(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 110505311 A
(43)申请公布日 2019.11.26

(21)申请号 201910862860.9

(22)申请日 2019.09.12

(71)申请人 杭州秘猿科技有限公司
地址 310013 浙江省杭州市西湖区文三路478号华星时代广场A座1301

(72)发明人 胡文超

(74)专利代理机构 北京德崇智捷知识产权代理有限公司 11467
代理人 高琦

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

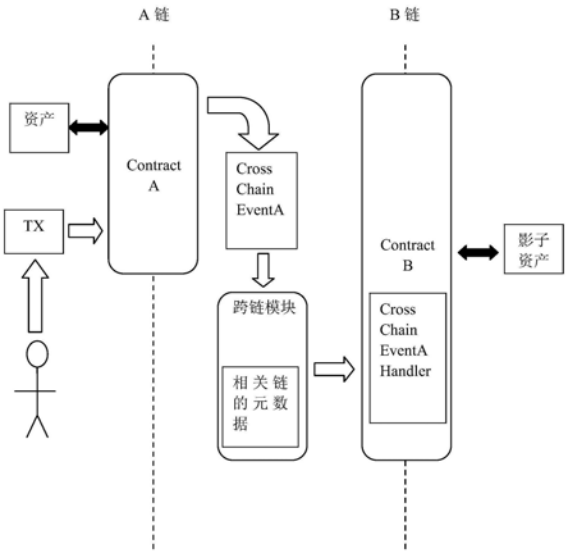
权利要求书2页 说明书6页 附图5页

(54)发明名称

一种同构区块链跨链交互方法和系统

(57)摘要

本发明提供了一种同构区块链跨链交互方法和系统。所述方法包括构造一个公共的跨链模块，用于维护跨链的元数据，使得每个链上合约都能够访问所述跨链模块中的所述元数据用于进行验证；调用统一的协议来生成、传输和验证跨链消息；对虚拟机进行功能扩展，使得所述虚拟机支持跨链事件和跨链调用，所述跨链事件被触发后自动转发给所述跨链模块进行处理，所述跨链函数，只接受所述跨链事件的跨链调用；链上所有的跨链合约共享所述跨链模块的数据和方法，所述跨链合约只需处理业务逻辑，不处理跨链数据维护和校验逻辑。通过构造一个通用的跨链模块和定义一系列交互协议，降低了开发难度，简化了交易操作，提升了用户体验，减少了链上的存储压力。



CN 110505311 A

1.一种同构区块链跨链交互方法,其特征在于,包括:

构造一个公共的跨链模块,用于维护跨链的元数据,使得每个链上合约都能够访问所述跨链模块中的所述元数据用于进行验证;

调用统一的协议来生成、传输和验证跨链消息;

对虚拟机进行功能扩展,使得所述虚拟机支持跨链事件和跨链调用,所述跨链事件被触发后自动转发给所述跨链模块进行处理,所述跨链函数,只接受所述跨链事件的跨链调用;

链上所有的跨链合约共享所述跨链模块的数据和方法,所述跨链合约只需处理业务逻辑,不处理跨链数据维护和校验逻辑。

2.根据权利要求1所述的同构区块链跨链交互方法,其特征在于,进一步包括:

在所述链上部署合约;

根据所述合约通过所述跨链模块进行跨链交易。

3.根据权利要求2所述的同构区块链跨链交互方法,其特征在于,所述在所述链上部署合约,进一步包括:

在 A 链上部署合约ContractA,用于执行用户指定的交易逻辑,并生成所述跨链事件CrossChainEventA;

在 B 链上部署合约 ContractB,其中包含针对CrossChainEventA的所述跨链函数CrossChainEventAHandler。

4.根据权利要求2或3所述的同构区块链跨链交互方法,其特征在于,根据所述合约通过所述跨链模块进行跨链交易,进一步包括:

用户向A 链的部署合约ContractA发送交易 TX,执行交易逻辑;

合约触发特殊的跨链事件CrossChainEventA后,由跨链模块负责生成对应的跨链消息传递到 B 链;

B链将所述消息分配给合约ContractB进行处理;

合约ContractB调用处理函数CrossChainEventAHandler,执行对应的逻辑,完成跨链交易。

5.根据权利要求4所述的同构区块链跨链交互方法,其特征在于,由跨链模块负责生成对应的跨链消息传递到 B 链后进一步包括:

B 链的跨链模块接收所述跨链消息,验证其合法性。

6.根据权利要求5所述的同构区块链跨链交互方法,其特征在于,元数据包括但不限于区块头、验证者名单。

7.一种同构区块链跨链交互装置,其特征在于,包括:

构造模块,构造一个公共的跨链模块,用于维护跨链的元数据,使得每个链上合约都能够访问所述跨链模块中的所述元数据用于进行验证;

调用模块,调用统一的协议来生成、传输和验证跨链消息;

扩展模块,对虚拟机进行功能扩展,使得所述虚拟机支持跨链事件和跨链调用,所述跨链事件被触发后自动转发给所述跨链模块进行处理,所述跨链函数,只接受所述跨链事件的跨链调用;

共享模块,链上所有的跨链合约共享所述跨链模块的数据和方法,所述跨链合约只需

处理业务逻辑,不处理跨链数据维护和校验逻辑。

8.根据权利要求7所述的同构区块链跨链交互装置,其特征在于,进一步包括:

部署模块,在所述链上部署合约;

交易模块,根据所述合约通过所述跨链模块进行跨链交易。

9.根据权利要求8所述的同构区块链跨链交互装置,其特征在于,所述部署模块进一步包括:

在 A 链上部署合约ContractA,用于执行用户指定的交易逻辑,并生成所述跨链事件CrossChainEventA;

在 B 链上部署合约 ContractB,其中包含针对CrossChainEventA的所述跨链函数CrossChainEventAHandler。

10.根据权利要求8或9所述的同构区块链跨链交互装置,其特征在于,所述交易模块,进一步包括:

用户向A 链的部署合约ContractA发送交易 TX,执行交易逻辑;

合约触发特殊的跨链事件CrossChainEventA后,由跨链模块负责生成对应的跨链消息传递到 B 链;

B链将所述消息分配给合约ContractB进行处理;

合约ContractB调用处理函数CrossChainEventAHandler,执行对应的逻辑,完成跨链交易。

11.根据权利要求10所述的同构区块链跨链交互装置,其特征在于,由跨链模块负责生成对应的跨链消息传递到 B 链后进一步包括:

B 链的跨链模块接收所述跨链消息,验证其合法性。

12.根据权利要求11所述的同构区块链跨链交互装置,其特征在于,元数据包括但不限于区块头、验证者名单。

13.一种电子设备,包括:

处理器;以及

被安排成存储计算机可执行指令的存储器,所述可执行指令在被执行时使所述处理器执行权利要求1-6任一项所述方法的操作。

14.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-6任一项所述方法的步骤。

一种同构区块链跨链交互方法和系统

技术领域

[0001] 本发明涉及互联网技术领域,特别是区块链进行跨链的数据交互。

背景技术

[0002] 区块链技术构造了一个无需信任的价值网络,跨链技术则将不同的专有链连接到了一起。

[0003] 由于区块链去中心化、无需信任的特性,不同区块链之间的跨链交互,往往需要用户自己在一条链上获取密码学证明,构造交易发往另一条链,链上进行校验,校验通过后根据发送的信息执行对应的操作,流程十分繁琐。

[0004] 图1为现有技术中以A、B两条链为例通过跨链转移资产的示意图,具体方案为:

[0005] 1.开发者在A链上部署合约ContractA,功能为锁定A链上的资产,并生成事件EventA;

[0006] 2.开发者在B链上部署合约ContractB,功能为接收A链生成的EventA事件的密码学证明,验证该事件是合法的,然后在B链上发行对应的影子资产。为了使合约拥有验证EventA事件的能力,合约必须维护A链的一些元信息(比如所有的区块头、或者验证者名单);

[0007] 3.用户往A链的ContractA发送交易TX1,锁定部分资产到合约;

[0008] 4.用户调用A链的接口,获取TX1对应的收据证明(receipt proof)、TX1对应区块的块头信息;

[0009] 5.用户使用收到的信息,构造一个符合ContractB要求的交易TX2,发送到B链。B链收到该交易后生成对应的影子资产,完成跨链交易。

[0010] 对于应用开发者来说,跨链合约里需要写复杂的逻辑来验证跨链交易的合法性,且需要额外维护与一些业务无关的状态(用于跨链验证的基本信息),开发负担大,且合约消耗的执行手续费很高,不利于获取用户。

[0011] 对于用户来说,进行一次跨链交易流程非常复杂。上述例子中,用户需要和两条链共计进行三次交互来完成一次资产跨链,涉及的操作十分繁琐,用户体验很差。且不同的合约可能定义不同的跨链交易格式,没有统一的标准,使得很难有第三方来开发和完善对应的工具。

[0012] 对于区块链本身来说,跨链操作里,交易合法性验证是和链有关的,业务逻辑是和合约相关的。在上述方案中,每个跨链合约都要各自进行跨链状态维护和验证,浪费了大量的存储和计算。

[0013] 综上所述,如何在保证信息安全的同时简化跨链交易,已成为亟待解决的技术问题。

发明内容

[0014] 本申请的目的在于,提出一种同构区块链跨链交互方案,通过构造一个通用的跨

链模块和定义一系列交互协议，使得跨链交互如同本地函数调用一样简单。为实现上述目的，本发明提供的同构区块链跨链交互方法，其特征在于，包括：

[0015] 构造一个公共的跨链模块，用于维护跨链的元数据，使得每个链上合约都能够访问所述跨链模块中的所述元数据用于进行验证；

[0016] 调用统一的协议来生成、传输和验证跨链消息；

[0017] 对虚拟机进行功能扩展，使得所述虚拟机支持跨链事件和跨链调用，所述跨链事件被触发后自动转发给所述跨链模块进行处理，所述跨链函数，只接受所述跨链事件的跨链调用；

[0018] 链上所有的跨链合约共享所述跨链模块的数据和方法，所述跨链合约只需处理业务逻辑，不处理跨链数据维护和校验逻辑。

[0019] 为实现上述目的，本发明还提供一种同构区块链跨链交互装置，其特征在于，包括：

[0020] 构造模块，构造一个公共的跨链模块，用于维护跨链的元数据，使得每个链上合约都能够访问所述跨链模块中的所述元数据用于进行验证；

[0021] 调用模块，调用统一的协议来生成、传输和验证跨链消息；

[0022] 扩展模块，对虚拟机进行功能扩展，使得所述虚拟机支持跨链事件和跨链调用，所述跨链事件被触发后自动转发给所述跨链模块进行处理，所述跨链函数，只接受所述跨链事件的跨链调用；

[0023] 共享模块，链上所有的跨链合约共享所述跨链模块的数据和方法，所述跨链合约只需处理业务逻辑，不处理跨链数据维护和校验逻辑。

[0024] 为实现上述目的，本发明还提供一种电子设备，包括：处理器；以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行上述方法的操作。

[0025] 为实现上述目的，本发明还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述方法的步骤。

[0026] 与现有技术相比，本发明的有益效果是：对于应用开发者来说，不再需要关心复杂的跨链消息验证逻辑，只需关心自己的业务逻辑。对于用户来说，进行一次跨链交互只需要发送一个交易，和发送普通交易没有任何差别，用户体验大大提升。对于区块链本身来说，原来跨到同一条链的所有合约都要维护的多份跨链元信息，被统一到一个地方，大大的减少了链上存储的数据量。

附图说明

[0027] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0028] 图1现有技术通过跨链转移资产的示意图

[0029] 图2本发明一实施例提供的跨链转移资产的示意图

[0030] 图3本发明一实施例提供的跨链转移资产方法的流程图

[0031] 图4本发明一实施例提供的开发者在所述链上部署合约的流程图

[0032] 图5本发明一实施例提供的用户在所述链上进行资源转移的流程图

[0033] 图6本发明一实施例提供的跨链转移资产装置的示意图

[0034] 图7本发明一个实施例提供的电子设备的结构示意图

具体实施方式

[0035] 为了使本申请的技术方案及优点更加清楚明白，以下结合附图对本申请的示例性实施例进行进一步详细的说明，显然，所描述的实施例仅是本申请的一部分实施例，而不是所有实施例的穷举。并且在不冲突的情况下，本说明中的实施例及实施例中的特征可以互相结合。

[0036] 当前跨链交互流程繁琐的原因主要有以下几点：

[0037] 1.跨链交易验证逻辑本身很复杂。由于区块链是无需信任的，为了保证跨链交互的安全性，必须通过一些复杂的密码学的方法来验证其正确性。

[0038] 2.跨链交易验证和业务逻辑耦合。跨链交易要传递的数据很简单，但是由于每一个跨链合约都要自己验证跨链交易的合法性，使得跨链交易的构造变得非常复杂。

[0039] 3.跨链信息生成和验证没有统一的规范。如果开发者各自实现，无法做到通用性，使用者的心智负担很高。

[0040] 针对现有技术的不足，本申请实施例提出了一种同构区块链跨链交互方法和装置，下面进行说明。

[0041] 图2为本发明一实施例提供的跨链转移资产的示意图，结合图3所示，本实施例提供一种同构区块链跨链交互方法，包括：

[0042] S301、构造一个公共的跨链模块，用于维护跨链的元数据，使得每个链上合约都能够访问所述跨链模块中的所述元数据用于进行验证；

[0043] 在步骤S301中，元数据包括但不限于区块头、验证者名单等。相对于现有技术中每个合约自己维护跨链元数据，本方案由跨链模块统一维护。使得每条链的合约都能访问里面的数据用于验证。

[0044] S302、调用统一的协议来生成、传输和验证跨链消息；

[0045] S303、对虚拟机进行功能扩展，使得所述虚拟机支持跨链事件和跨链调用，所述跨链事件被触发后自动转发给所述跨链模块进行处理，所述跨链函数，只接受所述跨链事件的跨链调用；

[0046] 在步骤S303中，对虚拟机进行功能扩展，在普通事件基础上，新增跨链事件，触发后自动转发给跨链模块进行处理，在普通函数基础上，新增跨链函数，只接受跨链事件的调用。链上所有的跨链合约共享所述跨链模块的数据和方法，所述跨链合约只需处理业务逻辑，不再处理跨链数据维护和校验逻辑。

[0047] S304、链上所有的跨链合约共享所述跨链模块的数据和方法，所述跨链合约只需处理业务逻辑，不处理跨链数据维护和校验逻辑。

[0048] 在步骤S304中，链上所有的跨链合约共享所述跨链模块的数据和方法，所述跨链合约本身只需关心自己的业务逻辑，只需处理业务逻辑，不再处理跨链数据维护和校验逻辑。

[0049] 如图4所示，采用上述同构区块链跨链交互的方法进行资产转移时，对应的跨链资产转移流程为：

[0050] S401、在所述链上部署合约；

[0051] 在步骤S401中，开发者需要在A链上部署合约Contract A，用于执行用户指定的交易逻辑，并生成所述跨链事件CrossChainEventA；在B链上部署合约Contract B，其中包含针对CrossChainEventA的所述跨链函数CrossChainEventAHandler。

[0052] S402、根据所述合约通过所述跨链模块进行跨链交易；

[0053] 采用上述的开发流程，对于应用开发者来说，不再需要关心复杂的跨链消息验证逻辑，只需关心自己的业务逻辑。

[0054] 图5为用户在所述链上进行资源转移的流程图，具体包括：

[0055] S501、用户向A链的部署合约ContractA发送交易TX，执行交易逻辑；

[0056] S502、合约触发特殊的跨链事件CrossChainEventA后，由跨链模块负责生成对应的跨链消息传递到B链；

[0057] 在步骤502中可以在B链的跨链模块接收该跨链消息后，需要验证合法性，以保证交易安全。

[0058] S503、B链将所述消息分配给合约ContractB进行处理；

[0059] S504、合约ContractB调用处理函数CrossChainEventAHandler，执行对应的逻辑，完成跨链交易。

[0060] 通过上述方法，进行跨链交易时用户进行一次跨链交互只需要发送一个交易。例如在A链触发消息，在B链写消息处理函数，A链消息触发后，跨链模块会自动完成其它工作，调用B链的处理函数。跨链交互和调用本地函数一样简单。

[0061] 图6为本发明一实施例提供的跨链转移资产装置的示意图，如图6所示，本发明实施例提供的跨链转移资产装置600包括构造模块601，调用模块602，扩展模块603，共享模块604，其中：

[0062] 构造模块601，构造一个公共的跨链模块，用于维护跨链的元数据，使得每个链上合约都能够访问所述跨链模块中的所述元数据用于进行验证；

[0063] 调用模块602，调用统一的协议来生成、传输和验证跨链消息；

[0064] 扩展模块603，对虚拟机进行功能扩展，使得所述虚拟机支持跨链事件和跨链调用，所述跨链事件被触发后自动转发给所述跨链模块进行处理，所述跨链函数，只接受所述跨链事件的跨链调用；

[0065] 共享模块604，链上所有的跨链合约共享所述跨链模块的数据和方法，所述跨链合约只需处理业务逻辑，不处理跨链数据维护和校验逻辑。

[0066] 使用上述同构区块链跨链交互的装置同时具有部署模块和交易模块的装置。

[0067] 其中部署模块用于开发者在A链上部署合约Contract A，用于执行用户指定的交易逻辑，并生成所述跨链事件CrossChainEventA；在B链上部署合约Contract B，其中包含针对CrossChainEventA的所述跨链函数CrossChainEventAHandler。

[0068] 交易模块用于用户根据所述合约通过所述跨链模块进行跨链交易。

[0069] 交易过程中，用户首先向A链的部署合约ContractA发送交易TX，执行交易逻辑；合约触发特殊的跨链事件CrossChainEventA后，由跨链模块负责生成对应的跨链消息传递到

B链;B链将所述消息分配给合约ContractB进行处理;合约ContractB调用处理函数CrossChainEventAHandler,执行对应的逻辑,完成跨链交易。

[0070] 图7是本说明书的一个实施例电子设备的结构示意图。请参考图7,在硬件层面,该电子设备包括处理器,可选地还包括内部总线、网络接口、存储器。其中,存储器可能包含内存,例如高速随机存取存储器(Random-Access Memory,RAM),也可能还包括非易失性存储器(non-volatile memory),例如至少1个磁盘存储器等。当然,该电子设备还可能包括其他业务所需要的硬件。

[0071] 处理器、网络接口和存储器可以通过内部总线相互连接,该内部总线可以是ISA(Industry Standard Architecture,工业标准体系结构)总线、PCI(Peripheral Component Interconnect,外设部件互连标准)总线或EISA(Extended Industry Standard Architecture,扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图7中仅用一个双向箭头表示,但并不表示仅有一根总线或一种类型的总线。

[0072] 存储器,用于存放程序。具体地,程序可以包括程序代码,所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器,并向处理器提供指令和数据。

[0073] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行,在逻辑层面上形成共享资源访问控制装置。处理器,执行存储器所存放的程序,并具体用于执行前述任意一种同构区块链跨链交互方法的操作。

[0074] 处理器可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器,包括中央处理器(Central Processing Unit,CPU)、网络处理器(Network Processor,NP)等;还可以是数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field－Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本说明书实施例中公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本说明书实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器,闪存、只读存储器,可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器,处理器读取存储器中的信息,结合其硬件完成上述方法的步骤。

[0075] 除了软件实现方式之外,本说明书实施例的电子设备并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限定于各个逻辑单元,也可以是硬件或逻辑器件。

[0076] 本说明书实施例还提出了一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现前述任意一种同构区块链跨链交互方法的操作。

[0077] 总之,以上所述仅为本说明书的较佳实施例而已,并非用于限定本说明书的保护范围。凡在本说明书的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本说明书的保护范围之内。

[0078] 上述实施例阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,

或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[0079] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0080] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0081] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

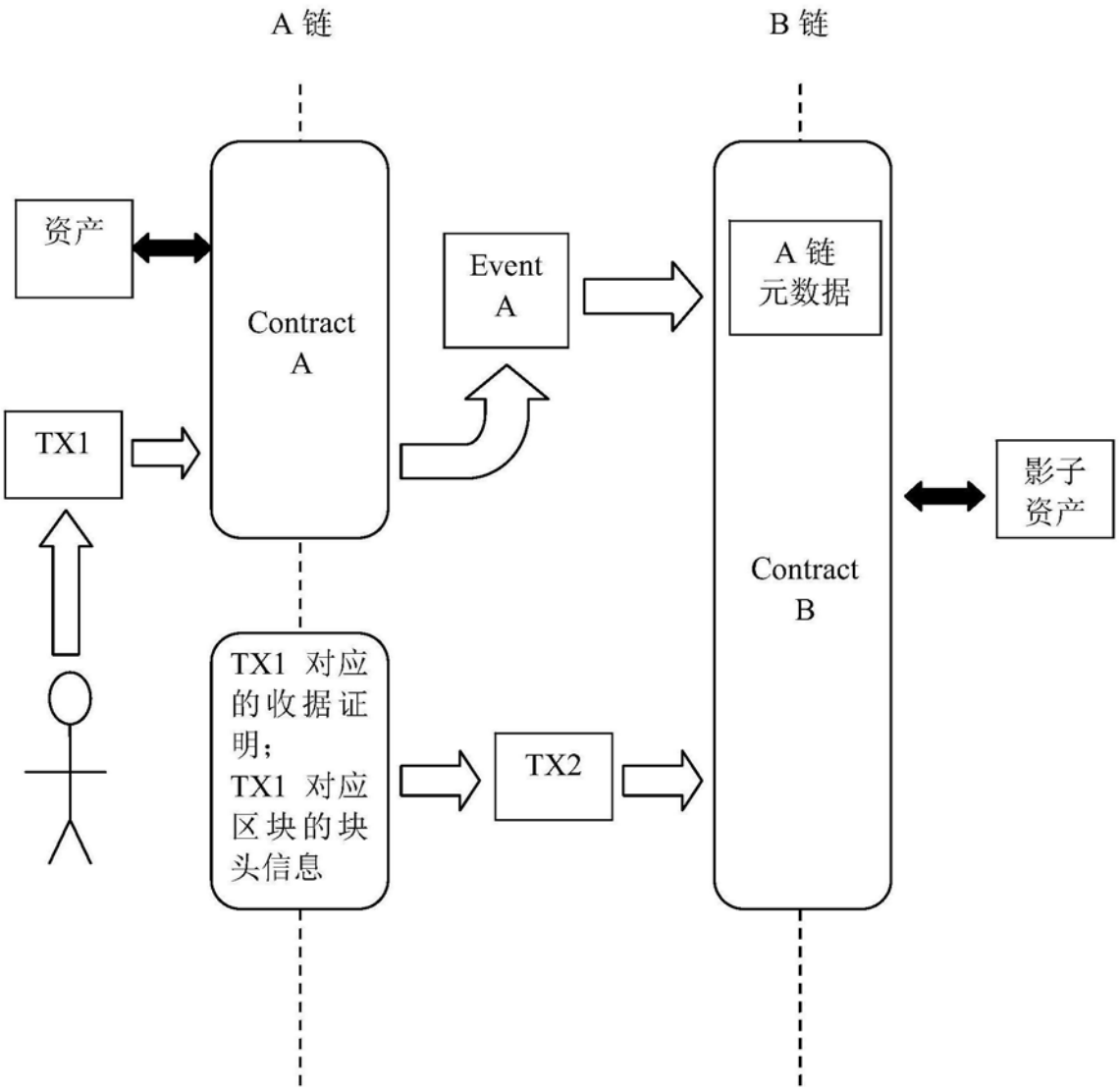

A 链
B 链
资产
Contract
A
Event
A
A 链
元数据
TX1
影子
资产
Contract
B
TX1 对应的收据证明；
TX1 对应区块的块头信息
TX2

图1

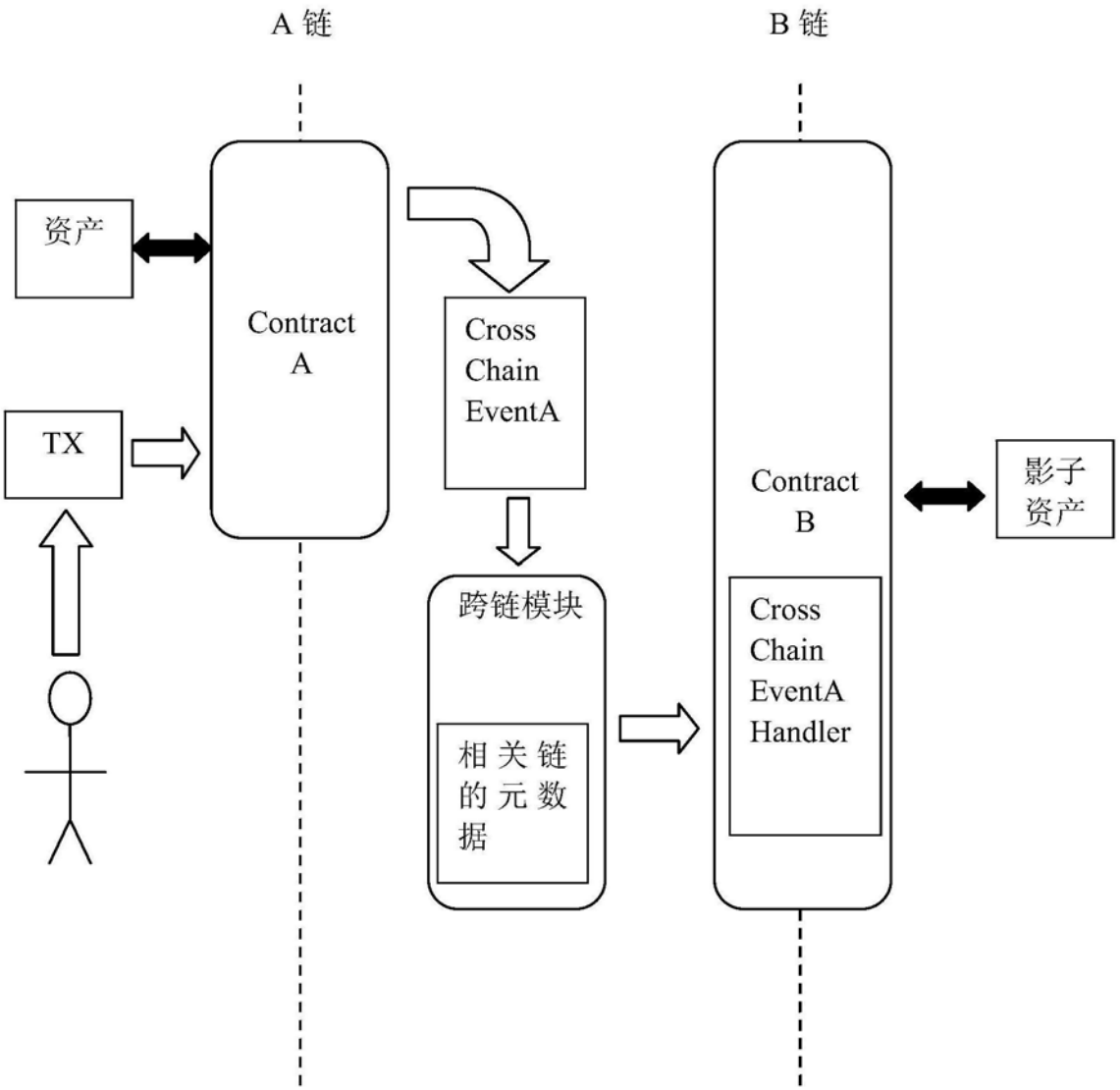

A 链
B 链
资产
Contract
A
TX
Cross
Chain
EventA
跨链模块
相关链的元数据
Contract
B
Cross
Chain
EventA
Handler
影子
资产

图2

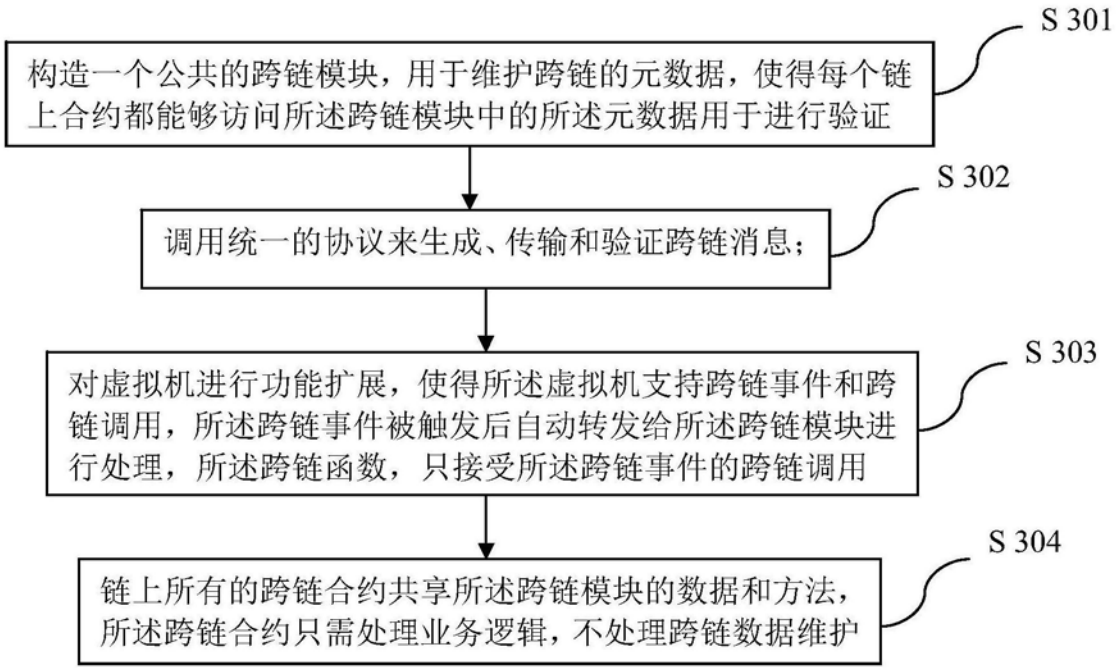

S 301
构造一个公共的跨链模块，用于维护跨链的元数据，使得每个链上合约都能够访问所述跨链模块中的所述元数据用于进行验证
S 302
调用统一的协议来生成、传输和验证跨链消息；
S 303
对虚拟机进行功能扩展，使得所述虚拟机支持跨链事件和跨链调用，所述跨链事件被触发后自动转发给所述跨链模块进行处理，所述跨链函数，只接受所述跨链事件的跨链调用
S 304
链上所有的跨链合约共享所述跨链模块的数据和方法，所述跨链合约只需处理业务逻辑，不处理跨链数据维护

图3

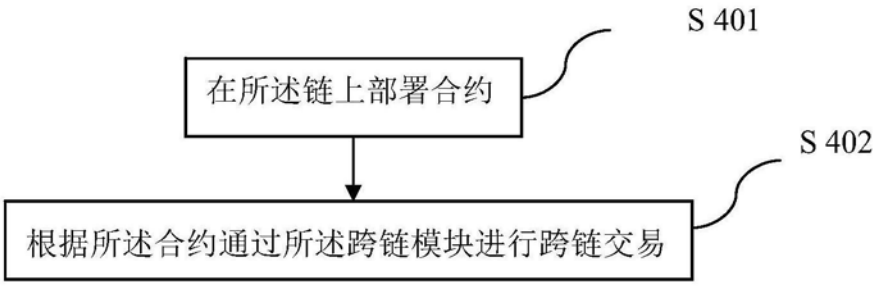

S 401
在所述链上部署合约
S 402
根据所述合约通过所述跨链模块进行跨链交易

图4

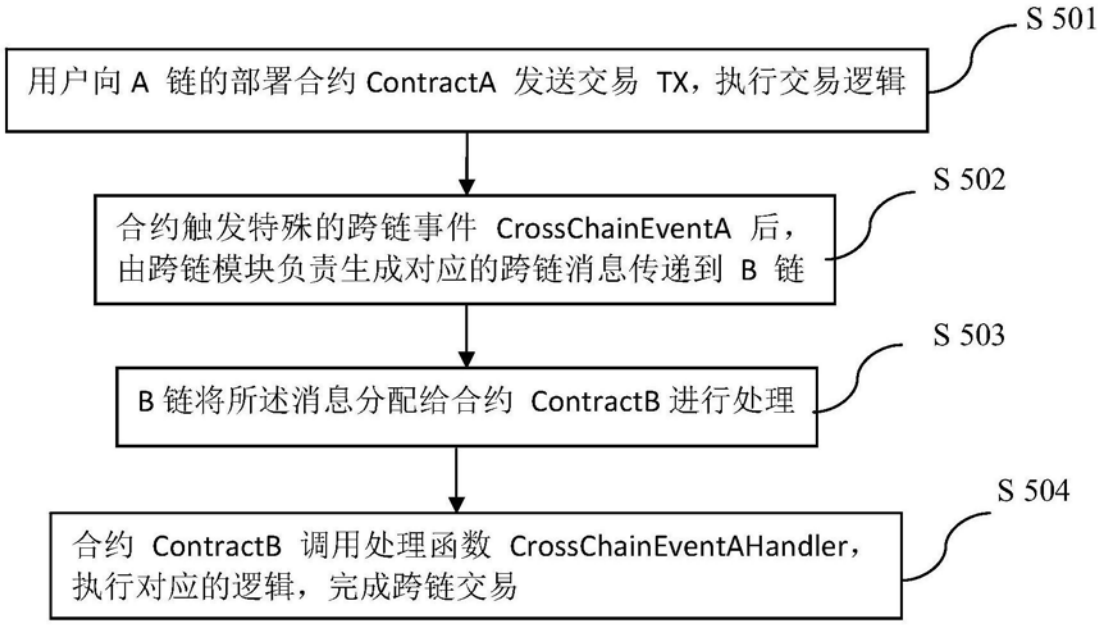

S 501
用户向 A 链的部署合约 ContractA 发送交易 TX，执行交易逻辑
S 502
合约触发特殊的跨链事件 CrossChainEventA 后，
由跨链模块负责生成对应的跨链消息传递到 B 链
S 503
B 链将所述消息分配给合约 ContractB 进行处理
S 504
合约 ContractB 调用处理函数 CrossChainEventAHandler，
执行对应的逻辑，完成跨链交易

图5

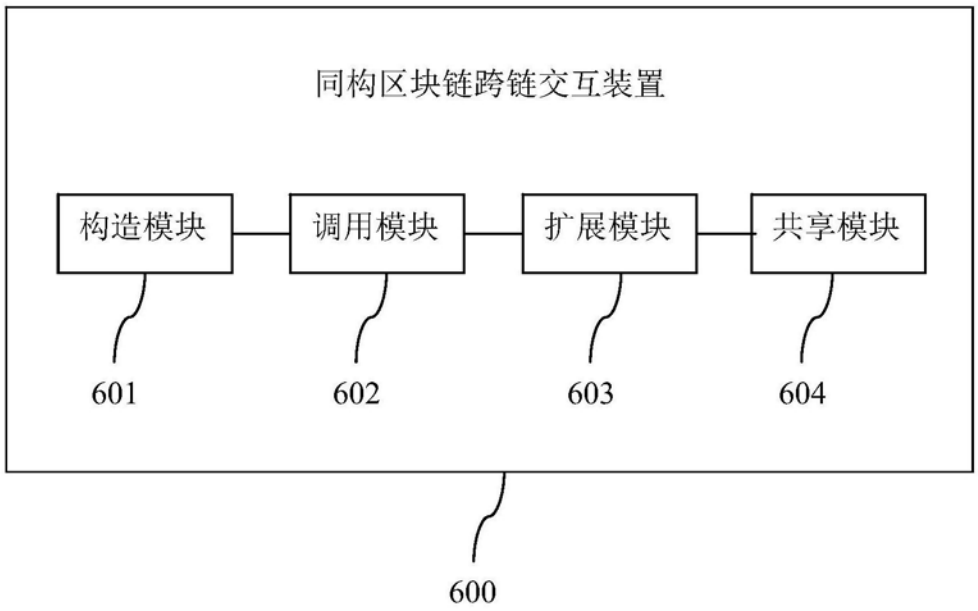

同构区块链跨链交互装置
构造模块
调用模块
扩展模块
共享模块
601
602
603
604
600

图6

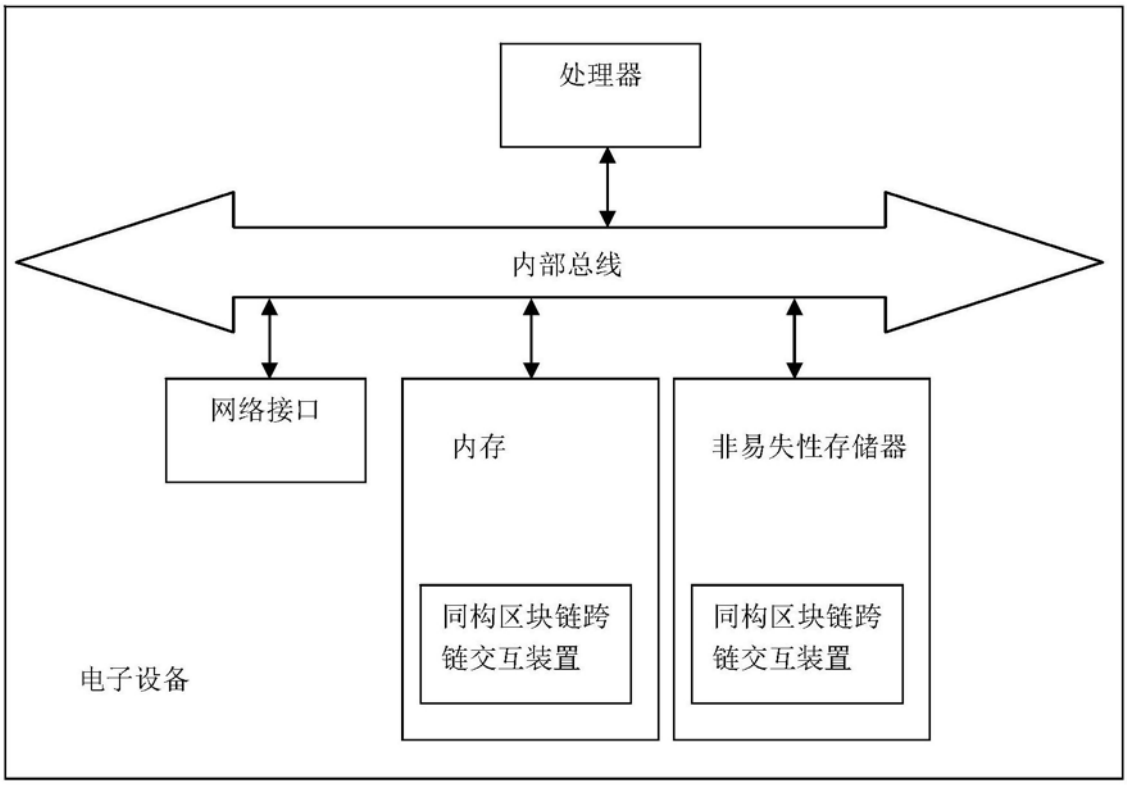


图7