(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 111147517 A
(43)申请公布日 2020.05.12

(21)申请号 201911422541.2

(22)申请日 2019.12.31

(71)申请人 上海分布信息科技有限公司
地址 200433 上海市杨浦区政学路88号创智天地企业中心5号楼301

(72)发明人 谢俊喜 王成 周佩文 丛宏雷

(74)专利代理机构 上海恒锐佳知识产权代理事务所(普通合伙) 31286
代理人 黄海霞

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

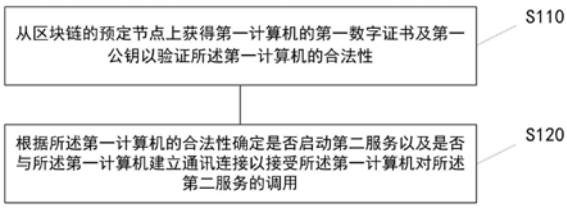
权利要求书2页 说明书7页 附图7页

(54)发明名称

安全通讯方法、装置、终端设备

(57)摘要

本发明公开了安全通讯方法、装置、终端设备，可以保证通讯安全性、可靠性。其中，所述的安全通讯方法包括：从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性，其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密；根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用。



CN 111147517 A

1.一种安全通讯方法,其特征在于,包括:

从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性,其中,所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密;

根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用。

2.根据权利要求1所述的安全通讯方法,其特征在于,还包括:

根据所述第一计算机的合法性确定是否与所述第一计算机建立通讯连接以调用所述第一计算机的第一服务。

3.根据权利要求1或2所述的安全通讯方法,其特征在于,还包括:

将当前计算机变更后的数字证书及公钥广播到所述区块链中预定节点。

4.根据权利要求1或2所述的安全通讯方法,其特征在于,还包括:

当所述第一计算机验证不合法时,检测所述预定节点的区块高度以验证所述预定节点是否同步最新的区块。

5.根据权利要求4所述的安全通讯方法,其特征在于,还包括:

从所述预定节点上获得所述第一计算机的更新后的第一数字证书及第一公钥以验证所述第一计算机的合法性。

6.一种安全通讯方法,其特征在于,包括:

从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性,其中,所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密;

根据所述第一计算机的合法性确定是否启动所述第二服务,以及确定是否与所述第一计算机建立通讯连接。

7.一种安全通讯装置,其特征在于,包括:

第一验证模块,用于从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性,其中,所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密;

第一决策模块,用于根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用。

8.一种安全通讯装置,其特征在于,包括:

第三验证模块,用于从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性,其中,所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密;

第三决策模块,用于根据所述第一计算机的合法性确定是否启动所述第二服务,以及确定是否与所述第一计算机建立通讯连接。

9.一种终端设备,其特征在于,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1-5任一项或权利要求6所述的方法。

10.一种计算机集群中不同计算机间安全通讯方法,其特征在于,包括:

第二计算机从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性,其中,所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密;

所述第二计算机根据所述第一计算机的合法性确定是否启动所述第二服务,以及确定是否与所述第一计算机建立通讯连接;

所述第一计算机从所述区块链上获取所述第二计算机的第二数字证书及第二公钥以验证所述第二计算机的合法性,其中,所述第二数字证书根据所述第二私钥加密生成并且配置成由所述第二公钥解密;

所述第一计算机根据所述第二计算机的合法性确定是否与所述第二计算机建立通讯连接以调用所述第二服务。

安全通讯方法、装置、终端设备

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及计算机集群中不同计算机间安全通讯方法、装置、终端设备。

背景技术

[0002] 计算机集群是指一组独立的计算机通过网络连接起来，共同协助完成计算工作。大多数计算机服务都是以计算机集群的方式运行。常见的计算机集群包括Web服务集群，数据库集群，云服务，区块链服务等。计算机集群中的网络都是基于TCP/IP技术，计算机间通过IP地址和TCP端口建立链接以相互通讯。TCP/IP网络为一个开放性网络，只需要知道对外的IP/端口信息即可与对应的计算机建立通讯。

[0003] 以目前主流的Web服务集群为例，其通常由Web服务器，业务服务器和数据库服务器组成，服务器间通过网络通讯进行交互。如图1所示。在Web服务集群中，每个服务器都只负责整体业务的一部分，某些核心业务的服务接口，尤其是核心数据库服务器，只能由其相关业务的计算机调用，必须防止核心业务服务器被其他恶意服务器调用，从而造成业务故障。

[0004] 为保障集群中服务器间的业务安全，目前主要有以下几种方式：(1)运维管理的方式。由负责运维计算机集群的运维工程师，人工停止所有的业务服务，更新业务配置和安全证书，然后重新启动所有业务。通过运维人员管理的方式有以下缺点：运维人员本身也是系统应对防范的风险点之一；运维人员的人工误操作的可能性也为业务安全带来一些不确定性风险；当发现安全风险后，由运维人员操作更新，有很大的延迟时间，相比自动更新有较大的风险敞口；配置更新将导致所有相关业务的重启。(2)中心配置服务器管理方式。所有计算机定期从中心配置服务器更新最新的业务配置和安全证书。当业务配置或安全证书更新后，所有计算机自动获得新的配置和安全证书，从而基于新的配置和证书保证自己的通讯安全。通过中心配置服务器管理方式有以下缺点：将整个计算机集群的证书风险汇聚到中心配置服务器。如果中心配置服务器被恶意攻击，或被网络隔离，将造成整个计算机集群的安全问题。计算机集群中每台计算机同步到的证书，无法保证是否被篡改。(3)基于CA(CertificateAuthority，即证书授权中心)服务器的方式。和中心配置服务器管理方式类似，但是脱离实际业务，无法满足业务安全所要求的只有业务关联的服务器才可以相互通讯。

[0005] 因此，有必要改进现有技术的计算机集群中不同计算机的通讯方法，以期使得通讯安全性、可靠性得到保证。

发明内容

[0006] 本发明的目的在于提供安全通讯方法、装置、终端设备，以保证通讯安全性、可靠性。

[0007] 本发明的目的采用以下技术方案实现：

[0008] 本发明的第一方面提供一种安全通讯方法，包括：从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性，其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密；根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用。

[0009] 这样，根据提供的安全通讯方法，能够通过区块链特性实时获取最新的证书变更；计算机集群中每个参与通讯的网络节点，获取到唯一、可信的通讯证书；所有公钥证书通过链上获取，不需要在本地程序加载证书文件；基于证书的双向验证，保证通讯双方的安全、可靠。

[0010] 可选地，还包括：根据所述第一计算机的合法性确定是否与所述第一计算机建立通讯连接以调用所述第一计算机的第一服务。

[0011] 通过根据第一计算机的合法性确定是否与第一计算机建立通讯连接以调用第一计算机的第一服务，可以保证调用第一计算机的第一服务的安全性、可靠性，避免对其他恶意服务的调用，从而造成业务故障。

[0012] 可选地，还包括：将当前计算机变更后的数字证书及公钥广播到所述区块链中预定节点。

[0013] 通过将当前计算机变更后的数字证书及公钥广播到区块链中预定节点，可以使得数字证书及公钥得到及时更新。

[0014] 可选地，还包括：当所述第一计算机验证不合法时，检测所述预定节点的区块高度以验证所述预定节点是否同步最新的区块。

[0015] 通过当第一计算机验证不合法时，检测预定节点的区块高度以验证预定节点是否同步最新的区块，可以来验证当前同步到的区块是否最新，同时验证当前的区块是否有效。

[0016] 可选地，还包括：从所述预定节点上获得所述第一计算机的更新后的第一数字证书及第一公钥以验证所述第一计算机的合法性。

[0017] 通过从预定节点上获得第一计算机的更新后的第一数字证书及第一公钥以验证第一计算机的合法性，可以同步最新的区块信息以避免合法性验证失效。

[0018] 本发明的第二方面提供一种安全通讯方法，包括：从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性，其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密；根据所述第一计算机的合法性确定是否启动所述第二服务，以及确定是否与所述第一计算机建立通讯连接。

[0019] 通过从第一计算机与第二计算机所属的区块链上获得第一计算机的第一数字证书及第一公钥以验证第一计算机的合法性，以此来确定是否启动第二服务以及是否与第一计算机建立通讯连接以接受第一计算机对第二服务的调用，可以保证通讯安全性、可靠性，避免当前计算机的第二服务被其他恶意的服务所调用，从而造成业务故障。

[0020] 本发明的第三方面提供一种安全通讯装置，包括：第一验证模块，用于从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性，其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密；第一决策模块，用于根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计

算机建立通讯连接以接受所述第一计算机对所述第二服务的调用。

[0021] 通过从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证第一计算机的合法性，以此来确定是否启动第二服务以及是否与第一计算机建立通讯连接以接受第一计算机对第二服务的调用，可以保证通讯安全性、可靠性，避免当前计算机的第二服务被其他恶意的服务所调用，从而造成业务故障。

[0022] 本发明的第四方面提供一种安全通讯装置，包括：第三验证模块，用于从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性，其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密；第三决策模块，用于根据所述第一计算机的合法性确定是否启动所述第二服务，以及确定是否与所述第一计算机建立通讯连接。

[0023] 通过从第一计算机与第二计算机所属的区块链上获得第一计算机的第一数字证书及第一公钥以验证第一计算机的合法性，以此来确定是否启动第二服务以及是否与第一计算机建立通讯连接以接受第一计算机对第二服务的调用，可以保证通讯安全性、可靠性，避免当前计算机的第二服务被其他恶意的服务所调用，从而造成业务故障。

[0024] 本发明的第五方面提供一种终端设备，包括：处理器；

[0025] 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本发明的第一方面或本发明的第二方面提供的所述方法。

[0026] 本发明的第六方面提供一种计算机集群中不同计算机间安全通讯方法，包括：第二计算机从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性，其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密；所述第二计算机根据所述第一计算机的合法性确定是否启动所述第二服务，以及确定是否与所述第一计算机建立通讯连接；所述第一计算机从所述区块链上获取所述第二计算机的第二数字证书及第二公钥以验证所述第二计算机的合法性，其中，所述第二数字证书根据所述第二私钥加密生成并且配置成由所述第二公钥解密；所述第一计算机根据所述第二计算机的合法性确定是否与所述第二计算机建立通讯连接以调用所述第二服务。

[0027] 通过从第一计算机与第二计算机所属的区块链上获得第一计算机的第一数字证书及第一公钥以验证第一计算机的合法性，以此来确定是否启动第二服务以及是否与第一计算机建立通讯连接以接受第一计算机对第二服务的调用，可以保证通讯安全性、可靠性，避免当前计算机的第二服务被其他恶意的计服务所调用，从而造成业务故障。

附图说明

[0028] 下面结合附图和实施例对本发明进一步说明。

[0029] 图1是Web服务集群的示意图；

[0030] 图2是本发明第一个实施例的一种安全通讯方法的示意图；

[0031] 图3是本发明第一个实施例的一种安全通讯方法的一具体实施方式的示意图；

[0032] 图4是本发明第一个实施例的一种安全通讯方法的又一具体实施方式的示意图；

[0033] 图5是本发明第一个实施例的一种安全通讯方法的又一具体实施方式的示意图；

[0034] 图6是本发明第一个实施例的一种安全通讯方法的又一具体实施方式的示意图；

[0035] 图7是本发明第二个实施例的一种安全通讯方法的示意图；

[0036] 图8是本发明第三个实施例的一种安全通讯装置的示意图；

[0037] 图9是本发明第四个实施例的一种安全通讯装置的示意图；

[0038] 图10是本发明五个实施例的一种计算机集群中不同计算机间安全通讯方法；

[0039] 图11是本发明第六个实施例的一种终端设备的示意图；

[0040] 图12是本发明实施例的一种安全通讯方法的示意图。

具体实施方式

[0041] 下面，结合附图以及具体实施方式，对本发明做进一步描述，需要说明的是，在不相冲突的前提下，以下描述的各实施例之间或各技术特征之间可以任意组合形成新的实施例。

[0042] 区块链具有数据一致性，不可篡改性等特点。本发明应用区块链技术实现计算机集群中不同计算机间业务安全通讯，实质上说，就是利用区块链特性，将双向通讯的数字证书保存到区块链上，实现多个站点、不同地域或者计算机集群之间相互信任，实现安全通讯。计算机集群中的每个节点实时同步到最新的区块，同时可以验证区块的有效性，并且保证区块中数据不可篡改。在计算机集群的每个参与者都可以获得一个唯一、可信、数据一致的数字证书及公钥。如果有某个进程作恶，可以及时更新数字证书到链上，计算机集群中每个服务器通过同步区块获取到最新的数字证书。例如，当进程A需要和进程B通讯时，进程A需要从最新的区块中拿到进程B的数字证书及公钥，同时进程B也需要从最新的区块中拿到进程A的数字证书及公钥。通讯双方建立双向认证，从而保证通讯安全性和可靠性。

[0043] 在本发明的第一个实施例中，提供一种安全通讯方法。如图2所示，本发明第一个实施例的安全通讯方法包括以下步骤：

[0044] S110、从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性。其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密。其中，预定节点可以是种子节点或者其他同步节点。

[0045] S120、根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用。

[0046] 根据本发明实施例提供的安全通讯方法，能够通过区块链特性实时获取最新的证书变更；计算机集群中每个参与通讯的网络节点，获取到唯一、可信的通讯证书；所有公钥证书通过链上获取，不需要在本地程序加载证书文件；基于证书的双向验证，保证通讯双方的安全、可靠。

[0047] 在一个具体实施方式中，如图3所示，本发明第一个实施例的安全通讯方法还可以包括以下步骤：

[0048] S130、根据所述第一计算机的合法性确定是否与所述第一计算机建立通讯连接以调用所述第一计算机的第一服务。

[0049] 在一个具体实施方式中，如图4所示，本发明第一个实施例的安全通讯方法还可以包括以下步骤：

[0050] S140、将当前计算机变更后的数字证书及公钥广播到所述区块链中预定节点。

[0051] 在一个具体实施方式中，如图5所示，本发明第一个实施例的安全通讯方法还可以

包括以下步骤：

[0052] S150、当所述第一计算机验证不合法时，检测所述预定节点的区块高度以验证所述预定节点是否同步最新的区块。

[0053] 在一个具体实施方式中，如图6所示，本发明第一个实施例的安全通讯方法还可以包括以下步骤：

[0054] S160、从所述预定节点上获得所述第一计算机的更新后的第一数字证书及第一公钥以验证所述第一计算机的合法性。

[0055] 在本发明的第二个实施例中，提供又一种安全通讯方法。如图7所示，本发明第二个实施例的安全通讯方法包括以下步骤：

[0056] S210、从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性。其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密。

[0057] S220、根据所述第一计算机的合法性确定是否启动所述第二服务，以及确定是否与所述第一计算机建立通讯连接。

[0058] 在本发明的第三个实施例中，提供一种安全通讯装置。如图8所示，所述装置包括：

[0059] 第一验证模块110，用于从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性，其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密；

[0060] 第一决策模块120，用于根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用。

[0061] 在一个具体实施方式中，本发明第三个实施例的安全通讯装置还可以包括以下模块中至少之一：

[0062] 第二决策模块，用于根据所述第一计算机的合法性确定是否与所述第一计算机建立通讯连接以调用所述第一计算机的第一服务。

[0063] 广播模块，用于将当前计算机变更后的数字证书及公钥广播到所述区块链中预定节点。

[0064] 检测模块，用于当所述第一计算机验证不合法时，检测所述预定节点的区块高度以验证所述预定节点是否同步最新的区块。

[0065] 第二验证模块，用于从所述预定节点上获得所述第一计算机的更新后的第一数字证书及第一公钥以验证所述第一计算机的合法性。

[0066] 在本发明的第四个实施例中，提供又一种安全通讯装置。如图9所示，所述装置包括：

[0067] 第三验证模块210，用于从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性，其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密。

[0068] 第三决策模块220，用于根据所述第一计算机的合法性确定是否启动所述第二服务，以及确定是否与所述第一计算机建立通讯连接。

[0069] 在本发明的第五个实施例中，提供一种计算机集群中不同计算机间安全通讯方法。如图10所示，所述方法包括以下步骤：

[0070] S310、第二计算机从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性。其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密；

[0071] S320、所述第二计算机根据所述第一计算机的合法性确定是否启动所述第二服务，以及确定是否与所述第一计算机建立通讯连接；

[0072] S330、所述第一计算机从所述区块链上获取所述第二计算机的第二数字证书及第二公钥以验证所述第二计算机的合法性。其中，所述第二数字证书根据所述第二私钥加密生成并且配置成由所述第二公钥解密；

[0073] S340、所述第一计算机根据所述第二计算机的合法性确定是否与所述第二计算机建立通讯连接以调用所述第二服务。

[0074] 参见图12所示，假设，基于区块链的证书管理方案是可以描述的，并且可以实时治理，随时完成证书变化和业务变化。本发明实施例的安全通讯方法可以详细描述如下：

[0075] (1)利用程序基于X509生成公钥证书信息。

[0076] (2)通过智能合约把公钥证书信息打包到最新的区块中。利用p2p网络，把最新的区块广播到同步节点。

[0077] (3)每个同步节点，在实时同步区块时，根据区块验证算法，确保区块的合法性。当同步到一个恶意区块时，同步节点验证无效，丢弃这个区块。重新到其他节点同步区块，直到区块有效。

[0078] (4)每个同步节点实时检测自己的区块高度，是否和其他节点一致。如果不一致，实时同步最新的区块，保证节点之间区块高度一致。

[0079] (5)假如服务A要与服务B通信，需要要进行TLS双向认证：

[0080] (5.1)服务B启动时，首先在程序里根据自己的私钥，生成对应的数字证书，同时实时同步证书链区块信息，通过证书链获取到A的公钥证书，以此来启动服务。

[0081] (5.2)服务A调用服务B时，也是实时同步证书链区块信息，通过证书链拿到B的公钥证书，同时根据自己的私钥，生成对应的数字证书。

[0082] (5.3)服务A与服务B，进行TLS双向认证，确认是否可以建立可信链接。确保通信的安全、可靠。

[0083] (5.4)如果两个服务中，其中某一个服务证书作恶。则双向TLS认证无效，服务间通讯失败。

[0084] (6)如果通讯过程中其中某一个服务作恶。实时更新证书链上的公钥证书，打包新的区块。服务通过同步节点实时同步到新的区块，获取最新的公钥证书，进行下一次通信时，避免服务通信双向验证失败。

[0085] (7)服务双方都需要通过证书链，实时同步最新的区块信息，获取最新的公钥证书，实时保证了每个服务证书的一致性。在通信时会建立一个双向信任的安全信道。

[0086] 在本发明的第六个实施例中，提供一种终端设备。如图11所示，该终端设备6包括：处理器60、存储器61以及存储在所述存储器61中并可在所述处理器60上运行的计算机程序62。所述处理器60执行所述计算机程序62时实现上述各个安全通讯方法实施例中的步骤。或者，所述处理器60执行所述计算机程序62时实现上述各装置实施例中各模块/单元的功能。

[0087] 示例性的，所述计算机程序62可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器61中，并由所述处理器60执行，以完成本发明。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序62在所述安全通讯装置/终端设备6中的执行过程。例如，所述计算机程序62可以被分割成第一验证模块、第一决策模块，各模块具体功能如下：

[0088] 第一验证模块用于从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性，其中，所述第一数字证书根据第一私钥加密生成并且配置成由所述第一公钥解密；第一决策模块用于根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用。

[0089] 所述终端设备6可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述终端6设备可包括，但不仅限于，处理器60、存储器61。本领域技术人员可以理解，图11仅仅是终端设备6的示例，并不构成对终端设备6的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述终端设备6还可以包括输入输出设备、网络接入设备、总线等。

[0090] 所称处理器60可以是中央处理单元(CentralProcessingUnit，CPU)，还可以是其他通用处理器、数字信号处理器(DigitalSignalProcessor，DSP)、专用集成电路(ApplicationSpecificIntegratedCircuit，ASIC)、现成可编程门阵列(Field-ProgrammableGateArray，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。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。

[0091] 所述存储器61可以是所述终端设备6的内部存储单元，例如终端设备6的硬盘或内存。所述存储器61也可以是所述终端设备6的外部存储设备，例如所述终端设备上配备的插接式硬盘，智能存储卡(SmartMediaCard，SMC)，安全数字(SecureDigital，SD)卡，闪存卡(FlashCard)等。进一步地，所述存储器61还可以既包括所述终端设备6的内部存储单元也包括外部存储设备。所述存储器61用于存储所述计算机程序以及所述终端设备所需的其他程序和数据。所述存储器61还可以用于暂时地存储已经输出或者将要输出的数据。

[0092] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中，上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0093] 本发明从使用目的上，效能上，进步及新颖性等观点进行阐述，其设置有的实用进步性，已符合专利法所强调的功能增进及使用要件，本发明以上的说明及附图，仅为本发明的较佳实施例而已，并非以此局限本发明，因此，凡一切与本发明构造，装置，特征等近似、雷同的，即凡依本发明专利申请范围所作的等同替换或修饰等，皆应属本发明的专利申请保护的范围之内。

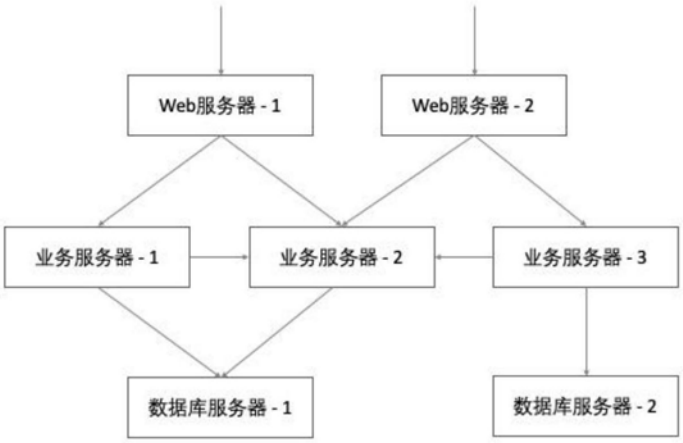

Web服务器 - 1
Web服务器 - 2
业务服务器 - 1
业务服务器 - 2
业务服务器 - 3
数据库服务器 - 1
数据库服务器 - 2

图1

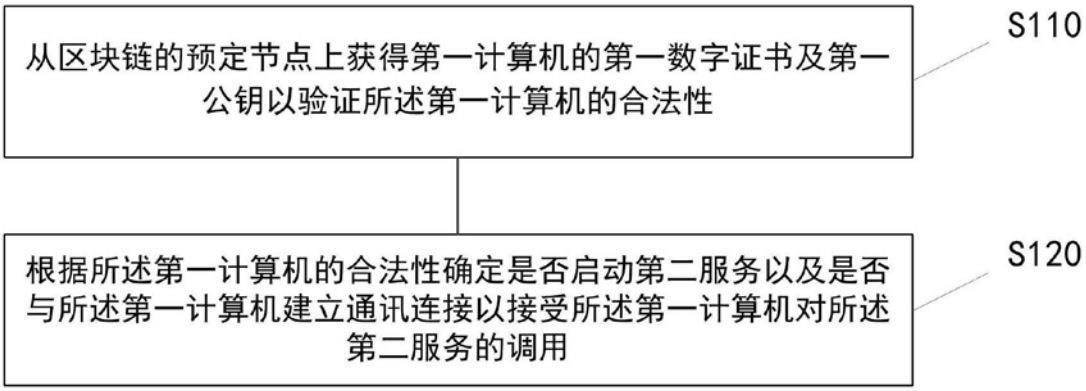

从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性
S110
根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用
S120

图2

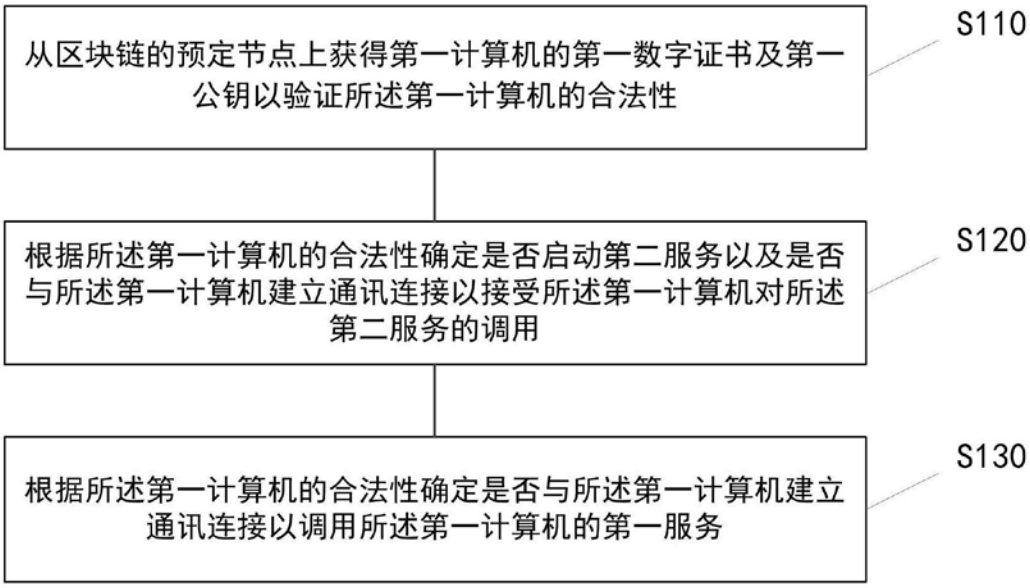

从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性
S110
根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用
S120
根据所述第一计算机的合法性确定是否与所述第一计算机建立通讯连接以调用所述第一计算机的第一服务
S130

图3

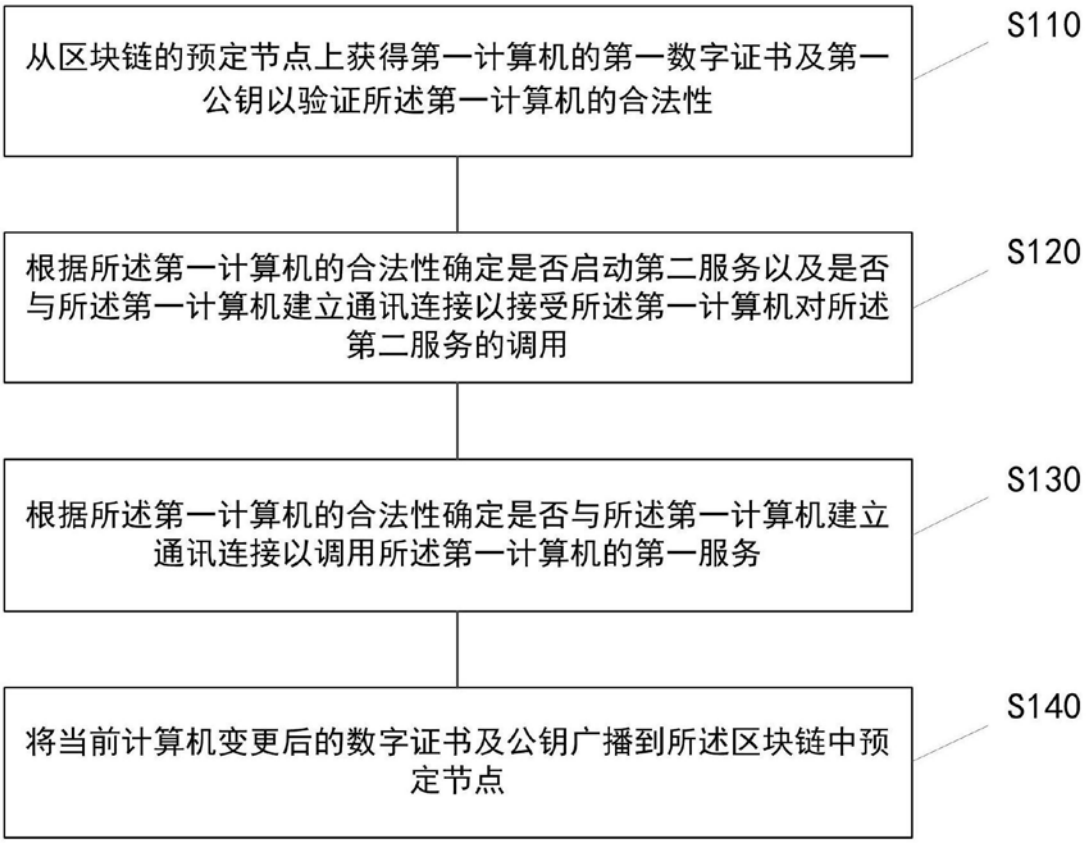

从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性
S110
根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用
S120
根据所述第一计算机的合法性确定是否与所述第一计算机建立通讯连接以调用所述第一计算机的第一服务
S130
将当前计算机变更后的数字证书及公钥广播到所述区块链中预定节点
S140

图4

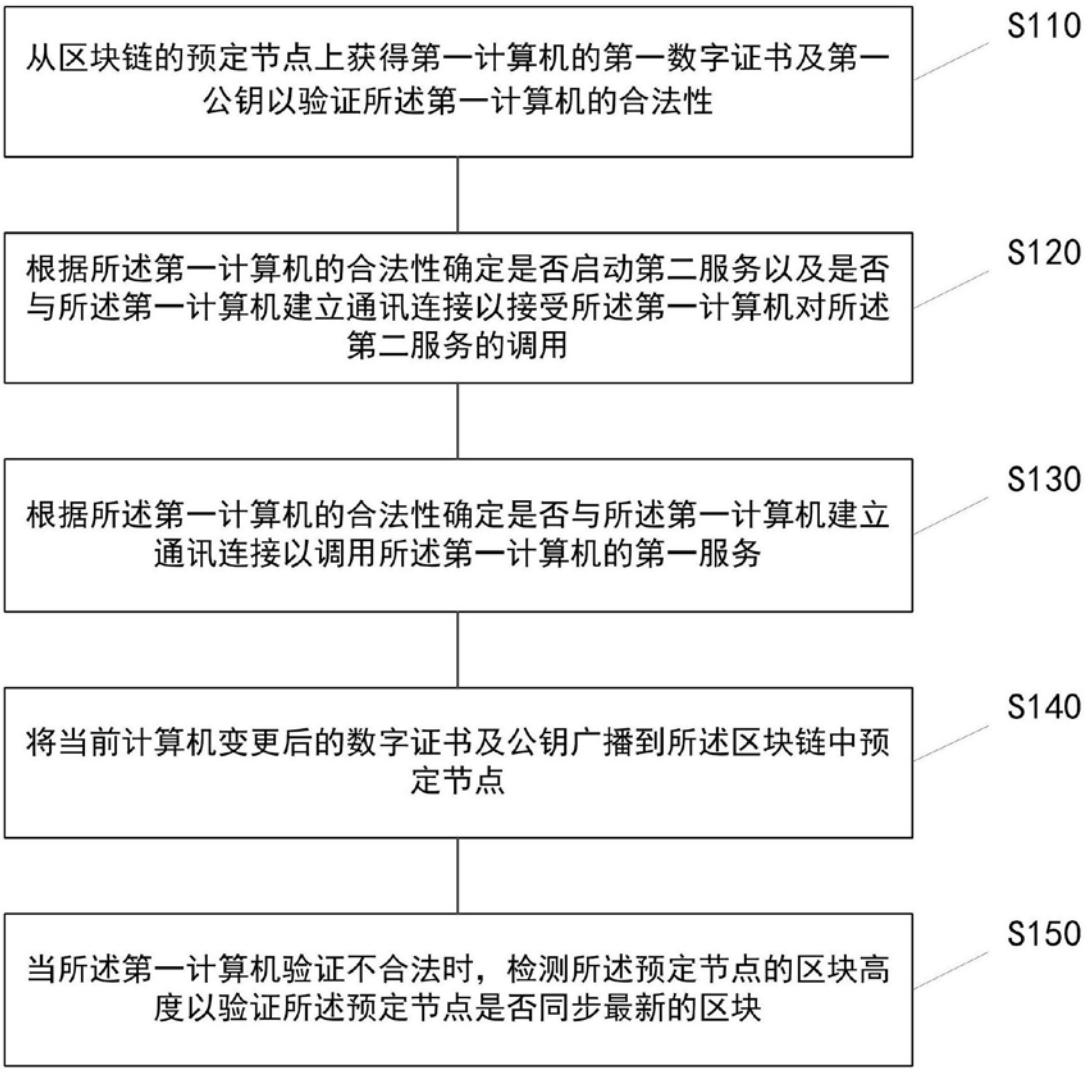

从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性
S110
根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用
S120
根据所述第一计算机的合法性确定是否与所述第一计算机建立通讯连接以调用所述第一计算机的第一服务
S130
将当前计算机变更后的数字证书及公钥广播到所述区块链中预定节点
S140
当所述第一计算机验证不合法时，检测所述预定节点的区块高度以验证所述预定节点是否同步最新的区块
S150

图5

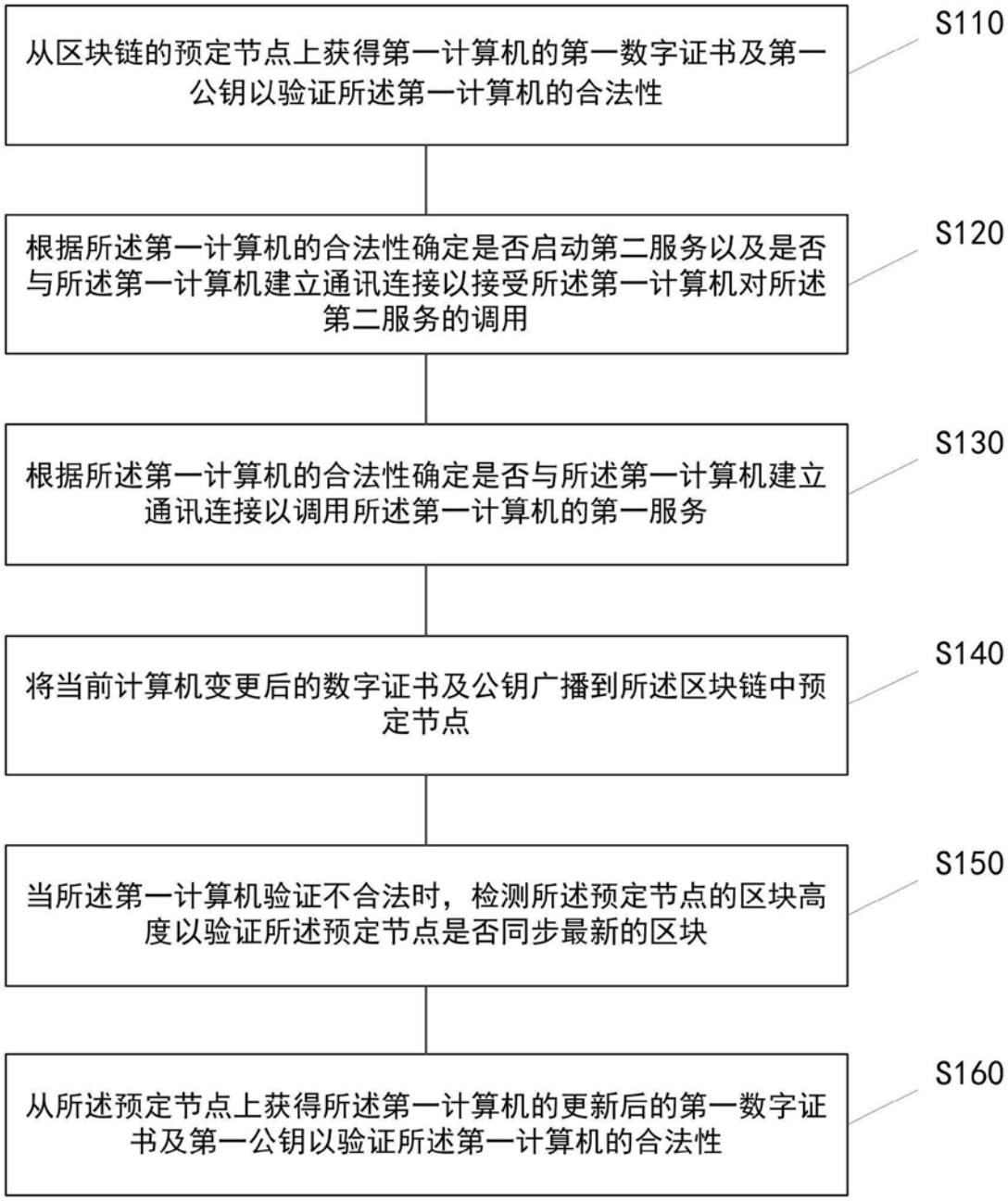

从区块链的预定节点上获得第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性
S110
根据所述第一计算机的合法性确定是否启动第二服务以及是否与所述第一计算机建立通讯连接以接受所述第一计算机对所述第二服务的调用
S120
根据所述第一计算机的合法性确定是否与所述第一计算机建立通讯连接以调用所述第一计算机的第一服务
S130
将当前计算机变更后的数字证书及公钥广播到所述区块链中预定节点
S140
当所述第一计算机验证不合法时，检测所述预定节点的区块高度以验证所述预定节点是否同步最新的区块
S150
从所述预定节点上获得所述第一计算机的更新后的第一数字证书及第一公钥以验证所述第一计算机的合法性
S160

图6

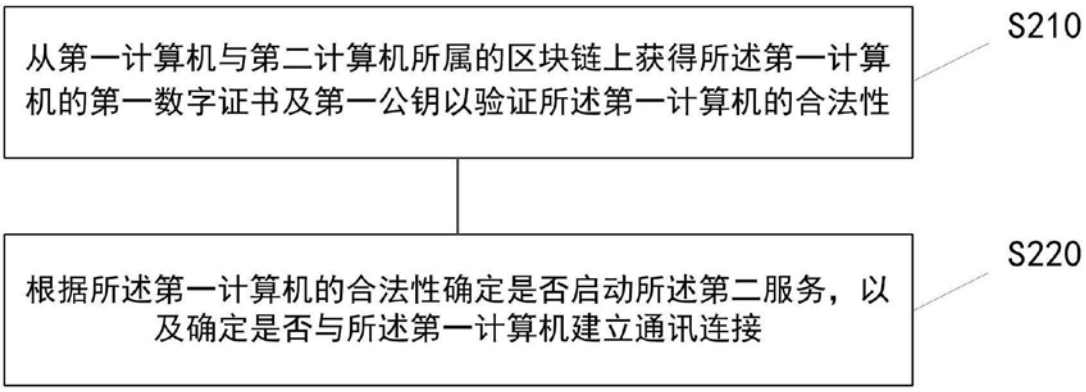

从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性
S210
根据所述第一计算机的合法性确定是否启动所述第二服务，以及确定是否与所述第一计算机建立通讯连接
S220

图7


第一验证模块
110
第一决策模块
120

图8


第三验证模块
210
第三决策模块
220

图9

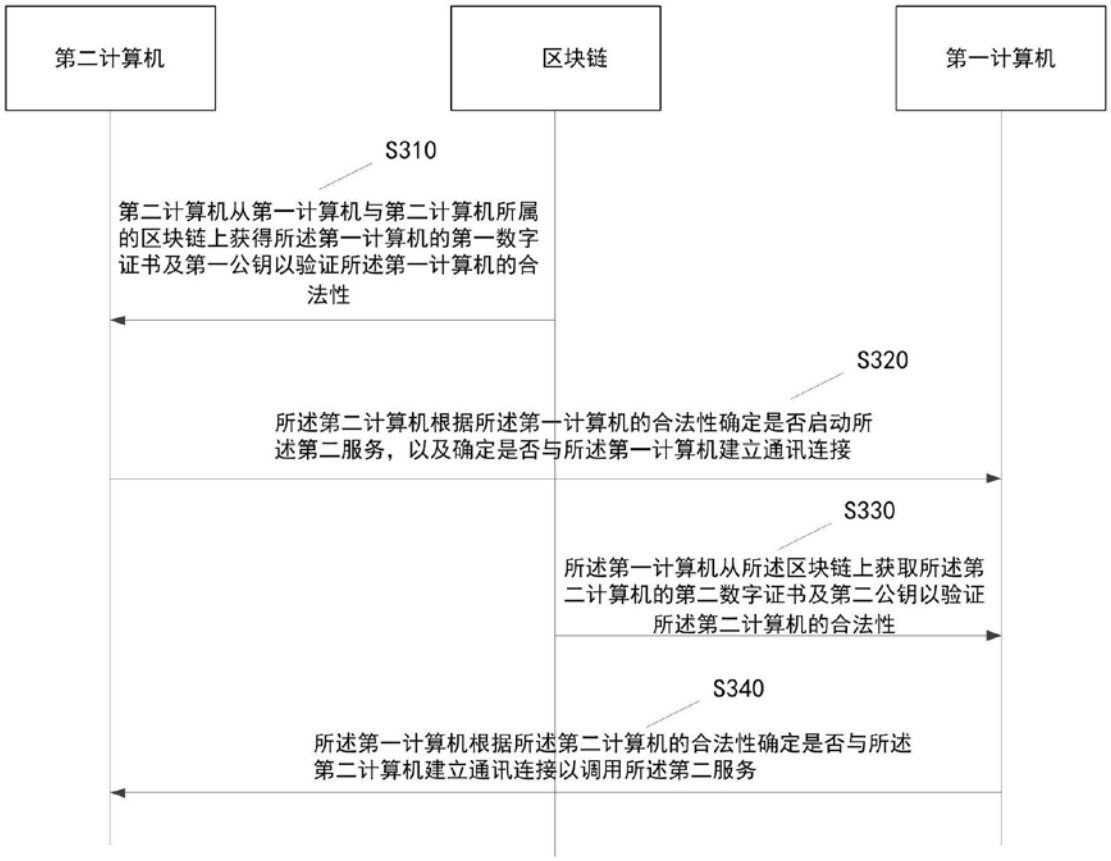

第二计算机
区块链
第一计算机
S310
第二计算机从第一计算机与第二计算机所属的区块链上获得所述第一计算机的第一数字证书及第一公钥以验证所述第一计算机的合法性
S320
所述第二计算机根据所述第一计算机的合法性确定是否启动所述第二服务，以及确定是否与所述第一计算机建立通讯连接
S330
所述第一计算机从所述区块链上获取所述第二计算机的第二数字证书及第二公钥以验证所述第二计算机的合法性
S340
所述第一计算机根据所述第二计算机的合法性确定是否与所述第二计算机建立通讯连接以调用所述第二服务

图10

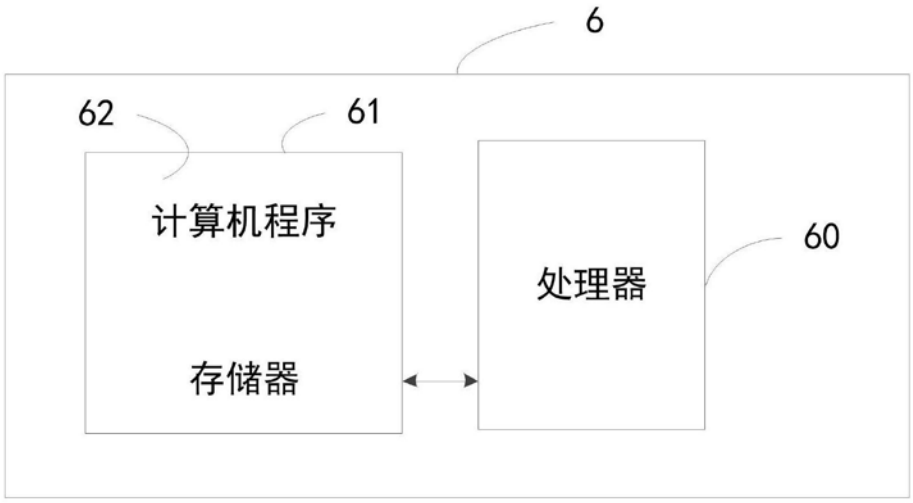

6
62
61
计算机程序
存储器
处理器
60

图11

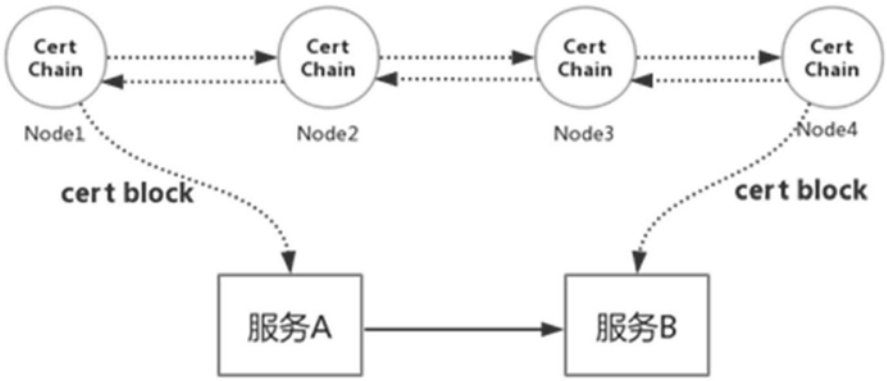

Cert Chain
Cert Chain
Cert Chain
Cert Chain
Node1
Node2
Node3
Node4
cert block
cert block
服务A
服务B

图12