(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 110035046 A
(43)申请公布日 2019.07.19

(21)申请号 201811364463.0

(22)申请日 2018.11.16

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

(72)发明人 邱鸿霖

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

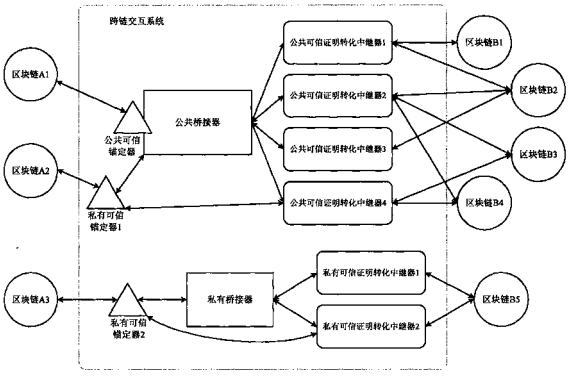
权利要求书1页 说明书6页 附图3页

(54)发明名称

跨区块链的交互系统

(57)摘要

本说明书一个或多个实施例提供一种跨区块链的交互系统，包括：一个或多个锚定器；其中，当任一锚定器被第一区块链选用时，任一锚定器中配置有第一区块链的客户端，以监听第一区块链上的跨链请求；一个或多个中继器；其中，当任一中继器被第二区块链选用时，任一中继器上配置有第二区块链的客户端，且任一中继器在跨链请求的请求对象为第二区决链时，基于跨链请求向第二区块链发起请求，并接收第二区块链返回的响应数据和链上证明，使任一中继器根据链上证明对响应数据进行验证，以及任一中继器在验证通过后根据已配置的可信证明转化技术生成相应的中继器证明，以使响应数据和中继器证明经由任一锚定器返回第一区块链。



CN 110035046 A

1.一种跨区块链的交互系统,包括:

一个或多个锚定器;其中,当任一锚定器被第一区块链选用时,所述任一锚定器中配置有所述第一区块链的客户端,以监听所述第一区块链上的跨链请求;

一个或多个中继器;其中,当任一中继器被第二区块链选用时,所述任一中继器上配置有所述第二区块链的客户端,且所述任一中继器在所述跨链请求的请求对象为所述第二区块链时,基于所述跨链请求向所述第二区块链发起请求,并接收所述第二区块链返回的响应数据和链上证明,使所述任一中继器根据所述链上证明对所述响应数据进行验证,以及所述任一中继器在验证通过后根据已配置的可信证明转化技术生成相应的中继器证明,以使所述响应数据和所述中继器证明经由所述任一锚定器返回所述第一区块链。

2.根据权利要求1所述的系统,所述任一锚定器为公共锚定器;或者,所述任一锚定器为所述第一区块链配置的私有锚定器。

3.根据权利要求1所述的系统,所述任一中继器为公共中继器;或者,所述任一中继器为所述第二区块链配置的私有中继器。

4.根据权利要求1所述的系统,当存在多个中继器时,多个中继器中的至少两个分别配置有不同的可信证明转化技术。

5.根据权利要求1所述的系统,还包括:

至少一个桥接器;其中,任一桥接器分别连接至所述任一锚定器与所述任一中继器,用于将所述任一锚定器提供的跨链请求转发至所述任一中继器,并将所述任一中继器提供的所述响应数据和所述中继器证明转发至所述任一锚定器。

6.根据权利要求5所述的系统,所述任一桥接器为公共桥接器;或者,所述桥接器为专用于所述第一区块链与所述第二区块链之间的私有桥接器。

7.根据权利要求5所述的系统,当所述任一桥接器为公共桥接器时,所述任一锚定器为公共锚定器和/或所述任一中继器为公共中继器;当所述任一桥接器为私有桥接器时,所述任一锚定器为私有锚定器且所述任一中继器为私有中继器。

8.根据权利要求1所述的系统,所述任一锚定器上配置有所述第一区块链的简单支付验证客户端;和/或,所述任一中继器上配置有所述第二区块链的简单支付验证客户端。

9.根据权利要求1所述的系统,所述可信证明转化技术包括下述任一:可信执行环节技术、权威证明共识技术、安全多方计算技术、零知识证明技术。

10.根据权利要求1所述的系统,所述任一中继器的信任根被预先发布,以使所述第一区块链根据所述信任根对所述响应数据和所述中继器证明进行验证。

跨区块链的交互系统

技术领域

[0001] 本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种跨区块链的交互系统。

背景技术

[0002] 在相关技术中，通过中继链可以实现不同区块链之间的跨链交互。中继链可以分别与各个区块链进行对接，并由该中继链上设置的若干验证者通过共识算法对各个区块链上的跨链数据进行验证，而其他区块链只需对接该中继链即可获得跨链数据。

发明内容

[0003] 有鉴于此，本说明书一个或多个实施例提供一种跨区块链的交互系统。

[0004] 为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[0005] 根据本说明书的一个或多个实施例，提出了一种跨区块链的交互系统，包括：

[0006] 一个或多个锚定器；其中，当任一锚定器被第一区块链选用时，所述任一锚定器中配置有所述第一区块链的客户端，以监听所述第一区块链上的跨链请求；

[0007] 一个或多个中继器；其中，当任一中继器被第二区块链选用时，所述任一中继器上配置有所述第二区块链的客户端，且所述任一中继器在所述跨链请求的请求对象为所述第二区块链时，基于所述跨链请求向所述第二区块链发起请求，并接收所述第二区块链返回的响应数据和链上证明，使所述任一中继器根据所述链上证明对所述响应数据进行验证，以及所述任一中继器在验证通过后根据已配置的可信证明转化技术生成相应的中继器证明，以使所述响应数据和所述中继器证明经由所述任一锚定器返回所述第一区块链。

附图说明

[0008] 图1是一示例性实施例提供的一种跨链交互的示意图。

[0009] 图2是一示例性实施例提供的一种跨链交互系统的结构示意图。

[0010] 图3是一示例性实施例提供的另一种跨链交互系统的结构示意图。

[0011] 图4是一示例性实施例提供的又一种跨链交互系统的结构示意图。

[0012] 图5是一示例性实施例提供的一种提供桥接功能的跨链交互系统的结构示意图。

具体实施方式

[0013] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[0014] 需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行

相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[0015] 图1是一示例性实施例提供的一种跨链交互的示意图。以如图1所示的区块链1与区块链2之间的跨链交互为例，该区块链1与区块链2可以通过跨链交互系统实现跨链交互，该跨链交互系统可以包括：可信锚定器和可信证明转化中继器；可信锚定器中可以配置区块链1的客户端，使得该可信锚定器与区块链1之间建立连接，而可信证明转化中继器中可以配置区块链2的客户端，使得可信证明转化中继器与区块链2之间建立连接。

[0016] 在一实施例中，可信锚定器、可信证明转化中继器上分别配置的客户端可以为SPV(Simplified Payment Verification，简单支付验证)客户端，可使可信锚定器、可信证明转化中继器的配置轻量化。当然，通过配置其他类型的客户端，同样可以实现相关跨链交互功能，本说明书并不对此进行限制。

[0017] 在一实施例中，当区块链1需要向区块链2调取跨链数据时，可以在区块链1上创建跨链请求，且该跨链请求的请求对象为区块链2。而通过已配置的区块链1的客户端，可信锚定器能够监听区块链1上创建的跨链请求，并基于该跨链请求所指示的请求对象为区块链2以及区块链2与可信证明转化中继器之间存在连接关系，将跨链请求传输至可信证明转化中继器，并由可信证明转化中继器进一步将跨链请求传输至区块链2。

[0018] 进一步地，通过已配置的区块链2的客户端，可信证明转化中继器可以调取区块链2针对上述跨链请求形成的响应数据，并将该响应数据返回至可信锚定器，而可信锚定器可以将该响应数据进一步返回至区块链1，从而完成区块链1与区块链2之间的跨链交互。

[0019] 除了响应数据之外，可信证明转化中继器还从区块链2调取相应的链上证明，且可信证明转化中继器可以根据该链上证明对响应数据进行验证，比如确定该响应数据存在于区块链2的区块链账本中等，本说明书并不对此进行限制。同时，可信证明转化中继器配置有可信证明转化技术，使得根据链上证明对响应数据实施验证操作后，如果验证结果为通过验证，该可信证明转化中继器可以基于可信证明转化技术生成中继器证明，相当于将链上证明转化为中继器证明。然后，可信证明转化中继器将响应数据与中继器证明返回至可信锚定器，并由可信锚定器进一步返回至区块链1；其中，可信证明转化中继器可以预先发布信任根，而区块链1可以预先获取并部署该信任根，使得该区块链1在获得上述的响应数据和中继器证明后，可以基于该信任根对响应数据和中继器证明进行验证，以确定可信证明转化中继器针对所提供的响应数据实施过验证且验证通过。

[0020] 可见，通过采用上述的跨链交互系统，使得可信锚定器、可信证明转化中继器均只需要配置存在接入需求的区块链的客户端，而无需配置所有参与跨链交互的区块链的客户端，使得可信锚定器与可信证明转化中继器均十分轻量化。同时，通过在可信证明转化中继器上配置可信证明转化技术，可以通过该中继器实现对响应数据可靠性的单点证明，区别于相关技术中基于共识算法的中继链，由于对中继器证明的转化过程相比于共识过程更为高效、便捷，使得在确保响应数据可靠性的情况下，能够提升跨链交互效率。并且，由于可信证明转化中继器得到的证明信息仅为一份(即中继器证明)，区别于相关技术中的中继链内的众多验证者所提供的多份证明信息(每一验证者提供一份证明信息)，能够极大地简化区

块链1对于证明信息的验证过程、有助于提升验证效率。

[0021] 基于上述结构的跨链交互系统，可以根据实际的流量、容量需求进行伸缩部署，具有极强的部署弹性。例如，图2是一示例性实施例提供的一种跨链交互系统的结构示意图。如图2所示，跨链交互系统中可以部署多个可信证明转化中继器，比如可信证明转化中继器1～4等，一方面可以增加可信证明转化中继器的数量、以扩展可支持的区块链数量，另一方面可以为各个可信证明转化中继器配置多种类型的可信证明转化技术，比如TEE(Trusted Execution Environment，可信执行环节技术)技术、POA(Proof of Authority，权威证明共识)技术、MPC(Secure Multi-Party Computation，安全多方计算)技术、零知识证明(Zero-Knowledge Proof)技术等，本说明书并不对此进行限制。由于不同的可信证明转化技术所实现的性能模型、安全边界等均不同，因而可以满足不同场景下的应用需求。

[0022] 在一实施例中，可以在可信证明转化中继器1中配置TEE技术、在可信证明转化中继器2中配置POA技术、在可信证明转化中继器3中配置MPC技术、在可信证明转化中继器4中配置零知识证明技术，而区块链2、区块链4～6可以根据实际需求选用特定的可信证明转化中继器，以用于对自身提供的链上证明进行可信证明转化。例如，区块链2可以选用可信证明转化中继器1～3，则可信证明转化中继器1～3中需要分别配置区块链2的客户端；区块链4可以选用可信证明转化中继器1，则可信证明转化中继器1中需要配置区块链4的客户端；区块链5可以选用可信证明转化中继器2、4，则可信证明转化中继器2、4中需要配置区块链5的客户端；区块链6可以选用可信证明转化中继器2、4，则可信证明转化中继器2、4中需要配置区块链6的客户端。

[0023] 在一实施例中，区块链2、区块链4～6等可以对可信证明转化中继器1～4进行共享，即可信证明转化中继器1～4为公共类型，这样可以减少跨链交互系统中相同的可信证明转化中继器(即配置有相同的可信证明转化技术)的数量，有助于简化系统复杂度。当然，本说明书并不限制在跨链交互系统中配置相同的可信证明转化中继器，比如当需要调用的区块链数量较多时，由于同一可信证明转化中继器的性能有限，可以配置多个相同的可信证明转化中继器，以实现性能需求的分流。再比如，可以基于数据隐私需求而配置相同的可信证明转化中继器；例如，图3是一示例性实施例提供的另一种跨链交互系统的结构示意图，假定可信证明转化中继器1为公共中继器、配置有TEE技术，而区块链2虽然希望采用TEE技术实现可信证明转化，但是不希望自身提供的响应数据被记录至可信证明转化中继器1中、避免发生外泄，那么区块链2可以配置专用的私有可信证明转化中继器，该私有可信证明转化中继器配置有TEE技术，且该私有可信证明转化中继器仅设有区块链2的客户端、其他区块链无法(如没有操作权限)在该私有可信证明转化中继器中设置自身的客户端，使得仅区块链2能够使用该私有可信证明转化中继器。

[0024] 在一实施例中，与中继器相类似地，可信锚定器也可以具有公共类型和私有类型，以满足不同的应用需求。比如图3所示，区块链3可以与公共可信锚定器相连，该公共可信锚定器中可以配置区块链3的客户端，使其能够监控区块链3上的跨链请求，并协助区块链3获得其他区块链提供的响应数据，这与图1所示的实施例相似，此处不再赘述。类似地，其他区块链也可以与该公共可信锚定器相连，使得该公共可信锚定器可以配置这些区块链的客户端、协助这些区块链完成跨链交互，此处不再赘述。再比如，区块链1可以配置私有可信锚定器，该私有可信锚定器上配置有区块链1的客户端，且其他区块链无法(如没有操作权限)在

该私有可信锚定器上配置自身的客户端，使得该私有可信锚定器仅用于监控区块链1上的跨链请求，并协助区块链1完成跨链交互。

[0025] 可见，基于如图3所示的跨链交互系统，作为调用方的区块链可以根据实际需求选用私有可信锚定器或公共可信锚定器、作为被调用方的区块链可以根据实际需求选用私有可信证明转化中继器或公共可信证明转化中继器，从而满足作为调用方或被调用方的区块链的隐私需求。

[0026] 需要指出的是：本说明书中的每一可信证明转化中继器在逻辑上可以视为“一个设备”，使得每一可信证明转化中继器在获取被调用方的区块链返回的跨链数据和链上证明后，可以基于对跨链数据和链上证明的验证结果，将链上证明转化为可信的中继器证明，且该中继器证明的数量仅为一份，区别于相关技术中的中继链内的多个验证者分别提供的多份证明。当然，每一可信证明转化中继器实际上可以运行于单台电子设备上，比如包含一独立主机的物理服务器、PC、笔记本电脑、手机等；或者，每一可信证明转化中继器可以运行于多台电子设备构成的设备集群上，比如主机集群承载的虚拟服务器等；本说明书并不对此进行限制。

[0027] 图4是一示例性实施例提供的又一种跨链交互系统的结构示意图。如图4所示，当区块链1选用私有可信锚定器时，该私有可信锚定器可以连接至公共类型的可信证明转化中继器1，而并不一定与如图3所示的私有可信证明转化中继器相连。实际上，如果作为调用方的区块链1存在隐私需求、作为被调用方的区块链2不存在隐私需求，那么区块链1可以选用私有可信锚定器、区块链2可以选用公共类型的可信证明转化中继器1，从而分别满足各个区块链的实际需求。

[0028] 在如图1-4所示的实施例中，跨链交互系统中的可信锚定器和可信证明转化中继器之间直接建立连接；而在其他实施例中，比如图5是一示例性实施例提供的一种提供桥接功能的跨链交互系统的结构示意图，可以通过设置桥接器，使得该桥接器分别连接至可信锚定器和可信证明转化中继器，实现可信锚定器与可信证明转化中继器之间的桥接功能。

[0029] 例如，通过设置公共桥接器，以连接至公共可信证明转化中继器1～4等公共可信证明转化中继器。其中，公共桥接器可以连接至公共可信锚定器，比如该公共可信锚定器可以直接配置于该公共桥接器处，当然本说明书并不对此进行限制；或者，该公共桥接器可以连接至私有可信锚定器1或其他的私有可信锚定器。那么，当区块链A1连接至公共可信锚定器、区块链B1～B4分别连接至各个公共可信证明转化中继器时，该区块链A1可以针对区块链B1～B4实现跨链交互；而当区块链A2连接至私有可信锚定器1、区块链B1～B4分别连接至各个公共可信证明转化中继器时，该区块链A2可以针对区块链B1～B4实现跨链交互。

[0030] 再例如，通过设置私有桥接器，可以分别连接至私有可信锚定器2和私有可信证明转化中继器1-2，当区块链A3连接至私有可信锚定器2、区块链B5连接至私有可信证明转化中继器1-2时，该区块链A3可以针对区块链B5实现跨链交互。

[0031] 当然，正如上文所述，公共桥接器、私有桥接器等桥接器并非必须，比如私有可信锚定器1可以直接连接至公共可信证明转化中继器4、私有可信锚定器2可以直接连接至私有可信证明转化中继器2，公共可信锚定器也可以直接连接至指定的公共或私有类型的可信证明转化中继器，从而实现相关区块链的跨链交互。

[0032] 虽然上述实施例中将桥接器划分为公共桥接器、私有桥接器，但实际上也可以不

予以区分，比如可以通过同一桥接器分别连接至公共可信锚定器、私有可信锚定器、公共可信证明转化中继器、私有可信证明转化中继器，只要能够实现相应的桥接功能即可。当然，对于存在较高的数据隐私需求的区块链而言，可以选择采用专门的桥接器，即相当于上述的私有桥接器。

[0033] 综上所述，本说明书通过提出一种新型的跨链交互系统，不需要中心化的中继链，而是采用单机形式的可信证明转化中继器与区块链连接，不仅相对更加轻量化，并且可以根据流量、容量需求而对采用的可信证明转化中继器进行灵活部署，还可以根据实际需求选择配置特定的可信证明转化技术、不限于采用诸如共识算法等方式。同时，区块链可以根据需求配置公共类型或私有类型的可信锚定器、可信证明转化中继器和桥接器，该公共类型的相关节点可以满足诸如公有链下的快捷配置，而私有类型的相关节点可以避免隐私数据被其他区块链获得，能够满足部分区块链的隐私需求，支持有访问权限的私有链或联盟链的应用需求。

[0034] 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，计算机的具体形式可以是个人计算机、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、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0035] 在一个典型的配置中，计算机包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0036] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0037] 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、磁盘存储、量子存储器、基于石墨烯的存储介质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。

[0038] 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。

[0039] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺

序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[0040] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0041] 应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在.....时”或“当.....时”或“响应于确定”。

[0042] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

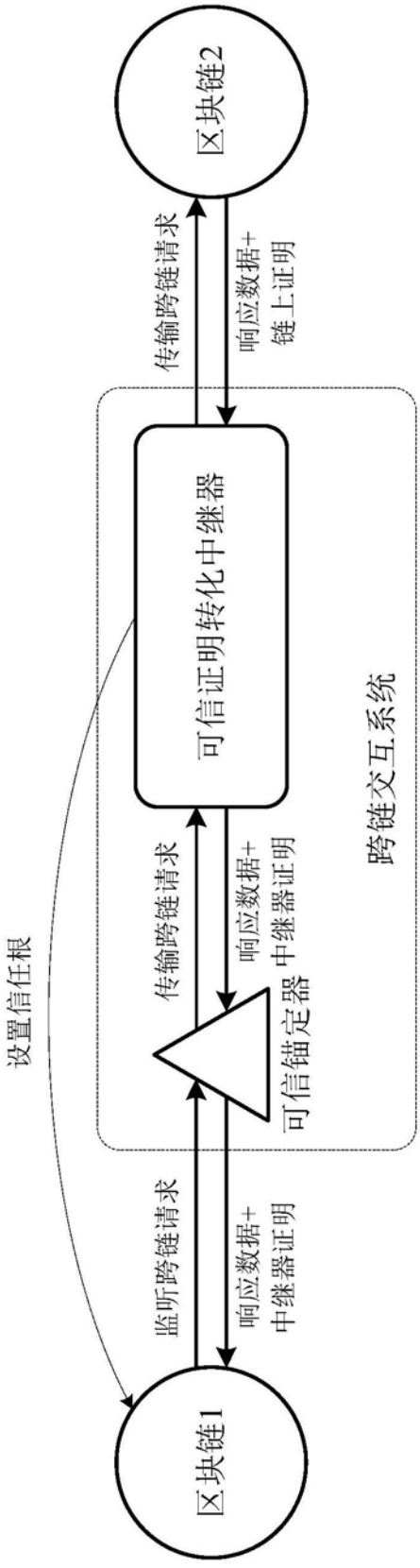

区块链2
传输跨链请求
响应数据+
链上证明
可信证明转化中继器
跨链交互系统
传输跨链请求
响应数据+
中继器证明
可信锚定器
设置信任根
监听跨链请求
响应数据+
中继器证明
区块链1

图1

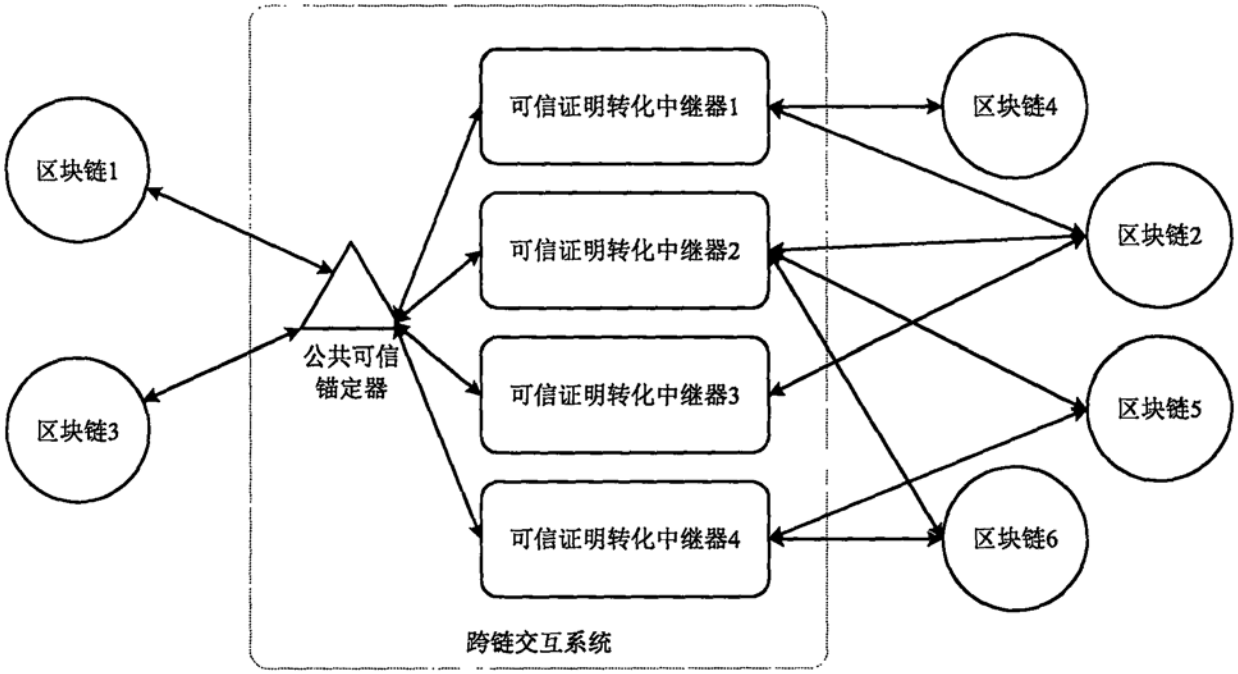

区块链1
区块链3
公共可信
锚定器
可信证明转化中继器1
可信证明转化中继器2
可信证明转化中继器3
可信证明转化中继器4
跨链交互系统
区块链4
区块链2
区块链5
区块链6

图2

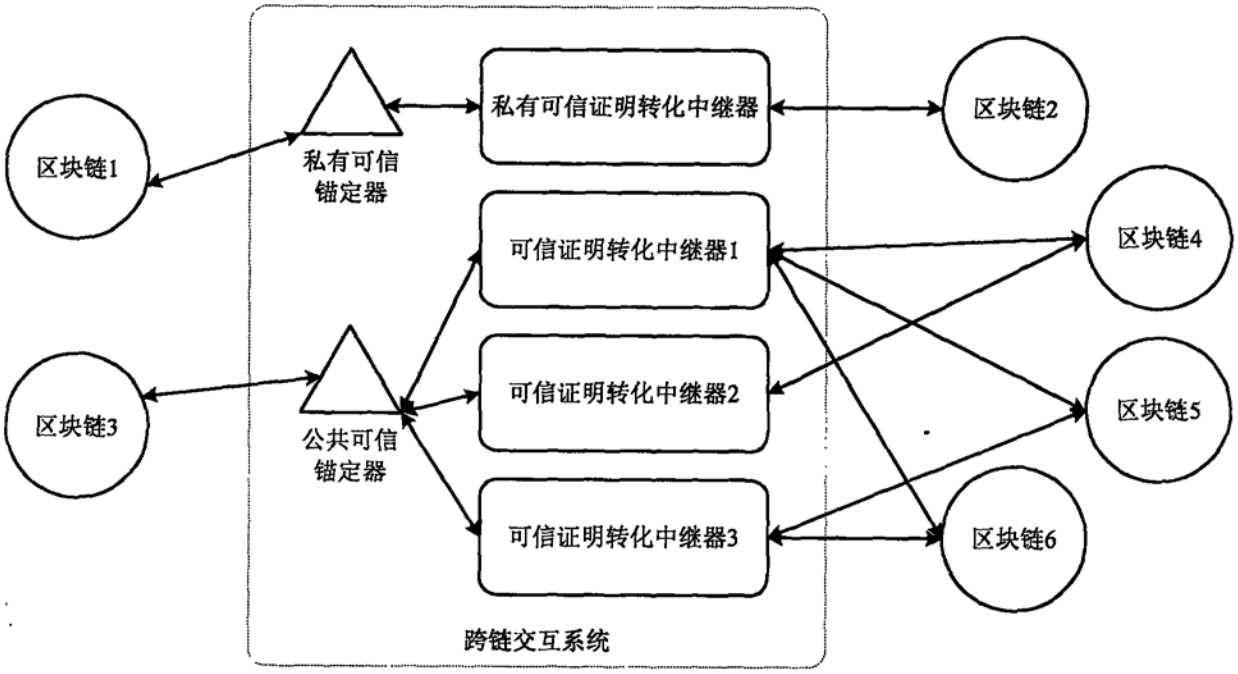

区块链1
区块链3
私有可信
锚定器
公共可信
锚定器
私有可信证明转化中继器
可信证明转化中继器1
可信证明转化中继器2
可信证明转化中继器3
跨链交互系统
区块链2
区块链4
区块链5
区块链6

图3

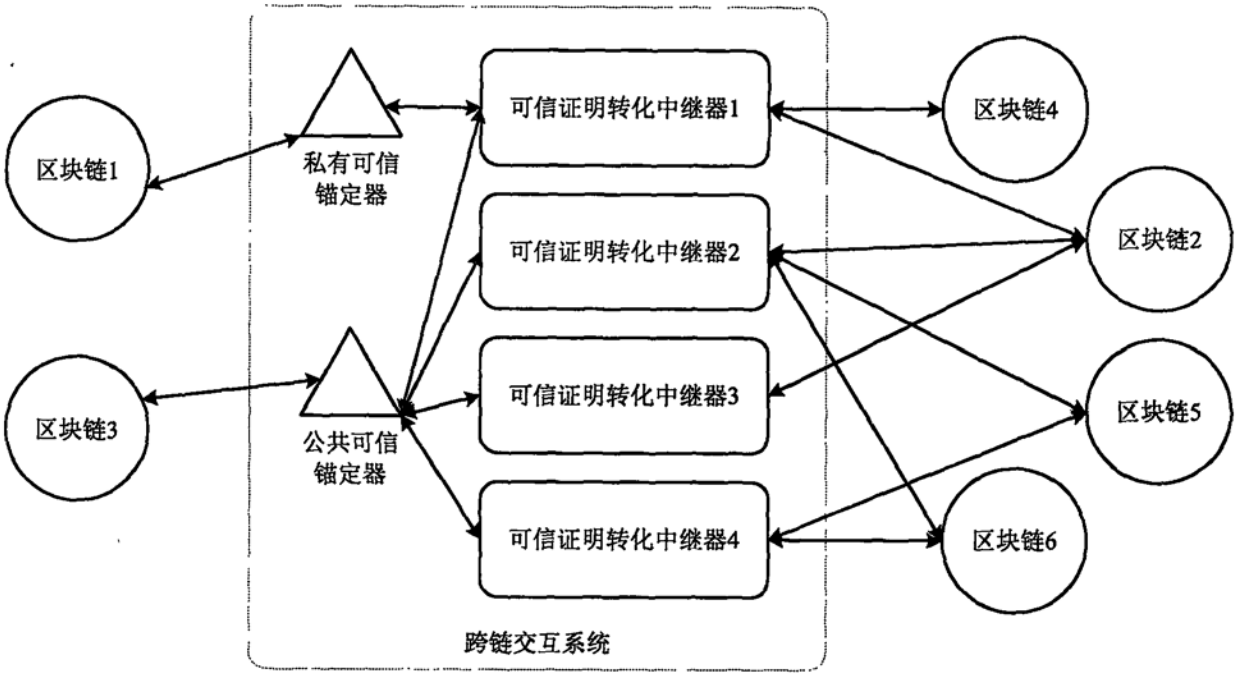

区块链1
私有可信锚定器
可信证明转化中继器1
区块链4
区块链2
可信证明转化中继器2
区块链3
公共可信锚定器
可信证明转化中继器3
区块链5
可信证明转化中继器4
区块链6
跨链交互系统

图4

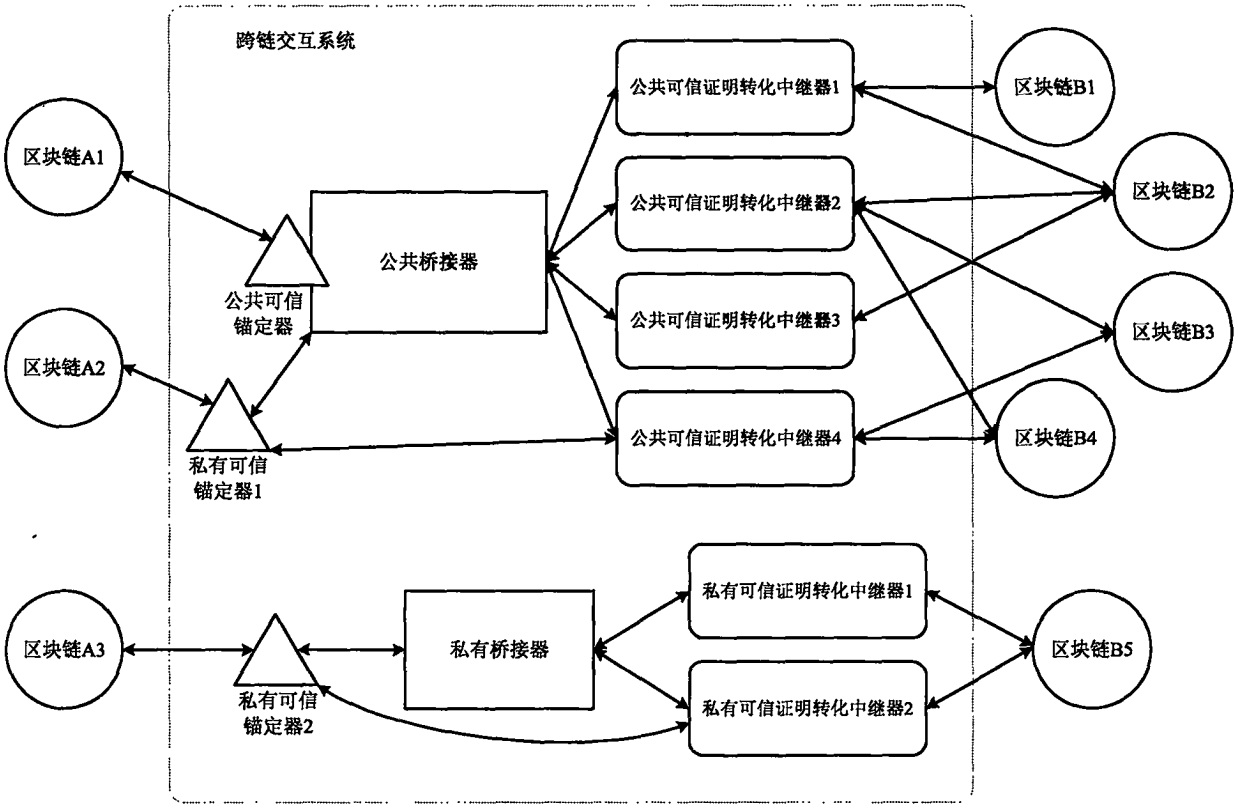

跨链交互系统
区块链A1
公共桥接器
公共可信证明转化中继器1
区块链B1
区块链B2
公共可信证明转化中继器2
公共可信锚定器
区块链A2
公共可信证明转化中继器3
区块链B3
私有可信锚定器1
公共可信证明转化中继器4
区块链B4
区块链A3
私有桥接器
私有可信证明转化中继器1
区块链B5
私有可信锚定器2
私有可信证明转化中继器2

图5