(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109003078 B
(45)授权公告日 2021.08.24

(21)申请号 201810681249.1
(22)申请日 2018.06.27
(65)同一申请的已公布的文献号
申请公布号 CN 109003078 A
(43)申请公布日 2018.12.14
(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心
(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.
G06Q 20/38(2012.01)
G06F 21/62(2013.01)

审查员 李慧

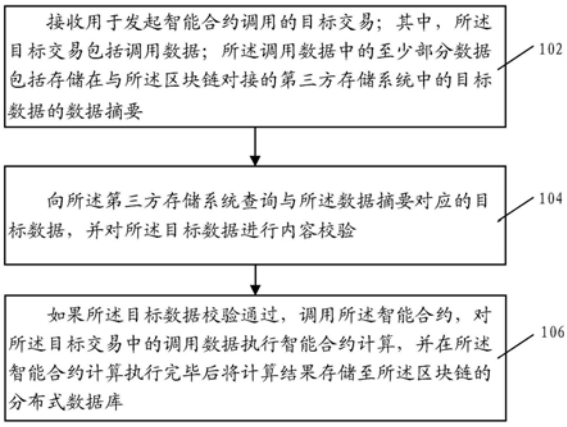
权利要求书2页 说明书13页 附图3页

(54)发明名称

基于区块链的智能合约调用方法及装置、电子设备

(57)摘要

本说明书一个或多个实施例提供一种基于区块链的智能合约调用方法及装置、电子设备，该方法可以包括：接收用于发起智能合约调用的目标交易；其中，所述目标交易包括调用数据；所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要；向所述第三方存储系统查询与所述数据摘要对应的目标数据，并对所述目标数据进行内容校验；如果所述目标数据校验通过，调用所述智能合约，对所述目标交易中的调用数据执行智能合约计算，并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。



CN 109003078 B

1.一种基于区块链的智能合约调用方法,包括:

接收用于发起智能合约调用的目标交易;其中,所述目标交易包括调用数据;所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要;

调用所述智能合约,由所述智能合约向所述第三方存储系统查询与所述数据摘要对应的目标数据,并对所述目标数据进行内容校验;

如果所述目标数据校验通过,由所述智能合约进一步对所述目标交易中的调用数据执行智能合约计算,并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。

2.根据权利要求1所述的方法,所述第三方存储系统中存储了所述目标数据与所述目标数据的数据摘要之间的对应关系;

所述向所述第三方存储系统查询与所述数据摘要对应的目标数据,包括:

将所述数据摘要作为查询索引向所述第三方存储系统发起查询,以查询与所述数据摘要对应的目标数据。

3.根据权利要求1所述的方法,所述对所述目标数据进行内容校验,包括:

基于预设的摘要算法计算所述目标数据的数据摘要;

确定计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要是否一致;

如果计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要一致,确定针对所述目标数据的校验通过。

4.根据权利要求1所述的方法,所述第三方存储系统包括中心化的内容可寻址存储CAS系统;或者,分布式的CAS存储系统。

5.根据权利要求1所述的方法,所述区块链为由若干成员区块链组成的联盟链中的任一成员区块链。

6.根据权利要求5所述的方法,所述第三方存储系统为所述联盟链中与所述区块链存在数据跨链引用关系的其它成员区块链。

7.一种基于区块链的智能合约调用装置,包括:

接收模块,接收用于发起智能合约调用的目标交易;其中,所述目标交易包括调用数据;所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要;

查询模块,调用所述智能合约,由所述智能合约向所述第三方存储系统查询与所述数据摘要对应的目标数据,并对所述目标数据进行内容校验;

调用模块,如果所述目标数据校验通过,由所述智能合约进一步对所述目标交易中的调用数据执行智能合约计算,并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。

8.根据权利要求7所述的装置,所述第三方存储系统中存储了所述目标数据与所述目标数据的数据摘要之间的对应关系;

所述查询模块:

将所述数据摘要作为查询索引向所述第三方存储系统发起查询,以查询与所述数据摘要对应的目标数据。

9.根据权利要求7所述的装置,所述查询模块进一步:

基于预设的摘要算法计算所述目标数据的数据摘要;

确定计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要是否一致;

如果计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要一致,确定针对所述目标数据的校验通过。

10.根据权利要求7所述的装置,所述第三方存储系统包括中心化的内容可寻址存储CAS系统;或者,分布式的CAS存储系统。

11.根据权利要求7所述的装置,所述区块链为由若干成员区块链组成的联盟链中的任一成员区块链。

12.根据权利要求11所述的装置,所述第三方存储系统为所述联盟链中与所述区块链存在数据跨链引用关系的其它成员区块链。

13.一种电子设备,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基于区块链的智能合约调用的控制逻辑对应的机器可执行指令,所述处理器被促使:

接收用于发起智能合约调用的目标交易;其中,所述目标交易包括调用数据;所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要;

调用所述智能合约,由所述智能合约向所述第三方存储系统查询与所述数据摘要对应的目标数据,并对所述目标数据进行内容校验;

如果所述目标数据校验通过,由所述智能合约进一步对所述目标交易中的调用数据执行智能合约计算,并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。

基于区块链的智能合约调用方法及装置、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，尤其涉及一种基于区块链的智能合约调用方法及装置、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，使得区块链技术已在众多的领域中广泛的进行应用。

发明内容

[0003] 本说明书提出一种基于区块链的智能合约调用方法，包括：

[0004] 接收用于发起智能合约调用的目标交易；其中，所述目标交易包括调用数据；所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要；

[0005] 向所述第三方存储系统查询与所述数据摘要对应的目标数据，并对所述目标数据进行内容校验；

[0006] 如果所述目标数据校验通过，调用所述智能合约，对所述目标交易中的调用数据执行智能合约计算，并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。

[0007] 可选的，所述第三方存储系统中存储了所述目标数据与所述目标数据的数据摘要之间的对应关系；

[0008] 所述向所述第三方存储系统查询与所述数据摘要对应的目标数据，包括：

[0009] 将所述数据摘要作为查询索引向所述第三方存储系统发起查询，以查询与所述数据摘要对应的目标数据。

[0010] 可选的，所述对所述目标数据进行内容校验，包括：

[0011] 基于预设的摘要算法计算所述目标数据的数据摘要；

[0012] 确定计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要是否一致；

[0013] 如果计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要一致，确定针对所述目标数据的校验通过。

[0014] 可选的，所述第三方存储系统包括中心化的内容可寻址存储CAS系统；或者，分布式的CAS存储系统。

[0015] 可选的，所述区块链为由若干成员区块链组成的联盟链中的任一成员区块链。

[0016] 可选的，所述第三方存储系统为所述联盟链中与所述区块链存在数据跨链引用关系的其它成员区块链。

[0017] 本说明书还提出一种基于区块链的智能合约调用装置，包括：

[0018] 接收模块，接收用于发起智能合约调用的目标交易；其中，所述目标交易包括调用数据；所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要；

[0019] 查询模块，向所述第三方存储系统查询与所述数据摘要对应的目标数据，并对所述目标数据进行内容校验；

[0020] 调用模块，如果所述目标数据校验通过，调用所述智能合约，对所述目标交易中的调用数据执行智能合约计算，并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。

[0021] 可选的，所述第三方存储系统中存储了所述目标数据与所述目标数据的数据摘要之间的对应关系；

[0022] 所述查询模块：

[0023] 将所述数据摘要作为查询索引向所述第三方存储系统发起查询，以查询与所述数据摘要对应的目标数据。

[0024] 可选的，所述查询模块进一步：

[0025] 基于预设的摘要算法计算所述目标数据的数据摘要；

[0026] 确定计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要是否一致；

[0027] 如果计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要一致，确定针对所述目标数据的校验通过。

[0028] 可选的，所述第三方存储系统包括中心化的内容可寻址存储CAS系统；或者，分布式的CAS存储系统。

[0029] 可选的，所述区块链为由若干成员区块链组成的联盟链中的任一成员区块链。

[0030] 可选的，所述第三方存储系统为所述联盟链中与所述区块链存在数据跨链引用关系的其它成员区块链。

[0031] 本说明书还提出一种电子设备，包括：

[0032] 处理器；

[0033] 用于存储机器可执行指令的存储器；

[0034] 其中，通过读取并执行所述存储器存储的与基于区块链的基于区块链的智能合约调用的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0035] 接收用于发起智能合约调用的目标交易；其中，所述目标交易包括调用数据；所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要；

[0036] 向所述第三方存储系统查询与所述数据摘要对应的目标数据，并对所述目标数据进行内容校验；

[0037] 如果所述目标数据校验通过，调用所述智能合约，对所述目标交易中的调用数据执行智能合约计算，并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。

[0038] 通过以上实施例，通过在用于发起智能合约调用的交易中携带存储在第三方存储

系统中的目标数据的数据摘要，使得区块链中接收到该交易的节点设备，可以基于该数据摘要向第三方存储系统查询对应的目标数据，对目标数据进行内容校验，并在该目标数据校验通过后，调用智能合约，对该交易中的调用数据执行智能合约计算，以及在智能合约计算执行完毕后将计算结果存储至区块链的分布式数据库，从而实现了可以在用于发起智能合约调用的交易中，引用与区块链对接的第三方存储系统中存储的目标数据作为调用数据，可以避免将上述第三方存储系统中存储的目标数据的原始内容同步至区块链中的各节点设备，而造成的在区块链上的数据冗余存储。

附图说明

[0039] 图1是一示例性实施例提供的一种基于区块链的智能合约调用方法的流程图。

[0040] 图2是一示例性实施例提供的一种联盟链的结构示意图。

[0041] 图3是一示例性实施例提供的一种电子设备的结构示意图。

[0042] 图4是一示例性实施例提供的一种基于区块链的智能合约调用装置的框图。

具体实施方式

[0043] 在传统的区块链的智能合约调用流程中，在调用智能合约时所需的调用数据(即输入给智能合约的调用参数)，通常全部来自于区块链的分布式数据库(即区块链账本)上存储的数据内容，并不能引用外部存储中存储的数据内容；因此，对于区块链网络中的各节点设备而言，在调用智能合约时参与智能合约计算的调用数据，通常全部来自于链上，进而形成了一种“数据使用闭环”。

[0044] 而本说明书中则旨在公开一种，在调用智能合约时引用第三方存储平台中存储的不可变数据内容作为交易内容，来打破区块链的“数据使用闭环”的技术方案。

[0045] 在实现时，区块链可以预先与第三方存储系统对接，在第三方存储系统中可以预先存储若干可供在区块链上部署的智能合约引用的不可变数据内容。

[0046] 而接入区块链的成员用户在发起智能合约调用时，可以在用于发起智能合约调用的交易中添加上述第三方存储系统中存储的数据内容的数据摘要，来引用上述第三方存储系统中存储的数据内容作为调用数据。

[0047] 当区块链上的节点设备收到上述成员用户发布的交易时，可以基于该数据摘要向上述第三方存储系统发起查询，来查询与该数据摘要对应的数据内容，并对查询到的数据内容进行内容校验；当内容校验通过，可以调用智能合约，声明智能合约中声明的智能合约程序，对该交易中的完整调用数据执行智能合约计算，并在智能合约计算执行完毕后将计算结果存储至区块链的分布式数据库。

[0048] 在以上实施例中，通过在用于发起智能合约调用的交易中携带存储在第三方存储系统中的目标数据的数据摘要，使得区块链中接收到该交易的节点设备，可以基于该数据摘要向第三方存储系统查询对应的目标数据，对目标数据进行内容校验，并在该目标数据校验通过后，调用智能合约，对该交易中的调用数据执行智能合约计算，以及在智能合约计算执行完毕后将计算结果存储至区块链的分布式数据库，从而实现了可以在用于发起智能合约调用的交易中，引用与区块链对接的第三方存储系统中存储的目标数据作为调用数据，可以避免将上述第三方存储系统中存储的目标数据的原始内容同步至区块链中的各节

点设备，而造成的在区块链上的数据冗余存储。

[0049] 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。

[0050] 请参考图1，图1是本说明书一实施例提供的一种基于区块链的智能合约调用方法，应用于区块链中的节点设备，执行以下步骤：

[0051] 步骤102，接收用于发起智能合约调用的目标交易；其中，所述目标交易包括调用数据；所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要；

[0052] 步骤104，向所述第三方存储系统查询与所述数据摘要对应的目标数据，并对所述目标数据进行内容校验；

[0053] 步骤106，如果所述目标数据校验通过，调用所述智能合约，对所述目标交易中的调用数据执行智能合约计算，并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。

[0054] 在本说明书描述的区块链，具体可以包括所支持的智能合约，可以引用与区块链对接的第三方存储系统中存储的不可变数据内容作为调用数据的任意类型的区块链网络。

[0055] 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，各个成员区块链中支持的智能合约，均可以跨链引用其它成员区块链中存储的数据内容作为调用数据。

[0056] 上述第三方存储系统，包括面向区块链提供可靠的数据存储服务的CAS(content-addressable-storage，内容可寻址存储)存储平台。所谓内容可寻址，是指不再采用数据在存储系统中的存储偏移量进行寻址，而是依靠数据的内容来进行寻址。

[0057] 在CAS存储平台中，可以将存储的数据内容的数据摘要，作为原始的数据内容的查询索引，并保存查询索引与原始的数据内容之间的对应关系，从而数据查询方可以通过将数据摘要作为查询索引，从CAS存储平台中查询对应的原始数据内容。

[0058] 例如，在一种实施方式中，上述数据摘要具体可以是针对数据内容进行hash计算得到的hash值；数据查询方可以将hash值作为查询索引，从CAS存储平台中查询与hash值对应的原始数据内容。

[0059] 其中，在实际应用中，上述第三方存储系统可以包括传统的中心化的CAS(content-addressable-storage，内容可寻址存储)系统；或者，也可以包括去中心化的分布式的CAS系统；

[0060] 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。而上述第三方存储系统，具体可以是部署在联盟链中的，可以与联盟链中的各成员区块链对接的诸如基于OSS(Object Storage Service，对象存储服务)架构的分布式系统。

[0061] 或者，在另一个例子中，也可以将上述联盟链中的除了上述区块链以外的与该区块链存在数据跨链引用关系的其它成员区块链，作为与该区块链对接的第三方存储系统，来实现各成员区块链之间的数据跨链引用。也即，上述第三方存储系统具体可以是一个与上述区块链存在跨链引用关系的其它区块链。以下以上述区块链为由若干成员区块链组成的联盟链中的成员区块链为例，并结合“第三方存储系统部署”、“调用数据引用”、以及“智能合约调用执行”几部分，对本说明书的技术方案进行详细说明。

[0062] 1)第三方存储系统部署

[0063] 在本说明书中,运营方可以预先搭建一个由若干成员区块链构成的联盟链。在该联盟链中,每一个成员区块链都是该联盟链中的一个联盟成员。而上述区块链具体可以是该联盟链中的任一成员区块链。

[0064] 联盟链的运营方,还可以在联盟链中部署第三方存储系统,与联盟链中的各个成员区块链进行对接,面向各成员区块链提供可靠的数据存储服务。

[0065] 例如,上述第三方存储系统可以面向各成员区块链提供持续可靠的API访问接口,使得联盟链中的各个成员区块链可以通过访问该API访问接口,与上述第三方存储系统进行对接。

[0066] 其中,在联盟链中部署第三方存储系统时,可以针对联盟链部署一个全局的第三方存储系统,也可以针对联盟链中的各成员区块链分别部署一个独立的第三方存储系统,在本说明书中不进行特别限定。

[0067] 在本说明书中,上述第三方存储系统,可以是支持内容可寻址的CAS存储系统。在实际应用中,上述第三方存储系统可以是传统的中心化的CAS系统,也可以是分布式的CAS系统。

[0068] 其中,上述分布式的CAS系统,可以包括传统的中心化的分布式系统,以及去中心化的分布式系统。

[0069] 在示出的一种实施方式中,上述第三方存储系统,具体可以是部署在联盟链中的,可以与联盟链中的各成员区块链对接的诸如基于OSS架构的中心化的分布式系统。

[0070] 在示出的另一种实施方式中,上述第三方存储系统,也可以是去中心化的分布式系统。在实现时,可以将上述联盟链中除了上述区块链以外的与该区块链存在数据跨链引用关系的其它成员区块链,作为与该区块链对接的第三方存储系统。即联盟链中的任一成员区块链可以作为与另一成员区块链对接的第三方存储系统,来实现数据的跨链引用。

[0071] 举例而言,在一种场景下,运营方可以基于实际的业务需求来搭建联盟链,并赋予联盟链中的各成员区块链不同的业务角色;即联盟链对应一个完整的业务流程,而各成员区块链可以分别对应上述完成的业务流程中的一个子流程。

[0072] 例如,在一个例子中,以运营方基于“在线租房交易”这一业务需求搭建的联盟链为例,组成该联盟链中的各成员区块链中可以包括“交易链”、“认证链”以及“数据链”。其中,“交易链”、“认证链”以及“数据链”可以分别对应“在线租房交易”这一业务流程中的一个子流程;比如,“数据链”用于维护租房用户的实名数据;“认证链”用于完成针对用户的租房实名认证;而“交易链”用于完成在线的租房交易。

[0073] 然后,运营方可以基于各成员区块链之间的单向的数据跨链引用关系,在业务层面将联盟链构建成一张DAG(Directed Acyclic Graph,有向无环图)结构的拓扑图。

[0074] 其中,需要说明的是,各成员区块链之间的单向的数据跨链引用关系,通常取决于实际的业务需求,在本说明书中不进行特别限定。

[0075] 例如,请参见图2,图2为一个例子中示出的DAG结构的联盟链的示意图。

[0076] 如图2所示,仍以运营方基于“在线租房”这一业务需求搭建的联盟链为例,组成该联盟链中的各成员区块链中可以包括“交易链”、“认证链”以及“数据链”。其中,“数据链”用于维护租房用户的实名数据,用户可以通过在“数据链”上发布交易将个人的实名数据存储

在“数据链”的分布式数据库中;“认证链”用于引用发布在“数据链”上的用户的实名数据完成针对用户的租房实名认证,用户可以通过在“认证链”上发布交易完成个人的实名认证,并将实名认证结果发布在“认证链”的分布式数据库;而“交易链”用于引用发布在“认证链”上的针对用户的实名认证结果,用户可以通过在“交易链”上发布交易完成在线租房交易,并将交易结果发布在“认证链”的分布式数据库。

[0077] 通过将与上述联盟链中的任一目标成员区块链存在数据跨链引用关系的其它成员区块链,作为与该目标成员区块链对接的分布式存储平台:

[0078] 一方面可以在业务层面实现各个成员区块链之间的跨链数据引用;

[0079] 另一方面,由于作为第三方存储系统的成员区块链在调用执行部署的智能合约时,如果参与智能合约计算的调用数据引用了第三方存储系统中存储的目标数据,则不再需要将上述被引用的目标数据的原始内容,同步至上述目标成员区块链中的各个节点设备,而且上述目标成员区块链中也不再需要存储上述被引用的目标数据的原始内容;

[0080] 因此,对于上述目标成员区块链而言,不再需要对该目标成员区块链中存储的目标数据的原始内容,与作为第三方存储系统的成员区块链同步的被引用的目标数据进行额外的数据关联,仅通过被引用的目标数据的数据摘要,就可以实现被引用的目标数据在两个不同的区块链上的数据关联,可以保证上述目标成员区块链上部署的智能合约所引用的目标数据和作为第三方存储系统的成员区块链上存储的上述被引用的目标数据,在业务语义上的一致性。

[0081] 2)调用数据引用

[0082] 在本说明书中,对于需要接入联盟链的用户,可以预先在联盟链中进行用户注册,取得联盟链返回的一对公钥和私钥。当注册完成后,联盟链可以为用户创建一个对应的账户对象。

[0083] 而对于注册完成的用户而言,可以通过联盟链中各个成员区块链提供的API接口,接入各个成员区块链,通过向各个成员区块链中发布基于持有的私钥签名后的交易,调用在各个成员区块链中部署的智能合约。

[0084] 比如,以图2中示出的联盟链中的“交易链”为例,联盟链的运营方可以在该“交易链”中发布用于完成在线租房核算的智能合约,而用户可以通过在该“交易链”中发布交易,来触发调用上述智能合约,来完成在线的租房交易的核算。

[0085] 其中,联盟链的运营方在联盟链上部署智能合约的具体过程,在本说明书中不再进行详细描述,本领域技术人员在将本说明书记载的技术方案付诸实践时,可以参考相关技术中的记载。

[0086] 例如,接入联盟链的多方成员可以共同协商一份智能合约,在智能合约中声明开发完成的智能合约程序(比如可以是一些可调用的函数相关的程序代码),然后将智能合约在联盟链中进行发布,由联盟链中的节点设备进行共识处理;当共识通过后,可以将上述智能合约收录存储至联盟链的分布式数据库,以完成智能合约的部署。

[0087] 在本说明书中,联盟链的运营方可以面向接入联盟链的成员用户开发客户端软件(比如APP),而成员用户可以通过客户端软件按照联盟链所支持的标准的交易格式,来组装交易数据,并通过调用各个成员区块链提供的API接口,将组成的交易数据发布至联盟链中由成员用户指定的目标成员区块链中,来发起对该目标成员区块链中部署的智能合约进行

调用。

[0088] 其中，在成员用户通过客户端软件组装的交易数据中，可以携带成员用户提供的调用数据，这些调用数据将作为输入给智能合约的调用参数。而在这些调用数据中，其中的至少部分调用数据，可以利用数据摘要来进行替代。

[0089] 在示出的一种实施方式中，成员用户在通过客户端软件来组装需要在上述目标成员区块链上执行的交易数据时，可以通过客户端软件来填写该交易中需要携带的调用数据；而客户端软件可以解析成员用户填写的调用数据，来确定成员用户填写的调用数据中是否存在，已经在与上述目标成员区块链对接的第三方存储系统中存储的数据。也即，确定成员用户填写的调用数据是否引用了第三方存储系统中存储的数据。

[0090] 如果成员用户填写的调用数据中存在已经在上述第三方存储系统中存储的数据时，可以向上述第三方存储系统查询这部分调用数据对应的数据摘要(即查询索引)，或者按照与上述第三方存储系统所支持的相同的数据摘要算法，针对这部分交易内容重新计算数据摘要，然后将该数据摘要填充到标准的交易格式中；

[0091] 例如，在实现时，可以在联盟链支持的标准的交易格式中，扩展出一个用于携带调用数据的数据摘要字段，客户端软件按照标准的交易格式组装交易数据时，可以将所有已经在上述第三方存储系统中存储的被引用数据的数据摘要，填充至该数据摘要字段。

[0092] 3)智能合约的调用执行

[0093] 在本说明书中，上述目标成员区块链中的节点设备，在收到上述成员用户基于私钥发布的该笔交易后，首先可以基于该用户持有的私钥对应的公钥对该用户进行身份认证；

[0094] 例如，在实际应用中，用户可以基于持有的私钥对发起的交易进行签名，区块链中的节点设备可以基于该用户持有的私钥对应的公钥，对签名进行认证；如果签名认证通过，此时针对该用户的身份认证通过。

[0095] 当身份认证通过后，该节点设备可以在上述目标成员区块链中发起对该笔交易进行共识处理，并在共识通过后，将该笔交易收录存储至该目标成员区块链的分布式数据库。一旦该笔交易被成功收录存储至上述目标成员区块链的分布式数据库，后续就可以基于收录至分布式数据库的该笔交易，来触发调用智能合约，执行该智能合约中声明的智能合约程序。

[0096] 例如，在实现时，在智能合约中的智能合约程序，通常会被预设严格的触发执行条件。而智能合约定期检查当前收录在分布式数据库中的交易，是否满足了上述执行条件，并将分布式数据中存储的满足了上述执行条件的交易加入到一个待验证的交易队列中，对该交易队列中的交易进行共识处理；如果共识通过，可以触发执行该智能合约中声明的智能合约程序。

[0097] 其中，需要说明的是，上述目标成员区块链中对交易进行共识处理时，所采用的共识算法，在本说明书中不进行特别限定，各个成员区块链支持的共识算法可以相同，也可以不同。例如，对于联盟链可以采用诸如PBFT等主流的共识算法，或者也可以由联盟链自主研发的共识算法。

[0098] 在本说明书中，基于上述交易来触发调用智能合约，执行该智能合约中声明的智能合约程序时，首先智能合约可以对上述交易中所携带的调用数据进行解析，以确定该交

易中携带的调用数据中是否存在数据摘要；

[0099] 例如，节点设备可以通过解析标准的交易格式中所扩展出的，用于携带交易内容的数据摘要字段是否为空值，来确定该交易中携带的交易内容中是否存在数据摘要。

[0100] 如果该交易中携带的调用数据中存在数据摘要，表明该交易中的部分调用数据，引用了上述第三方存储系统中已经存储的数据内容，在这种情况下，为了获取该交易中携带的完整的调用数据，智能合约可以向与上述目标成员区块链对接的第三方存储系统查询与该数据摘要对应的目标数据。

[0101] 在实现时，该智能合约可以构建一个查询请求，将上述数据摘要作为查询索引，携带在该查询请求中，然后将该查询请求提交给上述第三方存储系统，而上述第三方存储系统在收到该查询请求后，可以从该查询请求中读取查询索引，然后基于该查询索引，遍历本地存储的数据内容和数据摘要之间的对应关系，来查询与上述查询索引对应的目标数据，并将查询到的目标数据返回给上述智能合约。

[0102] 其中，需要说明的是，由于上述第三方存储系统，可以是与上述目标成员区块链存储跨链引用关系的其它成员区块链，因此在这种场景下，上述智能合约构建的查询请求，可以向该作为第三方存储系统的其它成员区块链中的节点设备进行广播发送。

[0103] 而在实际应用中，由于其它成员区块链中所采用的共识算法上的差异，可能会导致上述智能合约向上述其它成员区块链中的各节点设备分别发送查询请求后，可能会得到具有差异的查询结果。

[0104] 例如，区块链中所采用的共识算法，通常可以按照是否能达到分布式一致，划分为两类；其中，所谓分布式一致，是指通过共识算法的共识后，区块链中的各个节点设备上保存的数据完全相同。

[0105] 一类是，可以确保各节点设备能够达到分布式一致的共识算法；比如，pbft共识算法，由于采用容错机制来达成共识，因此可以确保各节点设备在共识完成后保存的数据完全相同；

[0106] 另一类是，无法确保各节点设备能够达到分布式一致的共识算法；比如，诸如pos或者pow共识算法，由于采用了竞争记账机制来达成共识，因此无法确保各节点设备在共识完成后保存的数据完成相同；比如，以pow共识算法为例，通过工作量计算取得记账权限的节点设备，可以只保存由该节点设备提议的区块的数据，造成各个节点设备本地存储的区块数据可能会存在差异。

[0107] 因此，一旦上述作为第三方存储系统的其它成员区块链采用的共识算法为以上示出的第二类共识算法，就可能出现上述智能合约在向上述其它成员区块链中的各节点设备分别发送查询请求后，可能会出现部分的节点设备在本地未查找到相关的数据，而其它的节点设备在其本地查找到了相关的数据的情况。

[0108] 在一种场景下，如果作为上述作为第三方存储系统的其它成员区块链采用的共识算法为以上示出的第一类共识算法，上述智能合约可以通过一个也支持这类共识算法的查询客户端，向上述其它成员区块链进行数据查询，来取得一致性的查询结果；

[0109] 例如，以pbft共识算法为例，假设上述作为第三方存储系统的其它成员区块链中的节点设备的数量为3f+1，上述智能合约在通过上述查询客户端将查询请求分别发送至上述其它成员区块链中的节点设备之后，如果收到了其中f+1个节点设备返回了相同的查询

结果，即可以认为该查询结果为最终的查询结果。

[0110] 在一种场景下，如果作为上述作为第三方存储系统的其它成员区块链采用的共识算法为以上示出的第二类共识算法，则需要在上述其它成员区块链上指定一个稳定可靠的节点设备作为查询节点，上述智能合约可以将查询请求发送给该查询节点，从该查询节点本地保存的数据中来查找相关的数据。

[0111] 也即，在这种场景下，可以认为该查询节点本地保存的数据，为面向数据引用方的一致性结果，只有该查询节点本地保存的数据，可以作为被部署在其它成员区块链上的智能合约进行引用。

[0112] 其中，需要说明的是，在实际应用中，在上述查询请求中除了可以携带作为查询索引的数据摘要以外，为了便于快速的查询到与数据摘要对应的目标数据，在该查询请求中还可以携带一些辅助查询参数；

[0113] 例如，以与上述目标成员区块链对接的第三方存储系统，为上述联盟链中与该目标成员区块链存储数据跨链引用关系的其它成员区块链为例，由于作为第三方存储系统的其它成员区块链中所保存的被引用的数据内容以及对应的数据摘要，通常已经以区块的形式被存储在区块链的分布式数据库中；因此，为了方便查询，在上述查询请求中，还可以携带上述数据摘要所在的成员区块链的编号、区块号等等作为辅助查询参数。

[0114] 在本说明书中，当上述智能合约从与上述目标成员区块链对接的第三方存储系统查询到与接收到的交易中所携带的数据摘要对应的目标数据后，可以发起调用上述智能合约，执行该智能合约中声明的智能合约程序，对该交易中所携带的完整的调用数据，进行智能合约计算。

[0115] 首先，上述智能合约可以针对查询到的该目标数据进行内容校验，以确保查询到的目标数据，与上述交易中携带的数据摘要对应的数据内容是否一致。

[0116] 在实现时，上述智能合约可以重新计算查询到的该目标数据的数据摘要，然后将重新计算得到的数据摘要，与接收到的上述交易中携带的数据摘要进行匹配，以确定重新计算得到的数据摘要，与接收到的上述交易中携带的数据摘要是否一致；

[0117] 如果二者一致，此时针对查询到的该目标数据的内容校验通过，该交易为有效交易，智能合约可以获取该交易中携带的完整的调用数据，然后将该完成的调用参数作为上述智能合约中声明的智能合约程序的输入参数，输入至上述智能合约程序中进行智能合约计算

[0118] 反之，如果二者不一致，此时针对查询到的该目标数据的内容校验不通过，在这种情况下，存储在上述第三方存储系统中的原始的被引用的目标数据，可能由于系统的不可靠性发生了修改更新，此时该交易为无效交易，此时可以直接终止针对上述智能合约的调用过程。

[0119] 其中，需要说明的是，上述智能合约重新计算查询到的该目标数据的数据摘要时，该目标数据的数据结构、对该目标数据执行的编码方式、以及所采用的摘要算法，均需要与上述第三方存储系统保持一致，以确保该节点设备和上述第三方存储系统在针对相同的目标数据进行数据摘要计算时，能够得到相同的计算结果。

[0120] 在本说明书中，当智能合约将上述交易中携带的完整的调用数据作为输入参数，输入至上述智能合约中声明的智能合约程序中完成智能合约计算之后，此时该笔交易执行

完毕,可以进一步将该智能合约计算的计算结果(即该笔交易的执行结果),在该目标成员区块链的分布式数据库中进行存储。

[0121] 其中,区块链的分布式数据库所记录的信息通常包括交易log以及交易state组成。

[0122] 交易log,用于存储交易日志,由一个个区块(block)按照发生顺序串联而成,是分布式数据库中的交易记录;上述交易在共识通过后,可以收录存储至交易log中相应的区块中。

[0123] 交易state,用于存储分布式数据库中记录的交易在执行完毕后所导致的状态变化;例如,区块链通常由很多小的对象组成(比如账户对象、合约对象以及资产对象等等),每在区块链的分布式数据库中收录一笔交易,该笔交易在执行完毕后,与该交易相关的状态都会同步的发生更新;比如,以在区块链中提交的在线转账交易为例,该笔交易通过调用相关的智能合约执行完毕后,与本次转账相关的账户对象的余额会同步的发生更新。

[0124] 在这种情况下,当上述智能合约完成针对上述交易中携带的完整的调用数据的智能合约计算后,可以进一步将上述智能合约计算的计算结果,在上述交易state中进行存储,对该笔交易所导致的相关对象的状态变化进行更新;比如,仍以在区块链中提交的在线转账交易为例,当上述智能合约完成针对上述交易中携带的完整的调用数据的智能合约计算后,可以在交易state中对与本次转账相关的账户对象的余额进行更新。

[0125] 在以上实施例中,通过在用于发起智能合约调用的交易中携带存储在第三方存储系统中的目标数据的数据摘要,使得区块链中接收到该交易的节点设备,可以基于该数据摘要向第三方存储系统查询对应的目标数据,对目标数据进行内容校验,并在该目标数据校验通过后,调用智能合约,对该交易中的调用数据执行智能合约计算,以及在智能合约计算执行完毕后将计算结果存储至区块链的分布式数据库,从而实现了可以在用于发起智能合约调用的交易中,引用与区块链对接的第三方存储系统中存储的目标数据作为调用数据,可以避免将上述第三方存储系统中存储的目标数据的原始内容同步至区块链中的各节点设备,而造成的在区块链上的数据冗余存储。

[0126] 例如,以与目标区块链对接的第三方存储系统为与该区块链存在数据跨链引用关系的其它区块链为例,假设该其它区块链包括5个节点设备,而该目标区块链包括50个节点设备;如果仍然采用将该其它区块链中存储的被引用数据内容同步至该目标区块链的方式,则需要将该被引用数据内容同步分别同步至该目标区块链中的50个节点,从而造成该被引用数据内容在该目标区块链中的大量冗余;而如果该目标区块链仅存储上述被引用数据内容的数据摘要,那么对于上述其它区块链而言,则不再需要将上述被引用数据内容分别向上述50个节点设备分别进行同步,从而可以显著降低上述目标区块链的数据存储冗余。

[0127] 与上述方法实施例相对应,本说明书还提供了一种基于区块链的智能合约调用装置的实施例。本说明书的基于区块链的智能合约调用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3所示,为本说明书的基于区块链的智能合约调用装置所在电子设备的一种硬件结构图,除了图3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。

[0128] 图4是本说明书一示例性实施例示出的一种基于区块链的智能合约调用装置的框图。

[0129] 请参考图4，所述基于区块链的智能合约调用装置30可以应用在前述图2所示的电子设备中，包括有：接收模块401、查询模块402和调用模块403。

[0130] 接收模块401，接收用于发起智能合约调用的目标交易；其中，所述目标交易包括调用数据；所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要；

[0131] 查询模块402，向所述第三方存储系统查询与所述数据摘要对应的目标数据，并对所述目标数据进行内容校验；

[0132] 调用模块403，如果所述目标数据校验通过，调用所述智能合约，对所述目标交易中的调用数据执行智能合约计算，并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。

[0133] 在本实施例中，所述第三方存储系统中存储了所述目标数据与所述目标数据的数据摘要之间的对应关系；

[0134] 所述查询模块402：

[0135] 将所述数据摘要作为查询索引向所述第三方存储系统发起查询，以查询与所述数据摘要对应的目标数据。

[0136] 在本实施例中，所述查询模块402进一步：

[0137] 基于预设的摘要算法计算所述目标数据的数据摘要；

[0138] 确定计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要是否一致；

[0139] 如果计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要一致，确定针对所述目标数据的校验通过。

[0140] 在本实施例中，所述第三方存储系统包括中心化的内容可寻址存储CAS系统；或者，分布式的CAS存储系统。

[0141] 在本实施例中，所述区块链为由若干成员区块链组成的联盟链中的任一成员区块链。

[0142] 在本实施例中，所述第三方存储系统为所述联盟链中与所述区块链存在数据跨链引用关系的其它成员区块链。

[0143] 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。

[0144] 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。

[0145] 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。

[0146] 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。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。

[0147] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的智能合约调用的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0148] 接收用于发起智能合约调用的目标交易；其中，所述目标交易包括调用数据；所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要；

[0149] 向所述第三方存储系统查询与所述数据摘要对应的目标数据，并对所述目标数据进行内容校验；

[0150] 如果所述目标数据校验通过，调用所述智能合约，对所述目标交易中的调用数据执行智能合约计算，并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库。

[0151] 在本实施例中，所述第三方存储系统中存储了所述目标数据与所述目标数据的数据摘要之间的对应关系；

[0152] 通过读取并执行所述存储器存储的与基于区块链的智能合约调用的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0153] 将所述数据摘要作为查询索引向所述第三方存储系统发起查询，以查询与所述数据摘要对应的目标数据。

[0154] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的智能合约调用的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0155] 基于预设的摘要算法计算所述目标数据的数据摘要；

[0156] 确定计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要是否一致；

[0157] 如果计算得到的数据摘要与所述目标交易中的所述目标数据的数据摘要一致，确定针对所述目标数据的校验通过。

[0158] 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。

[0159] 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。

[0160] 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。

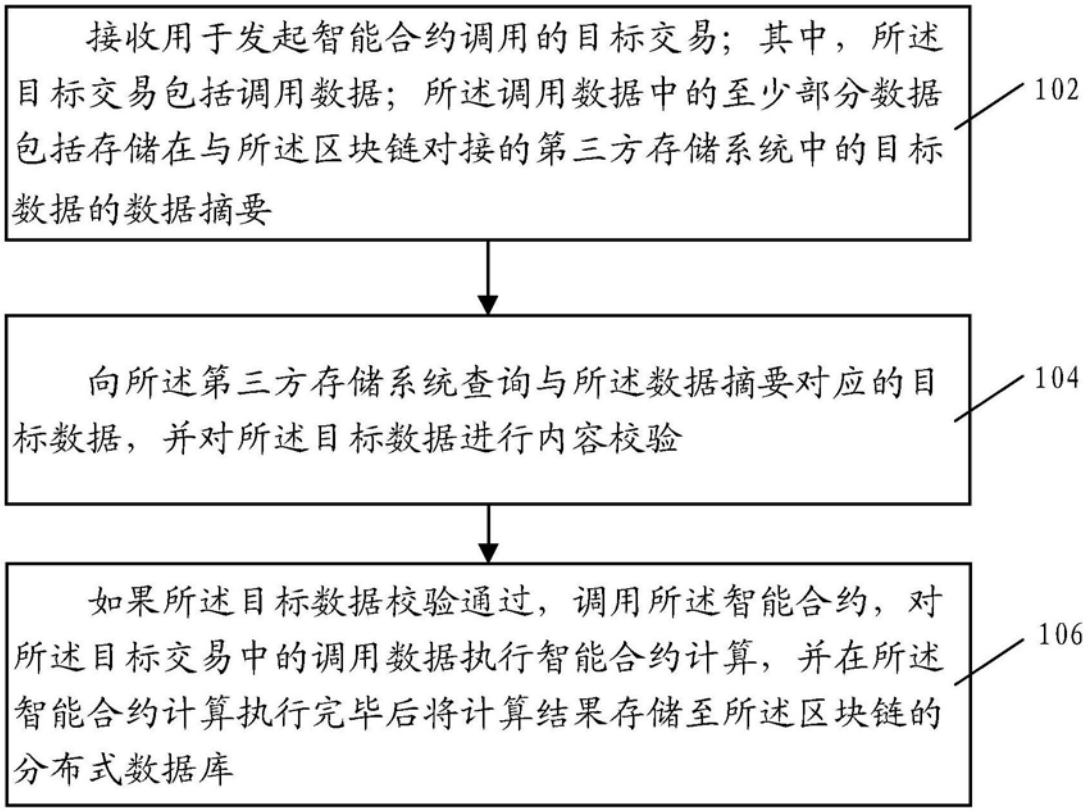

接收用于发起智能合约调用的目标交易；其中，所述目标交易包括调用数据；所述调用数据中的至少部分数据包括存储在与所述区块链对接的第三方存储系统中的目标数据的数据摘要
102
向所述第三方存储系统查询与所述数据摘要对应的目标数据，并对所述目标数据进行内容校验
104
如果所述目标数据校验通过，调用所述智能合约，对所述目标交易中的调用数据执行智能合约计算，并在所述智能合约计算执行完毕后将计算结果存储至所述区块链的分布式数据库
106

图1

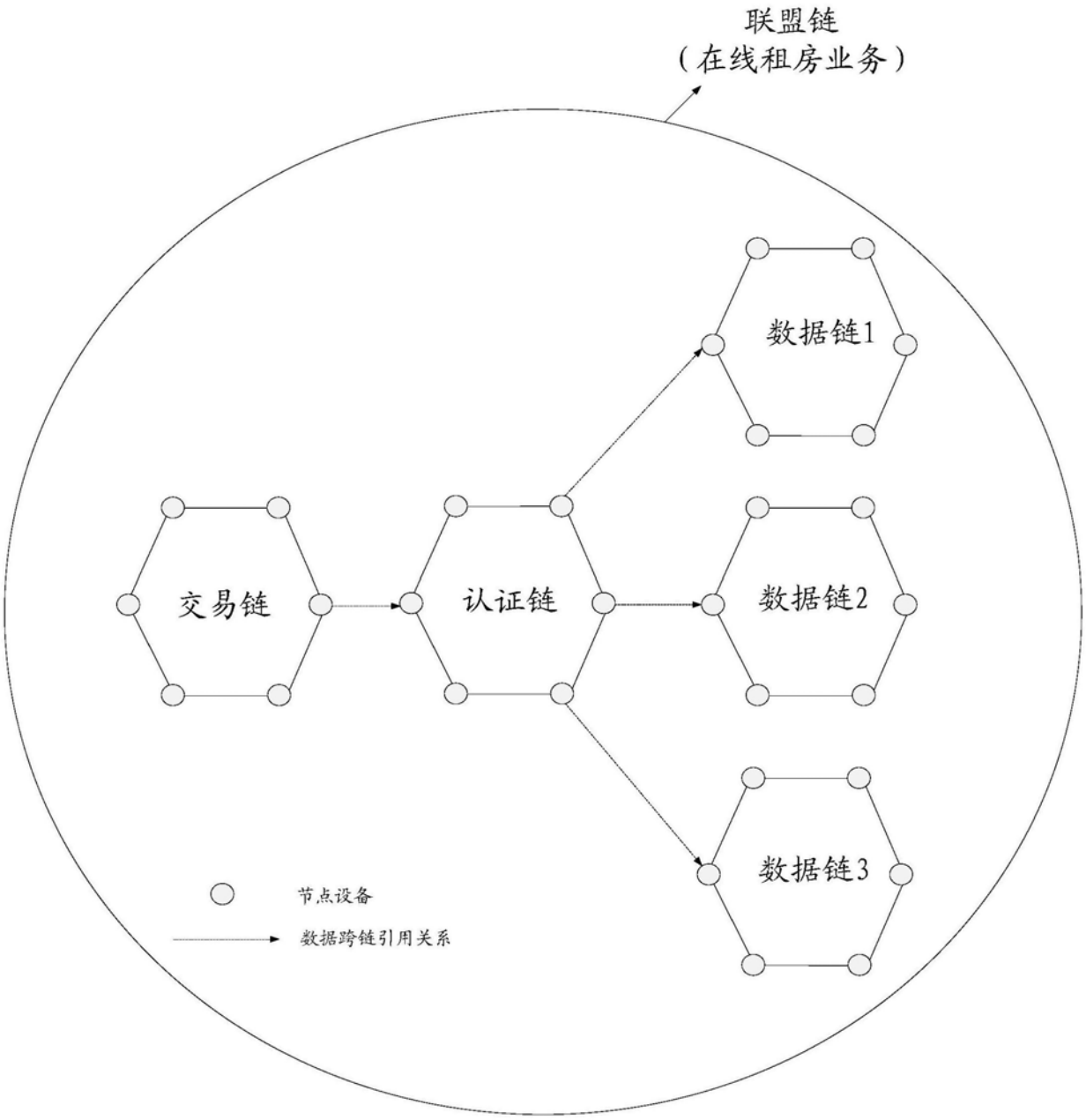


图2

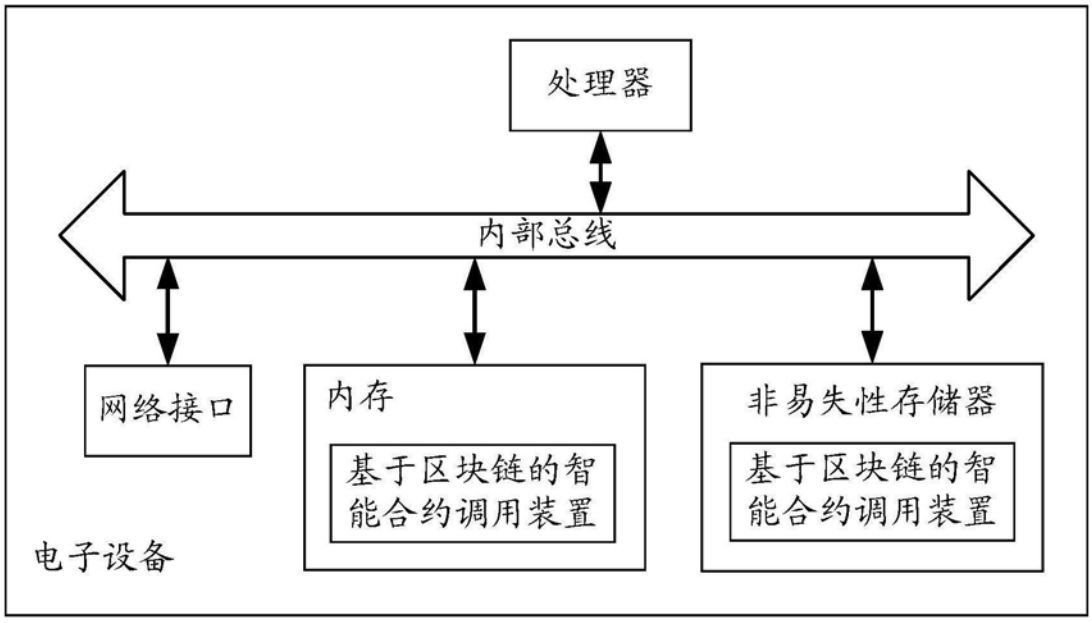

处理器
内部总线
网络接口
内存
基于区块链的智能合约调用装置
非易失性存储器
基于区块链的智能合约调用装置
电子设备

图3

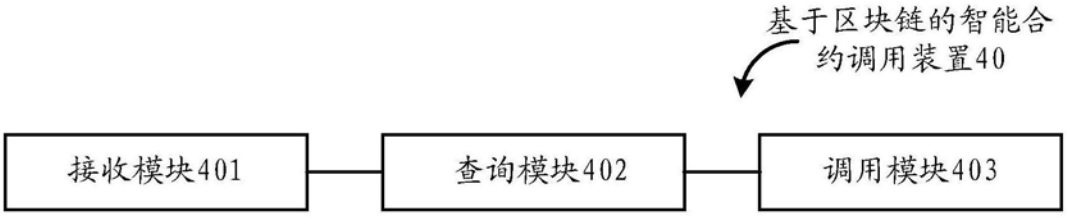

基于区块链的智能合约调用装置40
接收模块401
查询模块402
调用模块403

图4