(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108960830 B
(45)授权公告日 2022.07.15

(21)申请号 201810779278.1
(22)申请日 2018.07.16
(65)同一申请的已公布的文献号
申请公布号 CN 108960830 A
(43)申请公布日 2018.12.07
(73)专利权人 百度在线网络技术(北京)有限公司
地址 100085 北京市海淀区上地十街10号百度大厦三层
(72)发明人 肖伟
(74)专利代理机构 北京品源专利代理有限公司 11332
专利代理师 孟金喆
(51)Int.Cl.
G06Q 20/38(2012.01)
G06F 9/455(2006.01)
(56)对比文件
US 2018137465 A1,2018.05.17
CN 107707410 A,2018.02.16
CN 105893042 A,2016.08.24
JP 2009211622 A,2009.09.17
审查员 李晓霞

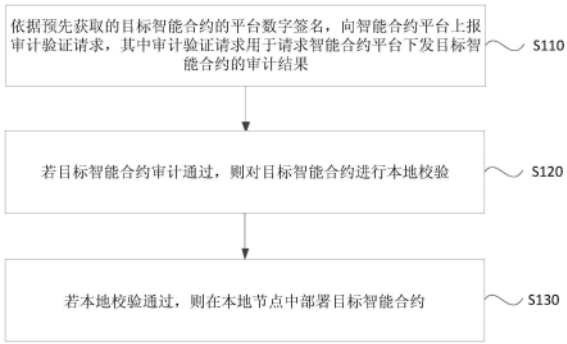
权利要求书3页 说明书12页 附图6页

(54)发明名称

智能合约的部署方法、装置、设备及存储介质

(57)摘要

本发明实施例公开了一种智能合约的部署方法、装置、设备及存储介质。其中，该方法由区块链网络中的节点执行，该方法包括：依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求，其中所述审计验证请求用于请求所述智能合约平台下发所述目标智能合约的审计结果；若所述目标智能合约审计通过，则对所述目标智能合约进行本地校验；若本地校验通过，则在本地节点中部署所述目标智能合约。本发明实施例提供的技术方案，区块链网络中的节点依据智能合约平台对智能合约的安全认证结果使用智能合约，解决了智能合约由于不被信任而导致不被使用的问题，保证了智能合约的安全性和可靠性。



CN 108960830 B

1.一种智能合约的部署方法,其特征在于,由区块链网络中的节点执行,所述方法包括:

依据预先获取的目标智能合约的平台数字签名,向智能合约平台上报审计验证请求,其中所述审计验证请求用于请求所述智能合约平台下发所述目标智能合约的审计结果;

若所述目标智能合约审计通过,则对所述目标智能合约进行本地校验;

若本地校验通过,则在本地节点中部署所述目标智能合约;

其中,区块链网络中的所有节点均部署有目标智能合约;

目标智能合约为基于内嵌合约机制采用原生语音言编写的智能合约,直接在物理机上执行;

智能合约平台是一个中心化或去中心化的智能合约存储系统。

2.根据权利要求1所述的方法,其特征在于,对所述目标智能合约进行本地校验,包括:

对本地的目标智能合约进行数字签名得到本地数字签名;

若所述平台数字签名与所述本地数字签名相同,则确定所述目标智能合约本地校验通过。

3.根据权利要求2所述的方法,其特征在于,对本地的目标智能合约进行数字签名得到本地数字签名之前,还包括:

若本地没有目标智能合约,则从所述智能合约平台拉取所述目标智能合约。

4.根据权利要求1-3任一项所述的方法,其特征在于,在本地节点中部署所述目标智能合约之后,还包括:

若接收到部署取消指令,则从本地节点中取消所述目标智能合约的部署,其中,所述部署取消指令是若区块链网络的区块生成节点检测到区块链网络中部署有所述目标智能合约的节点数量等于或小于所述区块链网络的节点总数量的一半生成的。

5.根据权利要求1-3任一项所述的方法,其特征在于,在本地节点中部署所述目标智能合约之后,还包括:

若接收到部署成功指令,则在本地节点中对所述目标智能合约进行初始化,其中所述部署成功指令是若区块链网络的区块生成节点检测到区块链网络中部署有所述目标智能合约的节点数量大于所述区块链网络的节点总数量的一半生成的。

6.根据权利要求1所述的方法,其特征在于,若本地节点是区块生成节点,则在本地节点中部署所述目标智能合约之后,还包括:

若检测到区块链网络中部署有所述目标智能合约的节点数量大于所述区块链网络的节点总数量的一半,则生成部署成功指令,并向区块链网络中的节点下发所述部署成功指令;

若检测到区块链网络中部署有所述目标智能合约的节点数量等于或小于所述区块链网络的节点总数量的一半,则生成部署取消指令,并向区块链网络中的节点下发所述部署取消指令。

7.根据权利要求1所述的方法,其特征在于,依据预先获取的目标智能合约的平台数字签名,向所述智能合约平台上报审计验证请求之前,还包括:

获取智能合约平台发布的目标智能合约的平台数字签名;或者,

获取区块链网络的创建节点发布的目标智能合约的平台数字签名。

8.根据权利要求1所述的方法，其特征在于，若本地节点是区块链网络的创建节点，则依据目标智能合约的平台数字签名，向所述智能合约平台上报审计验证请求之前，还包括：

从智能合约平台获取目标智能合约的平台数字签名，并向区块链网络中的其他节点发送所述平台数字签名。

9.一种智能合约的部署方法，其特征在于，由智能合约平台执行，所述方法包括：

接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求；

获取所述目标智能合约的审计结果，并向所述节点下发所述审计结果，使所述节点执行如下：若所述目标智能合约审计通过，则对所述目标智能合约进行本地校验；若本地校验通过，则在本地节点中部署所述目标智能合约；

其中，区块链网络中的所有节点均部署有目标智能合约；

目标智能合约为基于内嵌合约机制采用原生语音言编写的智能合约，直接在物理机上执行；

智能合约平台是一个中心化或去中心化的智能合约存储系统。

10.根据权利要求9所述的方法，其特征在于，接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求之前，还包括：

获取自定义智能合约的原代码；

获取并存储所述自定义智能合约的审计结果；

对所述自定义智能合约的原代码进行编译，确定编译后的可执行文件的平台数字签名，且向区块链网络中的节点发布所述平台数字签名，或者发布所述平台数字签名以及所述可执行文件。

11.根据权利要求9所述的方法，其特征在于，接收区块链网络中的节点依据目标智能合约的平台数字签名上报的审计验证请求之前，还包括：

响应区块链网络的创建节点发布的目标智能合约的部署请求，向所述创建节点发送所述目标智能合约的平台数字签名。

12.一种智能合约的部署装置，其特征在于，配置于区块链网络中的节点中，所述装置包括：

验证请求上报模块，用于依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求，其中所述审计验证请求用于请求所述智能合约平台下发所述目标智能合约的审计结果；

本地校验模块，用于若所述目标智能合约审计通过，则对所述目标智能合约进行本地校验；

智能合约部署模块，用于若本地校验通过，则在本地节点中部署所述目标智能合约；

其中，区块链网络中的所有节点均部署有目标智能合约；

目标智能合约为基于内嵌合约机制采用原生语音言编写的智能合约，直接在物理机上执行；

智能合约平台是一个中心化或去中心化的智能合约存储系统。

13.一种智能合约的部署装置，其特征在于，配置于智能合约平台中，所述装置包括：

验证请求接收模块，用于接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求；

审计结果下发模块，用于获取所述目标智能合约的审计结果，并向所述节点下发所述审计结果，使所述节点执行如下：若所述目标智能合约审计通过，则对所述目标智能合约进行本地校验；若本地校验通过，则在本地节点中部署所述目标智能合约；

其中，区块链网络中的所有节点均部署有目标智能合约；

目标智能合约为基于内嵌合约机制采用原生语音言编写的智能合约，直接在物理机上执行；

智能合约平台是一个中心化或去中心化的智能合约存储系统。

14.一种计算机设备，其特征在于，所述计算机设备包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-8中任一所述的智能合约的部署方法或者实现如权利要求9-11中任一所述的智能合约的部署方法。

15.一种存储介质，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1-8中任一所述的智能合约的部署方法或者实现如权利要求9-11中任一所述的智能合约的部署方法。

智能合约的部署方法、装置、设备及存储介质

技术领域

[0001] 本发明实施例涉及区块链技术领域，尤其涉及一种智能合约的部署方法、装置、设备及存储介质。

背景技术

[0002] 现有智能合约只有固定的几种模式，例如比特币的script模式，以太坊的solidity模式和或者EOS的WebAssembly模式。这几种智能合约的开发模式都有局限性，都不是用区块链的原生语言写，而是用其他语言写的。

[0003] 由于现有智能合约都不是用区块链的原生语言编写，现有智能合约都是在对CPU、内存、磁盘有制约条件的虚拟机中运行的，性能很差，虚拟机的限制也很多。

[0004] 采用原生语言编写可以在物理机上执行的智能合约虽然可以提高智能合约的性能，但是，原生语言的能力十分强大，并且智能合约直接运行在物理机上，而不是运行在虚拟机上，存在安全隐患。

发明内容

[0005] 本发明实施例提供了一种智能合约的部署方法、装置、设备及存储介质，解决了智能合约由于不被信任而导致不被使用的问题，保证了智能合约的安全性和可靠性。

[0006] 第一方面，本发明实施例提供了一种智能合约的部署方法，由区块链网络中的节点执行，该方法包括：

[0007] 依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求，其中所述审计验证请求用于请求所述智能合约平台下发所述目标智能合约的审计结果；

[0008] 若所述目标智能合约审计通过，则对所述目标智能合约进行本地校验；

[0009] 若本地校验通过，则在本地节点中部署所述目标智能合约。

[0010] 第二方面，本发明实施例提供了一种智能合约的部署方法，由智能合约平台执行，该方法包括：

[0011] 接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求；

[0012] 获取所述目标智能合约的审计结果，并向所述节点下发所述审计结果，使所述节点执行如下：若所述目标智能合约审计通过，则对所述目标智能合约进行本地校验；若本地校验通过，则在本地节点中部署所述目标智能合约。

[0013] 第三方面，本发明实施例提供了一种智能合约的部署装置，配置于区块链网络中的节点中，该装置包括：

[0014] 验证请求上报模块，用于依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求，其中所述审计验证请求用于请求所述智能合约平台下发所述目标智能合约的审计结果；

[0015] 本地校验模块，用于若所述目标智能合约审计通过，则对所述目标智能合约进行本地校验；

[0016] 智能合约部署模块，用于若本地校验通过，则在本地节点中部署所述目标智能合约。

[0017] 第四方面，本发明实施例提供了一种智能合约的部署装置，配置于智能合约平台中，该装置包括：

[0018] 验证请求接收模块，用于接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求；

[0019] 审计结果下发模块，用于获取所述目标智能合约的审计结果，并向所述节点下发所述审计结果，使所述节点执行如下：若所述目标智能合约审计通过，则对所述目标智能合约进行本地校验；若本地校验通过，则在本地节点中部署所述目标智能合约。

[0020] 第五方面，本发明实施例还提供了一种设备，该设备包括：

[0021] 一个或多个处理器；

[0022] 存储装置，用于存储一个或多个程序；

[0023] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现第一方面中任意所述的智能合约的部署方法或者实现第二方面中任意所述的智能合约的部署方法。

[0024] 第六方面，本发明实施例还提供了一种存储介质，其上存储有计算机程序，该程序被处理器执行时实现第一方面中任意所述的智能合约的部署方法或者实现第二方面中任意所述的智能合约的部署方法。

[0025] 本发明实施例提供的技术方案，区块链网络中的节点在部署目标智能合约时，依据智能合约平台对目标智能合约的审计结果及本地校验结果来部署目标智能合约，解决了智能合约直接在物理机上执行，由于存在安全隐患等不被信任而导致不被使用的问题，保证了智能合约的安全性和可靠度。

附图说明

[0026] 图1是本发明实施例一中提供的一种智能合约的部署方法的流程图；

[0027] 图2是本发明实施例二中提供的一种智能合约的部署方法的流程图；

[0028] 图3是本发明实施例三中提供的一种智能合约的部署方法的流程图；

[0029] 图4是本发明实施例四中提供的一种智能合约的部署方法的流程图；

[0030] 图5是本发明实施例五中提供的一种智能合约的部署装置的结构框图；

[0031] 图6是本发明实施例六中提供的一种智能合约的部署装置的结构框图；

[0032] 图7是本发明实施例七中提供的一种设备的结构示意图。

具体实施方式

[0033] 下面结合附图和实施例对本发明实施例作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明实施例，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明实施例相关的部分而非全部结构。

[0034] 实施例一

[0035] 图1为本发明实施例一提供的一种智能合约的部署方法的流程图，本实施例可用于解决基于内嵌合约机制采用原生语音言编写的智能合约直接在物理机上执行，由于存在安全隐患等而不被信任导致不被使用的情况。所适用的区块链可以是公有链、联盟链或者私链。整套智能合约的部署方法通常由区块链网络中的节点与智能合约平台配合执行，本发明实施例的方案应用于区块链网络中的节点，该方法可以由本发明实施例提供的智能合约的部署装置来执行，该装置可采用软件和/或硬件的方式实现，并可集成于承载区块链网络节点的计算设备中。参见图1，该方法具体包括：

[0036] S110，依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求，其中审计验证请求用于请求智能合约平台下发目标智能合约的审计结果。

[0037] 其中，目标智能合约是指基于插件机制所编写的可供区块链网络中的节点调用并执行的代码段，一个目标智能合约的执行可实现至少一种功能或处理一类事务请求；可选的，目标智能合约可以包括至少一个运行函数，以及与运行函数存在动态绑定关系、在运行中调用的函数；还可以包括初始化函数，用于为首次配置于本地节点中的目标智能合约中的函数的输入参数、变量或条件等赋予初始值，从而使目标智能合约能被运行；此外，目标智能合约中还可以包括各运行函数的回滚函数，运行函数与回滚函数一一对应，若运行函数没有包括回滚函数，则可以采用系统默认生成的运行函数的回滚函数。

[0038] 智能合约平台是一个中心化或去中心化的智能合约存储系统，可进行智能合约的审计、编译及下发等；典型的智能合约平台可以是一个承载智能合约审计、编译及下发等功能的计算机设备。平台数字签名是指智能合约平台采用签名算法如SHA256、平台公钥或私钥等对目标智能合约进行的唯一签名，可以是目标智能合约的哈希值或标识等。

[0039] 需要说明的是，目标智能合约的平台数字签名是唯一的，两者存在动态绑定关系，即可依据目标智能合约的平台数字签名在智能平台上查询到唯一的智能合约。

[0040] 并且，若本地节点是区块链网络的创建节点与本地节点不是创建节点，平台数字签名的获取方式存在区别。

[0041] 若本地节点不是区块链网络的创建节点，则本地节点可通过如下几种方式获取目标智能合约的平台数字签名：1)接收智能合约平台向区块链网络发布的目标智能合约的平台数字签名；2)接收区块链网络的创建节点在区块链网络中发布的目标智能合约的平台数字签名；3)从区块链网络中预先从智能合约平台或创建节点获取有平台数字签名的其他节点处获取。

[0042] 若本地节点是区块链网络的创建节点，则本地节点可以通过两种方式获取目标智能合约的平台数字签名：1)接收智能合约平台向区块链网络发布的目标智能合约的平台数字签名；2)向智能合约平台发送目标智能合约部署请求，接收智能合约平台下发的目标智能合约的平台数字签名。

[0043] 审计校验请求是本地节点依据预先获取的智能合约的平台数字签名及本地节点标识等生成的，用于指示智能合约平台依据目标智能合约的平台数字签名等到目标智能合约的审计结果，并依据本地节点标识向本地节点下发审计结果。其中，审计结果是指对目标智能合约的代码撰写规范、功能及安全性等进行认证的结果，可以包括审计通过和审计未通过两种情况。

[0044] 具体的，若本地节点需要部署一个目标智能合约，则可依据预先获取的目标智能

合约的平台数字签名及本地节点标识等生成审计校验请求，并上报至智能合约平台，以使智能合约平台向本地节点目标智能合约的审计结果；智能合约平台也可以向区块链网络中的其他节点下发该目标智能合约的审计结果，或者是本地节点将从智能合约平台接收的目标智能合约的审计结果转发至区块链网络中的其他节点。

[0045] S120，若目标智能合约审计通过，则对目标智能合约进行本地校验。

[0046] 其中，本地校验可以是对目标智能合约的平台数字签名进行校验，如可以采用与智能合约平台相同的签名算法对目标智能合约进行签名，并比较平台数字签名和本地签名的一致性。

[0047] 具体的，为了降低智能合约平台作假或目标智能合约的平台数字签名下发至区块链网络的过程中被外部设备截获篡改的概率，本地节点在确认目标智能合约审计通过后，可对目标智能合约进行本地校验，以保证目标智能合约的安全性和可靠性。

[0048] 可选的，若目标智能合约审计未通过，则将目标智能合约的平台数字签名从本地删除。

[0049] S130，若本地校验通过，则在本地节点中部署目标智能合约。

[0050] 具体的，若目标智能合约的本地校验通过，本地节点则将目标智能合约放入本地存储智能合约的文件中，以供本地节点调用。

[0051] 示例性的，在本地节点中部署目标智能合约之后，还可以包括：向区块链网络中的区块生成节点或其他节点发送本地部署成功信息。

[0052] 本发明实施例提供的技术方案，区块链网络中的节点在部署目标智能合约时，依据智能合约平台对目标智能合约的审计结果及本地校验结果即两级校验结果确定部署目标智能合约，解决了智能合约直接在物理机上执行，由于存在安全隐患等不被信任而导致不被使用的问题，保证了智能合约的安全性和可靠度。

[0053] 需要说明的是，为了保证区块链网络能够有序进行，区块链网络中的所有节点需要部署相同的智能合约。因此需要区块链网络中的区块生成节点对区块链网络中的节点部署目标智能合约的情况进行检测。

[0054] 若本地节点不是区块生成节点，示例性的，在本地节点中部署所述目标智能合约之后，还可以包括：若接收到部署取消指令，则从本地节点中取消目标智能合约的部署，其中，部署取消指令是若区块链网络的区块生成节点检测到区块链网络中部署有目标智能合约的节点数量等于或小于区块链网络的节点总数量的一半生成的。

[0055] 具体的，区块生成节点检测到区块链网络中50％以下的节点部署了一个目标智能合约，代表该目标智合约部署失败，此时区块生成节点生成部署取消指令发送至区块链网络中的其他节点，本地节点在接收到部署取消指令时，可以将目标智能合约从本地删除，并继续正常工作。可选的，若区块生成节点检测到区块链网络中的任一节点接收到部署取消指令后，不执行取消部署目标智能合约的操作，则将该节点剔除区块链网络。

[0056] 对应的，若本地节点不是区块生成节点，示例性的，在本地节点中部署所述目标智能合约之后，还可以包括：若接收到部署成功指令，则在本地节点中对目标智能合约进行初始化，其中部署成功指令是若区块链网络的区块生成节点检测到区块链网络中部署有目标智能合约的节点数量大于区块链系统网络的节点总数量的一半生成的。

[0057] 具体的，区块生成节点检测到区块链网络中50％以上的节点部署了一个目标智能

合约，代表该目标智合约部署成功，此时区块生成节点生成部署成功指令发送至区块链网络中的其他节点，以使区块链网络中的所有节点均部署该目标智能合约。本地节点在接收到部署成功指令时，可依据初始化函数对目标智能合约进行初始化，从而该目标智能合约被调用时可执行相应功能。

[0058] 若本地节点是区块生成节点，示例性的，在本地节点中部署目标智能合约之后，还可以包括：若检测到区块链网络中部署有目标智能合约的节点数量大于区块链网络的节点总数量的一半，则生成部署成功指令，并向区块链网络中的节点下发部署成功指令；

[0059] 若检测到区块链网络中部署有目标智能合约的节点数量等于或小于区块链网络的节点总数量的一半，则生成部署取消指令，并向区块链网络中的节点下发部署取消指令。

[0060] 本发明实施例提供的技术方案，在本地节点部署目标智能合约之后，通过区块链网络中的区块生成节点对区块链网络中的节点部署目标智能合约的情况进行检测，并下发部署取消指令或部署成功指令，提高了智能合约部署的灵活性，且保证了区块链网络中的所有节点部署相同的智能合约，从而使区块链网络能够有序进行。

[0061] 实施例二

[0062] 图2为本发明实施例二提供的一种智能合约的部署方法的流程图，本实施例在上述实施例一的基础上，进一步的优化。参见图2，该方法具体包括：

[0063] S210，获取智能合约平台发布的目标智能合约的平台数字签名；或者，获取区块链网络的创建节点发布的目标智能合约的平台数字签名。

[0064] 具体的，若本地节点不是区块链网络的创建节点，可以通过智能合约平台主动发布的方式获取目标智能合约的平台数字签名；还可以通过如下方式获取目标智能合约的平台数字签名：区块链网络的创建节点在创建区块链时主动向智能合约平台发送目标智能合约部署请求，并接收智能合约平台下发的智能合约的平台数字签名后，向区块链网络中的其他节点转发的目标智能合约的平台数字签名；本地节点接收区块链网络的创建节点在区块链网络中发布的目标智能合约的平台数字签名。

[0065] 若本地节点是区块链网络的创建节点，则本地节点可以通过如下两种方式获取目标智能合约的平台数字签名：1)接收智能合约平台向区块链网络发布的目标智能合约的平台数字签名；2)在创建区块链时主动向智能合约平台发送目标智能合约部署请求，接收智能合约平台下发的目标智能合约的平台数字签名。

[0066] S220，依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求，其中审计验证请求用于请求智能合约平台下发目标智能合约的审计结果。

[0067] 具体的，若本地节点不是区块链网络的创建节点，当需要部署一个目标智能合约时，可依据预先获取的目标智能合约的平台数字签名及本地节点标识等生成审计校验请求，并上报至智能合约平台，以使智能合约平台向本地节点目标智能合约的审计结果。

[0068] 可选的，若本地节点是区块链网络的创建节点，则依据目标智能合约的平台数字签名，向智能合约平台上报审计验证请求之前，还可以包括：从智能合约平台获取目标智能合约的平台数字签名，并向区块链网络中的其他节点发送平台数字签名。

[0069] 具体的，若本地节点是区块链网络的创建节点，当需要部署一个目标智能合约时，向区块链网络中的其他节点发送智能合约平台下发的目标智能合约的平台数字签名，以使其他节点存储该目标智能合约的平台数字签名，或者存储并依据自身需求执行部署目标智

能合约的操作。本地节点依据预先获取的目标智能合约的平台数字签名及本地节点标识等生成审计校验请求，并上报至智能合约平台，以使智能合约平台向本地节点目标智能合约的审计结果。

[0070] S230，若目标智能合约审计通过，则对本地的目标智能合约进行数字签名得到本地数字签名。

[0071] 其中，本地数字签名是指本地节点采用签名算法如SHA256、公钥或私钥等对目标智能合约进行的唯一签名，可以是目标智能合约的哈希值或标识等。

[0072] 本地的目标智能合约可以是本地节点从区块链网络中的其他节点如创建节点获取并存储在本地的；也可以是依据目标智能合约的平台数字签名从智能合约平台获取并存储在本地的。

[0073] 具体的，本地节点对本地的目标智能合约采用与智能合约平台相同的签名算法得到本地数字签名。

[0074] 示例性的，对本地的目标智能合约进行数字签名得到本地数字签名之前，还可以包括：若本地没有目标智能合约，则从智能合约平台拉取目标智能合约。

[0075] 为了提高效率，可选的，若本地没有目标智能合约，本地节点可向区块链网络中的其他节点发送包括目标智能合约的平台数字签名的获取请求，若接收到任一节点的回应信息，则从该节点中获取目标智能合约；若未接收到任一节点的回应信息，则从智能合约平台拉取该目标智能合约。

[0076] S240，若平台数字签名与本地数字签名相同，则确定目标智能合约本地校验通过。

[0077] 可选的，若平台数字签名与本地数字签名不相同，则确定目标智能合约本地校验未通过，此时，向区块链网络中的其他节点发送包括目标智能合约的平台数字签名的本地校验未通过信息；若接收到区块生成节点发送的本地校验未通过信息，则将目标智能合约从本地删除。

[0078] S250，若本地校验通过，则在本地节点中部署目标智能合约。

[0079] 本发明实施例提供的技术方案，提供了一种本地校验的方案，使区块链网络中的节点在部署目标智能合约时，能够依据智能合约平台对目标智能合约的审计结果及本地校验结果即两级校验结果确定部署目标智能合约，解决了智能合约直接在物理机上执行，由于存在安全隐患等不被信任而导致不被使用的问题，保证了智能合约的安全性和可靠度。

[0080] 实施例三

[0081] 图3为本发明实施例三提供的一种智能合约的部署方法的流程图，本实施例可用于解决基于内嵌合约机制采用原生语音言编写的智能合约直接在物理机上执行，由于存在安全隐患等而不被信任导致的不被使用的情况。所适用的区块链可以是公有链、联盟链或者私链。整套智能合约的部署方法通常由区块链网络中的节点与智能合约平台配合执行，本发明实施例的方案应用于智能合约平台，该方法可以由本发明实施例提供的智能合约的部署装置来执行，该装置可采用软件和/或硬件的方式实现。参见图3，该方法具体包括：

[0082] S310，接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求。

[0083] 其中，平台数字签名是指智能合约平台采用签名算法如SHA256、平台公钥或私钥等对目标智能合约进行的唯一签名，可以是目标智能合约的哈希值或标识等。

[0084] 审计验证请求是区块链网络中的节点依据预先获取的智能合约的平台数字签名及本地节点标识等生成的请求，用于指示智能合约平台依据目标智能合约的平台数字签名等到目标智能合约的审计结果，并依据本地节点标识下发至本地节点。

[0085] 为了提高智能合约的部署效率，智能合约平台在接收到目标智能合约的审计验证请求之前需完成对该目标智能合于的审计。示例性的，接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求之前，还可以包括如下操作：

[0086] A、获取自定义智能合约的原代码。

[0087] 其中，原代码是指采用区块链原生语言所编写的代码段，区块链原生语言是指可以编写区块链底层网络架构的语言，例如GO语言、Java语言或者C++语言等。

[0088] 自定义智能合约可以是区块链网络中的节点用户或其他非区块链网络的节点用户依据自身需求所编写，并上传至智能合约平台的。

[0089] 具体的，可以通过用户在智能合约平台上输入或上传自定义智能合约的原代码的方式；也可以是接收区块链网络中的任一节点发送的自定义智能合约的原代码方式，获取自定义智能合约的原代码。

[0090] B、获取并存储自定义智能合约的审计结果。

[0091] 具体的，当智能合约平台获取到自定义智能合约的原代码后，可依据预先设置的审计规则对该自定义智能合约进行审计，并将审计结果存储在本地。其中，审计规则是指预先设置的审核原则，如依据代码的撰写规则、功能、安全性及可靠性等进行审核。

[0092] C、对自定义智能合约的原代码进行编译，确定编译后的可执行文件的平台数字签名，且向区块链网络中的节点发布平台数字签名，或者发布平台数字签名以及可执行文件。

[0093] 其中，可执行文件是指可供区块链网络调用的代码，即为目标智能合约。

[0094] 具体的，若自定义智能合约的审计结果是审计通过，智能合约平台则对自定义智能合约的原代码进行编译得到可执行文件，并对可执行文件采用签名算法如SHA256等进行数字签名得到可执行文件的平台数字签名；本地建立可执行文件的平台数字签名、可执行文件及审计结果三者的关联关系，且向区块链网络中的节点发布平台数字签名，或者发布平台数字签名以及可执行文件。

[0095] 示例性的，若向智能合约平台发送审计验证请求的是区块链网络中的区块链的创建节点，则智能合约平台在接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求之前，还可以包括：响应区块链网络的创建节点发布的目标智能合约的部署请求，向创建节点发送目标智能合约的平台数字签名。

[0096] 其中，部署请求可以是创建节点在创建区块链，且需部署某一目标智能合约时，向智能合约平台所发送的请求。

[0097] 具体的，创建节点向智能合约平台发送目标智能合约的部署请求，智能合约平台接收到创建节点发送的目标智能合约的部署请求后，依据目标智能合约与目标智能合约的平台数字签名的关联关系，确定目标智能合约的平台数字签名，并向创建节点发送该目标智能合约的平台数字签名。

[0098] S320，获取目标智能合约的审计结果，并向节点下发审计结果，使节点执行如下：若目标智能合约审计通过，则对目标智能合约进行本地校验；若本地校验通过，则在本地节点中部署目标智能合约。

[0099] 具体的，当智能合约平台接收到区块链网络中的节点发送的包括目标智能合约的平台数字签名的审计验证请求时，依据预先存储的目标智能合约、目标智能合约的平台数字签名及目标智能合约的审计结果三者之间的关联关系，得到目标智能合约的审计结果，并依据审计验证请求中的本地节点标识向该节点发送目标智能合约的审计结果，以使该节点依据审计结果执行部署目标智能合约的操作。

[0100] 本发明实施例提供的技术方案，通过智能合约平台对用户发布的自定义智能合约进行审计，并下发至区块链网络中的节点，以使区块链网络中的节点依据审计结果及本地校验结果即两级校验结果部署目标智能合约，解决了智能合约直接在物理机上执行，由于存在安全隐患等不被信任而导致不被使用的问题，保证了智能合约的安全性和可靠度。

[0101] 实施例四

[0102] 图4为本发明实施例四提供的一种智能合约的部署方法的流程图，本实施在上述实施例的基础上，提供了一种区块链系统中节点与智能合约平台配合进行交互实现智能合约部署的优选示例。参见图4，该方法具体包括：

[0103] S410，区块链网络中的节点依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求。

[0104] S420，智能合约平台接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求。

[0105] S430，智能合约平台获取目标智能合约的审计结果，并向区块链网络中的节点下发审计结果。

[0106] S440，区块链网络中的节点接收智能合约平台下发的目标智能合约的审计结果。

[0107] S450，若目标智能合约审计通过，区块链网络中的节点则对目标智能合约进行本地校验。

[0108] S460，若本地校验通过，区块链网络中的节点则在本地节点中部署目标智能合约。

[0109] 本发明实施例提供的技术方案，区块链网络中的节点在部署目标智能合约时，向智能合约平台发送目标智能合约的审计验证请求，区块链网络中的节点依据智能合约平台对目标智能合约的审计结果及本地校验结果即两级校验结果确定部署目标智能合约，解决了智能合约直接在物理机上执行，由于存在安全隐患等不被信任而导致不被使用的问题，保证了智能合约的安全性和可靠度。

[0110] 实施例五

[0111] 图5为本发明实施例五提供的一种智能合约的部署装置的结构框图，该装置配置于区块链系统中的节点中，可执行本发明实施例一和实施例二所提供的智能合约的部署方法，具备执行方法相应的功能模块和有益效果。如图5所示，该装置可以包括：

[0112] 验证请求上报模块510，用于依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求，其中审计验证请求用于请求智能合约平台下发目标智能合约的审计结果；

[0113] 本地校验模块520，用于若目标智能合约审计通过，则对目标智能合约进行本地校验；

[0114] 智能合约部署模块530，用于若本地校验通过，则在本地节点中部署目标智能合约。

[0115] 本发明实施例提供的技术方案，区块链网络中的节点在部署目标智能合约时，依据智能合约平台对目标智能合约的审计结果及本地校验结果即两级校验结果确定部署目标智能合约，解决了智能合约直接在物理机上执行，由于存在安全隐患等不被信任而导致不被使用的问题，保证了智能合约的安全性和可靠度。

[0116] 示例性的，本地校验模块520具体用于：

[0117] 对本地的目标智能合约进行数字签名得到本地数字签名；若平台数字签名与本地数字签名相同，则确定目标智能合约本地校验通过。

[0118] 示例性的，上述装置还可以包括：

[0119] 智能合约获取模块，用于在对本地的目标智能合约进行数字签名得到本地数字签名之前，若本地没有目标智能合约，则从智能合约平台拉取目标智能合约。

[0120] 示例性的，上述装置还可以包括：

[0121] 部署指令接收模块，用于在本地节点中部署所述目标智能合约之后，若接收到部署取消指令，则从本地节点中取消目标智能合约的部署，其中，部署取消指令是若区块链网络的区块生成节点检测到区块链网络中部署有目标智能合约的节点数量等于或小于区块链网络的节点总数量的一半生成的。

[0122] 示例性的，部署指令接收模块，还用于在本地节点中部署所述目标智能合约之后，若接收到部署成功指令，则在本地节点中对目标智能合约进行初始化，其中部署成功指令是若区块链网络的区块生成节点检测到区块链网络中部署有目标智能合约的节点数量大于区块链网络的节点总数量的一半生成的。

[0123] 示例性的，上述装置还可以包括：

[0124] 部署指令下发模块，用于若本地节点是区块生成节点，则在本地节点中部署目标智能合约之后，若检测到区块链网络中部署有目标智能合约的节点数量大于区块链网络的节点总数量的一半，则生成部署成功指令，并向区块链网络中的节点下发部署成功指令；

[0125] 部署指令下发模块，还用于若检测到区块链网络中部署有目标智能合约的节点数量等于或小于区块链网络的节点总数量的一半，则生成部署取消指令，并向区块链网络中的节点下发部署取消指令。

[0126] 示例性的，上述装置还可以包括：

[0127] 平台签名获取模块，用于在依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求之前，获取智能合约平台发布的目标智能合约的平台数字签名；或者，获取区块链网络的创建节点发布的目标智能合约的平台数字签名。

[0128] 示例性的，上述装置还可以包括：

[0129] 第一平台签名发送模块，用于若本地节点是区块链网络的创建节点，则依据目标智能合约的平台数字签名，向智能合约平台上报审计验证请求之前，从智能合约平台获取目标智能合约的平台数字签名，并向区块链网络中的其他节点发送平台数字签名。

[0130] 实施例六

[0131] 图6为本发明实施例六提供的一种智能合约的部署装置的结构框图，该装置配置于智能合约平台中，可执行本发明实施例三所提供的智能合约的部署方法，具备执行方法相应的功能模块和有益效果。如图6所示，该装置可以包括：

[0132] 验证请求接收模块610，用于接收区块链系统中的节点依据目标智能合约的平台

数字签名上报的审计验证请求；

[0133] 审计结果下发模块620，用于获取目标智能合约的审计结果，并向节点下发审计结果，使节点执行如下：若目标智能合约审计通过，则对目标智能合约进行本地校验；若本地校验通过，则在本地节点中部署目标智能合约。

[0134] 本发明实施例提供的技术方案，通过智能合约平台对用户发布的自定义智能合约进行审计，并下发至区块链网络中的节点，以使区块链网络中的节点依据审计结果及本地校验结果即两级校验结果部署目标智能合约，解决了智能合约直接在物理机上执行，由于存在安全隐患等不被信任而导致不被使用的问题，保证了智能合约的安全性和可靠度。

[0135] 示例性的，上述装置还可以包括：

[0136] 原代码获取模块，用于在接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求之前，获取自定义智能合约的原代码；

[0137] 审计结果获取模块，用于获取并存储自定义智能合约的审计结果；

[0138] 第二平台签名发送模块，用于对自定义智能合约的原代码进行编译，确定编译后的可执行文件的平台数字签名，且向区块链网络中的节点发布平台数字签名，或者发布平台数字签名以及可执行文件。

[0139] 示例性的，第二平台签名发送模块，还用于在接收区块链网络中的节点依据目标智能合约的平台数字签名上报的审计验证请求之前，响应区块链网络的创建节点发布的目标智能合约的部署请求，向创建节点发送目标智能合约的平台数字签名。

[0140] 实施例七

[0141] 图7为本发明实施例七提供的一种设备的结构示意图，图7示出了适于用来实现本发明实施例实施方式的示例性设备的框图。图7显示的服务器仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。设备12典型的是承担区块链网络节点功能的计算设备；也可以是具有智能合约审计、编译及下发等功能的计算机设备。

[0142] 如图7所示，设备12以通用计算设备的形式表现。设备12的组件可以包括但不限于：一个或者多个处理器或者处理单元16，系统存储器28，连接不同系统组件(包括系统存储器28和处理单元16)的总线18。

[0143] 总线18表示几类总线结构中的一种或多种，包括存储器总线或者存储器控制器，外围总线，图形加速端口，处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说，这些体系结构包括但不限于工业标准体系结构(ISA)总线，微通道体系结构(MAC)总线，增强型ISA总线、视频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0144] 设备12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被设备12访问的可用介质，包括易失性和非易失性介质，可移动的和不可移动的介质。

[0145] 系统存储器28可以包括易失性存储器形式的计算机系统可读介质，例如随机存取存储器(RAM)30和/或高速缓存存储器32。设备12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例，存储系统34可以用于读写不可移动的、非易失性磁介质(图7未显示，通常称为“硬盘驱动器”)。尽管图7中未示出，可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器，以及对可移动非易失性光盘(例如CD-ROM，DVD-ROM或者其它光介质)读写的光盘驱动器。在这些情况下，每个驱动器可以通过一个或者多个数据介质接口与总线18相连。系统存储器28可以包括至少一个程序产

品，该程序产品具有一组(例如至少一个)程序模块，这些程序模块被配置以执行本发明实施例各实施例的功能。

[0146] 具有一组(至少一个)程序模块42的程序/实用工具40，可以存储在例如系统存储器28中，这样的程序模块42包括但不限于操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。程序模块42通常执行本发明实施例所描述的实施例中的功能和/或方法。

[0147] 设备12也可以与一个或多个外部设备14(例如键盘、指向设备、显示器24等)通信，还可与一个或者多个使得用户能与该设备12交互的设备通信，和/或与使得该设备12能与一个或多个其它计算设备进行通信的任何设备(例如网卡，调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口22进行。并且，设备12还可以通过网络适配器20与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。如图所示，网络适配器20通过总线18与设备12的其它模块通信。应当明白，尽管图中未示出，可以结合设备12使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0148] 处理单元16通过运行存储在系统存储器28中的程序，从而执行各种功能应用以及数据处理，例如实现本发明实施例所提供的智能合约的部署方法。

[0149] 实施例八

[0150] 本发明实施例八还提供一种计算机可读存储介质，其上存储有计算机程序(或称为计算机可执行指令)，该程序被处理器执行时可实现上述任意实施例所述的智能合约的部署方法。该计算机可读存储介质，可以配置于承载区块链网络节点的计算设备中，也可以配置于智能合约平台上。

[0151] 本发明实施例的计算机存储介质，可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0152] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0153] 计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0154] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明实施例操作的计算机程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、

Smalltalk、C++，还包括常规的过程式程序设计语言—诸如”C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0155] 注意，上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解，本发明不限于这里所述的特定实施例，对本领域技术人员来说能够进行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此，虽然通过以上实施例对本发明实施例进行了较为详细的说明，但是本发明实施例不仅仅限于以上实施例，在不脱离本发明构思的情况下，还可以包括更多其他等效实施例，而本发明的范围由所附的权利要求范围决定。

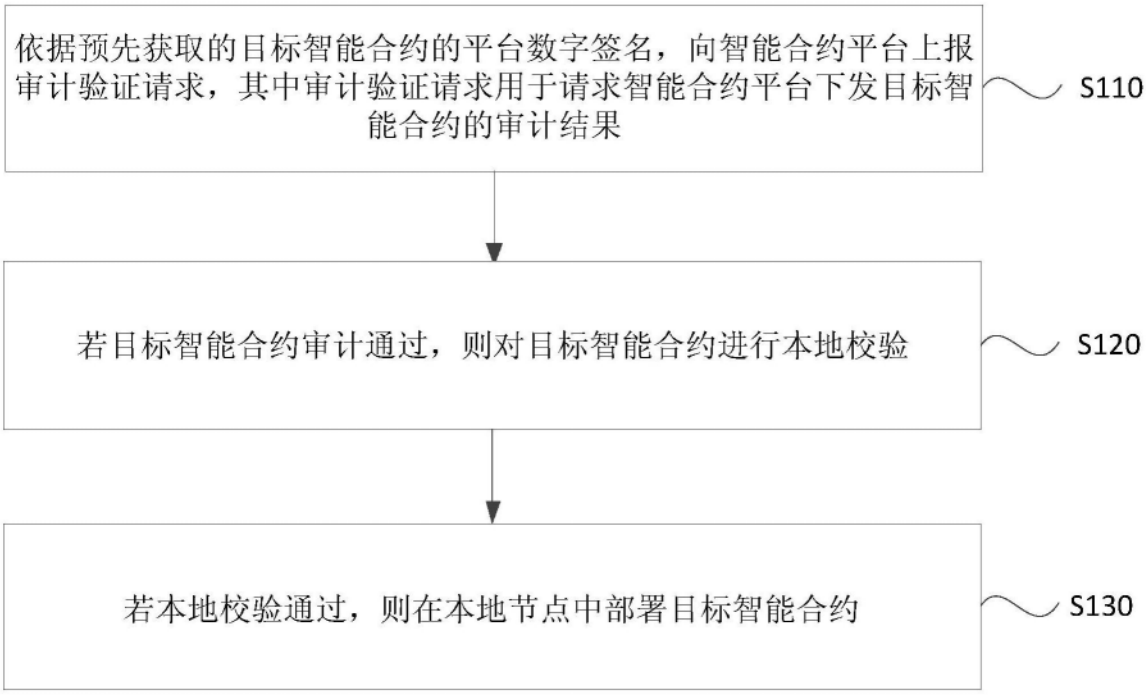

依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求，其中审计验证请求用于请求智能合约平台下发目标智能合约的审计结果
S110
若目标智能合约审计通过，则对目标智能合约进行本地校验
S120
若本地校验通过，则在本地节点中部署目标智能合约
S130

图1

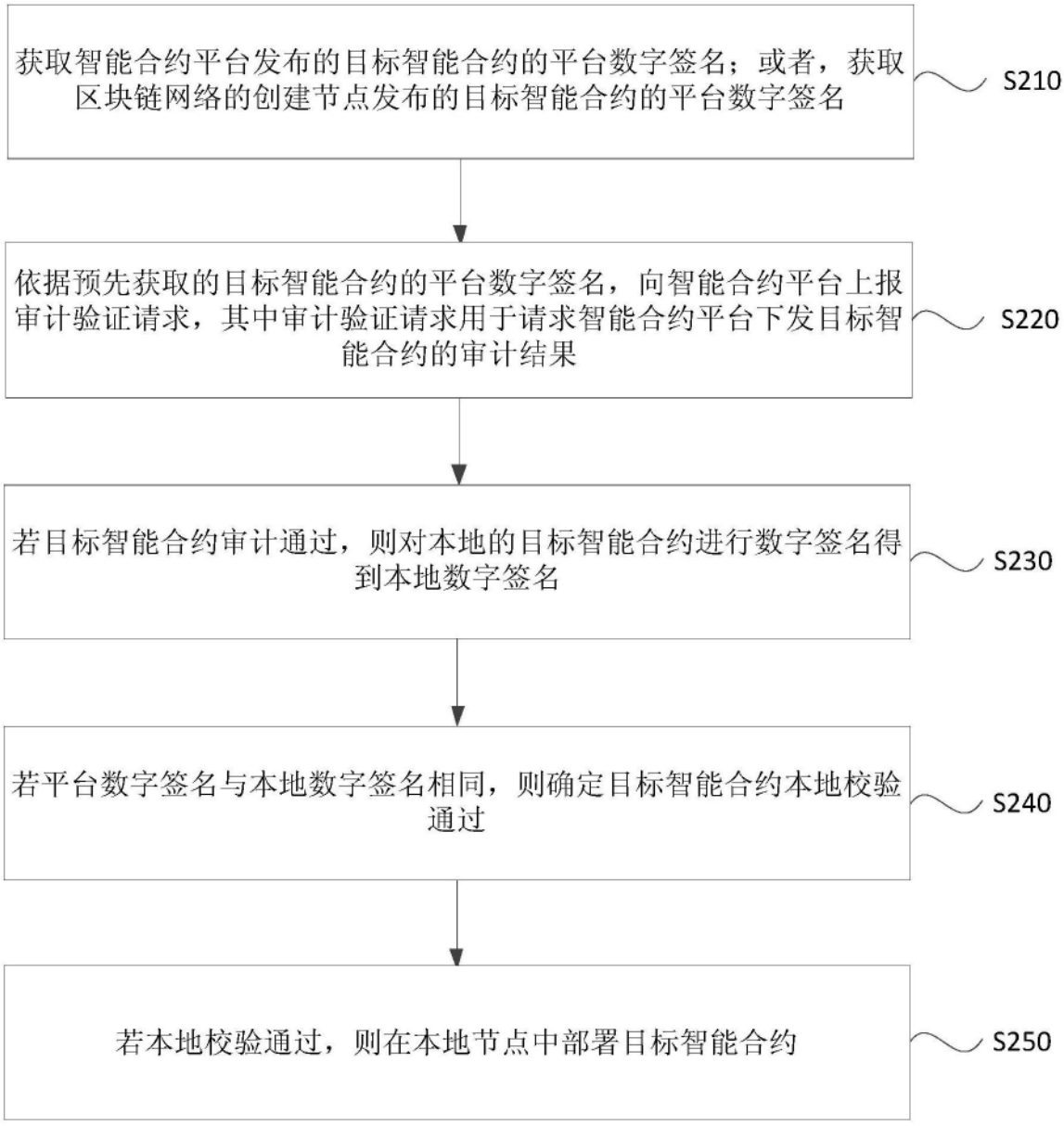

获取智能合约平台发布的目标智能合约的平台数字签名；或者，获取区块链网络的创建节点发布的目标智能合约的平台数字签名
S210
依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求，其中审计验证请求用于请求智能合约平台下发目标智能合约的审计结果
S220
若目标智能合约审计通过，则对本地的目标智能合约进行数字签名得到本地数字签名
S230
若平台数字签名与本地数字签名相同，则确定目标智能合约本地校验通过
S240
若本地校验通过，则在本地节点中部署目标智能合约
S250

图2

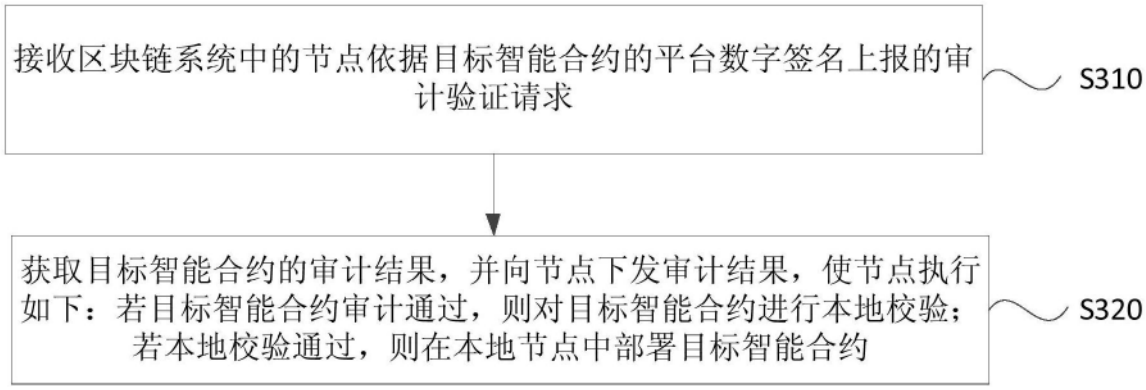

接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求
S310
获取目标智能合约的审计结果，并向节点下发审计结果，使节点执行如下：若目标智能合约审计通过，则对目标智能合约进行本地校验；若本地校验通过，则在本地节点中部署目标智能合约
S320

图3

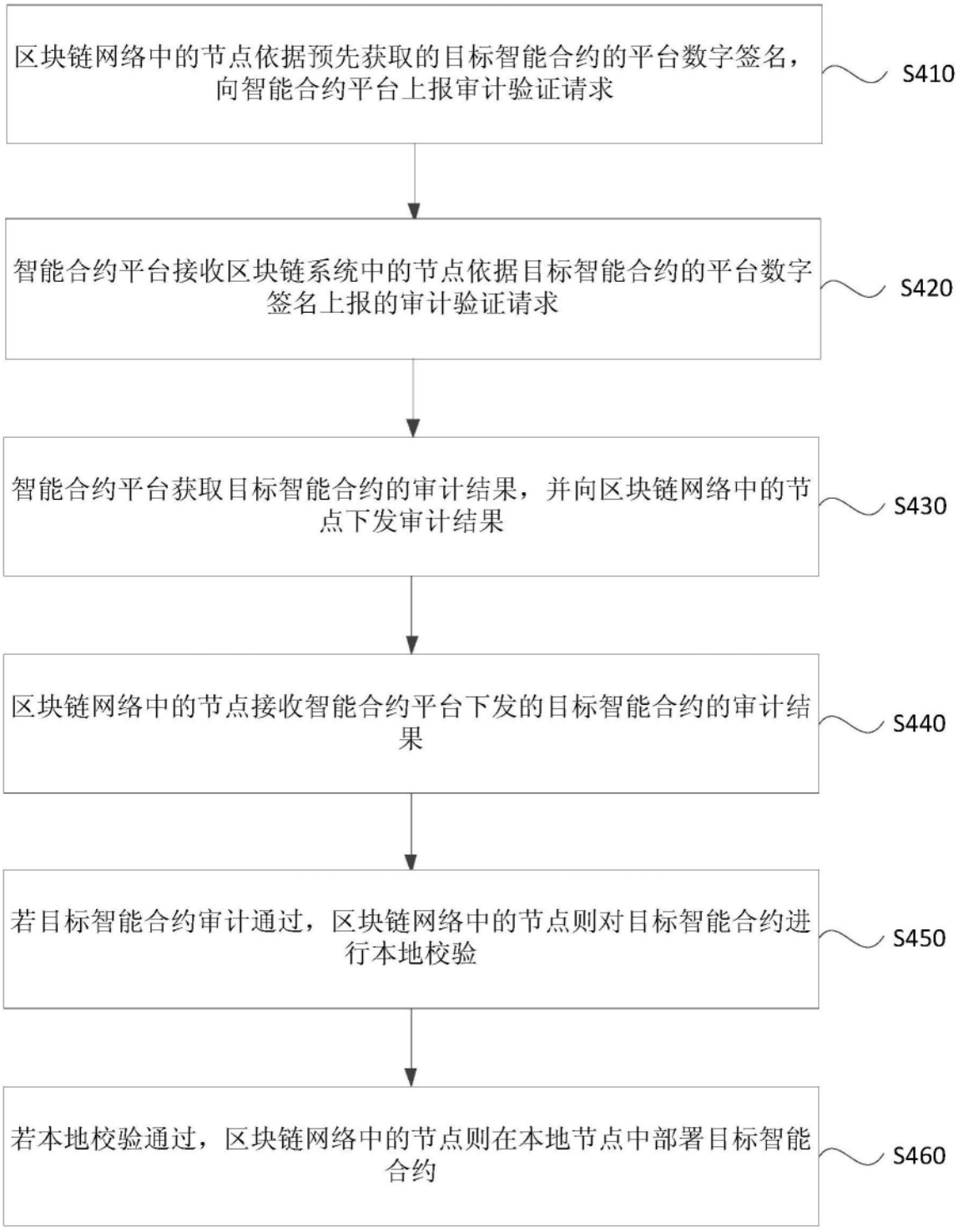

区块链网络中的节点依据预先获取的目标智能合约的平台数字签名，向智能合约平台上报审计验证请求
S410
智能合约平台接收区块链系统中的节点依据目标智能合约的平台数字签名上报的审计验证请求
S420
智能合约平台获取目标智能合约的审计结果，并向区块链网络中的节点下发审计结果
S430
区块链网络中的节点接收智能合约平台下发的目标智能合约的审计结果
S440
若目标智能合约审计通过，区块链网络中的节点则对目标智能合约进行本地校验
S450
若本地校验通过，区块链网络中的节点则在本地节点中部署目标智能合约
S460

图4

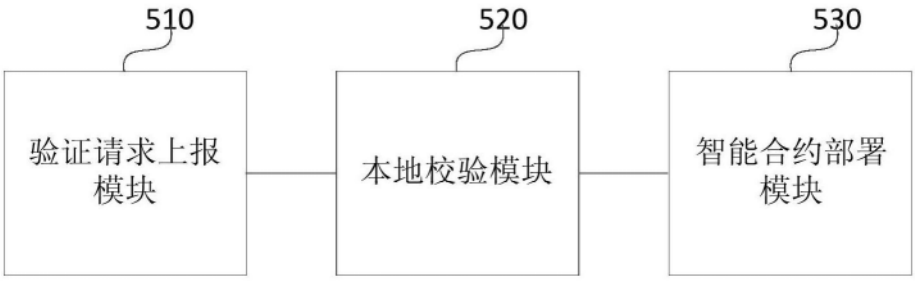

510
520
530
验证请求上报模块
本地校验模块
智能合约部署模块

图5


610
620
验证请求接收模块
审计结果下发模块

图6

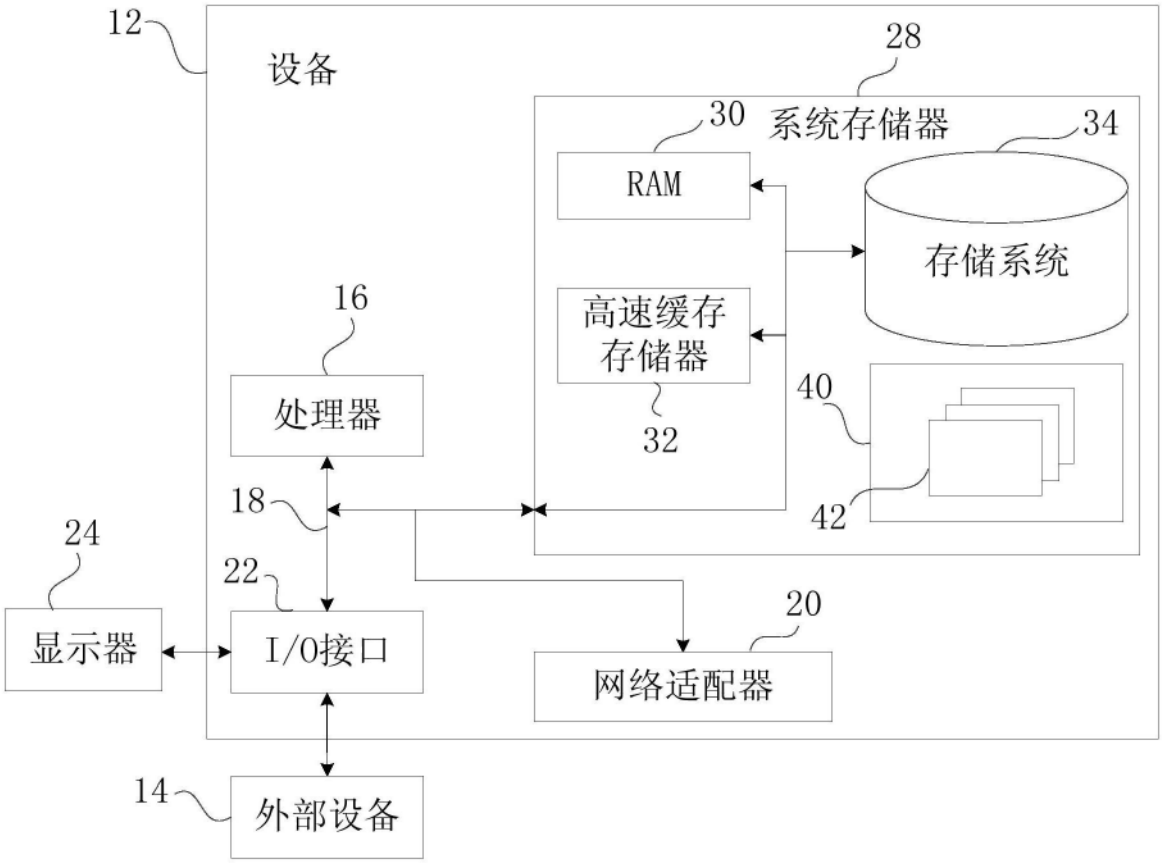

12
设备
28
30
系统存储器
34
RAM
存储系统
16
高速缓存
存储器
32
处理器
40
42
18
24
22
20
显示器
I/O接口
网络适配器
14
外部设备

图7