交易费用。

12.根据权利要求4所述的方法,其中,所述分布式交易共识网络具有管理员。

13.根据权利要求12所述的方法,还包括:由所述管理员向所述第一虚拟资金库或所述第二虚拟资金库收取第四交易费用。

14.根据权利要求13所述的方法,其中,所述管理员授权所述第一数字财产发行者或所述第二数字财产发行者发行一种或多种类型的数字财产。

15.根据权利要求1所述的方法,其中,所述第一数字财产发行者和所述第二数字财产发行者中的每一个是银行、投资机构、贸易机构和电信运营商中的一个。

16.根据权利要求1所述的方法,其中,所述分布式分户账使用区块链数据结构。

17.根据权利要求1所述的方法,其中,所述第一虚拟钱包对应于第一电话号码,并且所述第二虚拟钱包对应于第二电话号码。

18.一种计算机可读媒介,包括一个或多个其中嵌入有用于控制数字财产管理系统的计算机可读程序代码的计算机可用的非暂时性介质,所述计算机可读程序代码被配置为使所述数字财产管理系统在具有多个节点的分布式交易共识网络中执行交易流程,所述多个节点包括彼此通信连接且不同的第一数字财产发行者和第二数字财产发行者,该第一数字财产发行者和该第二数字财产发行者均为非货币数字财产发行者,所述流程包括:

(a)通过所述分布式交易共识网络接收交易请求,以将由所述第一数字财产发行者发行的第一类型数字财产从与所述第一数字财产发行者相关的第一虚拟钱包转移至与所述

第二数字财产发行者相关的第二虚拟钱包,其中所述第一类型数字财产为包含可辨识所述第一数字财产发行者的第一数据,可借由辨识所述第一数据要求所述第一类型数字财产仅可储存于与所述第一数字财产发行者相关的至少一虚拟钱包,包含所述第一虚拟钱包;

(b)使所述第二虚拟钱包接收由所述第二数字财产发行者发行的第二类型数字财产,其中所述第二类型数字财产包含可辨识所述第二数字财产发行者的第二数据,可借由辨识所述第二数据要求所述第二类型数字财产仅可储存于与所述第二数字财产发行者相关的至少一虚拟钱包,包含所述第二虚拟钱包;以及

(c)在分布式分户账中记录所请求的交易。

19.根据权利要求18所述的计算机可读媒介,其中,所述步骤(b)包括:

(b1)所述第一数字财产发行者将由所述第一数字财产发行者发行的所述第一类型数字财产从第一订户拥有的所述第一虚拟钱包转移至所述第一数字财产发行者拥有的第一虚拟资金库;

(b2)所述第一数字财产发行者将由所述第一数字财产发行者或所述第二数字财产发行者发行的一种或多种选定类型的数字财产从所述第一虚拟资金库转移至由所述第二数字财产发行者拥有的第二虚拟资金库,其中,从所述第一虚拟资金库包含的任何类型的数字财产中选择所述一种或多种选定类型的数字财产;

(b3)所述第二数字财产发行者将由所述第二数字财产发行者发行的所述第二类型数字财产从所述第二虚拟资金库转移至第二订户拥有的所述第二虚拟钱包。

20.一种通过分布式交易共识网络的多个节点实施的方法,其中,所述多个节点包括彼此通信连接且不同的第一电信运营商和第二电信运营商,该第一电信运营商和该第二电信运营商均为非货币数字财产发行者,所述方法包括:

(a)通过所述分布式交易共识网络接收交易请求,以将由所述第一电信运营商发行的第一类型数字财产从对应于第一电话号码的第一虚拟钱包转移至对应于第二电话号码的第二虚拟钱包,其中所述第一类型数字财产包含可辨识所述第一电信运营商的第一数据,可借由辨识所述第一电信运营商的数据要求所述第一类型数字财产仅可储存于与所述第一电信运营商相关的至少一虚拟钱包,包含所述第一虚拟钱包;

(b)使所述第二虚拟钱包接收由所述第二电信运营商发行的第二类型数字财产,其中所述第二类型数字财产包含可辨识所述第二电信运营商的第二数据,可借由辨识所述第二数据要求所述第二类型数字财产仅可储存于与所述第二电信运营商相关的至少一虚拟钱包,包含所述第二虚拟钱包;以及

(c)在分布式分户账中记录所请求的交易。

21.根据权利要求20所述的方法,其中,所述步骤(b)包括:

(b1)所述第一电信运营商将由所述第一电信运营商发行的所述第一类型数字财产从第一订户拥有的所述第一虚拟钱包转移至所述第一电信运营商拥有的第一虚拟资金库;

(b2)所述第一电信运营商将由所述第一电信运营商或由所述第二电信运营商发行的一种或多种选定类型的数字财产从所述第一虚拟资金库转移至所述第二电信运营商拥有的第二虚拟资金库,其中,从所述第一虚拟资金库包含的任何类型的数字财产中选择所述一种或多种选定类型的数字财产;

(b3)所述第二电信运营商将由所述第二电信运营商发行的所述第二类型数字财产从

所述第二虚拟资金库转移至第二订户拥有的所述第二虚拟钱包。

22.根据权利要求20所述的方法,其中,所述第一电话号码与所述第一电信运营商相关,并且所述第二电话号码与所述第二电信运营商相关。

23.一种数字财产管理系统,包括:

具有多个节点的分布式交易共识网络,其中,所述多个节点包括彼此通信连接且不同的第一数字财产发行者和第二数字财产发行者,该第一数字财产发行者和该第二数字财产发行者均为非货币数字财产发行者;

与所述第一数字财产发行者相关的第一虚拟钱包;

与所述第二数字财产发行者相关的第二虚拟钱包;

其中,在所述分布式交易共识网络接收到交易请求之后,所述第一数字财产发行者将由所述第一数字财产发行者发行的第一类型数字财产从所述第一虚拟钱包转移至所述第二虚拟钱包、使所述第二虚拟钱包接收由所述第二数字财产发行者发行的第二类型数字财产、并且在分布式分户账中记录所请求的交易;

其中所述第一类型数字财产为包含可辨识所述第一数字财产发行者的第一数据,可借由辨识所述第一数据要求所述第一类型数字财产仅可储存于与所述第一数字财产发行者相关的至少一虚拟钱包,包含所述第一虚拟钱包,所述第二类型数字财产包含可辨识所述第二数字财产发行者的第二数据,可借由辨识所述第二数据要求所述第二类型数字财产仅可储存于与所述第二数字财产发行者相关的至少一虚拟钱包,包含所述第二虚拟钱包。

24.根据权利要求23所述的系统,其中,所述第一类型数字财产是数字证券、数字债券、数字期货和数字贵金属中的一种,并且所述第二类型数字财产是数字证券、数字债券、数字期货和数字贵金属中的一种。

25.根据权利要求23所述的系统,其中,所述第一类型数字财产与所述第二类型数字财产相同。

26.根据权利要求23所述的系统,其中:

所述第一数字财产发行者拥有第一虚拟资金库,并且所述第二数字财产发行者拥有第二虚拟资金库;

所述第一数字财产发行者将由所述第一数字财产发行者发行的所述第一类型数字财产从所述第一虚拟钱包转移至所述第一虚拟资金库,并且将由所述第一数字财产发行者或由所述第二数字财产发行者发行的一种或多种选定类型的数字财产从所述第一虚拟资金库转移至所述第二虚拟资金库,其中,从所述第一虚拟资金库包含的任何类型的数字财产中选择所述一种或多种选定类型的数字财产;

所述第二数字财产发行者将由所述第二数字财产发行者发行的所述第二类型数字财产从所述第二虚拟资金库转移至所述第二虚拟钱包。

27.根据权利要求26所述的系统,其中,所述第一类型数字财产与所述第二类型数字财产相同。

28.根据权利要求27所述的系统,其中,当所述第一虚拟资金库包含由所述第二数字财产发行者发行的所述第一类型数字财产时,所述第一数字财产发行者优先从所述第一虚拟资金库将由所述第二数字财产发行者发行的所述第一类型数字财产转移至所述第二虚拟资金库;并且当所述第一虚拟资金库不包含由所述第二数字财产发行者发行的所述第一类

型数字财产的请求金额时,所述第一数字财产发行者从所述第一虚拟资金库将由所述第一数字财产发行者发行的所述第一类型数字财产的剩余金额转移至所述第二虚拟资金库。

29.根据权利要求27所述的系统,其中,所述第二数字财产发行者设置持有由所述第一数字财产发行者发行的所述第一类型数字财产的风险限额。

30.根据权利要求29所述的系统,其中,当所述交易使所述第二数字财产发行者持有由所述第一数字财产发行者发行的所述第一类型数字财产比由所述第二数字财产发行者设置的所述风险限额更多的金额时,所述第二数字财产发行者拒绝所述交易请求。

31.根据权利要求29所述的系统,其中,当用于转移由所述第一数字财产发行者发行的第一类数字财产的私钥被盗或丢失时,所述第二数字财产发行者将持有由所述第一数字财产发行者发行的所述第一类型数字财产的风险限额设置为零。

32.根据权利要求23所述的系统,其中,所述第一虚拟钱包存储由所述第一数字财产发行者发行的一种或多种类型的数字财产,但不存储由所述第二数字财产发行者发行的任何类型的数字财产;并且所述第二虚拟钱包存储由所述第二数字财产发行者发行的一种或多种类型的数字财产,但不存储由所述第一数字财产发行者发行的任何类型的数字财产。

33.根据权利要求23所述的系统,其中:

由所述第一数字财产发行者向所述第一虚拟钱包收取第一交易费用;以及

由所述第二数字财产发行者向所述第二虚拟钱包收取第二交易费用。

34.根据权利要求26所述的系统,其中,所述分布式交易共识网络具有管理员。

35.根据权利要求34所述的系统,其中,由所述管理员向所述第一虚拟资金库或所述第二虚拟资金库收取第四交易费用。

36.根据权利要求34所述的系统,其中,所述管理员授权所述第一数字财产发行者或所述第二数字财产发行者发行一种或多种类型的数字财产。

37.一种数字财产发行者子系统,用于在具有多个节点的分布式交易共识网络中执行数字财产交易,其中,所述多个节点包括彼此通信连接且不同的第一数字财产发行者和第二数字财产发行者,该第一数字财产发行者和该第二数字财产发行者均为非货币数字财产发行者,并且所述第二数字财产发行者是所述第一数字财产发行者的对等节点,所述子系统包括:

与所述第一数字财产发行者相关的第一虚拟钱包;

所述第一数字财产发行者接收交易请求、将由所述第一数字财产发行者发行的第一类型数字财产从所述第一虚拟钱包转移、并且使由所述第二数字财产发行者发行的第二类型数字财产被转移至与所述第二数字财产发行者相关的第二虚拟钱包,其中所述第一类型数字财产为包含可辨识所述第一数字财产发行者的第一数据,可借由辨识所述第一数据要求所述第一类型数字财产仅可储存于与所述第一数字财产发行者相关的至少一虚拟钱包,包含所述第一虚拟钱包,所述第二类型数字财产包含可辨识所述第二数字财产发行者的第二数据,可借由辨识所述第二数据要求所述第二类型数字财产仅可储存于与所述第二数字财产发行者相关的至少一虚拟钱包,包含所述第二虚拟钱包;

其中,所述第一数字财产发行者在分布式分户账中记录所述交易。

38.根据权利要求37所述的子系统,其中,所述第一类型数字财产是数字证券、数字债券、数字期货和数字贵金属中的一种,并且所述第二类型数字财产是数字证券、数字债券、

数字期货和数字贵金属中的一种。

39.根据权利要求37所述的子系统,其中,所述第一类型数字财产与所述第二类型数字财产相同。

40.根据权利要求37所述的子系统,其中:

所述第一数字财产发行者拥有第一虚拟资金库,并且所述第二数字财产发行者拥有第二虚拟资金库;

所述第一数字财产发行者将由所述第一数字财产发行者发行的所述第一类型数字财产从所述第一虚拟钱包转移至所述第一虚拟资金库,并且将由所述第一数字财产发行者或由所述第二数字财产发行者发行的一种或多种选定类型的数字财产从所述第一虚拟资金库转移至所述第二虚拟资金库,其中,从所述第一虚拟资金库包含的任何类型的数字财产中选择所述一种或多种选定类型的数字财产;

所述第二数字财产发行者将由所述第二数字财产发行者发行的所述第二类型数字财产从所述第二虚拟资金库转移至所述第二虚拟钱包。

41.根据权利要求40所述的子系统,其中:

所述第一类型数字财产与所述第二类型数字财产相同。

42.根据权利要求41所述的子系统,其中,当所述第一虚拟资金库包含由所述第二数字财产发行者发行的所述第一类型数字财产时,所述第一数字财产发行者优先从所述第一虚拟资金库将由所述第二数字财产发行者发行的所述第一类型数字财产转移至所述第二虚拟资金库;并且当所述第一虚拟资金库不包含由所述第二数字财产发行者发行的所述第一类型数字财产的请求金额时,所述第一数字财产发行者从所述第一虚拟资金库将由所述第一数字财产发行者发行的所述第一类型数字财产的剩余金额转移至所述第二虚拟资金库。

43.根据权利要求41所述的子系统,其中,所述第二数字财产发行者设置持有由所述第一数字财产发行者发行的所述第一类型数字财产的风险限额。

44.根据权利要求43所述的子系统,其中,当所述交易使所述第二数字财产发行者持有由所述第一数字财产发行者发行的所述第一类型数字财产比由所述第二数字财产发行者设置的所述风险限额更多的金额时,所述第二数字财产发行者拒绝所述交易请求。

45.根据权利要求43所述的子系统,其中,当用于转移由所述第一数字财产发行者发行的第一类数字财产的私钥被盗或丢失时,所述第二数字财产发行者将持有由所述第一数字财产发行者发行的所述第一类型数字财产的风险限额设置为零。

分布式交易共识网络的数字财产管理

[0001] 相关申请

[0002] 本申请要求于2016年7月25日申请的、临时申请号为62/366,119,题目为“基于区块链联盟的多币种清算和结算”的权益,其全部结合于此作为参考。

技术领域

[0003] 本发明总体涉及用于数字财产管理的系统、装置、计算机可读介质和方法,包括使用分布式交易共识网络中的加密技术的清算和结算交易。

背景技术

[0004] 金融交易的清算和结算既耗时又昂贵,特别是涉及国际交易。传统地,金融机构依靠中央清算所来处理清算和结算。加密货币合法的国家在2009年引入加密货币之后的近几年,在分散式、分布式的和对等网络中使用加密货币的相对快速的清算和结算变得可用,但是仍然没有被广泛采用。从那时起,许多加密货币已经变得可用。

发明内容

[0005] 本发明针对用于数字财产管理的方法和相关装置以及计算机可读介质,包括使用分布式交易共识网络中的加密技术来清算和结算数字财产的交易。

[0006] 本发明的目的是立即清算和结算两个虚拟钱包,即,第一数字财产发行者的客户拥有的第一虚拟钱包和第二数字财产发行者的客户拥有的第二虚拟钱包之间的交易,该第一数字财产发行者和该第二数字财产发行者均为非货币数字财产发行者。每个数字财产发行者都可以发行自己的数字财产。然而,每个虚拟钱包只能存储由与虚拟钱包相关的数字财产发行者发行的数字财产。因此,当完成交易时,虚拟钱包拥有者(作为发送者或接收者的客户)与其相关的数字财产发行者之间的清算和结算不需要额外的操作。一旦完成交易,则虚拟钱包拥有者可以立即花费他/她的数字财产或按照他或她的意愿将其转换为实质财产,而无需等待清算和结算。

[0007] 将在随后的描述中阐述本发明的附加特征和优势,并且部分地将从描述中显而易见,或可以通过本发明的实践来学习。通过书面描述及其权利要求以及附图中具体指出的结构和方法,将实现和获得本发明的目的和其它优势。

[0008] 为了实现这些和/或其它目的,如具体实施和广泛描述的,本发明提供了一种在分布式交易共识网络中应用的方法。该方法包括:(a)通过分布式交易共识网络接收交易请求,以将由第一数字财产发行者发行的第一类型数字财产从与第一数字财产发行者相关的第一虚拟钱包转移至与第二数字财产发行者相关的第二虚拟钱包,(b)使第二虚拟钱包接收由第二数字财产发行者发行的第二类型数字财产;以及(c)在分布式分户账中记录所请求的交易。第一类型数字财产可以与第二类型数字财产相同。

[0009] 此外,本发明提供了3个子交易流程以完成两个虚拟钱包之间的交易,其包括(b1)将由第一数字财产发行者发行的第一类型数字财产从第一订户拥有的第一虚拟钱包转移

至第一数字财产发行者拥有的第一虚拟资金库;(b2)将由第一数字财产发行者或第二数字财产发行者发行的第一类型数字财产从第一虚拟资金库转移至第二数字财产发行者拥有的第二虚拟资金库;以及(b3)将由第二数字财产发行者发行的第二类型数字财产从第二虚拟资金库转移至第二订户拥有的第二虚拟钱包。

[0010] 应当理解,先前的总体描述和以下的详细描述都是示例性和说明性的,并且旨在提供对要求保护的本发明的进一步说明

附图说明

[0011] 图1是示出分布式交易共识网络的示意图。

[0012] 图2是示出上述网络的示例性节点的框图。

[0013] 图3是示出非货币数字财产发行者、虚拟资金库、订户和虚拟钱包的框图。

[0014] 图4是示出示例性网络器件的示意图。

[0015] 图5A至图5C是示出用于发行非货币数字财产交易的数据结构的实例的表。

[0016] 图6A至图6C是示出用于两个虚拟钱包之间的非货币数字财产汇拨交易的数据结构的实例的表。

具体实施方式

[0017] 在下面给出的描述中使用的术语旨在以其最广泛的合理方式解释,即使其与该技术的某些特定实施例的详细描述结合使用。以下甚至可以强调某些术语;但是,任何旨在以任何受限方式解释的术语将在本具体描述部分中具体定义。

[0018] 下面介绍的实施例可以通过由软件和/或固件编程或配置的可编程电路实现,或完全通过专用电路实现,或通过这些形式的组合实现。这种专用电路(如果存在的话)可以是例如一个或多个专用集成电路(ASIC)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)等的形式。

[0019] 描述的实施例涉及一个或多个方法、系统、装置和存储处理器可执行流程步骤的计算机可读介质以管理数字财产,包括基于分布式交易共识网络中的加密技术,立即清算和结算两个虚拟钱包之间的数字财产的交易,以消除与传统清算和结算程序相关的风险、复杂性和时间消耗。可以使用本领域普通技术人员已知的各种加密算法。

[0020] 在一个实施例中,如图1所示,使用加密技术实现了本公开中称为TBCA(BlockChain Alliance,区块链联盟)网络的分布式交易共识网络100以管理数字财产,具体地,以大大简化交易的清算和结算流程。TBCA网络100包括多个节点,包括管理员110、数字财产发行者120、130、140、150、和其它节点180、190。如图2所示,每个节点通常包括实施计算和执行程序的处理器;用于存储软件、程序和数据的存储器;用于与用户通信的显示器;用于与用户和其它器件通信的输入/输出组件,以及经由布线或无线信道与网络连接的网络组件。

[0021] 管理员110(在本公开中称为TBCA)设置规则并且管理TBCA网络100。管理员110可以允许节点加入分布式交易共识网络100(TBCA网络)并且成为网络的成员。此外,管理员110(TBCA)可以授权非货币数字财产发行者120至150发行各种数字财产,诸如数字证券、数字债券、数字期货和数字贵金属。

[0022] 非货币数字财产发行者,例如120、150,可以发行自己的数字财产。在一个实施例中,非货币数字财产发行者可以是银行,例如美国银行(“BOA”)或大通银行;投资/贸易机构,例如富达或高盛;或电信运营商,例如AT&T Inc.(ATT),软银集团(SBT)。在一个实施例中,数字财产可以是数字证券、数字债券、数字期货和数字贵金属中的任何一种。如图3所示,非货币数字财产发行者120、150可以分别具有虚拟资金库121、151,以存储由其自身、其它非货币数字财产发行者或管理员110发行的各种数字财产。每个虚拟资金库均具有虚拟资金库ID,这在一些实施例中可以是虚拟资金库地址。此外,每个虚拟资金库均都有公钥和私钥。为了花费存储在虚拟资金库中的数字财产,非货币数字财产发行者必须使用与虚拟资金库相关的私钥来签署交易。

[0023] 分布式分户账本质上是可以在各个站点、地理位置或机构中的多个节点的整个分布式交易共识网络上被共享的数字财产数据库或数据结构。网络内的所有节点都可以具有自己的分户账副本。对分户账的任何改变都会在几分钟内(或在某些情况下几秒钟内)反映在所有副本中。存储在分户账中的数字财产的安全性和准确性通过使用密钥和签名以加密方式进行维护,以控制谁可以在分布式分户账中执行何种操作。在实施例中,区块链数据结构用于分布式分户账。然而,分布式分户账可以使用本领域普通技术人员已知的任何其它数据结构。

[0024] 为了最大化新块生成的吞吐量,使得TBCA网络100可以即时完成大量交易。非货币数字财产发行者130、140也可以允许其它节点180、190加入TBCA网络100以用于其它功能。例如,它们可以是验证者以验证交易和块,并且然后存储分布式分户账的完整或部分副本。

[0025] 非货币数字财产发行者的客户(称为“订户)可以打开并且拥有与非货币数字财产发行者相关的一个或多个虚拟钱包。每个虚拟钱包均具有虚拟钱包ID,在一些实施例中,该虚拟钱包ID可以是虚拟钱包地址。此外,每个虚拟钱包均具有公钥和私钥。为了花费存储在他或她的虚拟钱包中的数字财产,订户必须使用与虚拟钱包相关的私钥来签署交易。订户可以在一个或多个非货币数字财产发行者处打开并且拥有虚拟钱包。在如图3所示的一个实施例中,为订户(例如个人、投资者和/或贸易者)提供虚拟钱包122、152以存储、发送、接收和管理数字财产,包括多种类型的数字资产、信用和债务,诸如数字证券、数字债券、数字期货和数字贵金属。在一个实施例中,虚拟钱包可以是电子维护的数据文件,其可以包括认证信息、使用规则、子钱包(例如,用于单独维护数字安全相关信息、数字债券相关信息和数字期货相关信息)。此外,订户可以为虚拟钱包建立规则以促进电子交易。

[0026] 每个虚拟钱包122、152均与非货币数字财产发行者120、150相关,并且可以由虚拟钱包ID(或在一些实施例中的地址,例如,1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xq和16ULZUJwv1HZJkFrs8aa9c3xHTjiayyTNS)识别。在一个实施例中,虚拟钱包122只能存储、发送、接收和管理由与虚拟钱包122相关的非货币数字财产发行者120发行的各种数字财产,而不是由其它非货币数字财产发行者发行的数字财产。

[0027] 每笔交易均记录在分布式分户账中,该分布式分户账对TBCA网络100内的其它节点开放。在一个实施例中,分布式分户账包括链中的各块。每个块均由通过SHA256加密算法对块头进行两次散列(hash)形成的块散列(block hash)标识。此外,通过块头中的“先前块散列”字段,将每个块引用回先前的块(称为父块)。因此,散列序列将每个块链接至其父块,以创建一路返回至创建的第一个块的链。当这些块彼此堆叠在一起时,反向交易变得指数

级更难。因此,随着时间的推移,块中记录的交易变得越来越受信任。根据块和交易的大小,平均块可以包含数百笔交易。完整且最新的分布式分户帐存储在管理员、数字财产发行者和其它管理员110允许的节点的数据库(或文件)中,以存储这样的分户帐(“(整节点这)。某些节点可以选择为仅存储这种分户帐的部分。

[0028] 如图3所示,非货币数字财产发行者的客户可以经由网络设备(经由移动、WiFi或有线信道连接至任何互联网连接)(诸如服务器、台式电脑、笔记本电脑、平板电脑、手机、固定电话和PDA)请求由TBCA网络100处理和记录的交易。在一个实施例中,数字财产交易的基本构建块是未花费的交易输出(“UTXO”)。UTXO是由私钥锁定至特定虚拟钱包或虚拟资金库的不可分割的数字财产块,并且可以是任意值。客户的虚拟钱包可以包括来自数百个记录在块中的数百个先前交易的许多UTXO。客户可以请求交易以将特定价值的数字财产转移至餐厅,例如,付餐费。交易可以包括来自客户的虚拟钱包的一个或多个交易输入(输入UTXO)和送至接收虚拟钱包的一个或多个交易输出(输出UTXO),例如,付给餐厅的餐值和找回客户的零钱)。交易输入是指向UTXO的指针,这些指针从先前的交易生成并且之前从未花费过。交易输出是锁定为接收虚拟钱包的UTXO,将来可由其拥有者花费。作为一般规则,交易输入值的总和应等于交易输出值的总和。在常规数字财产交易中不应生成或丢失任何值。例外包括但不限于非货币数字财产发行者用于发行新数字财产的发行交易,以及非货币数字财产发行者用于设置持有由其它非货币数字财产发行者发行的特定类型数字财产的风险限额的风险限额交易。

[0029] 在一个实施例中,将客户的交易请求发送至钱包服务器,该钱包服务器收集所有必要信息并且将其发送至中间件。中间件构造原始交易并且将其发送回钱包服务器,然后钱包服务器使用他或她的虚拟钱包的私钥将其发送至密钥服务器以用于客户签名。钱包服务器将签名的交易传递回中间件,中间件将交易传播至TBCA网络100。钱包服务器、密钥服务器和中间件是便于实现交易的软件。在接收该交易之后,TBCA网络100上的节点(包括非货币数字财产发行者)将独立地检验和验证该交易,并且然后将验证的交易添加至交易库。在进一步传播之前,每个节点使用相同的标准独立验证每笔交易。将创建从交易库中提取交易的新块。在检验并且验证新块之后,然后将新块传播至其它节点。在接收新块之后,TBCA网络100上的节点将使用相同的标准独立地检验和验证新块。一旦节点验证了新块,则节点就会将新块连接至现有的区块链。然后,新拥有者可以花费来自这些交易的输出的UTXO。最终,除非TBCA网络100受到攻击、断开连接或故障,否则TBCA网络100上的每个完整节点均将具有相同分户帐或区块链的副本。要求多个节点(每个节点均利用相同标准的独立地验证相同的交易和/或块)在分布式分户帐上达成协议的共识是增强交易安全性的机制。分布式交易共识网络达成共识需要的节点越多,网络就越安全。是否达成共识可以通过本领域技术人员已知的各种规则和/或算法来确定。在一个实施例中,当发生分叉时,可以通过比较链中的块的长度(或深度)和具有较长链的分叉胜出来达到共识。作为分布式交易共识网络,TBCA网络100需要在每笔交易上均达成共识,然后将每笔交易分别记录在存储在多个节点中的分布式分户帐中。

[0030] 如前所述,每个虚拟钱包均与特定的非货币数字财产发行者相关,该非货币数字财产发行者可以是银行、金融机构、证券交易公司、投资公司、电信运营商等。每个虚拟钱包在TBCA网络100中均具有唯一的虚拟钱包ID。例如,作为订户,Mary可以具有多个虚拟钱包,

每个虚拟钱包均由虚拟钱包ID标识,并且经由账号分别与美国银行(“BOA”)、富达或高盛相关,或经由电话号码与AT&T Inc.(ATT)、软银集团(SBT)相关。在一个实施例中,每个虚拟钱包只能存储由与虚拟钱包相关的数字财产发行者发行的数字财产。例如,Mary的与美国银行相关的虚拟钱包只能存储由美国银行发行的数字财产;Mary的与ATT相关的虚拟钱包只能存储由ATT发行的数字财产。

[0031] 每个数字财产发行者均可以发行各种不同类型的数字财产,诸如数字证券,例如数字Apple股票、数字Google股票和数字共同基金;数字贵金属,例如数字黄金、数字铂金和数字银;和数字期货,例如咖啡豆、大豆和玉米的数字期货。每个数字财产的特征是数字财产的类型和其发行者的组合。在一个实施例中,该组合可以是数字财产类型的符号,以及随后的数字财产发行者的符号,其中英文句号”.”分隔两个符号。在一个实例中,富达(其符号为“FDT”)可以发行数字Apple股票和数字Google股票,在该实施例中,其可以标识为AAPL.FDT(在该实施例中,1AAPL.FDT的价值为1股Apple股票)和GOOG.FDT(在该实施例中,1GOOG.FDT的价值为1股Google股票)。高盛(“GMS”)可以发行具有24克拉纯度的数字黄金(其符号为“GLD999”)和纯度为999的数字铂金(其符号为“PTN999”),在本实施例中,其可以标识为GLD999.GMS(在该实施例中,1GLD999.GMS的价值为具有24克拉纯度的1克黄金)和PTN999.GMS(在该实施例中,1PTN999.GMS的价值为纯度为999的1克铂金)。

[0032] 在一个实施例中,趣味硬币(Favored Coin)(“FC”)字段用于指示数字财产的类型及其发行者。除了数值(或数字财产的量或单位)之外,每个输出UTXO还包括指示数字财产的类型及其发行者的FC字段。

[0033] 非货币数字财产发行者可以确定由其发行的数字财产的实际财务价值。在一个实施例中,数字财产的财务价值只能由其发行者识别。因此,数字财产的拥有者只能对其发行者索取其财务价值。在这样的实施例中,数字财产的功能类似于非货币数字财产发行者对接收数字财产的拥有者或其它非货币数字财产发行者的信用(称为“加密信用”)。

[0034] 每个非货币数字财产发行者均可以具有虚拟资金库以存储由其自身、其它非货币数字财产发行者和管理员110发行的数字财产,包括多种类型的数字资产和债务,例如数字证券、数字债券、数字期货、数字贵金属

[0035] 所描述的实施例可以大大减少两个虚拟钱包之间的交易中的清算和结算的工作力度。因为每个虚拟钱包只能存储由与虚拟钱包相关的非货币数字财产发行者发行的数字财产,所以当完成交易时,虚拟钱包拥有者(发件人或收件人)与其相关的非货币数字财产发行者之间的清算和结算不需要额外的操作。因此,虚拟钱包拥有者在他/她想要花费他/她的数字财产或将其转换为实质财产时不需要等待清算和结算。此外,由于第一非货币数字财产发行者发行并且存储在第二非货币数字财产发行者的虚拟资金库中的数字财产金额仅仅反映了第一非货币数字财产发行者对第二非货币数字财产发行者的债务,反之亦然,因此非货币数字财产发行者之间的清算不需要额外的操作。并且第一非货币数字财产发行者可以随时从第二非货币数字财产发行者处赎回数字财产(由第一非货币数字财产发行者发行),以结算它们之间的负债(如果有的话)。在第二非货币数字财产发行者的虚拟资金库需要将数字财产转移至第一非货币数字财产发行者的虚拟资金库的情况下,如果可能,第二非货币数字财产发行者的虚拟资金库将优先转移由第一非货币数字财产发行者发行的数字财产(抵消);并且然后转移由自身(第二非货币数字财产发行者)发行的数字财产

的剩余金额/价值。因此,如果有的话,第一非货币数字财产发行者和第二非货币数字财产发行者之间的信用或债务将保持在最小数量。通过这种方法,非货币数字财产发行者可以最小化其持有的由其它非货币数字财产发行者发行的数字财产。

[0036] 为了发行数字财产,首先,数字财产发行者必须授予发行特定类型数字财产的许可。在一些情况下,发行许可可以限制要发行的数字财产类型的金额(价值)。在该许可交易中,输出UTXO创建为接收数字财产发行者的虚拟资金库,其中,FC字段指示允许其发行的特定数字财产类型。在构建和签署许可交易之后,中间件将其发送至TBCA网络100,将许可交易记录到新块中。然后,数字财产发行者可以向钱包服务器发送发行请求,然后钱包服务器将必要的信息发送至中间件以生成原始交易。然后将原始交易发送至钱包服务器,钱包服务器将原始交易传递给密钥服务器以虚拟资金库的私钥签署。在原始交易返回之后,中间件将其发送至TBCA网络100。如果非货币数字财产发行者具有适当的发行许可,则将新发行交易记录在块中。否则,发行交易将被拒绝。图5A至图5C示出了发行交易的数据结构及其交易输入和输出的实施例。发行交易具有空输入UTXO列表,因为新的数字财产正在创建。然而,交易输入具有包含可以发行新的数字财产的数字财产发行者的虚拟资金库的签名和公钥的解锁脚本。发行交易的输出UTXO具有指示要发行的数字财产的金额和类型的数值和FC,并且包含将输出UTXO锁定至发行的数字财产发行者的虚拟资金库的脚本。

[0037] 在第二实施例(存款交易)中,为了完成该存款交易,Mary的钱包向钱包服务器发送了两个存款请求,包括第一个存款请求100单位和第二个存款请求1,000单位。将第一个存款请求(包括值为100、FC为20,以及Mary的虚拟钱包ID的信息)发送至中间件,然后中间设备构建原始交易并且将其发送回钱包服务器。钱包服务器将原始交易传递给密钥服务器,以使ATT的虚拟资金库签有其私钥,然后将签名的交易发送回中间件。中间件将签名的存款交易传播至TBCA网络100,该网络100验证存款交易并且将其记录到新块中。第一笔存款交易的输入UTXO是ATT发行交易的输出UTXO。第一笔存款交易有两个输出UTXO。第一笔存款交易的第一个输出UTXO的值为100、FC为20并且具有将该UTXO锁定至Mary的虚拟钱包的脚本。第二个输出UTXO的值为3000、FC为20并且具有将该UTXO锁定至ATT的虚拟资金库的脚本。将第二次存款请求(包括值为1000、FC为21以及Mary的虚拟钱包ID的信息)发送至中间件,然后中间件构建原始交易并且将其发送回钱包服务器。通过类似的流程,TBCA网络100将第二笔存款交易记录到新块中。第二笔存款交易的输入UTXO是来自ATT发行交易的另一输出UTXO。第二笔存款交易也具有两个输出UTXO。第二笔存款交易的第一个输出UTXO的值为1000、FC为21并且具有将该UTXO锁定至Mary的虚拟钱包的脚本。第二个输出UTXO的值为30000、FC为21并且具有将该UTXO锁定至ATT的虚拟资金库的脚本。完成存款交易后,Mary可以立即花费这些输出UTXO。

[0038] 在一个实施例中,Mary想要向Joe发送一些数字财产。Mary可以指定她想从她的虚拟钱包发送给Joe的数字财产的类型和金额。此外,Mary可以指定Joe将接收的数字财产的类型。

[0039] 在上述非货币数字财产汇拨交易中,Mary将其与ATT相关的虚拟钱包中的50单位转移至与SBT相关的Joe的虚拟钱包。要完成该非货币数字财产的汇拨交易,必须整体验证并确认三个子交易(交易集)。如果拒绝一个子交易,则必须拒绝所有三个子交易。图6A至图6C显示出了非货币数字财产汇拨交易的数据结构及非货币数字财产汇拨交易的交易输入

和输出的实施例。第一子交易具有来自Mary的虚拟钱包的输入UTXO(其中,值为100并且FC为20,)以及两个输出UTXO,第一个输出UTXO值为50并且FC为20,锁定至ATT的虚拟资金库,并且第二个输出UTXO(更改回Mary)值为50并且FC为20,锁定至Mary的虚拟钱包。第二子交易具有来自ATT的虚拟资金库的输入UTXO(其中,值为3000并且FC为20)以及两个输出UTXO,第一个输出UTXO值为50并且FC为20,锁定至SBT的虚拟资金库,并且第二个输出UTXO(更改回ATT)值为2,500并且FC为20,锁定至ATT的虚拟资金库。第三子交易具有来自SBT虚拟资金库的输入UTXO(其中,值为4,000并且FC为10),以及两个输出UTXO,第一个输出UTXO值为50并且FC为10,锁定至Joe的虚拟钱包,并且第二个输出UTXO(更改回SBT),值为3,500并且FC为10,锁定至SBT的虚拟资金库。利用所有必要的信息,中间件构建3个原始子交易并且将它们发送至钱包服务器,钱包服务器进一步将它们传递给密钥服务器以获得适当的签名。钱包服务器将3个签名的子交易发送回中间件,中间件将它们传播至TBCA网络100,TBCA网络100检验并且验证这3个子交易,只有在所有三个子交易都经过验证时才会写入新块。然后,新块将传播至其它节点,这将使这些节点用相同的标准独立验证新块。最终,每个节点的分户帐将包括记录汇款交易的新块。Joe可以立即交易新收到的50单位。

[0040] 第四实施例中,ATT可以向Mary收取交易费用,该费用可以从Mary的虚拟钱包中取出的50单位中扣除(Joe将收到更少的单位)或是对Mary的虚拟钱包额外和单独收费。类似地,SBT可以向Joe收取交易费用,该费用可以从Mary收到的单位中扣除(Joe将收到更少的单位),或是对Joe的虚拟钱包额外和单独收费。此外,管理员110(TBCA)可以向ATT和SBT收取交易费用。可以采取若干措施完成交易,其中,交易费用支付给ATT、SBT、和/或管理员。首先,可以相应地调整输入UTXO或输出UTXO的值以反映交易费用。其次,可以将具有交易费用值的一个或多个输出UTXO添加到适当的子交易中。

[0041] 在若干交易之后的某个时间,每个虚拟钱包仍然仅存储由与虚拟钱包相关的非货币数字财产发行者发行的数字财产。然而,非货币数字财产发行者很可能将由其它非货币数字财产发行者发行的数字财产保存在它们自己的虚拟资金库中。在下一笔交易中,当第一数字财产发行者(例如SBT)需要将第一类型数字财产(例如,第一非货币数字财产)转移至第二非货币数字财产发行者(例如,ATT)时,在一个实施例中,第一非货币数字财产发行者(例如,SBT)将优先将由第二非货币数字财产发行者发行的第一类型数字财产转移(返回)回至第二非货币数字财产发行者(例如,ATT)。如果这还不够,那么第一非货币数字财产发行者(例如,SBT)将由自己发行的第一类型数字财产的剩余单位转移至第二非货币数字财产发行者(例如,ATT)。通过这一流程,非货币数字财产发行者可以最小化其持有的由其它非货币数字财产发行者发行的数字财产并且最小化管理持有由其它非货币数字财产发行者发行的大量数字财产的风险。

[0042] 另外,在第七实施例(风险限额交易)中,非货币数字财产发行者可以为由特定非货币数字财产发行者发行的特定类型的数字财产设置风险限额。例如,SBT将ATT发行的非货币数字财产的风险限额设置为1M单位。因此,当交易将使非货币数字财产发行者持有由特定非货币数字财产发行者发行的特定类型的数字财产的金额超过风险限额时,该交易将被拒绝并且不能被记录。例如,如果交易将使SBT持有超过1M单位的ATT发行的非货币数字财产,则该交易将被拒绝。非货币数字财产发行者对由其它非货币数字财产发行者发行的特定类型数字财产的风险限额可以记录在分布式分户账(诸如区块链)中。因此,每个完整

节点(包括非货币数字财产发行者)都具有完整且最新的分布式分户账副本,可以独立验证子交易是否会使非货币数字财产发行者超过其风险限额。如果发生这种情况,将拒绝整个交易集。

[0043] 在一个实施例中,对于非货币数字财产发行者设置的风险限额,非货币数字财产发行者可以向钱包服务器发送设置-风险-限额请求,然后钱包服务器将必要的信息发送至中间件以生成原始交易。然后将原始交易发送至钱包服务器,钱包服务器将原始交易传递给密钥服务器以签署有虚拟资金库的私钥。签名的风险限额交易返回后,中间设备将签名的风险限额交易发送至TBCA网络100以记录到新块中。与发行数字财产交易一样,风险限额交易具有空输入UTXO列表,因为此设置不应使用UTXO。然而,风险限额交易输入具有包含设置风险限额的数字财产发行者的虚拟资金库的签名和公钥的解锁脚本。风险限额交易的输出UTXO具有指示由特定非货币数字财产发行者发行的特定类型的数字财产的最大金额的值和FC,该非货币数字财产发行者将被请求非货币数字财产发行者接受。在SBT将持有ATT发行的非货币数字财产的风险限额设置为100,000单位的实例中,风险限额交易的输出UTXO的值为100,000并且FC为20。该交易必须签有SBT虚拟资金库的私钥。

[0044] 当由特定非货币数字财产发行者发行的特定类型的数字财产受到损害时,例如,数字财产的私钥被盗或丢失,风险限额的设置也可以帮助管理损害并且解决问题。例如,转移一些数字财产的私钥被盗,管理员110可以将由该特定非货币数字财产发行者发行的这种数字财产的所有非货币数字财产发行者的风险限额设置为零,使得之后没有非货币数字财产发行者接收受损的数字财产。在该风险限额交易中,交易输入具有包含管理员110的虚拟资金库的签名和公钥的解锁脚本;交易输出具有值为零且FC为20的UTXO。在这种情况下,管理员110或该特定非货币数字财产发行者(例如,ATT)可以将相关的风险限额设置为零以在受到损害后拒绝特定类型的数字财产的所有交易。然后,该非货币数字财产发行者,例如ATT,可以发行相同类型的数字财产的新版本,根据其订户信息数据库,适当金额的新版数字财产转至其订户的虚拟钱包,以弥补因私钥被盗或丢失而造成的任何损失。

[0045] 同样,上述数字财产交易方法和相关装置可以应用于除数字货币外的所有类型的数字财产,诸如数字证券,例如数字Apple股票、数字Google股票和数字共同基金;数字贵金属,例如数字黄金、数字铂金和数字银;以及数字期货,例如,咖啡豆、大豆和玉米的数字期货。

[0046] 在不脱离本发明的精神或范围的情况下,可以对本发明的数字财产管理方法和相关装置中进行各种修改和变化对于本领域技术人员是显而易见的。因此,本发明旨在覆盖落入所附权利要求及其等同物的范围内的修改和变化。

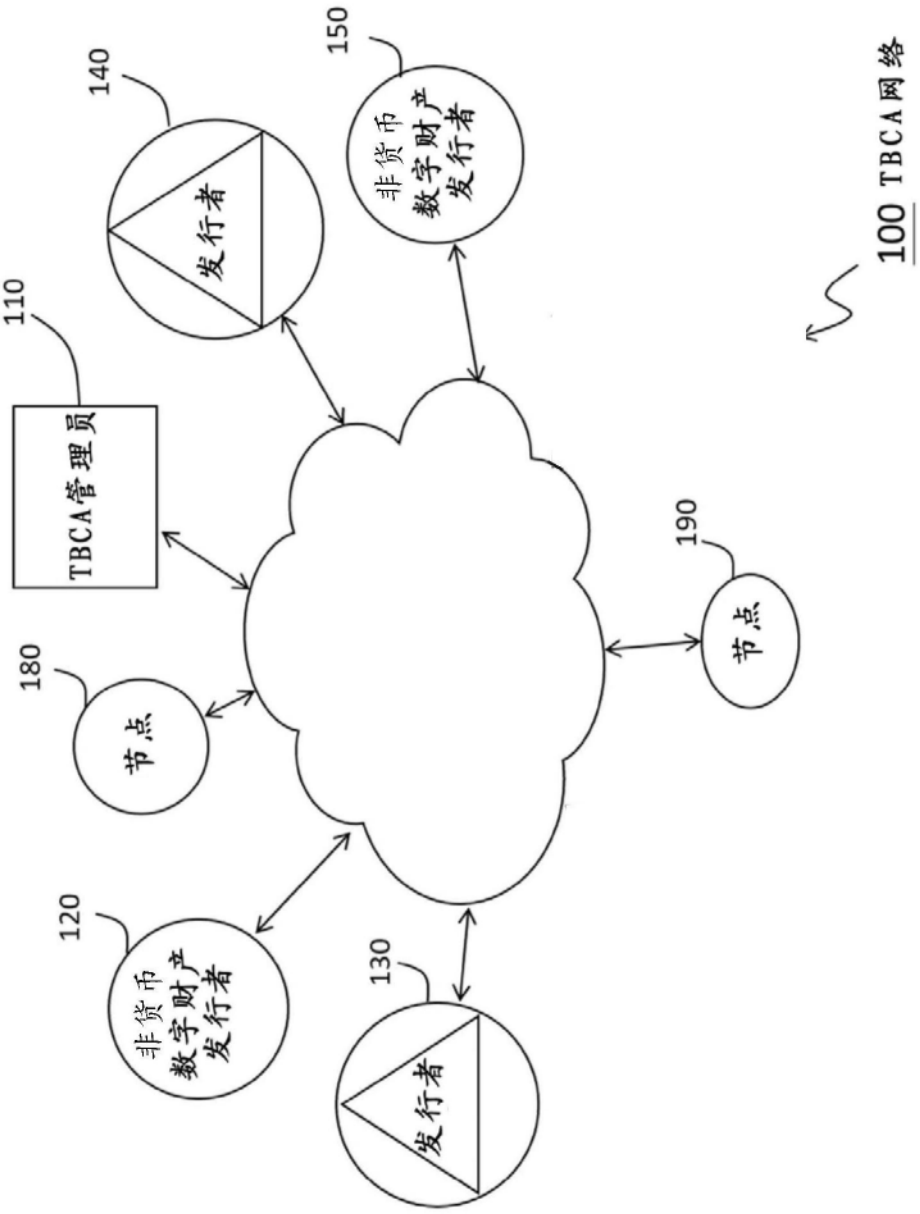

100 TBCA网络
140
发行者
150
非货币
数字财产
发行者
110
TBCA管理员
180
节点
190
节点
120
非货币
数字财产
发行者
130
发行者

图1

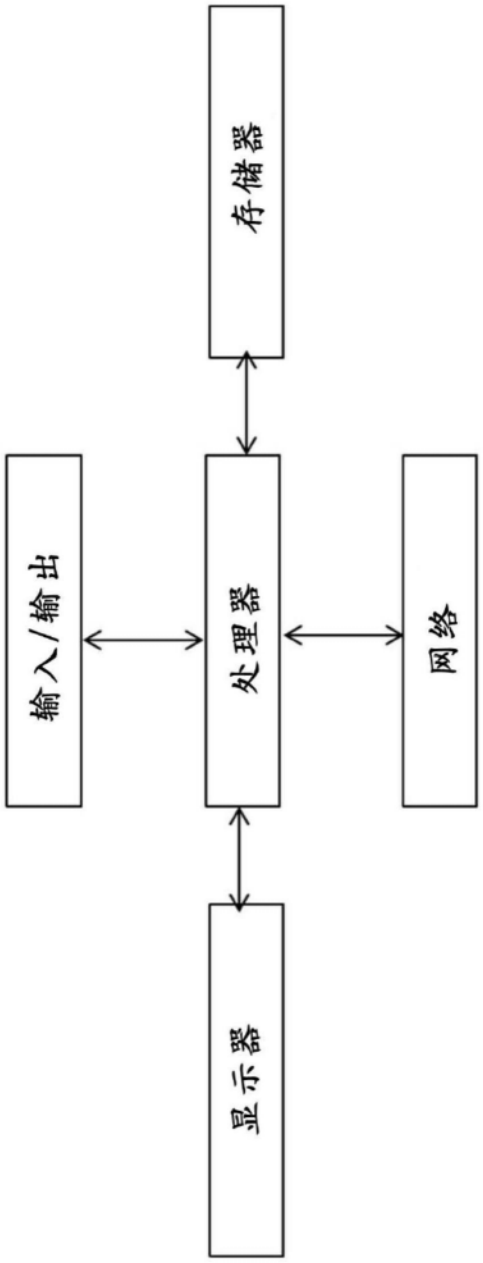


图2

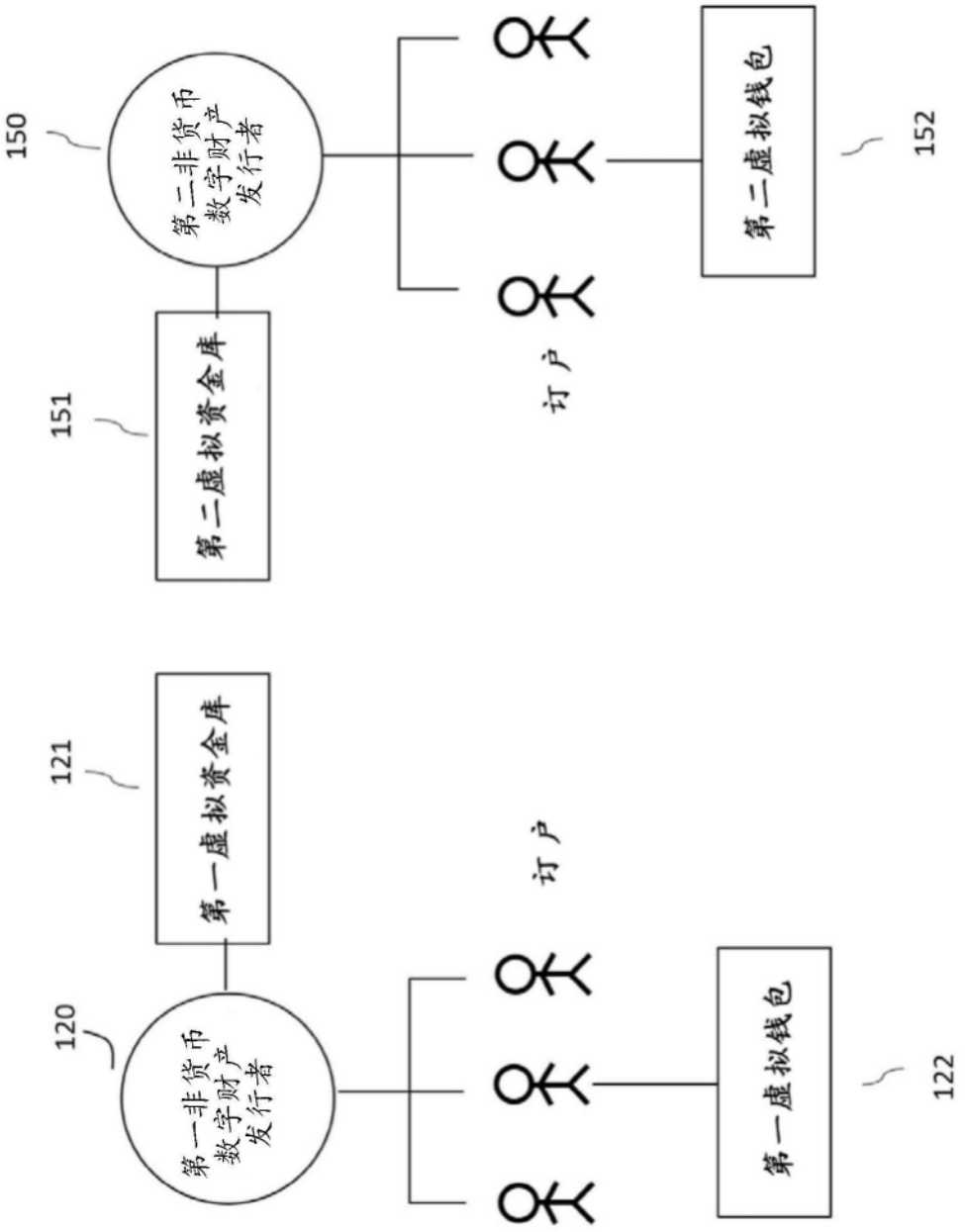

150
第二非货币数字财产发行者
151
第二虚拟资金库
订户
152
第二虚拟钱包
121
第一虚拟资金库
120
第一非货币数字财产发行者
订户
122
第一虚拟钱包

图3

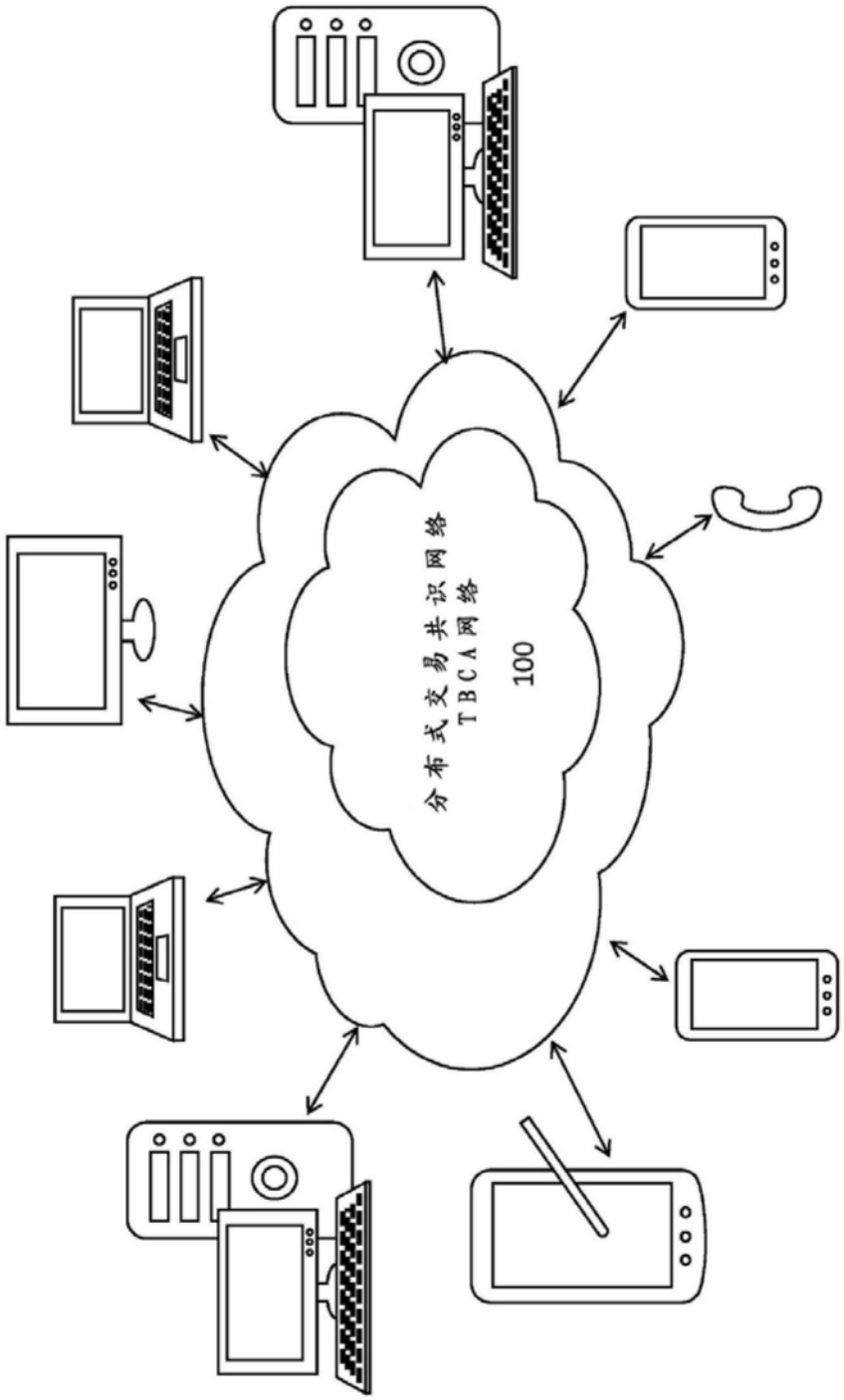


图4

发行交易		
4字节	版本号	1
1字节	包含的输入数量	1
变量	输入序列表	1交易输入
1字节	包含的输入数量	1
变量	输出序列表	1交易输出
4字节	交易最终时的块高度或时间戳	0

图5A

交易输入（发行交易）		
32字节	空白	
4字节	空白	
1-9字节	解锁脚本的大小	正整数
变量	解锁脚本（用于解锁输出中的ScriptPubKey的签名和公钥）	例如:473044220447d5ae4624357f6b1361daac5d3aaeae5e19755'fdf067f42aec5c7a5e51f2204117b06f77809295dd385da9b96567d3dc568e87d622ee37a758c836bb136e1212e0ac817fd21a44b43c6468d71a472e198521fcb66e36663b5a817398 6d7609f
4字节	序列号	0xFFFFFFFF

图5B

交易输出		
8字节	输出值	正整数
4字节	输出的FC（映射至诸如$JPY.SBT的货币）	整数>2，（0 和1保留）
1-9字节	ScriptPubKey的大小	正整数
变量	ScriptPubKey（锁定脚本）	OP_DUP OP_HASH160< 地址 > OP_EQUALVERIFY OP_CHECKSIG

图5C

标准交易		
4字节	版本号	1
1-9字节	包含的输入数量	正整数
变量	输入序列表	交易输入
1-9字节	包含的输出数量	正整数
变量	输出序列表	交易输出
4字节	交易最终时的块高度或时间戳	0

图6A

交易输入（标准交易）		
32字节	先前的交易散列	例如 :1979fe5abb7192c637cfa4c14a1e953ec0f02c54de28c8f82fc21245c0cab8ac
4字节	参考输出偏差（0索引）	非负整数
1-9字节	解锁脚本的大小	正整数
变量	解锁脚本（用于解锁的签名和公钥）	例如473044220447d5ae4624357f6b1361daac5d3aaeae5e197551fdf067f42aec5c7a5e51f2204117b06f77809295dd385da9b96567d3dc568e87d622ee37a758c836bb136e1212e0ac817fd21a44b43c6468d71a472e198521fcb66e36663b5a817398 6d7609f
4字节	序列号	0xFFFFFFFF

图6B

交易输出		
8字节	输出值	正整数
4字节	输出的FC（映射至诸如 GOOG.GMS的货币）	整数>2，（0 和1保留）
1-9字节	ScriptPubKey的大小	正整数
变量	ScriptPubKey（锁定脚本）	OP_DUP OP_HASH160 <地址> OP_EQUALVERIFY OP_CHECKSIG

图6C