(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112348672 A
(43)申请公布日 2021.02.09

(21)申请号 201910726868.2

(22)申请日 2019.08.07

(71)申请人 阿里巴巴集团控股有限公司
地址 开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 刘旸 王晓晴 邓玉明 吴汉卿 曹建农 杨燕妮 江山

(74)专利代理机构 北京思睿峰知识产权代理有限公司 11396
代理人 彭晓雪 赵爱军

(51)Int.Cl.
G06Q 40/04(2012.01)
G06Q 20/40(2012.01)
H04L 29/08(2006.01)

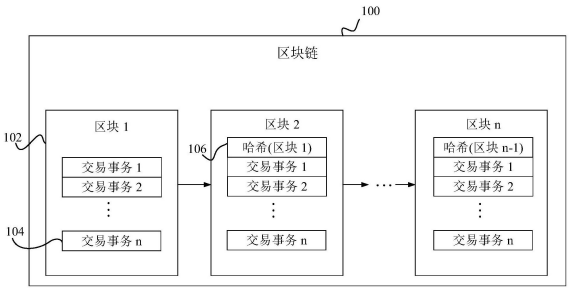
权利要求书5页 说明书17页 附图11页

(54)发明名称

跨链交易方法、装置、多区块链系统及计算设备

(57)摘要

本发明实施例公开了一种跨链交易方法，包括：第一区块链节点接收跨链交易事务，跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务，第一区块链节点存储有第一区块链；将跨链交易事务发送至公证节点，以便公证节点对跨链交易事务进行验证，并在验证通过后将第二交易事务发送至第二区块链节点，第二区块链节点存储有第二区块链；将第一交易事务发送至公证节点，以便公证节点对第一交易事务进行验证，并在验证通过后返回第一交易事务；以及将第一交易事务添加至第一区块链。本发明实施例还公开了相应的跨链交易装置、多区块链系统、计算设备及存储介质。



CN 112348672 A

1.一种跨链交易方法,包括:

第一区块链节点接收跨链交易事务,所述跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务,所述第一区块链节点存储有所述第一区块链;

将所述跨链交易事务发送至公证节点,以便所述公证节点对所述跨链交易事务进行验证,并在验证通过后将所述第二交易事务发送至第二区块链节点,所述第二区块链节点存储有所述第二区块链;

将所述第一交易事务发送至所述公证节点,以便所述公证节点对所述第一交易事务进行验证,并在验证通过后返回所述第一交易事务;以及

将所述第一交易事务添加至所述第一区块链。

2.如权利要求1所述的方法,其中,将所述第一交易事务发送至所述公证节点的步骤包括:

生成包括所述第一交易事务的区块,将所述区块发送至所述公证节点,以便所述公证节点对所述区块包含的数据进行验证,并在验证通过后返回所述区块。

3.如权利要求2所述的方法,其中,将所述第一交易事务添加至所述第一区块链的步骤包括:

将所述公证节点返回的、包括所述第一交易事务的区块广播至其他第一区块链节点,以便进行共识;

在第一区块链节点对所述区块达成共识的情况下,将所述区块添加至所述第一区块链。

4.如权利要求1所述的方法,其中,将所述跨链交易事务发送至公证节点的步骤包括:

生成包括所述跨链交易事务的区块,将所述区块发送至所述公证节点,以便所述公证节点对所述区块包含的数据进行验证,并在验证通过后将所述第二交易事务发送至所述第二区块链节点。

5.如权利要求1所述的方法,其中,将所述第一交易事务发送至所述公证节点的步骤包括:

再次接收所述第一交易事务;

将再次接收到的所述第一交易事务发送至所述公证节点。

6.如权利要求2或4所述的方法,其中,所述第一区块链节点对生成的区块进行签名,所述公证节点在对所述第一区块链节点发送的区块进行验证且验证通过后,对所述区块进行签名。

7.如权利要求1所述的方法,其中,所述公证节点存储有公证区块链,所述公证区块链至少包括所述第一区块链的数据和所述第二区块链的数据,所述区块链节点还存储有所述公证区块链的一部分。

8.一种跨链交易方法,包括:

第二区块链节点接收跨链交易事务中与第二区块链相关的第二交易事务,所述跨链交易事务包括与第一区块链相关的第一交易事务和所述第二交易事务,并由第一区块链节点发送至公证节点,以便所述公证节点将所述第二交易事务发送至所述第二区块链节点,所述第一区块链节点存储有所述第一区块链,所述第二区块链节点存储有所述第二区块链;

将所述第二交易事务发送至所述公证节点，以便所述公证节点对所述第二交易事务进行验证，并在验证通过后返回所述第二交易事务；以及

将所述第二交易事务添加至所述第二区块链。

9.如权利要求8所述的方法，其中，将所述第二交易事务发送至所述公证节点的步骤包括：

生成包括所述第二交易事务的区块，将所述区块发送至所述公证节点，以便所述公证节点对所述区块包含的数据进行验证，并在验证通过后返回所述区块。

10.如权利要求9所述的方法，其中，将所述第二交易事务添加至所述第二区块链的步骤包括：

将所述公证节点返回的、包括所述第二交易事务的区块广播至其他第二区块链节点，以便进行共识；

在第二区块链节点对所述区块达成共识的情况下，将所述区块添加至所述第二区块链。

11.如权利要求8所述的方法，其中，将所述第二交易事务发送至所述公证节点的步骤包括：

将所述第二交易事务发送至对应的第二客户端设备，以便所述第二客户端设备将所述第二交易事务发送至第二区块链节点；

再次接收所述第二交易事务；

将再次接收到的所述第二交易事务发送至所述公证节点。

12.如权利要求9所述的方法，其中，所述第二区块链节点对生成的区块进行签名，所述公证节点在对所述第二区块链节点发送的区块进行验证且验证通过后，对所述区块进行签名。

13.如权利要求8所述的方法，其中，所述公证节点存储有公证区块链，所述公证区块链至少包括所述第一区块链的数据和所述第二区块链的数据，所述区块链节点还存储有所述公证区块链的一部分。

14.一种跨链交易方法，包括：

公证节点接收第一区块链节点发送的跨链交易事务，所述跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务，所述第一区块链节点存储有所述第一区块链；

对所述跨链交易事务进行验证，并在验证通过后将所述第二交易事务发送至第二区块链节点，所述第二区块链节点存储有所述第二区块链；

接收第一区块链节点发送的所述第一交易事务；

对所述第一交易事务进行验证，并在验证通过后将所述第一交易事务返回至所述第一区块链节点，以便所述第一区块链节点将所述第一交易事务添加至所述第一区块链；

接收第二区块链节点发送的所述第二交易事务；以及

对所述第二交易事务进行验证，并在验证通过后将所述第二交易事务返回至所述第二区块链节点，以便所述第二区块链节点将所述第二交易事务添加至所述第二区块链。

15.如权利要求14所述的方法，其中，接收第一区块链节点发送的跨链交易事务的步骤包括：

接收第一区块链节点生成的包括所述跨链交易事务的区块；

对所述跨链交易事务进行验证的步骤包括：

对所述区块包含的数据进行验证。

16.如权利要求15所述的方法，其中，在验证通过后将所述第二交易事务发送至第二区块链节点的步骤包括：

将包括所述跨链交易事务的区块广播至其他公证节点，以便其他公证节点对所述区块包含的数据进行验证；

在超过预定比例的公证节点均对所述区块包含的数据验证通过的情况下，将所述第二交易事务发送至第二区块链节点。

17.如权利要求14所述的方法，其中，接收第一区块链节点发送的所述第一交易事务的步骤包括：

接收第一区块链节点生成的包括所述第一交易事务的区块；

对所述第一交易事务进行验证，并在验证通过后将所述第一交易事务返回至所述第一区块链节点的步骤包括：

对所述区块包含的数据进行验证，并在验证通过后将所述区块返回至所述第一区块链节点，以便所述第一区块链节点将所述区块添加至所述第一区块链。

18.如权利要求14所述的方法，其中，接收第二区块链节点发送的所述第二交易事务的步骤包括：

接收第二区块链节点生成的包括所述第二交易事务的区块；

对所述第二交易事务进行验证，并在验证通过后将所述第二交易事务返回至所述第二区块链节点的步骤包括：

对所述区块包含的数据进行验证，并在验证通过后将所述区块返回至所述第二区块链节点，以便所述第二区块链节点将所述区块添加至所述第二区块链。

19.如权利要求17或18所述的方法，其中，对所述第一交易事务进行验证，并在验证通过后将所述第一交易事务返回至所述第一区块链节点的步骤、或者对所述第二交易事务进行验证，并在验证通过后将所述第二交易事务返回至所述第二区块链节点的步骤还包括：

将所述区块广播至其他公证节点，以便其他公证节点对所述区块包含的数据进行验证；

在超过预定比例的公证节点均对所述区块包含的数据验证通过的情况下，将所述区块返回至所述区块链节点。

20.如权利要求15-18中任一项所述的方法，其中，所述区块链节点对生成的区块进行签名，所述公证节点在对所述区块链节点发送的区块进行验证且验证通过后，对所述区块进行签名。

21.如权利要求14所述的方法，其中，还包括：

对于接收到的、所述区块链节点生成的区块，所述公证节点记录所述区块包含的数据、发送所述区块的节点数据和/或所述区块所涉及的跨链数据；

将所记录的数据添加至所述公证节点存储的公证区块链。

22.如权利要求21所述的方法，其中，将所记录的数据添加至所述公证节点存储的公证区块链的步骤包括：

基于所记录的数据生成区块，并广播至其他公证节点，以便进行共识；

在公证节点对所述区块达成共识的情况下，将所述区块添加至所述公证区块链。

23.如权利要求14所述的方法，其中，所述区块链节点存储有所述公证区块链的一部分。

24.一种跨链交易装置，包括：

存储模块，适于存储第一区块链；

通信模块，适于接收跨链交易事务，所述跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务；还适于将所述跨链交易事务发送至公证节点，以便所述公证节点对所述跨链交易事务进行验证，并在验证通过后将所述第二交易事务发送至第二区块链节点，所述第二区块链节点存储有所述第二区块链；还适于将所述第一交易事务发送至所述公证节点，以便所述公证节点对所述第一交易事务进行验证，并在验证通过后返回所述第一交易事务；以及

处理模块，适于将所述第一交易事务添加至所述第一区块链。

25.一种跨链交易装置，包括：

存储模块，适于存储第二区块链；

通信模块，适于接收跨链交易事务中与第二区块链相关的第二交易事务，所述跨链交易事务包括与第一区块链相关的第一交易事务和所述第二交易事务，并由第一区块链节点发送至公证节点，所述第一区块链节点存储有所述第一区块链；还适于将所述第二交易事务发送至所述公证节点，以便所述公证节点对所述第二交易事务进行验证，并在验证通过后返回所述第二交易事务；以及

处理模块，适于在所述公证节点返回所述第二交易事务后，将所述第二交易事务添加至所述第二区块链。

26.一种跨链交易装置，包括：

存储模块，适于存储公证区块链；

通信模块，适于接收第一区块链节点发送的跨链交易事务，所述跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务，所述第一区块链节点存储有所述第一区块链；还适于接收第一区块链节点发送的所述第一交易事务；还适于接收第二区块链节点发送的所述第二交易事务；以及

数据验证模块，适于对所述跨链交易事务进行验证，并在验证通过后经由所述通信模块将所述第二交易事务发送至第二区块链节点，所述第二区块链节点存储有所述第二区块链；还适于对所述第一交易事务进行验证，并在验证通过后将所述第一交易事务返回至所述第一区块链节点，以便所述第一区块链节点将所述第一交易事务添加至所述第一区块链；还适于对所述第二交易事务进行验证，并在验证通过后将所述第二交易事务返回至所述第二区块链节点，以便所述第二区块链节点将所述第二交易事务添加至所述第二区块链。

27.一种多区块链系统，包括：

第一区块链系统，包括第一客户端设备和第一区块链节点，所述第一客户端设备存储有第一区块链或者其一部分，所述第一区块链节点存储有所述第一区块链，并包括如权利要求24所述的跨链交易装置；

第二区块链系统,包括第二客户端设备和第二区块链节点,所述第二客户端设备存储有第二区块链或者其一部分,所述第二区块链节点存储有所述第二区块链,并包括如权利要求25所述的跨链交易装置;以及

公证区块链系统,包括至少一个公证节点,所述公证节点存储有公证区块链,并包括如权利要求26所述的跨链交易装置,所述公证区块链至少包括所述第一区块链和所述第二区块链的数据,所述第一区块链节点和所述第二区块链节点还存储有所述公证区块链的一部分。

28.如权利要求27所述的系统,其中,所述公证节点至少由所述第一区块链节点和所述第二区块链节点投票产生。

29.一种计算设备,包括:

一个或多个处理器;和

存储器;

一个或多个程序,其中所述一个或多个程序存储在所述存储器中并被配置为由所述一个或多个处理器执行,所述一个或多个程序包括用于执行根据权利要求1-23所述方法中的任一方法的指令。

30.一种存储一个或多个程序的计算机可读存储介质,所述一个或多个程序包括指令,所述指令当计算设备执行时,使得所述计算设备执行根据权利要求1-23所述方法中的任一方法。

跨链交易方法、装置、多区块链系统及计算设备

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种跨链交易方法、装置、多区块链系统及计算设备。

背景技术

[0002] 区块链(blockchain)是存储交易列表的数据结构，并且可以被看作记录(一个或多个)源标识符与(一个或多个)目的地标识符之间的交易的分布式电子账本(ledger)。由于具有去中心化、公开透明、各节点均可以参与记账、存储在区块链中的数据具备不可篡改、并且各节点之间可以快速的进行数据同步的特性，利用区块链技术来搭建去中心化系统，并在区块链的分布式数据库中收录各种执行程序进行自动执行，已在众多的领域中广泛的进行应用。

[0003] 现今，主流的区块链系统均为单链系统，其所有对区块链的操作均实现在一条区块链上。这种单链系统存在很多不足，如系统的吞吐量，安全性，灵活性等。不论对于公有链还是私有链，跨链技术就是实现多区块链间价值的关键，是区块链向外拓展和连接的桥梁。

[0004] 如何管理多条区块链、实现跨区块链间的交易，一种可能的、较直接的解决方案是将所有区块链的数据融合为一条新的区块链进行统一管理。但是，这种解决方法一方面会使得原有各条区块链所对应的不同组成机构(如不同供应链、不同企业或组织)失去自身的管理自主性。另一方面，新的区块链在融合多条链的数据后，会要求区块链中的所有节点拥有更大的数据存储空间以存储其他链的数据。这对系统使用者的网络带宽和存储空间提出了更高的要求。

[0005] 另一种可行的方案是设计区块链之间的跨链协议。然而所涉及到的区块链数量越多会导致需要设计大量协议，这样系统不够灵活，并且该跨链协议仅支持单链对单链的跨链，无法达成多链间的跨链。如果要设计多链间的跨链协议，协议复杂度会更高，且单链需要维护的跨链协议也会更繁琐。

[0006] 因此，需要一种更为先进的多区块链系统方案，以便对多条区块链进行管理、实现跨区块链间的交易。

发明内容

[0007] 为此，本发明实施例提供一种跨链交易方法、装置、多区块链系统及计算设备，以力图解决或至少缓解上面存在的问题。

[0008] 根据本发明实施例的一个方面，提供了一种跨链交易方法，包括：第一区块链节点接收跨链交易事务，跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务，第一区块链节点存储有第一区块链；将跨链交易事务发送至公证节点，以便公证节点对跨链交易事务进行验证，并在验证通过后将第二交易事务发送至第二区块链节点，第二区块链节点存储有第二区块链；将第一交易事务发送至公证节点，以便公证节点对第一交易事务进行验证，并在验证通过后返回第一交易事务；以及将第一交易事

务添加至第一区块链。

[0009] 可选地，在根据本发明实施例的方法中，将第一交易事务发送至公证节点的步骤包括：生成包括第一交易事务的区块，将区块发送至公证节点，以便公证节点对区块包含的数据进行验证，并在验证通过后返回区块。

[0010] 可选地，在根据本发明实施例的方法中，将第一交易事务添加至第一区块链的步骤包括：将公证节点返回的、包括第一交易事务的区块广播至其他第一区块链节点，以便进行共识；在第一区块链节点对区块达成共识的情况下，将区块添加至第一区块链。

[0011] 可选地，在根据本发明实施例的方法中，将跨链交易事务发送至公证节点的步骤包括：生成包括跨链交易事务的区块，将区块发送至公证节点，以便公证节点对区块包含的数据进行验证，并在验证通过后将第二交易事务发送至第二区块链节点。

[0012] 可选地，在根据本发明实施例的方法中，将第一交易事务发送至公证节点的步骤包括：再次接收第一交易事务；将再次接收到的第一交易事务发送至公证节点。

[0013] 根据本发明实施例的另一个方面，提供了一种跨链交易方法，包括：第二区块链节点接收跨链交易事务中与第二区块链相关的第二交易事务，跨链交易事务包括与第一区块链相关的第一交易事务和第二交易事务，并由第一区块链节点发送至公证节点，以便公证节点将第二交易事务发送至第二区块链节点，第一区块链节点存储有第一区块链，第二区块链节点存储有第二区块链；将第二交易事务发送至公证节点，以便公证节点对第二交易事务进行验证，并在验证通过后返回第二交易事务；将第二交易事务添加至第二区块链。

[0014] 根据本发明实施例的另一个方面，提供了一种跨链交易方法，包括：公证节点接收第一区块链节点发送的跨链交易事务，跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务，第一区块链节点存储有第一区块链；对跨链交易事务进行验证，并在验证通过后将第二交易事务发送至第二区块链节点，第二区块链节点存储有第二区块链；接收第一区块链节点发送的第一交易事务；对第一交易事务进行验证，并在验证通过后将第一交易事务返回至第一区块链节点，以便第一区块链节点将第一交易事务添加至第一区块链；接收第二区块链节点发送的第二交易事务；以及对第二交易事务进行验证，并在验证通过后将第二交易事务返回至第二区块链节点，以便第二区块链节点将第二交易事务添加至第二区块链。

[0015] 根据本发明实施例的另一个方面，提供了一种跨链交易装置，包括：存储模块，适于存储第一区块链；通信模块，适于接收跨链交易事务，跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务；还适于将跨链交易事务发送至公证节点，以便公证节点对跨链交易事务进行验证，并在验证通过后将第二交易事务发送至第二区块链节点，第二区块链节点存储有第二区块链；还适于将第一交易事务发送至公证节点，以便公证节点对第一交易事务进行验证，并在验证通过后返回第一交易事务；以及处理模块，适于将第一交易事务添加至第一区块链。

[0016] 根据本发明实施例的另一个方面，提供了一种跨链交易装置，包括：存储模块，适于存储第二区块链；通信模块，适于接收跨链交易事务中与第二区块链相关的第二交易事务，跨链交易事务包括与第一区块链相关的第一交易事务和第二交易事务，并由第一区块链节点发送至公证节点，第一区块链节点存储有第一区块链；还适于将第二交易事务发送至公证节点，以便公证节点对第二交易事务进行验证，并在验证通过后返回第二交易事务；

以及处理模块，适于在公证节点返回第二交易事务后，将第二交易事务添加至第二区块链。

[0017] 根据本发明实施例的另一个方面，提供了一种跨链交易装置，包括：存储模块，适于存储公证区块链；通信模块，适于接收第一区块链节点发送的跨链交易事务，跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务，第一区块链节点存储有第一区块链；还适于接收第一区块链节点发送的第一交易事务；还适于接收第二区块链节点发送的第二交易事务；以及数据验证模块，适于对跨链交易事务进行验证，并在验证通过后经由通信模块将第二交易事务发送至第二区块链节点，第二区块链节点存储有第二区块链；还适于对第一交易事务进行验证，并在验证通过后将第一交易事务返回至第一区块链节点，以便第一区块链节点将第一交易事务添加至第一区块链；还适于对第二交易事务进行验证，并在验证通过后将第二交易事务返回至第二区块链节点，以便第二区块链节点将第二交易事务添加至第二区块链。

[0018] 根据本发明实施例的另一个方面，提供了一种多区块链系统，包括：第一区块链系统，包括第一客户端设备和第一区块链节点，第一客户端设备存储有第一区块链或者其一部分，第一区块链节点存储有第一区块链，并包括根据本发明实施例的跨链交易装置；第二区块链系统，包括第二客户端设备和第二区块链节点，第二客户端设备存储有第二区块链或者其一部分，第二区块链节点存储有第二区块链，并包括根据本发明实施例的跨链交易装置；以及公证区块链系统，包括至少一个公证节点，公证节点存储有公证区块链，并包括根据本发明实施例的跨链交易装置，公证区块链至少包括第一区块链和第二区块链的数据，第一区块链节点和第二区块链节点还存储有公证区块链的一部分。

[0019] 根据本发明实施例的另一个方面，提供了一种计算设备，包括：一个或多个处理器；存储器；以及一个或多个程序，其中一个或多个程序存储在存储器中并被配置为由一个或多个处理器执行，该一个或多个程序包括用于执行根据本发明实施例的方法的指令。

[0020] 根据本发明实施例的还有一个方面，提供了一种存储一个或多个程序的计算机可读存储介质，一个或多个程序包括指令，该指令当被计算设备执行时，使得计算设备执行根据本发明实施例的方法。

[0021] 根据本发明实施例的跨链交易方案，在多个子区块链系统外增设有记录有全部子区块链数据的公证链区块链系统。由子区块链系统的区块链节点进行交易事务的收集、区块的生成及后期通过验证的区块的共识，由公证链系统的公证节点进行区块的合法性和/或有效性验证。这样，保证了多区块链系统中数据、事务的原子性，也充分发挥了区块链节点和公证节点的作用，能让这两种节点互相监督、互相约束，从而降低多区块链系统的中心化程度。

[0022] 其中，根据本发明实施例的跨链交易方案，跨链智能合约部署于公证节点，由公证节点来管理，各子区块链系统不需维护跨链智能合约，极大地降低了管理操作的复杂度。

[0023] 其中，根据本发明实施例的跨链交易方案，在维持了原有子区块链系统的管理自主性的同时，还易于部署(例如在多区块链系统中添加新的子区块链系统)及易于系统升级，提升了多区块链系统的灵活性。

[0024] 其中，根据本发明实施例的跨链交易方案，各个子区块链系统的区块链节点仅存储各自维护的区块链和公证链的一部分，维持了原有系统使用者(交易发起方和交易接受方)对网络带宽及存储空间的要求。同时，对子区块链系统来说，将交易事务的收集、区块的

生成及后期通过验证的区块的共识等分离开，可以有效避免子区块链系统中可能存在的恶意节点的攻击。

[0025] 上述说明仅是本发明实施例技术方案的概述，为了能够更清楚了解本发明实施例的技术手段，而可依照说明书的内容予以实施，并且为了让本发明实施例的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明实施例的具体实施方式。

附图说明

[0026] 为了实现上述以及相关目的，本文结合下面的描述和附图来描述某些说明性方面，这些方面指示了可以实践本文所公开的原理的各种方式，并且所有方面及其等效方面旨在落入所要求保护的主题的范围内。通过结合附图阅读下面的详细描述，本公开的上述以及其它目的、特征和优势将变得更加明显。遍及本公开，相同的附图标记通常指代相同的部件或元素。

[0027] 图1示出了根据本发明一个实施例的区块链100的示意图；

[0028] 图2示出了根据本发明一个实施例的区块链系统200的示意图；

[0029] 图3示出了根据本发明一个实施例的多区块链系统300的示意图；

[0030] 图4示出了根据本发明一个实施例的计算设备400的示意图；

[0031] 图5示出了根据本发明一个实施例的跨链交易方法500的流程图；

[0032] 图6示出了根据本发明一个实施例的跨链交易方法600的流程图；

[0033] 图7示出了根据本发明一个实施例的跨链交易方法700的流程图；

[0034] 图8示出了根据本发明一个实施例的跨链交易方法800的交互流程图；

[0035] 图9示出了根据本发明一个实施例的跨链交易装置900的示意图；

[0036] 图10示出了根据本发明一个实施例的跨链交易装置1000的示意图；以及

[0037] 图11示出了根据本发明一个实施例的跨链交易装置1100的示意图。

具体实施方式

[0038] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0039] 图1示出了根据本发明一个实施例的区块链100的示意图。如图1所示，区块链100可以包括多个区块(block，也称之为数据块)102。区块102是包括诸如支付收据之类的交易事务(transaction)104的数据结构。当新的交易事务104请求提交至区块链100、且通过验证后，可以生成包含此交易数据104的新的区块102并添加至区块链100。每个新区块102可以包括一组经验证的交易数据104和紧接在前的区块102的内容的散列(即哈希)106。例如，区块“2”包括区块“1”的内容的散列，区块“n”包括区块“n-1”的内容的散列等等。比特币(Bitcoin®)和以太坊(Ethereum®)为应用区块链技术的典型示例。

[0040] 图2示出了根据本发明一个实施例的区块链系统200的架构图。该区块链系统200包括多个区块链节点(NODE)。这些区块链节点彼此对等，并通常可以实现为位于一个或多个网络中的计算设备。在一些实施方式中，区块链100分散地存储在多个区块链节点上。每

个区块链节点均可以存储区块链100(也就是账本204)的副本或者其一部分。本领域技术人员可以理解,在不引起歧义的情况下,账本和区块链是可以互相替代的同等概念。

[0041] 账本204包括已经验证并添加到区块链100的区块102。在另一些实施方式中,部分或全部区块链100可以以集中方式存储。

[0042] 如图2所示,区块链节点可以经由通信链路206(例如,有线或无线连接、因特网等)彼此通信,以便发送和接收与账本204相关的数据。例如,当新区块102被添加到账本204时,区块链节点可以经由通信路径206通信或同步此新区块102。

[0043] 图3示出了根据本发明一个实施例的多区块链系统300的示意图。多区块链系统300可以包括多个子区块链系统和公证区块链系统,例如图3所示出的第一区块链系统310、第二区块链系统320和公证区块链系统330。

[0044] 子区块链系统可以包括对应于该子区块链系统的客户端设备和区块链节点。子区块链系统中的区块链节点存储有该子区块链系统维护的区块链,客户端设备则可以存储该子区块系统维护的区块链、或者其一部分(例如区块链的区块头)。此外,子区块链系统中的区块链节点还可以存储公证区块链系统维护的公证区块链的一部分(例如区块头)。

[0045] 每个子区块链系统中的区块链节点可以经由彼此之间的通信路径来进行通信,例如数据同步。每个子区块链系统中的客户端设备可以通过网络与该区块链系统中的区块链节点进行通信。例如,客户端设备可以生成交易事务,并发送给对应的区块链节点。又例如,区块链节点可以将新的区块或者其区块头发送给对应的客户端设备。

[0046] 公证区块链系统可以包括公证节点。公证节点存储有公证区块链系统维护的公证区块链,该公证区块链至少可以包括多区块链系统300内各个子区块链系统维护的区块链的数据。在根据本发明的一个实施方式中,公证节点可以多个子区块链系统中的区块链节点共同投票产生。

[0047] 公证节点可以经由彼此之间的通信路径来进行通信。公证节点还可以通过网络与各个子区块链系统中的区块链节点进行通信。

[0048] 如图3所示,第一区块链系统310包括对应于第一区块链系统310的第一客户端设备311和第一区块链节点312。第二区块链系统320包括对应于第一区块链系统320的第二客户端设备321和第二区块链节点322。公证区块链系统330可以包括公证节点331。

[0049] 公证节点331可以由第一区块链节点312和第二区块链节点322共同投票产生,并存储有公证区块链系统330维护的公证区块链332。公证区块链332至少可以包括第一区块链系统310维护的第一区块链313和第二区块链系统310维护的第二区块链323的数据。

[0050] 第一区块链节点312存储有第一区块链系统310维护的第一区块链313,还可以存储公证区块链332的一部分。第一客户端设备311可以存储第一区块链313、或者第一区块链313的一部分。

[0051] 类似地,第二区块链节点322存储有第二区块链系统320维护的第二区块链323,还可以存储公证区块链332的一部分。第二客户端设备321可以存储第二区块链323、或者第二区块链323的一部分。

[0052] 其中,第一区块链节点312可以经由彼此之间的通信路径来进行通信。第一客户端设备311可以通过网络与第一区块链节点312进行通信。例如,第一区块链系统310的用户可以经由第一客户端设备311向第一区块链节点312发送交易事务,以与第一区块链系统310

的其他用户进行交易。

[0053] 第二区块链节点322可以经由彼此之间的通信路径来进行通信。第二客户端设备321可以通过网络与第二区块链节点322进行通信。例如，第二区块链系统320的用户可以经由第二客户端设备321向第二区块链节点322发送交易事务，以与第二区块链系统320的其他用户进行交易。

[0054] 公证节点331可以经由彼此之间的通信路径来进行通信。公证节点还可以通过网络与第一区块链节点312和第二区块链节点322进行通信。

[0055] 应当指出，公证节点还可以被称为验证节点、仲裁节点、或者可信节点等等，本发明对节点的具体名称不做限制，任何起到类似作用但具有其他名称的节点均在本发明的保护范围之内。

[0056] 根据本发明的实施方式，为了实现不同区块链间的跨链交易事务，第一区块链节点312可以包括跨链交易装置900，第二区块链节点322可以包括跨链交易装置1000，公证节点331可以包括跨链交易装置1100。

[0057] 在根据本发明的实施方式中，上述多区块链系统300中的各部件(节点和设备等等)均可以通过如下所述的计算设备400来实现。

[0058] 图4示出了根据本发明一个实施例的计算设备400的示意图。如图4所示，在基本的配置402中，计算设备400典型地包括系统存储器406和一个或者多个处理器404。存储器总线408可以用于在处理器404和系统存储器406之间的通信。

[0059] 取决于期望的配置，处理器404可以是任何类型的处理器，包括但不限于：微处理器(μP)、微控制器(μC)、数字信息处理器(DSP)或者它们的任何组合。处理器404可以包括诸如一级高速缓存410和二级高速缓存412之类的一个或者多个级别的高速缓存、处理器核心414和寄存器416。示例的处理器核心414可以包括运算逻辑单元(ALU)、浮点数单元(FPU)、数字信号处理核心(DSP核心)或者它们的任何组合。示例的存储器控制器418可以与处理器404一起使用，或者在一些实现中，存储器控制器418可以是处理器404的一个内部部分。

[0060] 取决于期望的配置，系统存储器406可以是任意类型的存储器，包括但不限于：易失性存储器(诸如RAM)、非易失性存储器(诸如ROM、闪存等)或者它们的任何组合。系统存储器406可以包括操作系统420、一个或者多个应用422以及程序数据424。在一些实施方式中，应用422可以布置为在操作系统上由一个或多个处理器404利用程序数据424执行指令。

[0061] 计算设备400还可以包括有助于从各种接口设备(例如，输出设备442、外设接口444和通信设备446)到基本配置402经由总线/接口控制器430的通信的接口总线440。示例的输出设备442包括图形处理单元448和音频处理单元450。它们可以被配置为有助于经由一个或者多个A/V端口452与诸如显示器或者扬声器之类的各种外部设备进行通信。示例外设接口444可以包括串行接口控制器454和并行接口控制器456，它们可以被配置为有助于经由一个或者多个I/O端口458和诸如输入设备(例如，键盘、鼠标、笔、语音输入设备、触摸输入设备)或者其他外设(例如打印机、扫描仪等)之类的外部设备进行通信。示例的通信设备446可以包括网络控制器460，其可以被布置为便于经由一个或者多个通信端口464与一个或者多个其他计算设备462通过网络通信链路的通信。

[0062] 网络通信链路可以是通信介质的一个示例。通信介质通常可以体现为在诸如载波或者其他传输机制之类的调制数据信号中的计算机可读指令、数据结构、程序模块，并且可

以包括任何信息递送介质。“调制数据信号”可以是这样的信号，它的数据集中的一个或者多个或者它的改变可以在信号中编码信息的方式进行。作为非限制性的示例，通信介质可以包括诸如有线网络或者专线网络之类的有线介质，以及诸如声音、射频(RF)、微波、红外(IR)或者其它无线介质在内的各种无线介质。这里使用的术语计算机可读介质可以包括存储介质和通信介质二者。

[0063] 计算设备400可以实现为服务器，例如数据库服务器、应用程序服务器和WEB服务器等，也可以实现为包括桌面计算机和笔记本计算机配置的个人计算机。当然，计算设备400也可以实现为小尺寸便携(或者移动)电子设备的一部分。

[0064] 在根据本发明的实施例中，计算设备400可以实现为跨链交易装置900/1000/1100，并被配置为执行根据本发明实施例的跨链交易方法500/600/700。其中，计算设备400的应用422中包含执行根据本发明实施例的跨链交易方法500/600/700的多条指令，而程序数据424还可以存储多区块链系统300的配置数据等内容。

[0065] 图5示出了根据本发明一个实施例的跨链交易方法500的流程图。跨链交易方法500可以在第一区块链节点312包括的跨链交易装置900中执行。

[0066] 如图5所示，跨链交易方法500始于步骤S510。在步骤S510中，第一区块链节点312接收跨链交易事务。该跨链交易事务由第一客户端设备311生成。在一些实施例中，该第一区块链节点312接收的跨链交易事务可以是由第一客户端设备311发送过来的，也可以是由其他第一区块链节点312广播过来的。

[0067] 可以理解地，跨链交易事务为涉及至少两条区块链的交易事务。因此，一笔跨链交易事务可以分解成分别与该跨链交易事务所涉及的各条区块链相关的多笔交易事务。

[0068] 在本发明的实施方式中，第一客户端设备311生成的跨链交易事务可以包括与第一区块链313相关的第一交易事务和与第二区块链323相关的第二交易事务。其中，交易事务通常可以包括该交易事务的交易对象(例如可以包括付款方和收款方)、交易金额、交易所涉及的区块链标识等等，本发明对此不做限制。

[0069] 例如，假设第一区块链系统310采用货币X，第二区块链系统320采用货币Y，货币X与货币Y之间的汇率为1:10。第一区块链系统310的用户Alice需要向第二区块链系统320的用户Bob转账10个单位的货币X，那么此时在Alice的第一客户端设备生成的跨链交易事务中，第一交易事务为在第一区块链系统310中Alice向Bob汇款10个单位的货币X，第二交易事务为在第二区块链系统320中Bob接受Alice所汇的100个单位的货币Y。

[0070] 而后，在步骤S520中，第一区块链节点312将所接收的跨链交易事务发送至公证节点331，以便公证节点331对该跨链交易事务进行验证，并在验证通过后将该跨链交易事务中的第二交易事务发送至第二区块链节点322。

[0071] 具体地，第一区块链节点312可以生成包括跨链交易事务的区块，将包括跨链交易事务的区块发送至公证节点331。

[0072] 在一些实施例中，第一区块链节点312还可以将所接收的跨链交易事务广播至其他第一区块链节点312。

[0073] 公证节点331接收包括跨链交易事务的区块之后，可以解析该区块，对该区块包含的数据进行验证，从而实现对跨链交易事务的验证。可以理解地，区块包含的数据即为一系列的交易事务。在各种实施例中，公证节点331可以对交易事务的合法性和/或有效性进行

验证。例如，公证节点331可以验证交易事务是否具有合法的客户端设备签名和/或区块链节点签名，还可以验证交易事务中付款方是否具有足够资产来进行支付等等。本发明实施例对针对数据所进行的验证的具体内容不做限制。

[0074] 在一些实施例中，如果交易事务具有合法的客户端设备签名和/或区块链节点签名，且交易事务中付款方具有足够资产来进行支付，则验证通过，否则验证不通过。

[0075] 公证节点331在对上述包括跨链交易事务的区块包含的数据验证通过后，可以将该跨链交易事务中与第二区块链323相关的第二交易事务发送至第二区块链系统320中的第二区块链节点322。

[0076] 第一区块链节点312将跨链交易事务发送至公证节点331之后，还可以在步骤S530中，将第一交易事务发送至公证节点331，以便公证节点331对第一交易事务进行验证，并在验证通过后返回第一交易事务。

[0077] 在一些实施例中，第一区块链节点312可以再次接收上述跨链交易事务中与第一区块链313相关的第一交易事务，并将再次接收到的该第一交易事务发送至公证节点331。其中，该第一交易事务可以是由生成跨链交易事务的第一客户端设备311直接发送过来的；也可以是由该第一客户端设备311发送给其他第一区块链节点312，其他第一区块链节点312广播过来的。需要注意的是，区别于前述步骤S510，此时第一区块链节点312接收到的仅是第一交易事务，不是跨链交易事务。

[0078] 具体地，第一区块链节点312可以生成包括第一交易事务的区块，将包括第一交易事务的区块发送至公证节点331。

[0079] 在一些实施例中，第一区块链节点312还可以将所接收的第一交易事务广播至其他第一区块链节点312。

[0080] 公证节点331接收包括第一交易事务的区块之后，可以解析该区块，对该区块包含的数据进行验证，从而实现对第一交易事务的验证。其中，针对区块包含的数据进行验证的具体内容已在前文详细描述，此处不再赘述。

[0081] 公证节点331在对上述包括第一交易事务的区块包含的数据验证通过后，可以将该包括第一交易事务的区块返回至第一区块链节点312。

[0082] 第一区块链节点312在接收经公证节点331验证通过并返回的第一交易事务之后，可以在步骤S540中，将第一交易事务添加至第一区块链313。

[0083] 具体地，第一区块链节点312可以接收经公证节点331验证通过并返回的、包括第一交易事务的区块，将该包括第一交易事务的区块广播至其他第一区块链节点312，以便进行共识。在第一区块链系统310内多个第一区块链节点312对该包括第一交易事务的区块达成共识的情况下，各第一区块链节点312可以将该包括第一交易事务的区块添加至各自存储的第一区块链313。本发明实施例可以采用各种共识机制来进行共识，例如工作量证明机制(Proof of Work-PoW)、权益证明机制(Proof of Stake-PoS)和拜占庭共识机制等等，本发明实施例对所采用的共识机制不做限制。

[0084] 应当指出，根据本发明的实施方式，在第一区块链系统310中，第一区块链节点312将交易事务(跨链交易事务或者第一交易事务)发送给公证节点331时，可以选择一个公证节点331进行发送，也可以广播给多个公证节点331，本发明对此不做限制。其中，第一区块链节点312可以对其生成的区块进行签名，之后再将经第一区块链节点签名的区块发送出

去。另外，公证节点331也可以对其接收到的、通过验证的区块进行签名，之后再将经公证节点331签名的区块返回。

[0085] 图6示出了根据本发明一个实施例的跨链交易方法600的流程图。跨链交易方法600可以在第二区块链节点322包括的跨链交易装置1000中执行。

[0086] 如图6所示，跨链交易方法600始于步骤S610。在步骤S610中，第二区块链节点322可以接收跨链交易事务中与第二区块链323相关的第二交易事务。

[0087] 如前文所描述地，该跨链交易事务由第一客户端设备311生成，并可以包括与第一区块链313相关的第一交易事务和与第二区块链323相关的第二交易事务。该跨链交易事务由第一区块链节点312(以区块的形式)发送至公证节点331，以便公证节点331对该跨链交易事务进行验证且验证通过后，将该跨链交易事务中与第二区块链323相关的第二交易事务发送至第二区块链节点322。

[0088] 而后，在步骤S620中，第二区块链节点322将第二交易事务发送至公证节点331，以便公证节点331对第二交易事务进行验证，并在验证通过后返回该第二交易事务。

[0089] 在一些实施例中，第二区块链节点322在步骤S610之后，可以先将接收到的第二交易事务发送至对应的第二客户端设备321。例如，可以将第二交易事务发送至收款方对应的第二客户端设备321。在前述Alice与Bob的示例中，也就是将第二交易事务发送至Bob的第二客户端设备。

[0090] 第二客户端设备321接收第二交易事务，可以对该第二交易事务进行确认后，再将该第二交易事务发送至第二区块链节点322。

[0091] 这样，第二区块链节点322可以再次接收该第二交易事务，并将再次接收到的第二交易事务发送至公证节点331。在一些实施例中，该第二交易事务可以是由第二客户端设备321直接发送过来的；也可以是由该第二客户端设备321发送给其他第二区块链节点322，其他第二区块链节点322广播过来的。

[0092] 具体地，第二区块链节点322可以生成包括第二交易事务的区块，将该包括第二交易事务的区块发送至公证节点331。

[0093] 在一些实施例中，第二区块链节点322还可以将第二交易事务广播至其他第二区块链节点322。

[0094] 公证节点331接收包括第二交易事务的区块之后，可以解析该区块，对该区块包含的数据进行验证，从而实现对第二交易事务的验证。可以理解地，区块包含的数据即为一系列的交易事务。在各种实施例中，公证节点331可以对交易事务的合法性和/或有效性进行验证。例如，公证节点331可以验证交易事务是否具有合法的客户端设备和/或区块链节点签名，还可以验证交易事务中付款方是否具有足够资产来进行支付等等。本发明实施例对针对数据所进行的验证的具体内容不做限制。

[0095] 在一些实施例中，如果交易事务具有合法的客户端设备和/或区块链节点签名，且交易事务中付款方具有足够资产来进行支付，则验证通过，否则验证不通过。

[0096] 公证节点331在对上述包括第二交易事务的区块包含的数据验证通过后，可以将该包括第二交易事务的区块返回至第二区块链节点322。

[0097] 第二区块链节点322在接收经公证节点331验证通过并返回的第二交易事务之后，可以在步骤S630中，将第二交易事务添加至第二区块链323。

[0098] 具体地，第二区块链节点322可以接收经公证节点331验证通过并返回的、包括第二交易事务的区块，将该包括第二交易事务的区块广播至其他第二区块链节点322，以便进行共识。在第二区块链系统320内多个第二区块链节点322对该包括第二交易事务的区块达成共识的情况下，各第二区块链节点322可以将该包括第二交易事务的区块添加至各自存储的第二区块链323。本发明实施例可以采用各种共识机制来进行共识，例如工作量证明机制(Proof of Work-PoW)、权益证明机制(Proof of Stake-PoS)和拜占庭共识机制等等，本发明实施例对所采用的共识机制不做限制。

[0099] 应当指出，根据本发明的实施方式，在第二区块链系统320中，第二区块链节点322将交易事务发送给公证节点331时，可以选择一个公证节点331进行发送，也可以广播给多个公证节点331，本发明对此不做限制。其中，第二区块链节点322可以对其生成的区块进行签名，之后再将经第二区块链节点322签名的区块发送出去。另外，公证节点331也可以对其接收到的、通过验证的区块进行签名，之后再将经公证节点331签名的区块返回。

[0100] 图7示出了根据本发明一个实施例的跨链交易方法700的流程图。跨链交易方法700可以在公证节点331包括的跨链交易装置1100中执行。

[0101] 如图7所示，跨链交易方法700始于步骤S710。在步骤S710中，公证节点331可以接收第一区块链节点312发送的跨链交易事务。如前文所描述地，该跨链交易事务包括与第一区块链313相关的第一交易事务和与第二区块链323相关的第二交易事务。具体地，公证节点331可以接收由第一区块链节点312生成的包括跨链交易事务的区块。

[0102] 而后，在步骤S720中，公证节点331可以对跨链交易事务进行验证，并在验证通过后将跨链交易事务中与第二区块链323相关的第二交易事务发送至第二区块链节点322。

[0103] 具体地，公证节点331接收包括跨链交易事务的区块之后，可以解析该区块，对该区块包含的数据进行验证，从而实现对跨链交易事务的验证。可以理解地，区块包含的数据即为一系列的交易事务。在各种实施例中，公证节点331可以对交易事务的合法性和/或有效性进行验证。例如，公证节点331可以验证交易事务是否具有合法的客户端设备和/或区块链节点签名，还可以验证交易事务中付款方是否具有足够资产来进行支付等等。本发明实施例对针对数据所进行的验证的具体内容不做限制。

[0104] 在一些实施例中，如果交易事务具有合法的客户端设备和/或区块链节点签名，且交易事务中付款方具有足够资产来进行支付，则验证通过，否则验证不通过。

[0105] 其中，公证节点331还可以将包括跨链交易事务的区块广播至其他公证节点，以便其他公证节点同样对区块包含的数据进行验证。在一些实施例中，在超过预定比例的公证节点均对该区块包含的数据验证通过的情况下，公证节点331才可以将跨链交易事务中的第二交易事务发送至第二区块链节点322。其中，预定比例通常可以为3/2。

[0106] 接着，在步骤S730中，公证节点331可以接收第二区块链节点发送的、跨链交易事务中与第二区块链323相关的第二交易事务。在一些实施例中，第二区块链节点322接收到公证节点331发送的第二交易事务之后，可以将第二交易事务发送给对应的第二客户端设备321。第二客户端设备321确认第二交易事务之后，再将第二交易事务发送至第二区块链节点322。于是第二区块链节点322接收第二交易事务，将其发送给公证节点331。

[0107] 具体地，公证节点331可以接收第二区块链节点322生成的包括第二交易事务的区块。

[0108] 而后，公证节点331可以在步骤S740中，对第二交易事务进行验证，并在验证通过后将第二交易事务返回至第二区块链节点322，以便第二区块链节点322将第二交易事务添加至第二区块链323。

[0109] 具体地，公证节点331可以对包括第二交易事务的区块包含的数据进行验证，并在验证通过后将该区块返回至第二区块链节点322，以便第二区块链节点322将该区块添加至第二区块链323。

[0110] 其中，公证节点331还可以将包括第二交易事务的区块广播至其他公证节点，以便其他公证节点同样对该区块包含的数据进行验证。在一些实施例中，在超过预定比例的公证节点均对该区块包含的数据验证通过的情况下，公证节点331才可以将该区块返回至第二区块链节点322。其中，预定比例通常可以为3/2。

[0111] 相应地，公证节点331还可以在步骤S750中，接收第一区块链节点312发送的、跨链交易事务中与第一区块链313相关的第一交易事务。在一些实施例中，第一客户端设备311在发送跨链交易事务之后，可以将跨链交易事务中的第一交易事务再次发送至第一区块链节点312。于是第一区块链节点322接收第一交易事务，将其发送给公证节点331。

[0112] 具体地，公证节点331可以接收第一区块链节点312生成的包括第一交易事务的区块。

[0113] 而后，公证节点331可以在步骤S760中，对第一交易事务进行验证，并在验证通过后将第一交易事务返回至第一区块链节点312，以便第一区块链节点312将第一交易事务添加至第一区块链313。

[0114] 具体地，公证节点331可以对包括第一交易事务的区块包含的数据进行验证，并在验证通过后将该区块返回至第一区块链节点312，以便第一区块链节点312将该区块添加至第一区块链313。

[0115] 其中，公证节点331还可以将包括第一交易事务的区块广播至其他公证节点，以便其他公证节点同样对该区块包含的数据进行验证。在一些实施例中，在超过预定比例的公证节点均对该区块包含的数据验证通过的情况下，公证节点331才可以将该区块返回至第一区块链节点312。其中，预定比例通常可以为3/2。

[0116] 此外，根据本发明的实施方式，对于接收到的、区块链节点(第一区块链节点和/或第二区块链节点)生成的区块，公证节点331还可以在步骤S770中，记录该区块包含的数据、发送该区块的节点数据和/或该区块所涉及的跨链数据，并在步骤S780中将所记录的数据添加至公证节点331存储的公证区块链332。其中，跨链数据可以指示该区块包含的跨链交易事务所涉及的多条区块链以及每条区块链上所涉及的节点。

[0117] 具体地，公证节点331可以基于所记录的数据生成区块，并广播至其他公证节点，以便进行共识。在公证区块链系统330内多个公证节点331对该区块达成共识的情况下，各公证节点331可以将该区块添加至各自所存储的公证区块链332。

[0118] 本发明实施例可以采用各种共识机制来进行共识，例如工作量证明机制(Proof of Work-PoW)、权益证明机制(Proof of Stake-PoS)和拜占庭共识机制等等，本发明实施例对所采用的共识机制不做限制。

[0119] 应当指出，根据本发明的实施方式，在公证区块链系统330中，公证节点331可以对其接收到的、通过验证的区块进行签名。

[0120] 综上所述，全文是以第一区块链系统及第一客户端设备、第一区块链节点作为跨链交易事务中的交易发起方，第二区块链系统及第二客户端设备、第二区块链节点作为跨链交易事务中的交易接收方来对根据本发明实施例的跨链交易方案进行描述。本领域技术人员应当理解，多区块链系统100中的任一子区块链系统及对应客户端设备和区块链节点都既可以是跨链交易事务中的交易发起方、也可以是跨链交易事务中的交易接收方。

[0121] 也就是说，第一区块链系统及第一客户端设备和第一区块链节点、第二区块链系统及第二客户端设备和第二区块链节点均可以包括对方所包含的跨链交易装置，并执行对方所执行的跨链交易方法。

[0122] 此外，本领域技术人员应当理解，客户端设备在发起跨链交易事务之前，还可以生成用于部署相应跨链智能合约的交易事务，并将该交易事务发送至对应区块链节点。对应区块链节点将该交易事务以区块的形式发送至公证节点。公证节点至少可以记录该区块的数据从而记录该交易事务，并基于所记录的数据生成公证区块链的包括该交易事务的区块。公证节点可以将包括该交易事务的区块添加至所存储的公证区块链中，从而完成了对该交易事务包含的跨链智能合约的部署。之后公证节点就可以调用所部署的相应跨链智能合约，来处理接收到的跨链交易事务。

[0123] 图8示出了根据本发明一个实施例的跨链交易方法800的交互流程图。跨链交易方法800可以在多区块链系统300中执行。

[0124] 如图8所示，跨链交易方法800始于步骤S810。在步骤S810中，第一客户端设备311生成跨链交易事务。接着，在步骤S820中，第一客户端设备311将跨链交易事务发送至第一区块链节点312。第一客户端设备311可以随机或按照某种策略选择一个或多个第一区块链节点312进行发送，本发明对此不做限制。

[0125] 第一区块链节点312接收跨链交易事务，可以在步骤S830中，生成包括跨链交易事务的区块，并对该区块进行签名。接着，在步骤S840中，第一区块链节点312将经第一区块链节点312签名的包括跨链交易事务的区块发送至公证节点331。

[0126] 公证节点331在步骤S850中，对包括跨链交易事务的区块进行验证，并在验证通过后对该区块进行签名。接着，在步骤S860中，在超过预定比例的公证节点均对该区块签名的情况下，公证节点331将跨链交易事务中与第二区块链323相关的第二交易事务发送至第二区块链节点322。公证节点331可以随机或按照某种策略选择一个或多个第二区块链节点322进行发送，本发明对此不做限制。

[0127] 第二区块链节点322在步骤S870中，将第二交易事务发送至对应的第二客户端设备321。第二客户端设备321接收并确认第二交易事务之后，可以在步骤S880中，将第二交易事务发送至第二区块链节点322。第二客户端设备321可以随机或按照某种策略选择一个或多个第二区块链节点322进行发送，本发明对此不做限制。

[0128] 第二区块链节点322接收第二交易事务，并在步骤S890中，生成包括第二交易事务的区块，并对该区块进行签名。接着，在步骤S891中，第二区块链节点322将经第二区块链节点322签名的包括第二交易事务的区块发送至公证节点331。第二区块链节点322可以随机或按照某种策略选择一个或多个公证节点331进行发送，本发明对此不做限制。

[0129] 公证节点331接收包括第二交易事务的区块，可以在步骤S892中，对包括第二交易事务的区块进行验证，并在验证通过后对该区块进行签名。接着，在步骤S893中，在超过预

定比例的公证节点均对该区块签名的情况下，公证节点331将经公证节点331签名的包括第二交易事务的区块返回至第二区块链节点322。

[0130] 第二区块链节点322接收公证节点331返回的包括第二交易事务的区块，在第二区块链系统320内多个第二区块链节点对该包括第二交易事务的区块达成共识的情况下，在步骤S894中，将该包括第二交易事务的区块添加至所存储的第二区块链323。

[0131] 相应地，第一客户端设备311在步骤S820之后，还可以在步骤S821中，将跨链交易事务中与第一区块链313相关的第一交易事务再次发送至第一区块链节点312。第一客户端设备311可以随机或按照某种策略选择一个或多个第一区块链节点312进行发送，本发明对此不做限制。

[0132] 第一区块链节点312接收第一交易事务，接着可以在步骤S822中，生成包括第一交易事务的区块，并对该区块进行签名。接着，在步骤S823中，第一区块链节点312将经第一区块链节点312签名的包括第一交易事务的区块发送至公证节点331。第一区块链节点312可以随机或按照某种策略选择一个或多个公证节点331进行发送，本发明对此不做限制。

[0133] 公证节点331接收包括第一交易事务的区块，接着可以在步骤S824中，对包括第一交易事务的区块进行验证，并在验证通过后对该区块进行签名。接着，在步骤S825中，在超过预定比例的公证节点均对该区块签名的情况下，公证节点331将经公证节点331签名的包括第一交易事务的区块返回至第一区块链节点312。

[0134] 第一区块链节点312接收公证节点331返回的包括第一交易事务的区块之后，可以在第一区块链系统310内多个第一区块链节点对该包括第一交易事务的区块达成共识的情况下，在步骤S826中，将该包括第一交易事务的区块添加至所存储的第一区块链313。

[0135] 此外，公证节点331在接收区块链节点发送的区块(例如，包括跨链交易事务的区块、或者包括第一交易事务的区块、或者包括第二交易事务的区块)之后，还可以在步骤S851中记录区块包含的数据、发送区块的节点数据和/或区块所涉及的跨链数据，基于所记录的数据生成区块。接着，在公证区块链系统330内多个公证节点对该区块达成共识的情况下，公证节点331在步骤S852中，将该区块添加至所存储的公证区块链332。

[0136] 关于跨链交易方法800中各步骤的详细处理逻辑和实施过程可以参见前文结合图1-图7对跨链交易方法500～700的相关描述，此处不再赘述。

[0137] 图9示出了根据本发明一个实施例的跨链交易装置900。跨链交易装置900可以驻留在第一区块链节点312中。如图9所示，跨链交易装置900可以包括存储模块910、通信模块920和处理模块930。

[0138] 存储模块910适于存储第一区块链。通信模块920则适于接收跨链交易事务，跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务。通信模块920还适于将跨链交易事务发送至公证节点，以便公证节点对跨链交易事务进行验证，并在验证通过后将第二交易事务发送至第二区块链节点，第二区块链节点存储有所述第二区块链。通信模块920还适于将第一交易事务发送至公证节点，以便公证节点对第一交易事务进行验证，并在验证通过后返回第一交易事务。处理模块930与通信模块920和存储模块910相连接，适于将公证节点返回的第一交易事务添加至存储模块910所存储的第一区块链。

[0139] 关于跨链交易装置900中各模块的详细处理逻辑和实施过程可以参见前文结合图

1-图7对跨链交易方法500～700的相关描述，此处不再赘述。

[0140] 图10示出了根据本发明一个实施例的跨链交易装置1000。跨链交易装置1000可以驻留在第二区块链节点322中。如图10所示，跨链交易装置1000可以包括存储模块1010、通信模块1020和处理模块1030。

[0141] 存储模块1010适于存储第二区块链。通信模块1020适于接收跨链交易事务中与第二区块链相关的第二交易事务。跨链交易事务包括与第一区块链相关的第一交易事务和该第二交易事务，并由第一区块链节点发送至公证节点，所述第一区块链节点存储有所述第一区块链。通信模块1020还适于将第二交易事务发送至公证节点，以便公证节点对第二交易事务进行验证，并在验证通过后返回第二交易事务。

[0142] 处理模块1030与存储模块1010和通信模块1020相连接，并适于在公证节点返回第二交易事务后，将第二交易事务添加至存储模块1010所存储的第二区块链。

[0143] 关于跨链交易装置1000中各模块的详细处理逻辑和实施过程可以参见前文结合图1-图7对跨链交易方法500～700的相关描述，此处不再赘述。

[0144] 图11示出了根据本发明一个实施例的跨链交易装置1100。跨链交易装置1100可以驻留在公证节点331中。如图11所示，跨链交易装置1100可以包括存储模块1110、通信模块1120和数据验证模块1130。

[0145] 存储模块1110适于存储公证区块链。通信模块1120适于接收第一区块链节点发送的跨链交易事务，跨链交易事务包括与第一区块链相关的第一交易事务和与第二区块链相关的第二交易事务，第一区块链节点存储有第一区块链。通信模块1120还适于接收第一区块链节点发送的第一交易事务和接收第二区块链节点发送的第二交易事务。

[0146] 数据验证模块1130与存储模块1110和通信模块1120相连接，并适于对跨链交易事务进行验证，并在验证通过后经由通信模块1120将第二交易事务发送至第二区块链节点，第二区块链节点存储有第二区块链；还适于对第一交易事务进行验证，并在验证通过后将第一交易事务返回至第一区块链节点，以便第一区块链节点将第一交易事务添加至第一区块链；还适于对第二交易事务进行验证，并在验证通过后将第二交易事务返回至第二区块链节点，以便第二区块链节点将第二交易事务添加至第二区块链。

[0147] 跨链交易装置1100还可以包括处理模块1140，处理模块1140适于对接收到的区块链节点生成的区块，记录该区块包含的数据、发送该区块的节点数据和/或该区块所涉及的跨链数据，并基于所记录的数据生成公证区块链的区块。处理模块1140还适于在公证节点对该生成的区块达成共识的情况下，将该生成的区块添加至所存储的公证区块链332。

[0148] 关于跨链交易装置1100中各模块的详细处理逻辑和实施过程可以参见前文结合图1-图7对跨链交易方法500～700的相关描述，此处不再赘述。

[0149] 根据本发明实施例的跨链交易方案，在多个子区块链系统外增设有记录有全部子区块链数据的公证链区块链系统。由子区块链系统的区块链节点进行交易事务的收集、区块的生成及后期通过验证的区块的共识，由公证链系统的公证节点进行区块的合法性和/或有效性验证。这样，保证了多区块链系统中数据、事务的原子性，也充分发挥了区块链节点和公证节点的作用，能让这两种节点互相监督、互相约束，从而降低多区块链系统的中心化程度。

[0150] 其中，根据本发明实施例的跨链交易方案，跨链智能合约部署于公证节点，由公证

节点来管理，各子区块链系统不需维护跨链智能合约，极大地降低了管理操作的复杂度。

[0151] 其中，根据本发明实施例的跨链交易方案，在维持了原有子区块链系统的管理自主性的同时，还易于部署(例如在多区块链系统中添加新的子区块链系统)及易于系统升级，提升了多区块链系统的灵活性。

[0152] 其中，根据本发明实施例的跨链交易方案，各个子区块链系统的区块链节点仅存储各自维护的区块链和公证链的一部分，维持了原有系统使用者(交易发起方和交易接受方)对网络带宽及存储空间的要求。同时，对子区块链系统来说，将交易事务的收集、区块的生成及后期通过验证的区块的共识等分离开，可以有效避免子区块链系统中可能存在的恶意节点的攻击。

[0153] 与现有的中心化公证人方案和哈希锁方案相比，根据本发明实施例的跨链交易方案为主动式发起交易，无需等待第三方介入。并且，方案耗时较少，省去了中心化公证人方案中的初始化时间和哈希锁方案中猜解随机密码的步骤。本方案的执行最少时间仅为区块平均生成时间(Block Generation Time)，即区块链中交易广播到确认的最小时限。此外，根据本发明实施例的跨链交易方案为全跨链模式，不仅做到了跨链交易事务的验证，而且做到了区块链间的资产转移。交易不再只是发生在各自的区块链内，而且在区块链间达成了共识。资产确实从一条区块链转移到另一条区块链，不仅仅是持有者的变化。

[0154] 而现有的中心化公证人方案需要引入交易双方都能够共同信任的第三方充当公证人，一方面公证人节点的初始化相当耗时，另一方面该方案为被动交易，交易的达成(通过或被拒绝)依赖于公证人集合的签名。现有的哈希锁方案则依赖于随机密码的计算，而这一计算步骤同样相当耗时。同时，以上两种方案均为半跨链模式，尽管做到了跨链交易事务验证，但交易还是发生在各自的链内，并未做到真正的跨链交易。

[0155] 此外，本领域技术人员应当理解，根据本发明实施例的方法不仅可以应用于前文所描述的区块链场景，还可以应用于诸如两个闭环系统之间的跨系统交易之类的非区块链场景。

[0156] 以第一银行系统和第二银行系统之间的货币兑换为例，可以在两个银行系统之外架设公证系统。第一银行系统节点将跨系统交易发送给公证系统节点，可以理解地，跨系统交易应当包括与第一银行系统相关的第一交易事务和第二交易事务。公证系统节点对跨系统交易进行验证后将其中的第二交易事务发送给第二银行系统节点。

[0157] 第一银行系统和第二银行系统再分别将各自相关的交易事务发送给公证系统节点，由公证系统节点进行验证后返回。第一银行系统和第二银行系统分别接收经公证系统节点验证后的交易事务，各自执行并记录该交易事务。

[0158] 其中的详细处理逻辑和实施过程可以参见前文结合图1-图7对多区块链系统200以及跨链交易方法的相关描述，此处不再赘述。这里描述的各种技术可结合硬件或软件，或者它们的组合一起实现。从而，本发明实施例的方法和设备，或者本发明实施例的方法和设备的某些方面或部分可采取嵌入有形媒介，例如可移动硬盘、U盘、软盘、CD-ROM或者其它任意机器可读的存储介质中的程序代码(即指令)的形式，其中当程序被载入诸如计算机之类的机器，并被机器执行时，该机器变成实践本发明实施例的设备。

[0159] 在程序代码在可编程计算机上执行的情况下，计算设备一般包括处理器、处理器可读的存储介质(包括易失性和非易失性存储器和/或存储元件)，至少一个输入装置，和至

少一个输出装置。其中，存储器被配置用于存储程序代码；处理器被配置用于根据该存储器中存储的程序代码中的指令，执行本发明实施例的方法。

[0160] 以示例而非限制的方式，可读介质包括可读存储介质和通信介质。可读存储介质存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息。通信介质一般以诸如载波或其它传输机制等已调制数据信号来体现计算机可读指令、数据结构、程序模块或其它数据，并且包括任何信息传递介质。以上的任一种的组合也包括在可读介质的范围之内。

[0161] 在此处所提供的说明书中，算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与本发明实施例的示例一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明实施例也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明实施例的内容，并且上面对特定语言所做的描述是为了披露本发明实施例的最佳实施方式。

[0162] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明实施例的实施例可以在没有这些具体细节的情况下被实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0163] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明实施例的示例性实施例的描述中，本发明实施例的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明实施例要求比在每个权利要求中所明确记载的特征更多特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明实施例的单独实施例。

[0164] 本领域那些技术人员应当理解在本文所公开的示例中的设备的模块或单元或组件可以布置在如该实施例中所描述的设备中，或者可替换地可以定位在与该示例中的设备不同的一个或多个设备中。前述示例中的模块可以组合为一个模块或者此外可以分成多个子模块。

[0165] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0166] 此外，本领域的技术人员能够理解，尽管在此所描述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明实施例的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0167] 此外，上述实施例中的一些在此被描述成可以由计算机系统的处理器或者由执行上述功能的其它装置实施的方法或方法元素的组合。因此，具有用于实施上述方法或方法

元素的必要指令的处理器形成用于实施该方法或方法元素的装置。此外，装置实施例的在此所描述的元素是如下装置的例子：该装置用于实施由为了实施该发明的目的的元素所执行的功能。

[0168] 如在此所使用的那样，除非另行规定，使用序数词“第一”、“第二”、“第三”等等来描述普通对象仅仅表示涉及类似对象的不同实例，并且并不意图暗示这样被描述的对象必须具有时间上、空间上、排序方面或者以任意其它方式的给定顺序。

[0169] 尽管根据有限数量的实施例描述了本发明实施例，但是受益于上面的描述，本技术领域内的技术人员明白，在由此描述的本发明实施例的范围内，可以设想其它实施例。此外，应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明实施例的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明实施例的范围，对本发明实施例所做的公开是说明性的而非限制性的，本发明实施例的范围由所附权利要求书限定。

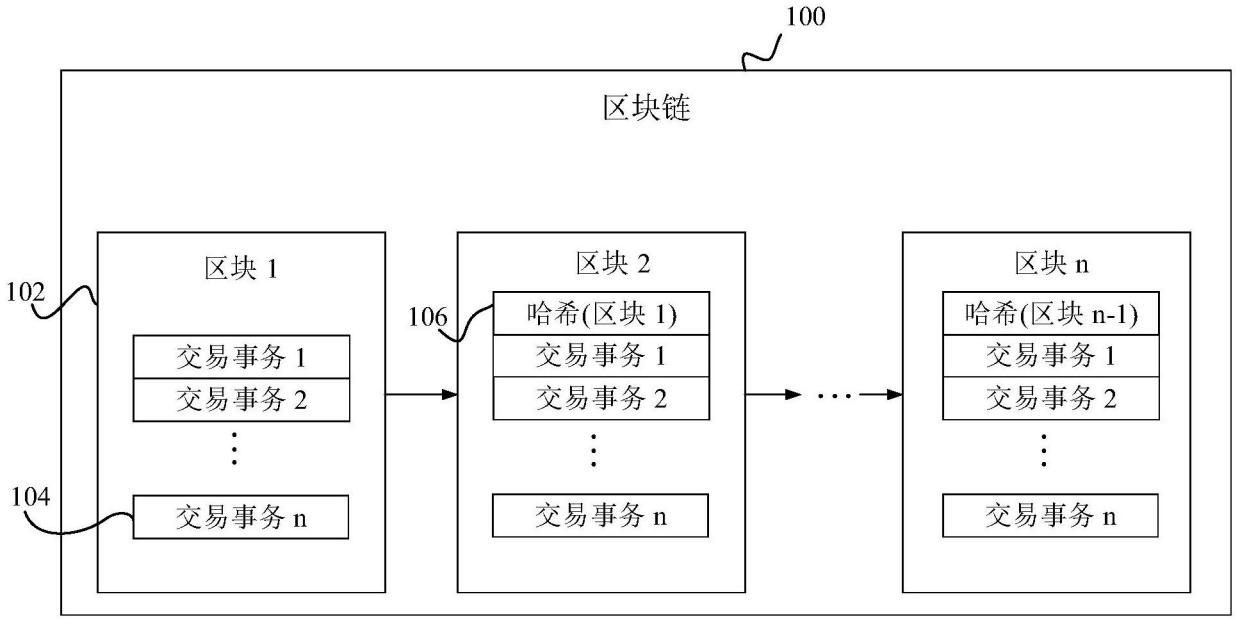

100
区块链
区块 1
102
交易事务 1
交易事务 2
104
交易事务 n
区块 2
106
哈希(区块 1)
交易事务 1
交易事务 2
交易事务 n
区块 n
哈希(区块 n-1)
交易事务 1
交易事务 2
交易事务 n

图1

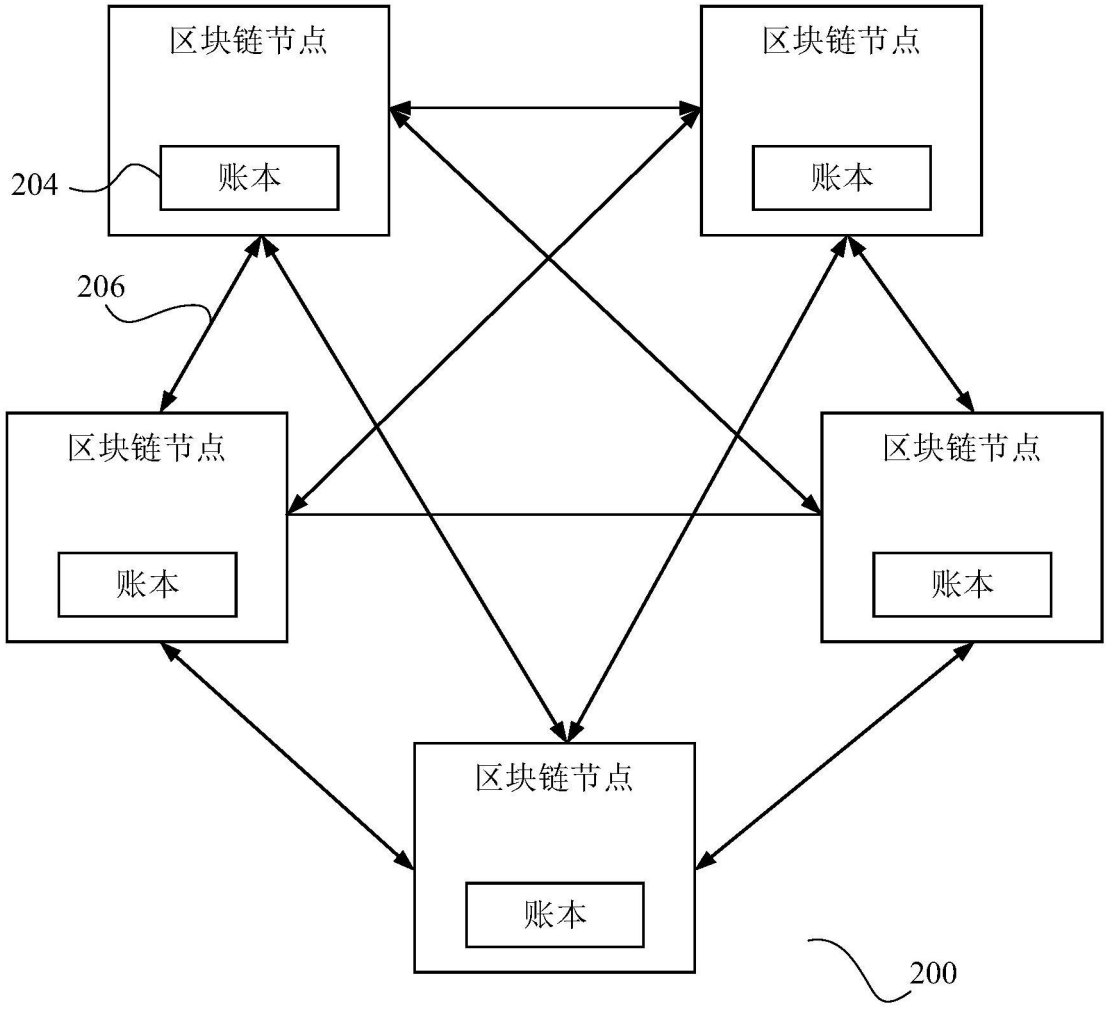


图2

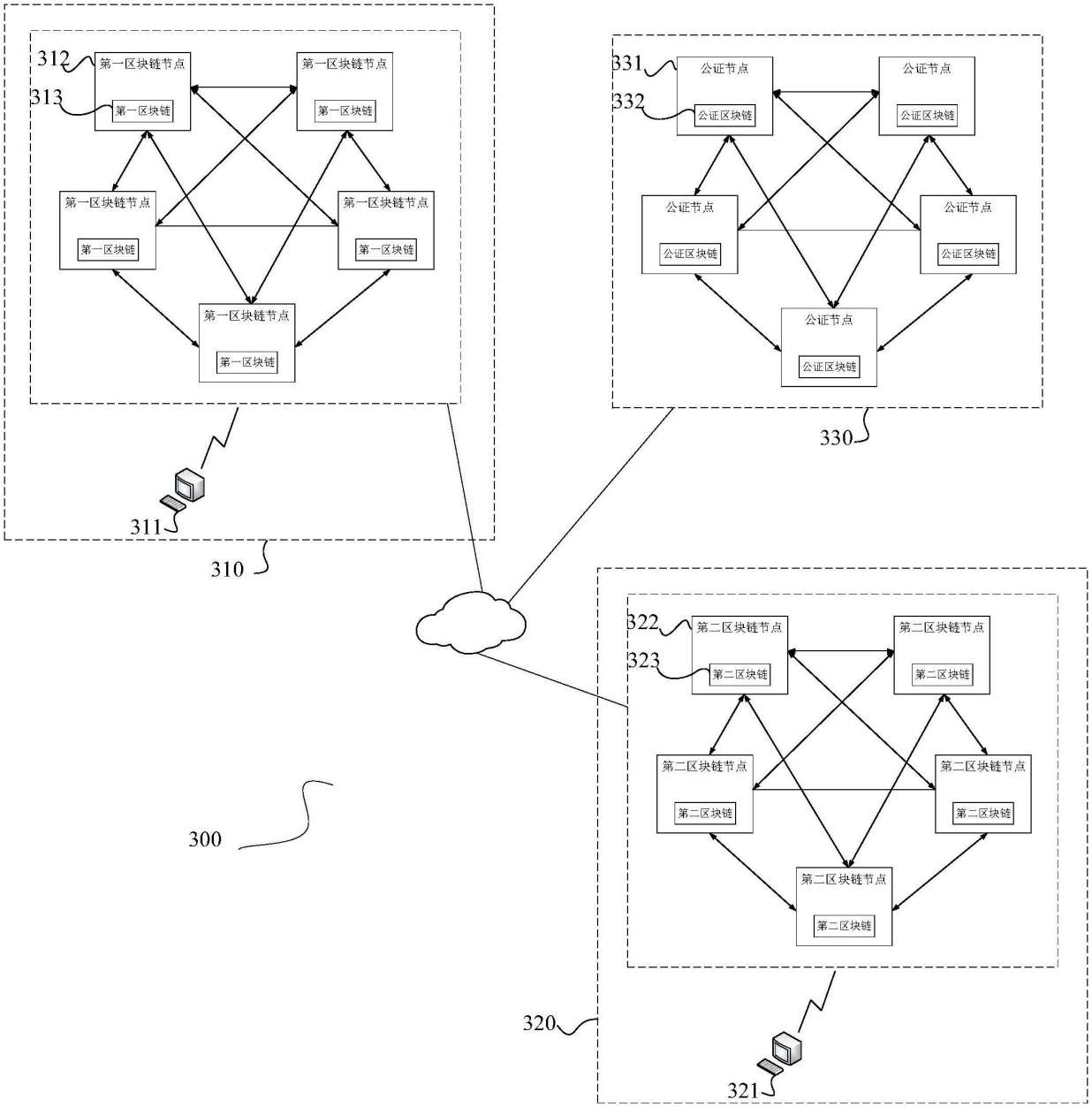

312
第一区块链节点
第一区块链
313
第一区块链节点
第一区块链
第一区块链节点
第一区块链
第一区块链节点
第一区块链
第一区块链节点
第一区块链
311
310
331
公证节点
公证区块链
332
公证节点
公证区块链
公证节点
公证区块链
公证节点
公证区块链
公证节点
公证区块链
330
322
第二区块链节点
第二区块链
323
第二区块链节点
第二区块链
第二区块链节点
第二区块链
第二区块链节点
第二区块链
第二区块链节点
第二区块链
300
320
321

图3

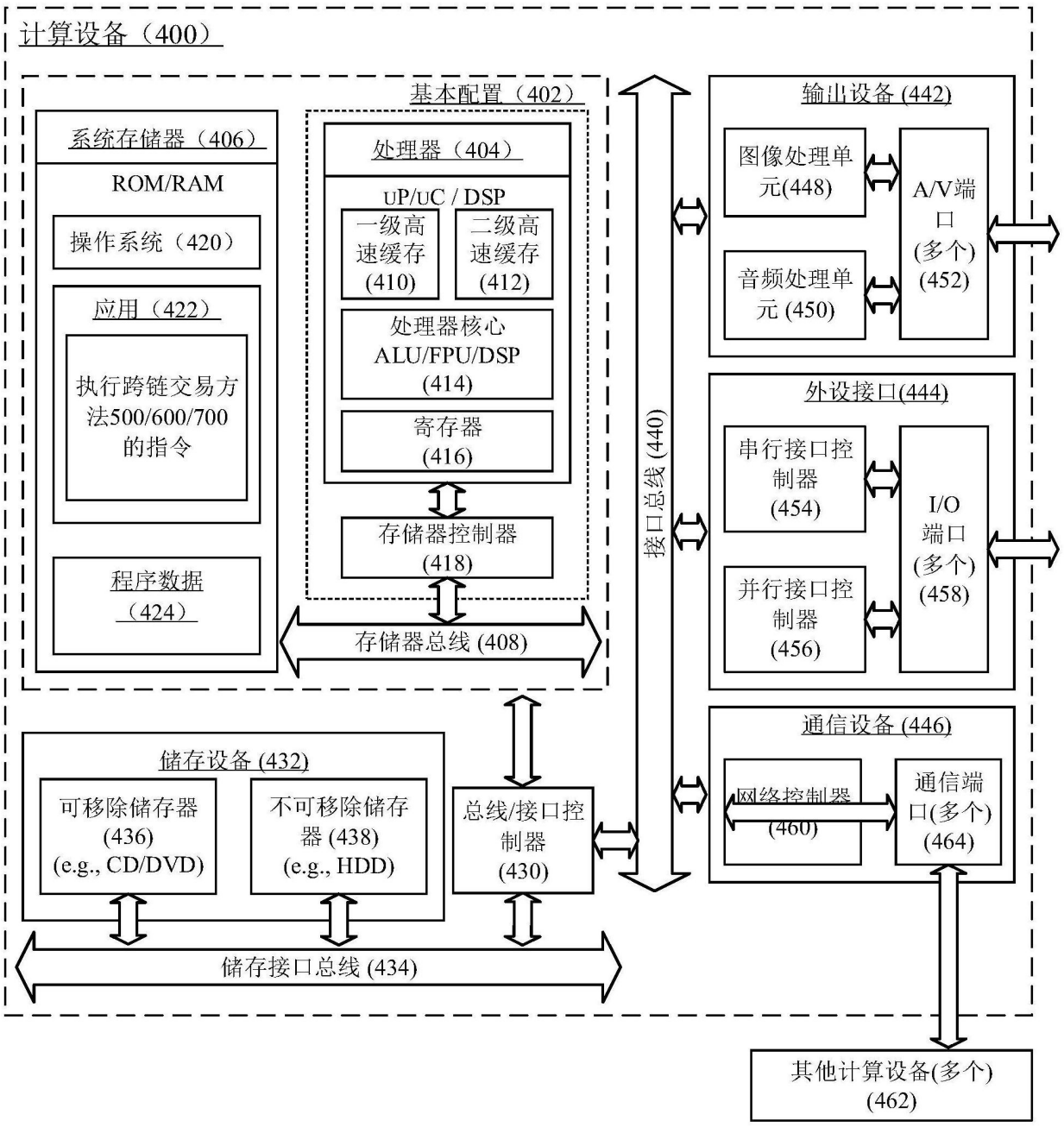

计算设备（400）
基本配置（402）
系统存储器（406）
ROM/RAM
操作系统（420）
应用（422）
执行跨链交易方法500/600/700的指令
程序数据（424）
处理器（404）
uP/uC / DSP
一级高速缓存(410)
二级高速缓存(412)
处理器核心ALU/FPU/DSP(414)
寄存器(416)
存储器控制器(418)
存储器总线 (408)
接口总线 (440)
输出设备 (442)
图像处理单元(448)
音频处理单元 (450)
A/V端口(多个)(452)
外设接口(444)
串行接口控制器(454)
并行接口控制器(456)
I/O端口(多个)(458)
通信设备 (446)
网络控制器(460)
通信端口(多个)(464)
储存设备 (432)
可移除储存器(436)(e.g., CD/DVD)
不可移除储存器 (438)(e.g., HDD)
总线/接口控制器(430)
储存接口总线 (434)
其他计算设备(多个)(462)

图4

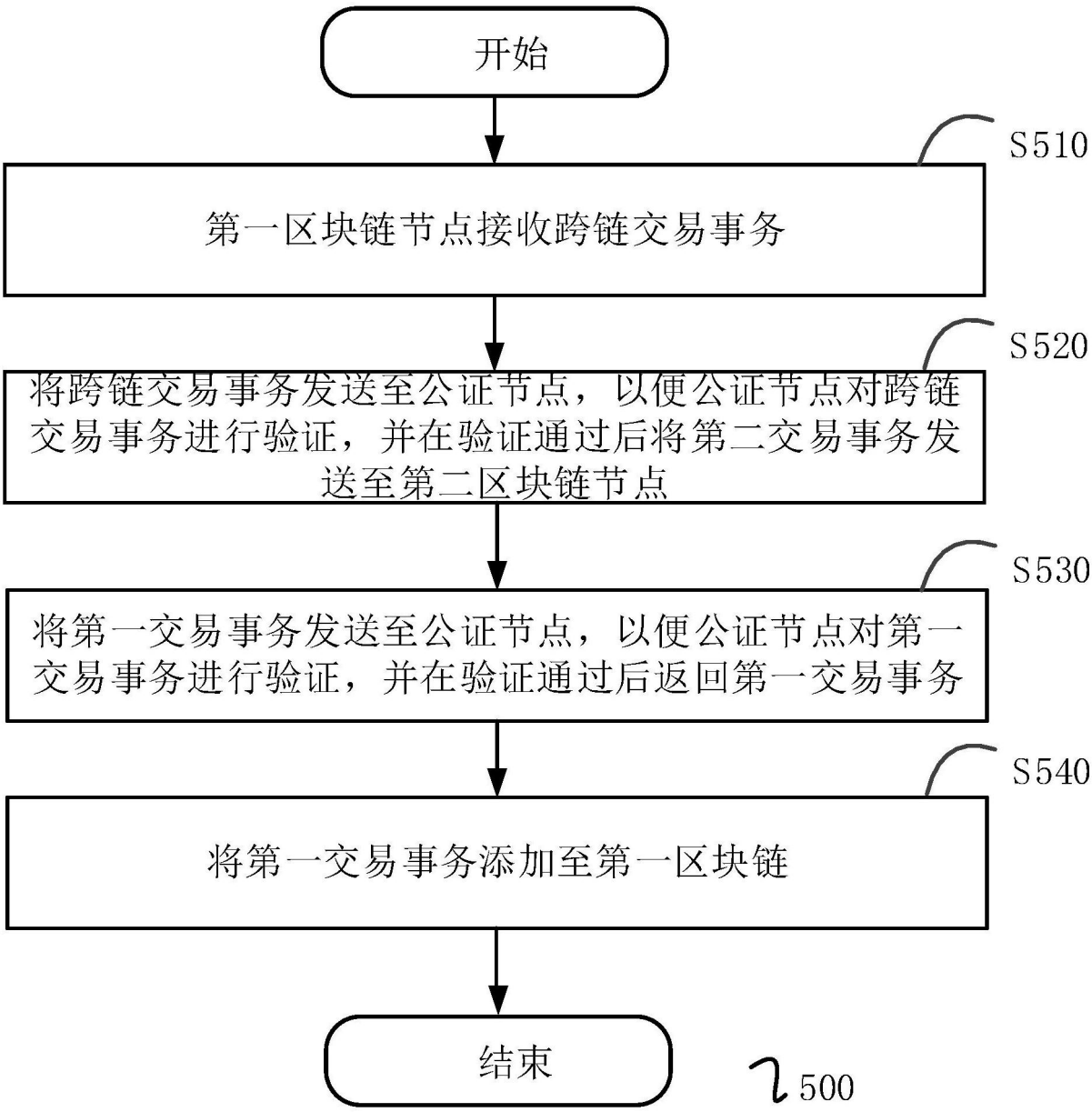

开始
S510
第一区块链节点接收跨链交易事务
S520
将跨链交易事务发送至公证节点，以便公证节点对跨链交易事务进行验证，并在验证通过后将第二交易事务发送至第二区块链节点
S530
将第一交易事务发送至公证节点，以便公证节点对第一交易事务进行验证，并在验证通过后返回第一交易事务
S540
将第一交易事务添加至第一区块链
结束
500

图5

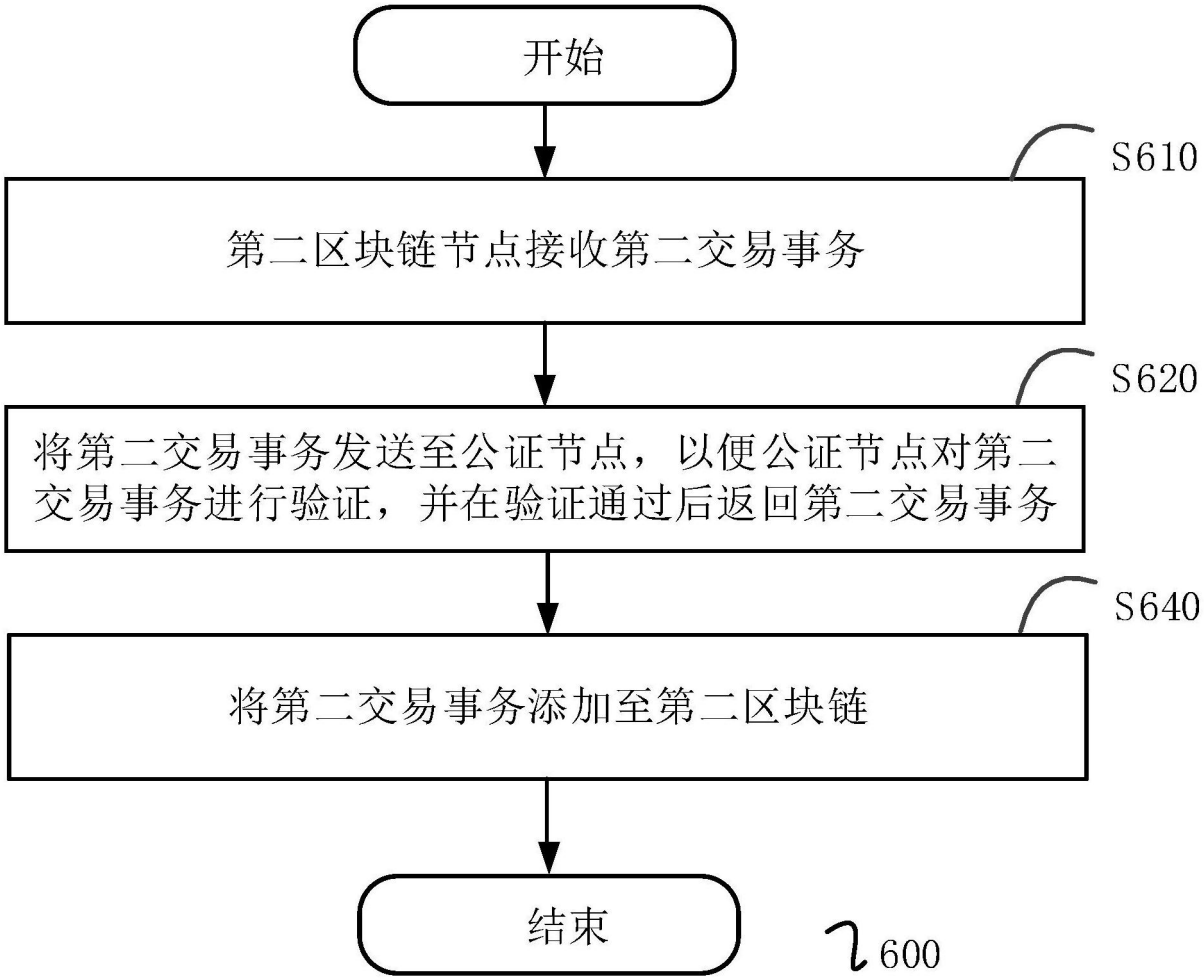

开始
S610
第二区块链节点接收第二交易事务
S620
将第二交易事务发送至公证节点，以便公证节点对第二交易事务进行验证，并在验证通过后返回第二交易事务
S640
将第二交易事务添加至第二区块链
结束
600

图6

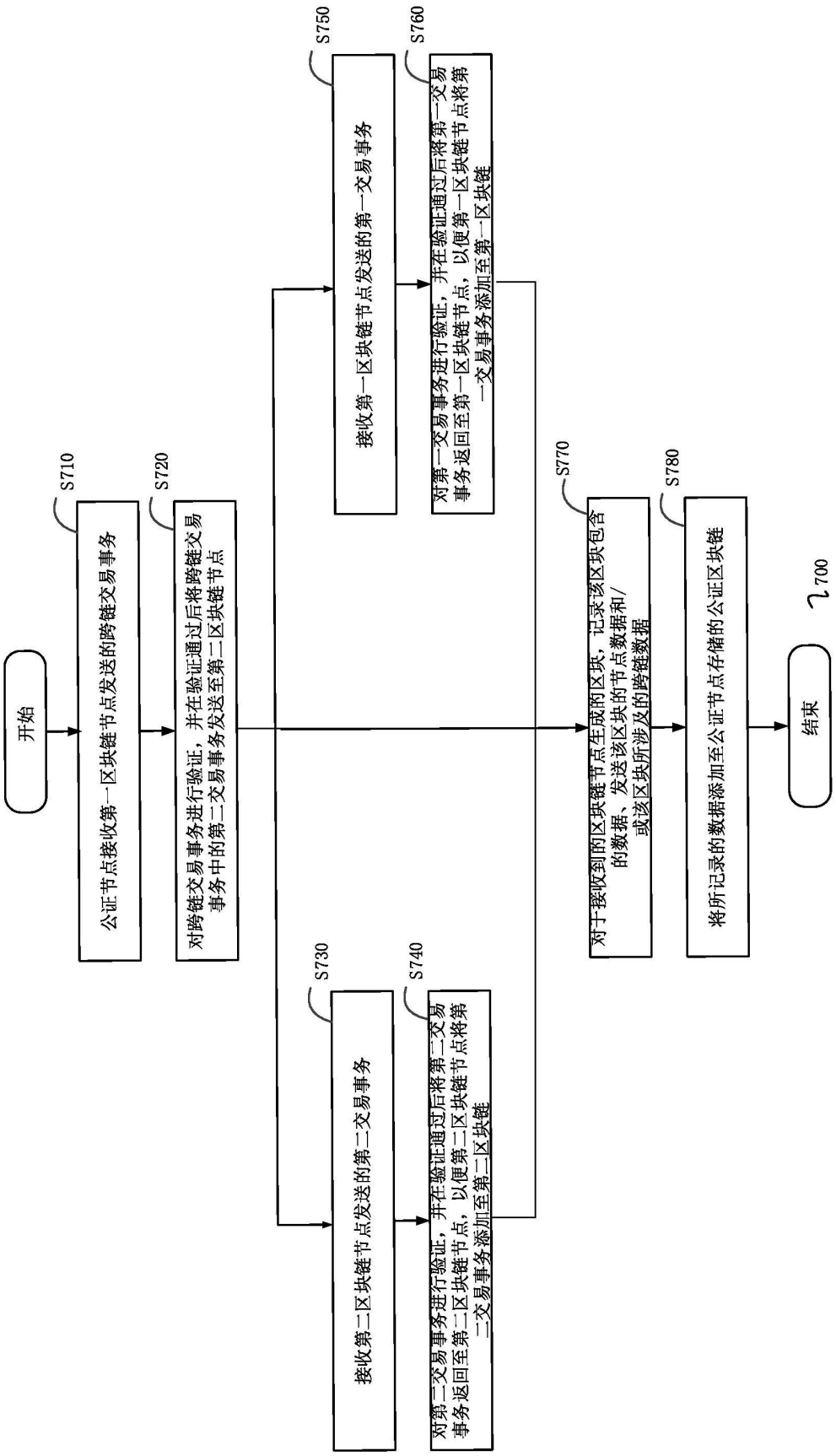

开始
公证节点接收第一区块链节点发送的跨链交易事务
S710
对跨链交易事务进行验证，并在验证通过后将跨链交易事务中的第二交易事务发送至第二区块链节点
S720
接收第二区块链节点发送的第二交易事务
S730
对第二交易事务进行验证，并在验证通过后将第二交易事务返回至第二区块链节点，以便第二区块链节点将第二交易事务添加至第二区块链
S740
接收第一区块链节点发送的第一交易事务
S750
对第一交易事务进行验证，并在验证通过后将第一交易事务返回至第一区块链节点，以便第一区块链节点将第一交易事务添加至第一区块链
S760
对于接收到的区块链节点生成的区块，记录该区块包含的数据、发送该区块的节点数据和/或该区块所涉及的跨链数据
S770
将所记录的数据添加至公证节点存储的公证区块链
S780
结束
700

图7

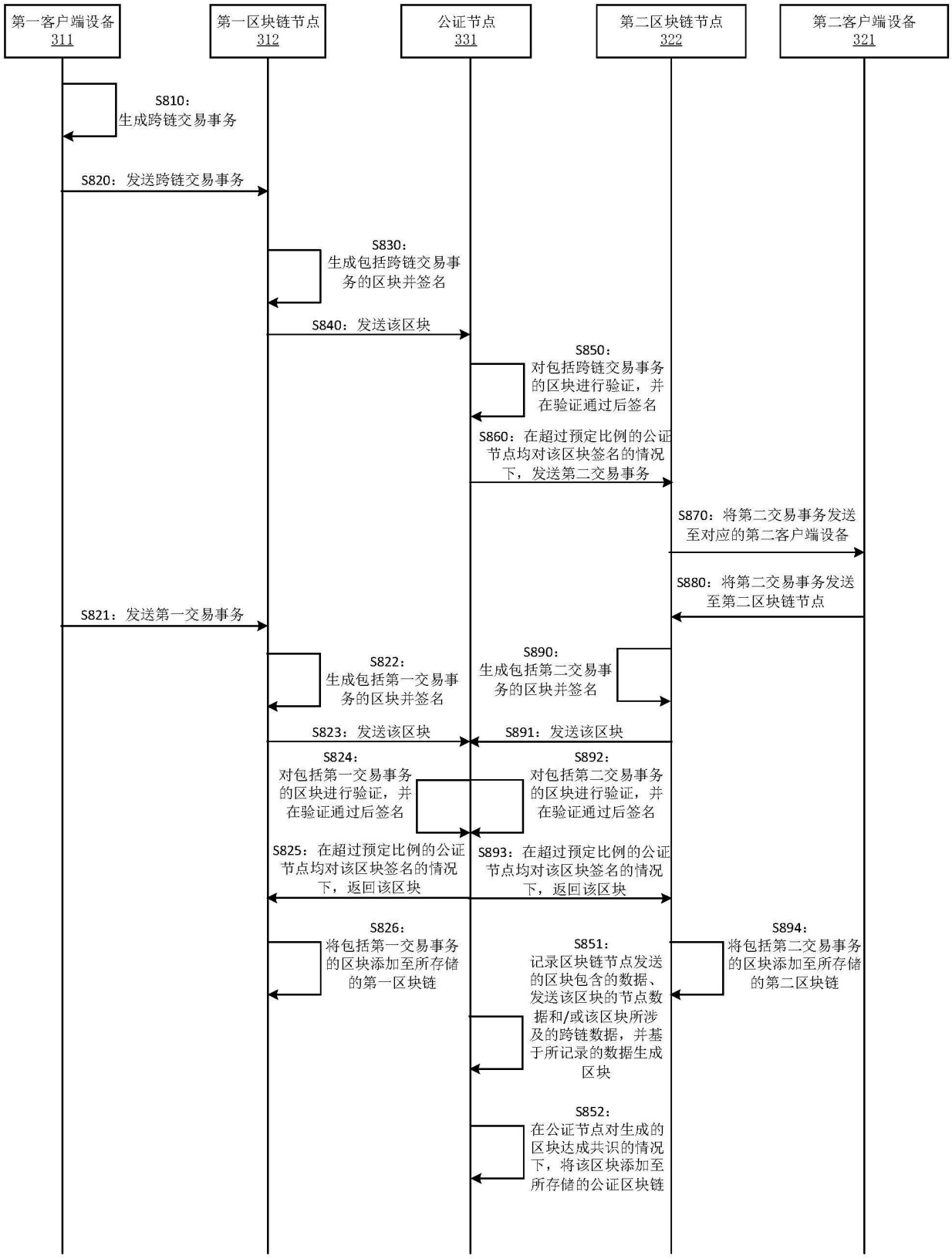

第一客户端设备
311
第一区块链节点
312
公证节点
331
第二区块链节点
322
第二客户端设备
321
S810：
生成跨链交易事务
S820：发送跨链交易事务
S830：
生成包括跨链交易事务的区块并签名
S840：发送该区块
S850：
对包括跨链交易事务的区块进行验证，并在验证通过后签名
S860：在超过预定比例的公证节点均对该区块签名的情况下，发送第二交易事务
S870：将第二交易事务发送至对应的第二客户端设备
S880：将第二交易事务发送至第二区块链节点
S821：发送第一交易事务
S822：
生成包括第一交易事务的区块并签名
S890：
生成包括第二交易事务的区块并签名
S823：发送该区块
S891：发送该区块
S824：
对包括第一交易事务的区块进行验证，并在验证通过后签名
S892：
对包括第二交易事务的区块进行验证，并在验证通过后签名
S825：在超过预定比例的公证节点均对该区块签名的情况下，返回该区块
S893：在超过预定比例的公证节点均对该区块签名的情况下，返回该区块
S826：
将包括第一交易事务的区块添加至所存储的第一区块链
S851：
记录区块链节点发送的区块包含的数据、发送该区块的节点数据和/或该区块所涉及的跨链数据，并基于所记录的数据生成区块
S894：
将包括第二交易事务的区块添加至所存储的第二区块链
S852：
在公证节点对生成的区块达成共识的情况下，将该区块添加至所存储的公证区块链

图8

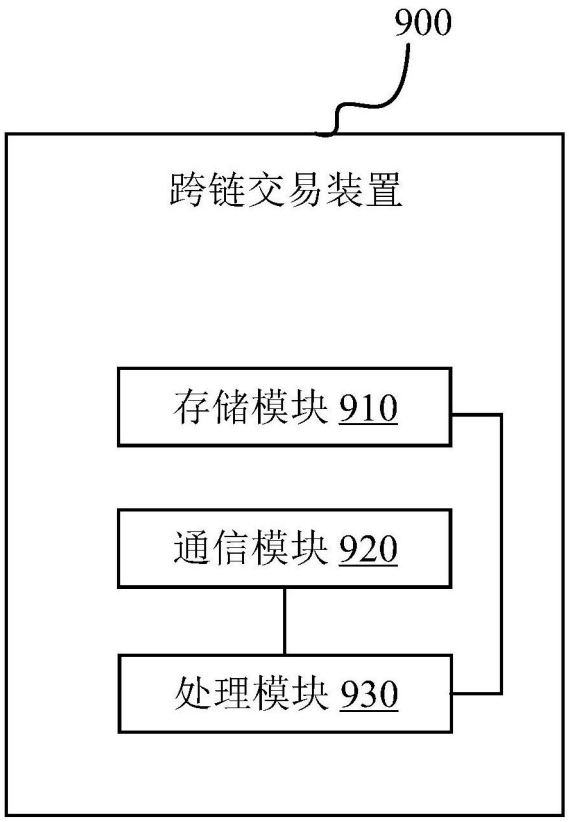


图9

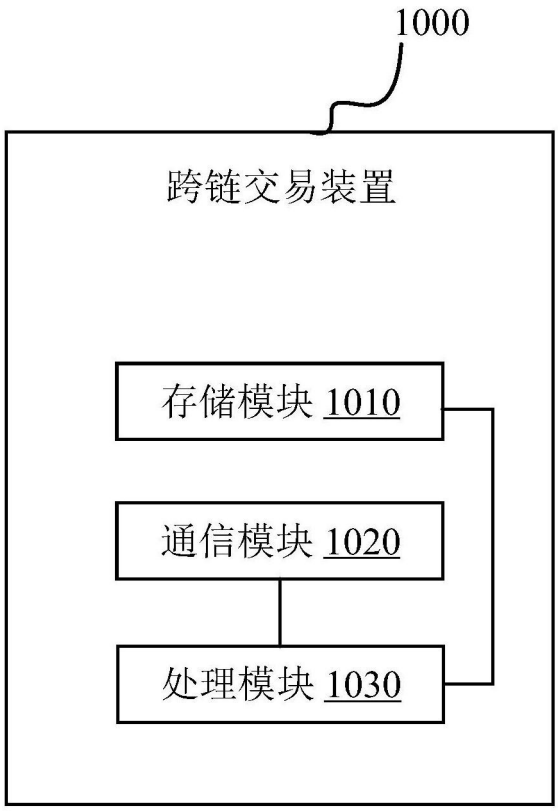


图10

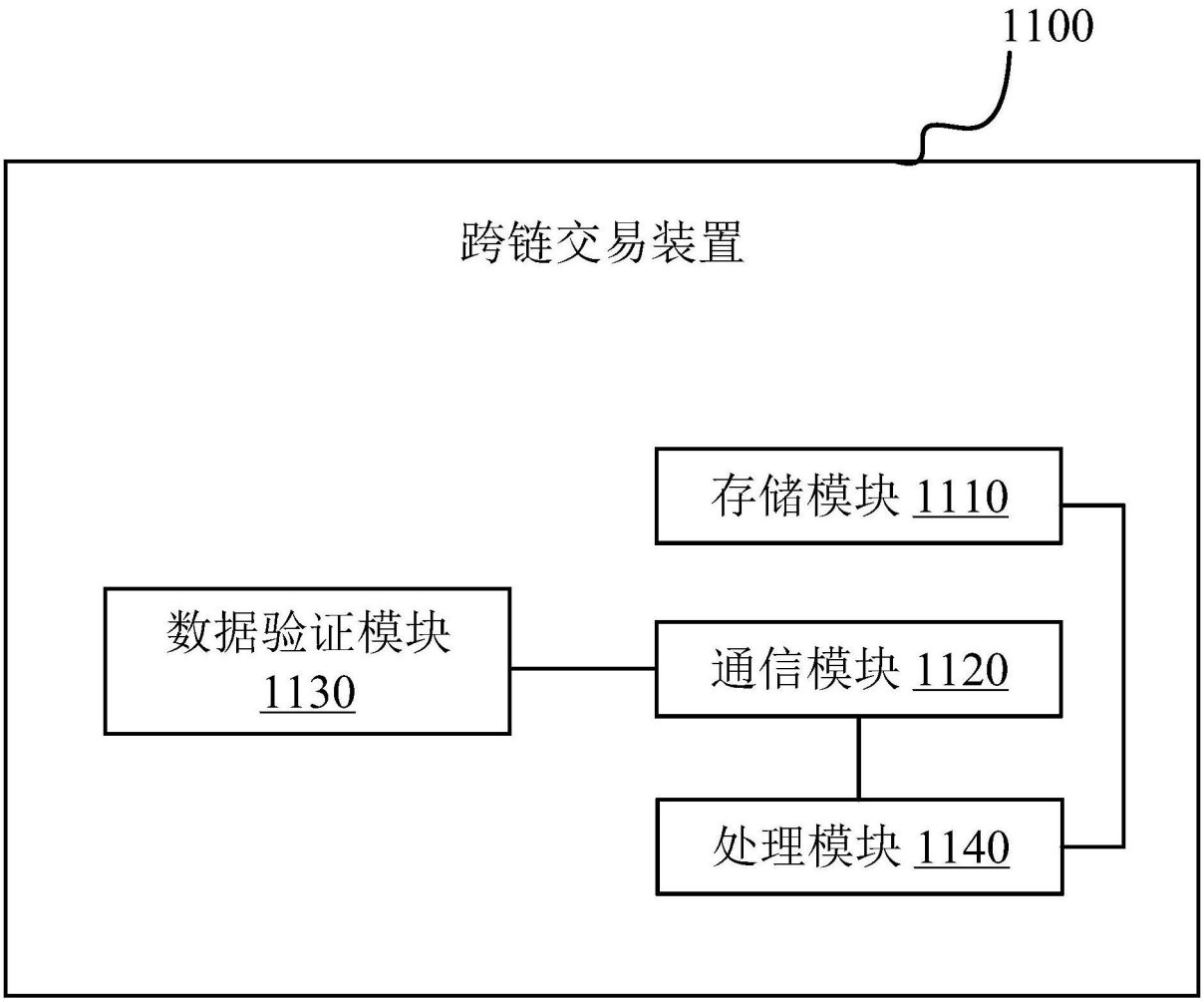


图11