



(12)发明专利申请

(10)申请公布号 CN 108712257 A

(43)申请公布日 2018. 10. 26

(21)申请号 201810291308.4

(22)申请日 2018.04.03

(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 9/32(2006.01)

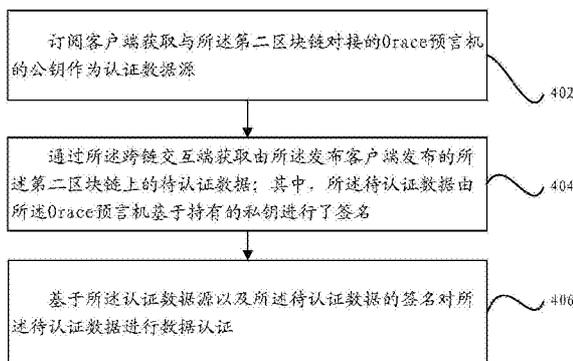
权利要求书2页 说明书13页 附图4页

(54)发明名称

跨区块链的认证方法及装置、电子设备

(57)摘要

本说明书一个或多个实施例提供一种跨区块链的认证方法及装置、电子设备,应用于由订阅客户端、发布客户端、以及跨链交互端组成的跨链交互系统;其中,所述订阅客户端与第一区块链对应;所述发布客户端与第二区块链对应;所述跨链交互端与所述订阅客户端和所述发布客户端分别对接;包括:所述订阅客户端获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源;通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,所述待认证数据由所述Orace预言机基于持有的私钥进行了签名;基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。



1. 一种跨区块链的认证方法,应用于由订阅客户端、发布客户端、以及跨链交互端组成的跨链交互系统;其中,所述订阅客户端与第一区块链对应;所述发布客户端与第二区块链对应;所述跨链交互端与所述订阅客户端和所述发布客户端分别对接;所述方法包括:

所述订阅客户端获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源;

通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,所述待认证数据由所述Orace预言机基于持有的私钥进行了签名;

基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。

2. 根据权利要求1所述的方法,所述获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源,包括:

获取用户配置的与所述第二区块链对应的Orace预言机的公钥作为认证数据源;或者,

通过所述跨链交互端获取由所述发布客户端发布的与所述第二区块链对应的Orace预言机的公钥作为认证数据源。

3. 根据权利要求1所述的方法,通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据,包括:

向所述跨链交互端发起订阅请求;其中,所述订阅请求用于向所述跨链交互端指示订阅条件,以使所述跨链交互端基于所述订阅条件,向所述发布客户端请求所述第二区块链上满足所述订阅条件的待认证数据;

获取所述发布客户端发布的满足所述订阅条件,且由所述Orace预言机基于持有的私钥进行了签名的待认证数据。

4. 根据权利要求1所述的方法,所述基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证,包括:

基于所述认证数据源中保存的所述Orace预言机的公钥对所述待认证数据的签名进行验证;如果所述签名验证通过,确定针对所述待认证数据的数据认证通过。

5. 根据权利要求1所述的方法,所述发布客户端与所述Orace预言机对接;所述Orace预言机用于对所述第二区块链中的数据的数据认证,在数据认证通过后基于持有的私钥对认证通过的数据进行签名,并将签名后的数据主动推送至所述发布客户端;或者,响应于所述发布客户端的数据获取请求,将签名后的数据推送至所述发布客户端。

6. 根据权利要求1所述的方法,与所述第二区块链对应的Orace预言机为所述发布客户端。

7. 根据权利要求1所述的方法,所述订阅客户端对应于所述第一区块链上的节点设备;所述发布客户端以及所述Orace预言机对应于所述第二区块链上的节点设备。

8. 一种跨区块链的认证装置,应用于由订阅客户端、发布客户端、以及跨链交互端组成的跨链交互系统;其中,所述订阅客户端与第一区块链对应;所述发布客户端与第二区块链对应;所述跨链交互端与所述订阅客户端和所述发布客户端分别对接;所述方法包括:

第一获取模块,获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源;

第二获取模块,通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,所述待认证数据由所述Orace预言机基于持有的私钥进行了签名;

认证模块,基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。

9. 根据权利要求8所述的装置,所述第一获取模块:

获取用户配置的与所述第二区块链对应的Orace预言机的公钥作为认证数据源;或者,通过所述跨链交互端获取由所述发布客户端发布的与所述第二区块链对应的Orace预言机的公钥作为认证数据源。

10. 根据权利要求8所述的装置,所述第二获取模块:

向所述跨链交互端发起订阅请求;其中,所述订阅请求用于向所述跨链交互端指示订阅条件,以使所述跨链交互端基于所述订阅条件,向所述发布客户端请求所述第二区块链上满足所述订阅条件的待认证数据;

获取所述发布客户端发布的满足所述订阅条件,且由所述Orace预言机基于持有的私钥进行了签名的待认证数据。

11. 根据权利要求8所述的装置,所述认证模块:

基于所述认证数据源中保存的所述Orace预言机的公钥对所述待认证数据的签名进行验证;如果所述签名验证通过,确定针对所述待认证数据的数据认证通过。

12. 根据权利要求8所述的装置,所述发布客户端与所述Orace预言机对接;所述Orace预言机用于对所述第二区块链中的数据进行数据认证,在数据认证通过后基于持有的私钥对认证通过的数据进行签名,并将签名后的数据主动推送至所述发布客户端;或者,响应于所述发布客户端的数据获取请求,将签名后的数据推送至所述发布客户端。

13. 根据权利要求8所述的装置,与所述第二区块链对应的Orace预言机为所述发布客户端。

14. 根据权利要求8所述的装置,所述订阅客户端对应于所述第一区块链上的节点设备;所述发布客户端以及所述Orace预言机对应于所述第二区块链上的节点设备。

15. 一种电子设备,包括:

处理器;

用于存储机器可执行指令的存储器;

其中,通过读取并执行所述存储器存储的与基于区块链的跨区块链的认证的控制逻辑对应的机器可执行指令,所述处理器被促使:

获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源;

通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,跨链交互端位于由订阅客户端、发布客户端、以及跨链交互端组成的跨链交互系统中;所述订阅客户端与第一区块链对应;所述发布客户端与第二区块链对应;所述跨链交互端与所述订阅客户端和所述发布客户端分别对接;所述待认证数据由所述Orace预言机基于持有的私钥进行了签名;

基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。

## 跨区块链的认证方法及装置、电子设备

### 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认证方法及装置、电子设备。

### 背景技术

[0002] 区块链技术,也被称之为分布式账本技术,是一种由若干台计算设备共同参与“记账”,共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备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。

### 发明内容

[0003] 本说明提出一种跨区块链的认证方法,应用于由订阅客户端、发布客户端、以及跨链交互端组成的跨链交互系统;其中,所述订阅客户端与第一区块链对应;所述发布客户端与第二区块链对应;所述跨链交互端与所述订阅客户端和所述发布客户端分别对接;所述方法包括:

[0004] 所述订阅客户端获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源;

[0005] 通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,所述待认证数据由所述Orace预言机基于持有的私钥进行了签名;

[0006] 基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。

[0007] 可选的,所述获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源,包括:

[0008] 获取用户配置的与所述第二区块链对应的Orace预言机的公钥作为认证数据源;或者,

[0009] 通过所述跨链交互端获取由所述发布客户端发布的与所述第二区块链对应的Orace预言机的公钥作为认证数据源。

[0010] 可选的,通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据,包括:

[0011] 向所述跨链交互端发起订阅请求;其中,所述订阅请求用于向所述跨链交互端指示订阅条件,以使所述跨链交互端基于所述订阅条件,向所述发布客户端请求所述第二区块链上满足所述订阅条件的待认证数据;

[0012] 获取所述发布客户端发布的满足所述订阅条件,且由所述Orace预言机基于持有的私钥进行了签名的待认证数据。

[0013] 可选的,所述基于所述认证数据源以及所述待认证数据的签名对所述待认证数据

进行数据认证,包括:

[0014] 基于所述认证数据源中保存的所述Orace预言机的公钥对所述待认证数据的签名进行验证;如果所述签名验证通过,确定针对所述待认证数据的数据认证通过。

[0015] 可选的,所述发布客户端与所述Orace预言机对接;所述Orace预言机用于对所述第二区块链中的数据进行数据认证,在数据认证通过后基于持有的私钥对认证通过的数据进行签名,并将签名后的数据主动推送至所述发布客户端;或者,响应于所述发布客户端的数据获取请求,将签名后的数据推送至所述发布客户端。

[0016] 可选的,与所述第二区块链对应的Orace预言机为所述发布客户端。

[0017] 可选的,所述订阅客户端对应于所述第一区块链上的节点设备;所述发布客户端以及所述Orace预言机对应于所述第二区块链上的节点设备。

[0018] 本说明书还提出一种跨区块链的认证装置,应用于由订阅客户端、发布客户端、以及跨链交互端组成的跨链交互系统;其中,所述订阅客户端与第一区块链对应;所述发布客户端与第二区块链对应;所述跨链交互端与所述订阅客户端和所述发布客户端分别对接;所述方法包括:

[0019] 第一获取模块,获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源;

[0020] 第二获取模块,通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,所述待认证数据由所述Orace预言机基于持有的私钥进行了签名;

[0021] 认证模块,基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。

[0022] 可选的,所述第一获取模块:

[0023] 获取用户配置的与所述第二区块链对应的Orace预言机的公钥作为认证数据源;或者,

[0024] 通过所述跨链交互端获取由所述发布客户端发布的与所述第二区块链对应的Orace预言机的公钥作为认证数据源。

[0025] 可选的,所述第二获取模块:

[0026] 向所述跨链交互端发起订阅请求;其中,所述订阅请求用于向所述跨链交互端指示订阅条件,以使所述跨链交互端基于所述订阅条件,向所述发布客户端请求所述第二区块链上满足所述订阅条件的待认证数据;

[0027] 获取所述发布客户端发布的满足所述订阅条件,且由所述Orace预言机基于持有的私钥进行了签名的待认证数据。

[0028] 可选的,所述认证模块:

[0029] 基于所述认证数据源中保存的所述Orace预言机的公钥对所述待认证数据的签名进行验证;如果所述签名验证通过,确定针对所述待认证数据的数据认证通过。

[0030] 可选的,所述发布客户端与所述Orace预言机对接;所述Orace预言机用于对所述第二区块链中的数据进行数据认证,在数据认证通过后基于持有的私钥对认证通过的数据进行签名,并将签名后的数据主动推送至所述发布客户端;或者,响应于所述发布客户端的数据获取请求,将签名后的数据推送至所述发布客户端。

- [0031] 可选的,与所述第二区块链对应的Orace预言机为所述发布客户端。
- [0032] 可选的,所述订阅客户端对应于所述第一区块链上的节点设备;所述发布客户端以及所述Orace预言机对应于所述第二区块链上的节点设备。
- [0033] 本说明书还提出一种电子设备,包括:
- [0034] 处理器;
- [0035] 用于存储机器可执行指令的存储器;
- [0036] 其中,通过读取并执行所述存储器存储的与基于区块链的跨区块链的认证的控制逻辑对应的机器可执行指令,所述处理器被促使:
- [0037] 获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源;
- [0038] 通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,跨链交互端位于由订阅客户端、发布客户端、以及跨链交互端组成的跨链交互系统中;所述订阅客户端与第一区块链对应;所述发布客户端与第二区块链对应;所述跨链交互端与所述订阅客户端和所述发布客户端分别对接;所述待认证数据由所述Orace预言机基于持有的私钥进行了签名;
- [0039] 基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。
- [0040] 通过以上实施例,订阅客户端通过获取与第二区块链对接的Orace预言机的公钥作为认证数据源,进而在通过跨链交互端获取到由发布客户端发布的第二区块链上由所述Orace预言机基于持有的私钥进行签名后的待认证数据时,可以基于所述认证数据源以及所述待认证数据的签名对该待认证数据进行数据认证;
- [0041] 一方面,由于第二区块链上的数据会由与第二区块链对接的Orace预言机基于持有的私钥进行了签名,订阅客户端只需要将Orace预言机的公钥作为认证数据源进行存储,就可以基于Orace预言机的公钥和数据携带的签名对第二区块链上的数据进行认证,因此可以降低订阅客户端对第二区块链上的数据进行认证的复杂度;
- [0042] 另一方面,由于第一区块链和第二区块链之间可以采用订阅和发布的方式,通过跨链交互端来进行数据同步,因此对于不同的区块链之间,可以在互相隔离的前提下,实现无入侵的侧链锚定,进而可以高效的与其它区块链进行锚定,搭建出低复杂度、高扩展性的跨链网络。

## 附图说明

- [0043] 图1是一示例性实施例提供的一种跨区块链的交互系统的架构示意图。
- [0044] 图2是一示例性实施例提供的另一种跨区块链的交互系统的架构示意图。
- [0045] 图3是一示例性实施例提供的另一种跨区块链的交互系统的架构示意图。
- [0046] 图4是一示例性实施例提供的一种跨区块链的认证方法的流程图。
- [0047] 图5是一示例性实施例提供的一种跨区块链的关联转账系统的结构示意图。
- [0048] 图6是一示例性实施例提供的一种电子设备的结构示意图。
- [0049] 图7是一示例性实施例提供的一种跨区块链的认证装置的框图。

## 具体实施方式

[0050] 侧链技术,是指在一个区块链的基础上,将该区块链作为主链进一步扩展出一个侧链,并实现侧链与主链之间的侧链锚定的技术。

[0051] 其中,所谓侧链,是具备认证来自主链上的数据的能力的区块链;例如,在侧链上可以验证一笔交易、区块或者其它形式的区块链数据是否包含在主链的区块中。如果一个区块链具备认证另一个区块链上的数据的能力,那么该区块链就称之该另一个区块链的侧链。相应的,所谓侧链锚定,则是指在侧链上设置认证根(通常包括认证数据源和认证规则),使得该侧链具备认证来自主链上的数据的能力的过程。

[0052] 本说明书则旨在提出一种基于订阅和发布模型的侧链锚定框架,使得不同的区块链可以在互相隔离的前提下实现无入侵的侧链锚定。

[0053] 在实现时,可以搭建一个由订阅客户端、发布客户端以及跨链交互端组成的跨链交互系统;其中,订阅客户端与第一区块链对应;发布客户端与第二区块链对应;跨链交互端可以与订阅客户端和发布客户端分别对接。同时,第二区块链可以对接一个Orace预言机作为与第二区块链的授信节点。

[0054] Orace预言机用于对第二区块链中的数据的数据认证,并在数据认证通过后基于持有的私钥对认证通过的数据进行签名。而订阅客户端可以获取Orace预言机的公钥作为认证数据源。

[0055] 当订阅客户端通过跨链交互端获取到由发布客户端发布的所述第二区块链上的,由Orace预言机基于持有的私钥进行签名后的待认证数据后,可以基于上述认证数据源和上述待认证数据源的签名,对该待认证数据源进行数据认证。

[0056] 在以上技术方案中,一方面,由于第二区块链上的数据会由与第二区块链对接的Orace预言机基于持有的私钥进行了签名,订阅客户端只需要将Orace预言机的公钥作为认证数据源进行存储,就可以基于Orace预言机的公钥和数据携带的签名对第二区块链上的数据进行认证,因此可以降低订阅客户端对第二区块链上的数据进行认证的复杂度;

[0057] 另一方面,由于第一区块链和第二区块链之间可以采用订阅和发布的方式,通过跨链交互端来进行数据同步,因此对于不同的区块链之间,可以在互相隔离的前提下,实现无入侵的侧链锚定,进而可以高效的与其它区块链进行锚定,搭建出低复杂度、高扩展性的跨链网络。

[0058] 下面通过具体实施例并结合具体的应用场景对本说明书进行描述。

[0059] 请参见图1,图1是一示例性实施例提供的一种跨区块链的交互系统的架构示意图。

[0060] 如图1所示,上述跨区块链的交互系统可以是一个基于发布和订阅模型搭建的侧链锚定框架,具体可以包括:

[0061] 第一区块链和第二区块链,第一区块链为本说明书中与订阅客户端对应的锚定链(即可以作为侧链);相应的,第二区块链为本说明书中与发布客户端对应的被锚定链(即可以作为主链)。

[0062] 其中,需要说明的是,在本说明书中,“第一区块链”、“第二区块链”只是用于区分不同区块链所扮演的角色;第一区块链泛指可以作为侧链的一类区块链,而第二区块链泛指可以作为主链的一类区块链,并不特指某一区块链为“第一区块链”或“第二区块链”。

[0063] 订阅客户端,该订阅客户端对应于第一区块链,用于维护第一区块链订阅的来自

第二区块链的数据。

[0064] 如图1所示,在一实施例中,该订阅客户端具体可以对应于第一区块链的节点设备,用于维护该区块链节点对应的消息队列,该消息队列包含该区块链节点所订阅的数据。

[0065] 例如,该订阅客户端可以是依托于第一区块链,在第一区块链上使用智能合约实现的客户端组件;或者,也可以基于该订阅客户端对接的节点设备的原生扩展能力实现的客户端组件。

[0066] 在另一实施例中,上述订阅客户端,也可以配置在独立与第一区块链之外的设备、节点或者平台等处,通过实现的桥接接口与第一区块链进行桥接。

[0067] 发布客户端,该发布客户端对应于第二区块链,用于获取并发布第二区块链上共识完成的数据。

[0068] 例如,在实现时,发布客户端可以实现桥接接口,提供面向第二区块链的数据查询服务,与第二区块链进行桥接。基于区块链的分布式记账特性,第二区块链上的所有区块链节点之间可以通过共识维护相同内容的全量记账数据,即区块链账本,而发布客户端可以从该区块链账本上获取允许发布的信息,以供跨链交互端获取。

[0069] 在一实施例中,该发布客户端具体可以对应于第二区块链上的节点设备。在另一实施例中,发布客户端也可以配置在独立于第二区块链之外的设备、节点或平台等处;在另一实施例中,发布客户端可以配置在第二区块链内的区块链节点上。

[0070] 跨链交互端,通过桥接接口与第一区块链和第二区块链分别进行对接,并基于实现的数据搬运逻辑,实现第一区块链和第二区块链之间的跨链数据同步。在一实施例中,该跨链交互端可以接收订阅客户端发起的订阅请求,该订阅请求中包含订阅条件,该订阅条件用于向跨链交互端指示相关的订阅需求。跨链交互端可以向订阅客户端发起状态询问消息,来询问订阅客户端维护的数据状态,并根据订阅客户端返回的数据状态,来确定订阅客户端维护的数据中是否包含满足上述订阅条件的数据;

[0071] 例如,在实现时,该订阅客户端具体可以对应于第一区块链的节点设备,并通过维护该区块链节点对应的消息队列,来维护该区块链节点所订阅的数据。在这种情况下,跨链交互端可以向订阅客户端发起状态询问消息,来询问上述消息队列的队列状态,并根据订阅客户端返回的上述消息队列的队列状态,来确定该消息队列中是否包含满足该订阅条件的消息。

[0072] 一方面,如果订阅客户端维护的数据中包含满足上述订阅条件的数据,跨链交互端无需重复获取该数据;另一方面,如果订阅客户端维护的数据中不包含满足上述订阅条件的数据,则跨链交互端需要从上述的发布客户端处获取满足该订阅条件的数据;例如,跨链交互端可以向发布客户端请求满足上述订阅条件的数据,并将发布客户端返回的数据发送至订阅客户端,以对订阅客户端维护的数据进行更新。

[0073] 其中,在本说明书中,跨链交互端仅用于在发布客户端与订阅客户端之间搬运数据,并不需要对搬运的数据进行持久化存储,也不需要维护所搬运的数据的数据状态。在一实施例中,跨链交互端可以配置在独立于第一区块链和第二区块链之外的设备、节点或平台等处;在另一实施例中,跨链交互端也可以配置在第一区块链,或者第二区块链的节点设备上。

[0074] 请继续参见图2,在实际应用中,在订阅客户端与发布客户端之间可以配置多个相

互独立的跨链交互端,即订阅客户端以及发布客户端,可以分别与多个独立的跨链交互端对接;比如,如图2中示出的,跨链交互端1与跨链交互端2等。

[0075] 通过这种方式,可以在跨链交互端遭受诸如拒绝服务攻击的情况下,可以将遭受跨链攻击的跨链交互端所承载的服务,快速的切换至另一跨链交互端;比如,如图2所示,如果跨链交互端1遭受拒绝服务攻击时,可以将跨链交互端1所承载的服务,立即切换至跨链交互端2,使得订阅客户端仍然可以通过跨链交互端2获得发布客户端发布的消息。

[0076] 请参见图3,在一实施例中,上述第二区块链具体可以对接一个Orace预言机作为授信节点。该Orace预言机可以与第二区块链上的节点设备对应。例如,在实现时,可以在第二区块链的节点设备中选定一个或者多个节点设备作为授信节点,充当Orace预言机的角色。

[0077] 上述Orace预言机用于对第二区块链中的数据进行数据认证,并在数据认证通过后基于持有的私钥对认证通过的数据进行签名,然后将签名后的数据主动推送至发布客户端;或者,在接收到来自发布客户端的数据获取请求时,响应于该数据获取请求,将签名后的数据推送至所述发布客户端。

[0078] 其中,上述Orace预言机可以与上述订阅客户端保持对接(即Orace预言机位于第二区块链和订阅客户端之间),而订阅客户端可以获取Orace预言机的公钥作为认证数据源进行存储,来具备对第二区块链上的数据的认证能力;

[0079] 例如,在一种情况下,订阅客户端可以获取用户配置的上述Orace预言机的公钥作为认证数据源在本地进行存储;或者,在另一种情况下,上述Orace预言机的公钥具体也可以依托于以上示出的系统架构,通过发布客户端和跨链交互端向上述订阅客户端进行在线发布,在这种情况下,订阅客户端可以通过所述跨链交互端获取由发布客户端发布的Orace预言机的公钥作为认证数据源。

[0080] 其中,需要说明的是,在实际应用中,也可以对上述发布客户端和上述Orace预言机的功能进行整合;例如,在一个实施例中,上述发布客户端也可以充当与第二区块链对接的Orace预言机的角色,在这种情况下,使得在以上示出的系统架构中,不再需要在第二区块链和上述发布客户端之前独立部署作为授信节点的Orace预言机。

[0081] 在以上实施例中,通过在基于发布和订阅模型搭建的跨链交互系统中,引入与发布客户端与订阅客户端分别进行桥接的跨链交互端,采用发布和订阅的信息交互模式,来完成第一区块链和第二区块链之间的数据同步,一方面,可以实现第一区块链与第二区块链之间的数据隔离,使得第一区块链和第二区块链之间不再需要直接进行数据交互,来完成数据的同步;另一方面,由于通过在发布客户端与订阅客户端之间引入跨链交互端,可以实现发布客户端与订阅客户端在业务层面的解耦,因此可以显著降低发布客户端和订阅客户端的开发难度;例如,并不需要依托于第一区块链,来实现与发布客户端相关的业务逻辑;也并不需要依托于第二区块链,来实现与订阅客户端相关的业务逻辑,仅需要在第一区块链和第二区块链上分别实现订阅客户端和发布客户端的相关业务逻辑即可。

[0082] 请参考图4,图4是本说明书一实施例提供的一种跨区块链的认证方法,应用于如图1所示出的跨链交互系统中的订阅客户端,执行以下步骤:

[0083] 步骤402,所述订阅客户端获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源;

[0084] 步骤404,通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,所述待认证数据由所述Oracle预言机基于持有的私钥进行了签名;

[0085] 步骤406,基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。

[0086] 在本实施例描述的区块链,具体可以包括可以作为侧链与其它区块链网络进行锚定的任意类型的区块链网络。

[0087] 例如,在一个场景中,上述区块链具体可以是一个由若干成员区块链组成的联盟链中的任一成员区块链。在该联盟链中,各个成员区块链均可以作为侧链,与其它的成员区块链进行锚定。

[0088] 上述待认证的数据,具体可以包括收录在第一区块链的各区块中的,任意形式的数据;例如,上述待认证数据,可以包括但不限于交易(transfer)、区块、状态、事件,等等。

[0089] 在本说明书中,可以通过在上述订阅客户端中,设置对应于第二区块链的认证根,使得订阅客户端可以具备第二区块链上的数据的认证能力,将第一区块链作为侧链,与第一区块链进行锚定。

[0090] 其中,在订阅客户端中设置的认证根,通常包括认证数据源和认证规则两部分内容。

[0091] 其中,需要说明的是,上述认证数据源所包含的具体内容,通常取决于第一区块链和第二区块链所支持的数据认证协议;

[0092] 例如,以上述第一区块链和第二区块链支持SPV(Simplified Payment Verification,轻简支付验证)认证协议为例,在这种场景下,在订阅客户端中设置的认证数据源,可以仅包含第一区块链中存储的所有区块的区块头数据。

[0093] 而在上述第一区块链和第二区块链均支持Oracle(预言机)协议的场景下,在订阅客户端中设置的认证数据源,则可以包含与第二区块链对接的Oracle预言机对第一区块链中的数据进行签名时所使用的私钥对应的公钥或者公钥集合。

[0094] 上述认证规则,包括对第二区块链中的数据进行认证的认证逻辑;其中,需要说明的是,一方面,上述认证规则中所包含的认证逻辑的种类,通常取决于收录在第二区块链中的数据的具体类型;

[0095] 例如,在实际应用中,第二区块链中的数据可以包括但不限于交易、区块、状态、事件,等等。相应的,上述认证规则具体可以包括但不限于交易认证逻辑、区块认证逻辑、状态认证逻辑、事件认证逻辑,等等。另一方面,上述认证规则中所包含的认证逻辑的具体内容,通常取决于第一区块链和第二区块链所支持的数据认证协议;

[0096] 例如,以上述第一区块链和第二区块链支持SPV协议为例,在这种场景下,在订阅客户端中设置的认证规则所包含的认证逻辑,具体可以是认证订阅客户端收到的来自第二区块链中的待认证数据,是否包含在上述第二区块链的区块中的认证逻辑;如果确认上述待认证数据包含在上述第二区块链的区块中,此时针对该待认证数据的认证通过。

[0097] 而在上述第一区块链和第二区块链均支持Oracle协议的场景下,在订阅客户端中设置的认证规则所包含的认证逻辑,具体可以是基于设置的与第二区块链对接的Oracle预言机对第二区块链中的数据进行签名时所使用的私钥对应的公钥或者公钥集合,对订阅客

户端收到的来自第二区块链中的待认证数据携带的签名进行验证的认证逻辑;如果经过验证确认上述待认证数据携带的签名为上述信任节点的合法签名,此时针对该待认证数据的认证通过。

[0098] 以下以上述第一区块链和第二区块链均支持Orace协议,以及上述待认证数据为收录在上述第二区块链的区块中的交易为例,对订阅客户端对第二区块链上的数据进行认证的过程进行详细描述。

[0099] 在本实施例中,在将第一区块链作为侧链锚定到作为主链的第二区块链时,可以在订阅客户端上配置对应于第二区块链的认证根。

[0100] 一方面,上述订阅客户端可以获取与第二区块链对接的上述Orace预言机的公钥或者公钥集合,作为认证数据源在本地存储。

[0101] 其中,获取上述Orace预言机的公钥或者公钥集合的方式具体可以包括以下两种情形:

[0102] 在一种情形下,订阅客户端可以获取用户配置的上述Orace预言机的公钥作为认证数据源在本地进行存储。

[0103] 在另一种情形下,上述Orace预言机的公钥具体也可以依托于以上示出的系统架构,通过发布客户端和跨链交互端向上述订阅客户端进行在线发布,在这种情况下,订阅客户端可以通过所述跨链交互端获取由发布客户端发布的Orace预言机的公钥作为认证数据源。

[0104] 另一方面,可以在上述订阅客户端上配置用于对第二区块链中的交易进行认证的认证规则。对于Orace协议而言,上述认证规则具体可以包括基于行数Orace预言机的公钥或者公钥集合,对订阅客户端收到的来自第二区块链中的待认证数据携带的签名进行验证的认证逻辑。当按照以上描述的方式,在订阅客户端上配置完成对应于第二区块链的认证根后,此时上述订阅客户端已经具备对来自第二区块链上的待认证数据进行认证的能力。

[0105] 在本说明书中,与第二区块链对接的Orace预言机,可以对第二区块链中的数据进行认证,并在认证通过后,基于持有的私钥对认证通过的数据进行签名。

[0106] 其中,Orace预言机对第二区块链中的数据进行认证时,所采用的认证规则,在本说明书中不进行特别限定,本领域技术人员在将本说明书的技术方案付诸实现时,可以基于实际的需求来定义设置认证规则。

[0107] 而订阅客户端可以通过跨链交互端与发布交互端进行跨链交互,获取由所述发布客户端发布的第二区块链上的待认证交易。

[0108] 在实现时,订阅客户端可以向跨链交互端发起订阅请求;其中,在该订阅请求中,可以携带指示订阅需求的订阅条件。其中,上述订阅请求中所携带的订阅条件所指示的订阅需求,具体可以是获取第二区块链中各区块中收录的交易。

[0109] 当然,在实际应用中,上述订阅条件所是指的订阅需求,具体也可以是获取第二区块链中各区块的区块头数据的需求。

[0110] 例如,在第一区块链和第二区块链同时支持SPV协议的场景下,基于SPV协议而言,订阅客户端对第二区块链上的数据进行认证时所采用的上述认证数据源,通常是上述第二区块链中各区块的区块头数据,即由第二区块链中各区块的区块头组成的“轻简链”。因此,在这个场景下,上述订阅条件所指示的订阅需求,具体可以是获取第二区块链中各区块链

的区块头数据的需求，

[0111] 当跨链交互端获取到上述订阅请求后，可以解析该订阅请求，获取该订阅请求中携带的订阅条件所指示的订阅需求。

[0112] 当跨链交互端获取到订阅客户端的订阅需求后，可以向订阅客户端发起状态询问消息，来询问订阅客户端维护的数据状态，并根据订阅客户端返回的数据状态，来确定订阅客户端维护的数据中是否包含由满足上述订阅条件的数据。

[0113] 例如，当订阅客户端通过消息队列来维护订阅的数据时，跨链交互端可以向订阅客户端发起状态询问消息，来询问上述消息队列的队列状态，并根据订阅客户端返回的上述消息队列的队列状态，来确定订阅客户端维护的数据中是否包含满足上述订阅条件的数据。

[0114] 一方面，如果订阅客户端维护的数据中已经维护了满足上述订阅条件的交易时，跨链交互端无需从第二区块链中重复的获取交易；

[0115] 另一方面，如果订阅客户端维护的数据中并不包含满足上述订阅条件的交易时，则跨链交互端需要从上述的发布客户端处获取满足上述订阅条件的交易；例如，跨链交互端可以向发布客户端发送数据同步请求，向发布客户端请求第二区块链中的各区块中收录的满足指定条件的交易，并将发布客户端返回的交易发送至订阅客户端，以对订阅客户端维护的交易进行更新。

[0116] 当然，在实际应用中，如果跨链交互端通过以上示出的状态询问过程，确定第二区块链中新增了满足条件的交易，此时也可以通过以上示出的数据同步方式，将第二区块链中新增的满足条件的交易，发送至订阅客户端，对订阅客户端维护的交易进行及时的更新。

[0117] 在本实施例中，当订阅客户端获取到由发布客户端发布的第二区块链上的待认证交易后，可以基于配置的认证数据源中的公钥或者公钥集合，以及上述待认证交易的签名，对该待认证交易进行数据认证。

[0118] 其中，基于认证数据源中的公钥或者公钥集合，以及上述待认证交易的签名，对该待认证交易进行数据认证的过程，即为基于认证数据源中的公钥，对待认证交易的签名进行解密的过程。

[0119] 在实现时，订阅客户端可以从配置的认证数据源中读取Orace预言机的公钥，然后基于该Orace预言机的公钥对待认证交易的签名进行解密；如果基于读取到的公钥，对该待认证交易的签名成功解密后，表明该待认证交易为经过Orace预言机授权的授信交易，此时针对该待认证交易的认证通过；相反，如果基于读取到的公钥，对该待认证交易的签名解密失败，表明该待认证交易并不是经过Orace预言机授权的授信交易，此时针对该待认证交易的认证失败。

[0120] 可见，通过这种方式，由于第二区块链上的交易，经由与第二区块链对接的Orace预言机提前进行了认证，并且认证通过的交易基于Orace预言机持有的私钥进行了签名；对于订阅客户端而言，对第二区块链上的交易进行跨链认证的过程，可以简化为对第二区块链上的交易的签名进行验证的过程；因此，可以简化订阅客户端对第二区块链上的交易进行跨链认证时的认证流程，降低跨链认证的复杂度。

[0121] 为了便于理解，以跨区块链的关联转账场景为例进行说明。

[0122] 请参见图5，图5是一示例性实施例提供的一种跨区块链的关联转账系统的结构示

意图;如图5所示,假定用户A分别在区块链1上存在账户A1、在区块链2上存在账户A2,用户B分别在区块链1上存在账户B1、在区块链2上存在账户B2,其中区块链1上的账户A1与账户B1用于维护某一类型的资产对象(比如证券)、区块链2上的账户A2与账户B2用于维护另一类型的资产对象(比如人民币),那么当用户A希望将证券出售给用户B时,可以采用下述的关联转账逻辑实现:从账户A2向账户B2转入指定数量的证券资产,然后由账户B1向账户A1转入指定数额的人民币。

[0123] 为了提升转账过程中的可靠性,可以通过在区块链1、区块链2上分别设定相应的智能合约,从而自动化地完成上述的两次转账过程,而避免用户在手动转账过程中出现有意或无意的转账数额错误、延迟等,确保转账过程快速、准确完成。

[0124] 而基于本说明书的技术方案,可以基于以上描述的过程,将区块链1作为侧链,锚定至作为主链的区块链2。在这种情况下,来自区块链2上的,已经完成了的从账户A2向账户B2转入指定数量的证券资产的交易,可以由与区块链2对接的Orace预言机基于持有的私钥进行签名。用户可以将来自区块链2上的,已经完成了的从账户A2向账户B2转入指定数量的证券资产的该交易,作为输入提交至上述智能合约进行执行,而上述订阅客户端(比如SPV钱包),可以基于配置的区块链2的认证数据源(即Orace预言机的公钥或者公钥集合),对该交易的签名进行验证;如果签名验证通过,表明该交易是经过Orace预言机授权的授信交易,此时针对该交易的认证通过;如果该交易认证通过,此时可以调用上述智能合约,触发在区块链1中执行由账户B1向账户A1转入指定数额的人民币的交易。

[0125] 通过以上各实施例可见,订阅客户端通过获取与第二区块链对接的Orace预言机的公钥作为认证数据源,进而在通过跨链交互端获取到由发布客户端发布的第二区块链上由所述Orace预言机基于持有的私钥进行签名后的待认证数据时,可以基于所述认证数据源以及所述待认证数据的签名对该待认证数据进行数据认证;

[0126] 一方面,由于第二区块链上的数据会由与第二区块链对接的Orace预言机基于持有的私钥进行了签名,订阅客户端只需要将Orace预言机的公钥作为认证数据源进行存储,就可以基于Orace预言机的公钥和数据携带的签名对第二区块链上的数据进行认证,因此可以降低订阅客户端对第二区块链上的数据进行认证的复杂度;

[0127] 另一方面,由于第一区块链和第二区块链之间可以采用订阅和发布的方式,通过跨链交互端来进行数据同步,因此对于不同的区块链之间,可以在互相隔离的前提下,实现无入侵的侧链锚定,进而可以高效的与其它区块链进行锚定,搭建出低复杂度、高扩展性的跨链网络。

[0128] 与上述方法实施例相对应,本说明书还提供了一种跨区块链的认证装置的实施例。本说明书的跨区块链的认证装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现,也可以通过硬件或者软硬件结合的方式实现。以软件实现为例,作为一个逻辑意义上的装置,是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言,如图6所示,为本说明书的跨区块链的认证装置所在电子设备的一种硬件结构图,除了图6所示的处理器、内存、网络接口、以及非易失性存储器之外,实施例中装置所在的电子设备通常根据该电子设备的实际功能,还可以包括其他硬件,对此不再赘述。

[0129] 图7是本说明书一示例性实施例示出的一种跨区块链的认证装置的框图。

[0130] 请参考图7,所述跨区块链的认证装置70可以应用在前述图6所示的电子设备中,所述电子设备位于由订阅客户端、发布客户端、以及跨链交互端组成的跨链交互系统;其中,所述订阅客户端与第一区块链对应;所述发布客户端与第二区块链对应;所述跨链交互端与所述订阅客户端和所述发布客户端分别对接;所述装置70包括有:第一获取模块701、第二获取模块702和认证模块703。

[0131] 第一获取模块701,获取与所述第二区块链对接的Orace预言机的公钥作为认证数据源;

[0132] 第二获取模块702,通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,所述待认证数据由所述Orace预言机基于持有的私钥进行了签名;

[0133] 认证模块703,基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。

[0134] 在本实施例中,所述第一获取模块701:

[0135] 获取用户配置的与所述第二区块链对应的Orace预言机的公钥作为认证数据源;或者,

[0136] 通过所述跨链交互端获取由所述发布客户端发布的与所述第二区块链对应的Orace预言机的公钥作为认证数据源。

[0137] 在本实施例中,所述第二获取模块702:

[0138] 向所述跨链交互端发起订阅请求;其中,所述订阅请求用于向所述跨链交互端指示订阅条件,以使所述跨链交互端基于所述订阅条件,向所述发布客户端请求所述第二区块链上满足所述订阅条件的待认证数据;

[0139] 获取所述发布客户端发布的满足所述订阅条件,且由所述Orace预言机基于持有的私钥进行了签名的待认证数据。

[0140] 在本实施例中,所述认证模块703:

[0141] 基于所述认证数据源中保存的所述Orace预言机的公钥对所述待认证数据的签名进行验证;如果所述签名验证通过,确定针对所述待认证数据的数据认证通过。

[0142] 在本实施例中,所述发布客户端与所述Orace预言机对接;所述Orace预言机用于对所述第二区块链中的数据进行数据认证,在数据认证通过后基于持有的私钥对认证通过的数据进行签名,并将签名后的数据主动推送至所述发布客户端;或者,响应于所述发布客户端的数据获取请求,将签名后的数据推送至所述发布客户端。

[0143] 在本实施例中,与所述第二区块链对应的Orace预言机为所述发布客户端。

[0144] 在本实施例中,所述订阅客户端对应于所述第一区块链上的节点设备;所述发布客户端以及所述Orace预言机对应于所述第二区块链上的节点设备。

[0145] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程,在此不再赘述。

[0146] 对于装置实施例而言,由于其基本对应于方法实施例,所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的,其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的,作为模块显示的部件可以是或者也可以不是物理模块,即可以位于一个地方,或者也可以分布到多个网络模块上。可以根据实际的

需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[0147] 上述实施例阐明的系统、装置、模块或模块,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。

[0148] 与上述方法实施例相对应,本说明书还提供了一种电子设备的实施例。所述电子设备位于由订阅客户端、发布客户端、以及跨链交互端组成的跨链交互系统;其中,所述订阅客户端与第一区块链对应;所述发布客户端与第二区块链对应;所述跨链交互端与所述订阅客户端和所述发布客户端分别对接;该电子设备包括:处理器以及用于存储机器可执行指令的存储器;其中,处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中,所述设备还可能包括外部接口,以能够与其他设备或者部件进行通信。

[0149] 在本实施例中,通过读取并执行所述存储器存储的与跨区块链的认证的控制逻辑对应的机器可执行指令,所述处理器被促使:

[0150] 获取与所述第二区块链对接的Oracle预言机的公钥作为认证数据源;

[0151] 通过所述跨链交互端获取由所述发布客户端发布的所述第二区块链上的待认证数据;其中,所述待认证数据由所述Oracle预言机基于持有的私钥进行了签名;

[0152] 基于所述认证数据源以及所述待认证数据的签名对所述待认证数据进行数据认证。

[0153] 在本实施例中,通过读取并执行所述存储器存储的与跨区块链的认证的控制逻辑对应的机器可执行指令,所述处理器被促使:

[0154] 获取用户配置的与所述第二区块链对应的Oracle预言机的公钥作为认证数据源;或者,

[0155] 通过所述跨链交互端获取由所述发布客户端发布的与所述第二区块链对应的Oracle预言机的公钥作为认证数据源。

[0156] 在本实施例中,通过读取并执行所述存储器存储的与跨区块链的认证的控制逻辑对应的机器可执行指令,所述处理器被促使:

[0157] 向所述跨链交互端发起订阅请求;其中,所述订阅请求用于向所述跨链交互端指示订阅条件,以使所述跨链交互端基于所述订阅条件,向所述发布客户端请求所述第二区块链上满足所述订阅条件的待认证数据;

[0158] 获取所述发布客户端发布的满足所述订阅条件,且由所述Oracle预言机基于持有的私钥进行了签名的待认证数据。

[0159] 在本实施例中,通过读取并执行所述存储器存储的与跨区块链的认证的控制逻辑对应的机器可执行指令,所述处理器被促使:

[0160] 基于所述认证数据源中保存的所述Oracle预言机的公钥对所述待认证数据的签名进行验证;如果所述签名验证通过,确定针对所述待认证数据的数据认证通过。

[0161] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化,这些变型、

用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的真正范围和精神由下面的权利要求指出。

[0162] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来限制。

[0163] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

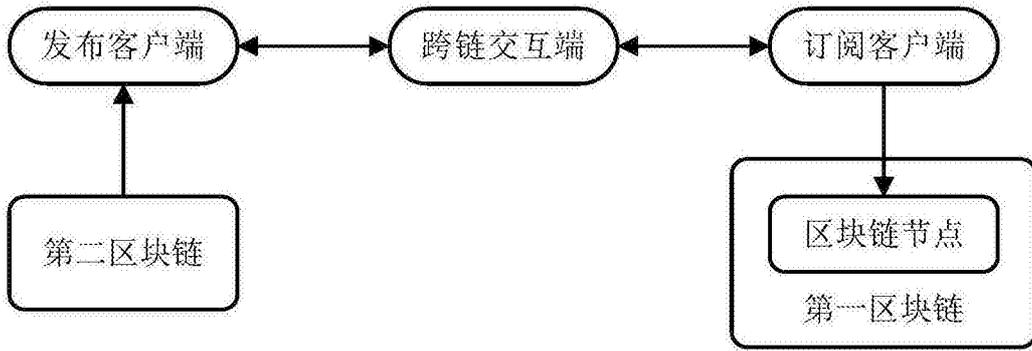


图1

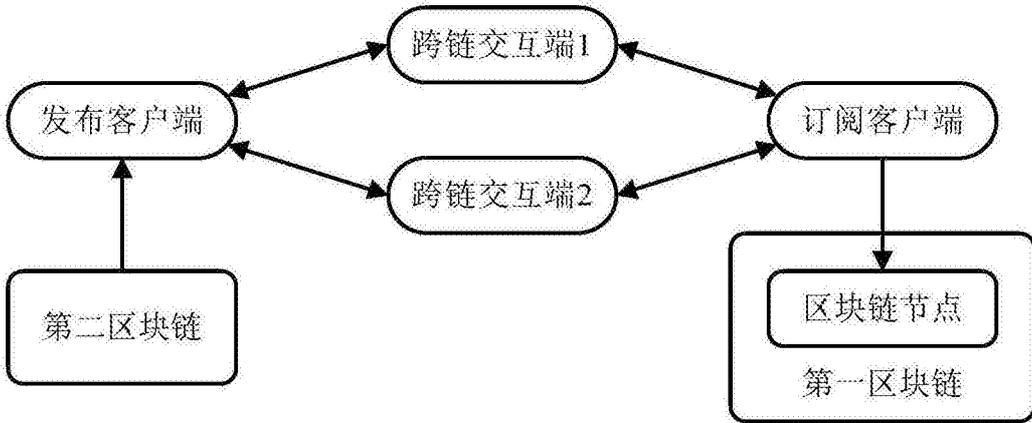


图2

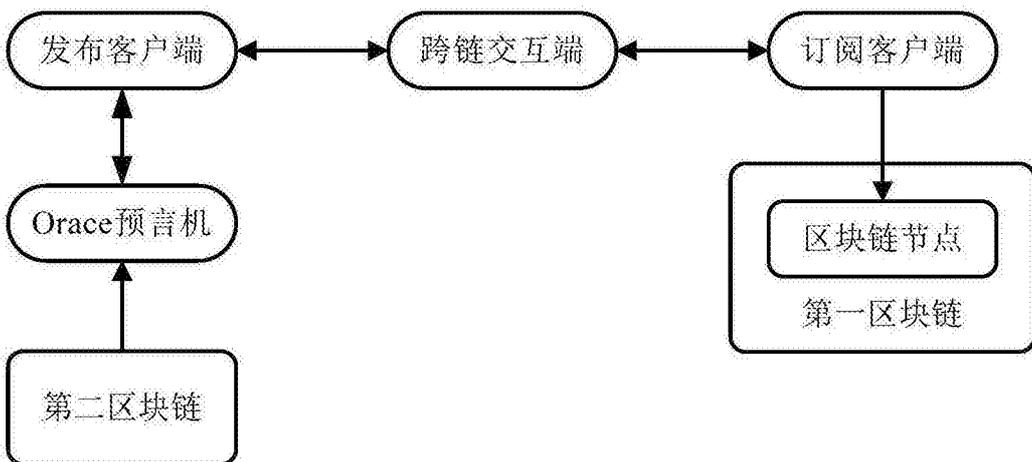


图3

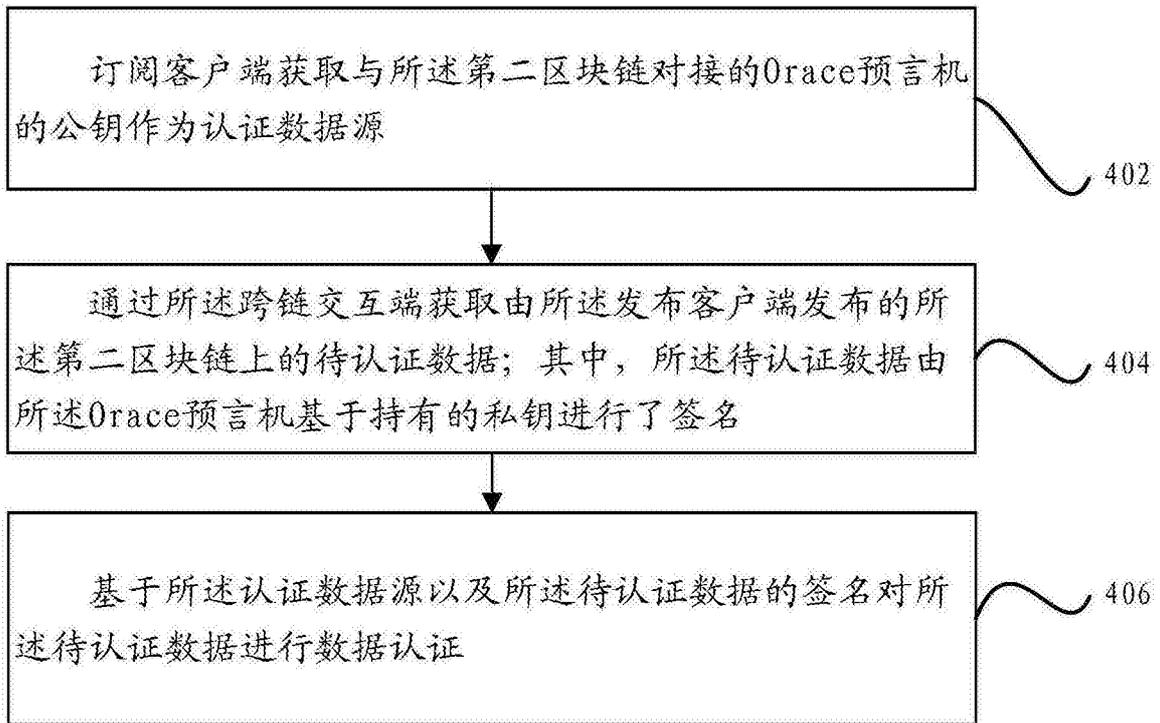


图4

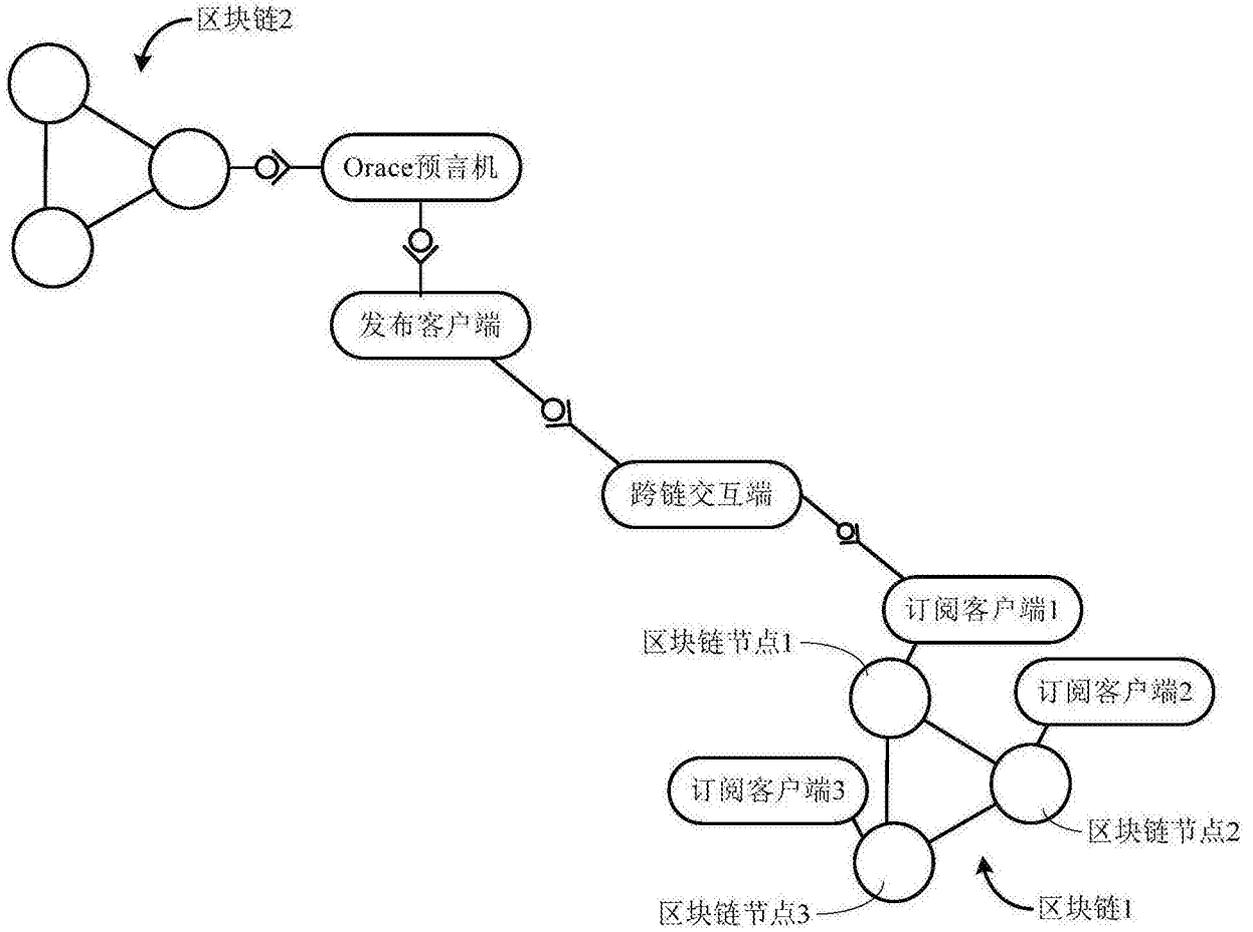


图5

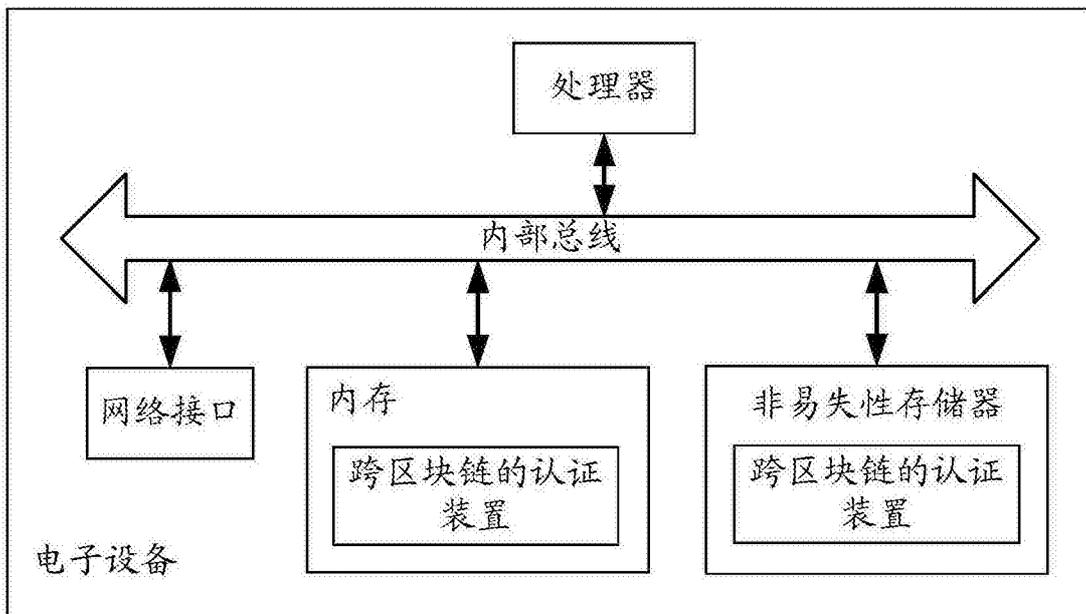


图6

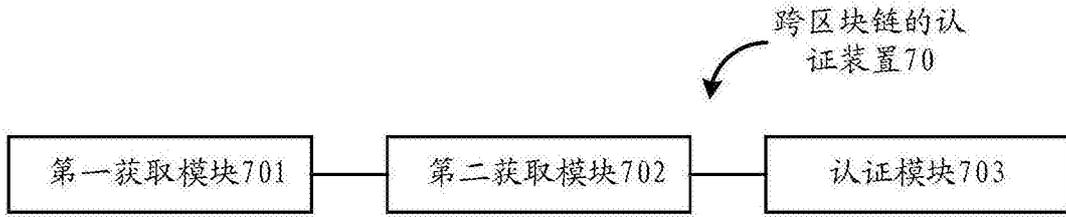


图7