

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号

WO 2020/119506 A1

(43) 国际公布日

2020 年 6 月 18 日 (18.06.2020)

(51) 国际专利分类号:

H04L 29/06 (2006.01)

(21) 国际申请号:

PCT/CN2019/122453

(22) 国际申请日:

2019 年 12 月 2 日 (02.12.2019)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201811529919.4 2018 年 12 月 14 日 (14.12.2018) CN

(71) 申请人: 深圳壹账通智能科技有限公司
(ONE CONNECT SMART TECHNOLOGY CO.,LTD.
(SHENZHEN)) [CN/CN]; 中国广东省深圳市
前海深港合作区前湾一路 1 号 A 栋 201
室, Guangdong 518000 (CN)。

(72) 发明人: 冯承勇 (FENG, Chengyong); 中国广东省
深圳市前海深港合作区前湾一路 1 号 A 栋
201 室, Guangdong 518000 (CN)。

(74) 代理人: 深圳中一联合知识产权代
理有限公司 (SHENZHEN ZHONGYI UNION
INTELLECTUAL PROPERTY AGENCY CO.,LTD.);
中国广东省深圳市福田区园岭街道深
南中路 1014 号报春大厦 9 楼 (5 号信箱),
Guangdong 518028 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家
保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,
BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,
CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,
JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,
LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

(54) Title: IDENTITY AUTHENTICATION METHOD BASED ON ALLIANCE CHAIN, AND TERMINAL DEVICE

(54) 发明名称: 一种基于联盟链的身份认证方法及终端设备

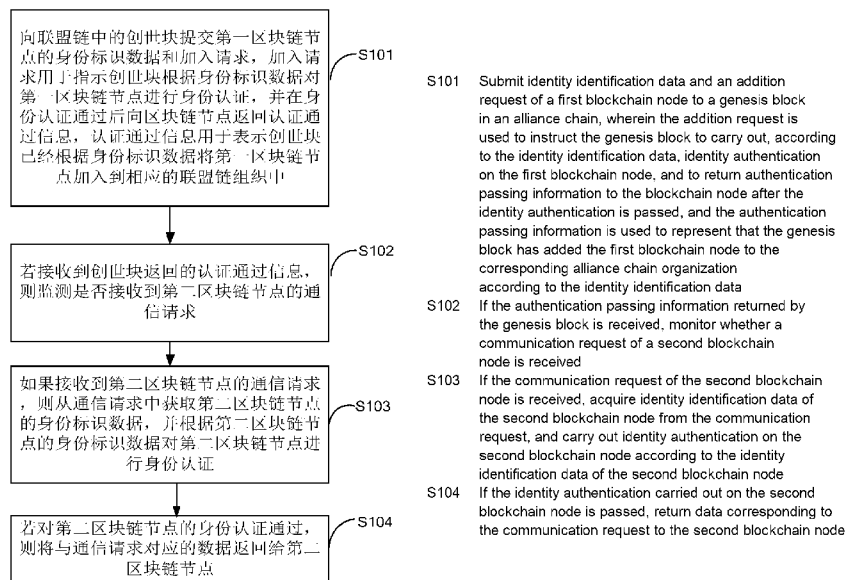


图 1

(57) Abstract: The present application is applicable to the technical field of blockchains. Provided are an identity authentication method based on an alliance chain, and a terminal device. The method comprises: submitting identity identification data and an addition request of a first blockchain node to a genesis block in an alliance chain; if authentication passing information returned by the genesis block is received, monitoring whether a communication request of a second blockchain node is received; if the communication request of the second blockchain node is received, acquiring identity identification data of the second blockchain node from the communication request, and carrying out identity authentication on the second blockchain node according to the identity identification data of the second

MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

blockchain node; and if the identity authentication carried out on the second blockchain node is passed, returning data corresponding to the communication request to the second blockchain node. By means of the method, the reliability of the identity authentication method based on an alliance chain is effectively improved.

(57) 摘要: 本申请适用于区块链技术领域, 提供了一种基于联盟链的身份认证方法及终端设备, 包括: 向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求; 若接收到所述创世块返回的认证通过信息, 则监测是否接收到第二区块链节点的通信请求; 如果接收到第二区块链节点的通信请求, 则从所述通信请求中获取所述第二区块链节点的身份标识数据, 并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证; 若对所述第二区块链节点的身份认证通过, 则将与所述通信请求对应的数据返回给所述第二区块链节点。通过上述方法, 有效提高了基于联盟链的身份认证方法的可靠性。

一种基于联盟链的身份认证方法及终端设备

[0001] 本申请要求于2018年12月14日提交中国专利局、申请号为201811529919.4、发明名称为“一种基于联盟链的身份认证方法及终端设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及区块链技术领域，尤其涉及一种基于联盟链的身份认证方法及终端设备。

背景技术

[0003] 在联盟链中，通常使用数字证书来进行可信身份认证（数字证书是由电子认证机构（CA，Certificate Authority）颁发的）。为了区分联盟链中多个参与组织，以及每个组织中参与的多个联盟链节点，通常采用的方案是为每个组织建设一个单独的根CA来代表联盟链中的一个组织，并由这个根CA为该组织中的每个节点签发数字证书以证明节点在组织的身份。联盟链在认证节点身份的时候，通过验证节点的数字证书的有效签发根CA来判断该节点属于哪个组织。

[0004] 一个组织可能参加多个不同的联盟链，即一个组织可能有多个根CA，那么该组织内的每个节点都会有不同的根CA签发的数字证书，即每个节点对应多个数字证书，这将导致在对组织内的节点进行身份认证时出现较高的错误率，进而导致身份认证的可靠性较低。

发明概述

技术问题

[0005] 本申请实施例的目的之一在于：提供了一种基于联盟链的身份认证方法及终端设备，以解决现有的基于联盟链的身份认证方法可靠性较低的问题。

问题的解决方案

技术解决方案

[0006] 为解决上述技术问题，本申请实施例采用的技术方案是：

[0007] 本申请实施例的第一方面，提供了一种基于联盟链的身份认证方法，可以包括

:

- [0008] 向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据所述身份标识数据对所述第一区块链节点进行身份认证，并在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中；
- [0009] 若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求；
- [0010] 如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证；
- [0011] 若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。
- [0012] 本申请实施例的第二方面，提供链一种基于联盟链的身份认证装置，所述装置包括：
- [0013] 提交单元，用于向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据所述身份标识数据对所述第一区块链节点进行身份认证，并在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中；
- [0014] 监测单元，用于若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求；
- [0015] 认证单元，用于如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证；
- [0016] 返回单元，用于若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。
- [0017] 本申请实施例的第三方面，提供了一种计算机可读存储介质，所述计算机可读

存储介质存储有计算机可读指令，所述计算机可读指令被处理器执行时实现如下步骤：

- [0018] 向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据所述身份标识数据对所述第一区块链节点进行身份认证，并在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中；
- [0019] 若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求；
- [0020] 如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证；
- [0021] 若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。
- [0022] 本申请实施例的第四方面，提供了一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：
- [0023] 向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据所述身份标识数据对所述第一区块链节点进行身份认证，并在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中；
- [0024] 若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求；
- [0025] 如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证；
- [0026] 若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返

回给所述第二区块链节点。

发明的有益效果

对附图的简要说明

附图说明

[0027] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例或示范性技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

[0028] 图1是本申请实施例提供的基于联盟链的身份认证方法的实现流程示意图；

[0029] 图2是本申请实施例提供的基于联盟链的身份认证装置的示意图；

[0030] 图3是本申请实施例提供的终端设备的示意图。

发明实施例

本发明的实施方式

[0031] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0032] 应当理解，当在本说明书和所附权利要求书中使用时，术语“包括”指示所描述特征、整体、步骤、操作、元素和/或组件的存在，但并不排除一个或多个其它特征、整体、步骤、操作、元素、组件和/或其集合的存在或添加。

[0033] 还应当理解，在此本申请说明书中所使用的术语仅仅是出于描述特定实施例的目的而并不意在限制本申请。如在本申请说明书和所附权利要求书中所使用的那样，除非上下文清楚地指明其它情况，否则单数形式的“一”、“一个”及“该”意在包括复数形式。

[0034] 还应当进一步理解，在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合，并且包括这

些组合。

[0035] 如在本说明书和所附权利要求书中所使用的那样，术语“如果”可以依据上下文被解释为“当...时”或“一旦”或“响应于确定”或“响应于检测到”。类似地，短语“如果确定”或“如果检测到[所描述条件或事件]”可以依据上下文被解释为意指“一旦确定”或“响应于确定”或“一旦检测到[所描述条件或事件]”或“响应于检测到[所描述条件或事件]”。

[0036] 为了说明本申请所述的技术方案，下面通过具体实施例来进行说明。

[0037] 图1是本申请实施例提供的基于联盟链的身份认证方法的实现流程示意图，如图所示，所述方法可以包括以下步骤：

[0038] 步骤S101，向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据所述身份标识数据对所述第一区块链节点进行身份认证，并在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中。

[0039] 在实际应用中，某个区块链节点A想要加入一个联盟链B，首先需要通过该联盟链B的创世块中记录的身份认证规则。区块链节点A向联盟链系统发送加入联盟链的加入请求，联盟链系统创世块接收到加入请求后，获取区块链节点A的身份标识数据，并与联盟链创世块中记录的身份认证规则相比对。

[0040] 这里，区块链节点A的身份标识数据可以是由代表联盟链组织成员身份的CA机构签发的数字证书，节点的身份标识数据可以放置于数字证书DN项目中或自定义的数字证书扩展项中。

[0041] 其中，所述身份标识数据为区块链节点的数字证书中的扩展项信息。

[0042] 所述扩展项信息包括：

[0043] 联盟链的名称、联盟链组织的标识、区块链节点的名称和区块链节点的类型。

[0044] 联盟链的名称即表示区块链节点所属的联盟链网络，联盟链组织的标识即表示区块链节点所属的联盟链组织，区块链节点名称即表示区块链节点在该组织内的唯一标识名称，区块链节点的类型表示区块链节点能够处理的事务类型，例如，区块链节点A可以执行付款交易，区块链节点B可以执行收款交易。

- [0045] 当然，还可以增加其他的数字证书的扩展项，只要能够用于说明区块链节点的身份的信息都可以作为扩展项。一个合法的CA机构不能无限制地创建合法的根CA，但是对于扩展项信息却没有要求。所以，将区块链节点的身份标识数据放置于数字证书扩展项中，当一个组织有多个根CA时，组织内的节点的只需一张数字证书，这张数字证书的扩展项中可以包括该节点所属的所有根CA的信息，这样有利于区块链节点的管理。
- [0046] 在一个实施例中，所述创世块根据该身份标识数据对所述第一区块链节点进行身份认证，包括：
- [0047] 判断该身份标识数据中联盟链的名称是否与所述创世块对应的联盟链的名称相同。
- [0048] 若所述身份标识数据中联盟链的名称与所述创世块对应的联盟链的名称相同，则判断所述创世块中存储的预设组织成员列表中是否存在该身份标识数据中联盟链组织的标识。
- [0049] 若所述创世块中存储的预设组织成员列表中不存在该身份标识数据中联盟链组织的标识，则对所述第一区块链节点的身份认证通过。
- [0050] 创世块对第一区块链节点进行身份认证，是基于联盟链的第一重身份认证。只有经过了创世块的认证，第一区块链节点才能够加入到创世块所属的联盟链中，第一区块链节点只有加入到了联盟链中，才能与该联盟链中的各区块链节点进行数据交互。
- [0051] 步骤S102，若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求。
- [0052] 在创世块通过了对第一区块链节点的身份认证后，第一区块链节点可以加入到创世块所属的联盟链中，进而第一区块链节点可以与该联盟链中的其他节点即第二区块链节点进行数据交互。但是，在进行数据交互之前，第一区块链节点需要对第二区块链节点进行身份认证，即第二重身份认证。如下述步骤。
- [0053] 步骤S103，如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证。

- [0054] 在一个实施例中，所述根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证，包括：
- [0055] S1031，验证所述第二区块链节点的扩展项信息中联盟链的名称是否与所述第一区块链节点的扩展项信息中联盟链的名称相同。
- [0056] 这一步骤用于验证第一区块链节点与第二区块链节点是否属于相同的联盟链。
- [0057] 可选的，所述验证所述第二区块链节点的扩展项信息中联盟链的名称是否与所述第一区块链节点的扩展项信息中联盟链的名称相同，包括：
- [0058] 将所述第一区块链节点的扩展项信息中联盟链的名称转换为第一字符串，并将所述第二区块链节点的扩展项信息中联盟链的名称转换为第二字符串。
- [0059] 分别将所述第一字符串中的每个字符与所述第二字符串中对应的字符进行比对。
- [0060] 若所述第一字符串的每个字符与所述第二字符串中对应的字符相同，则判定所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同。
- [0061] S1032，若所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同，则验证所述创世块中存储的预设组织成员列表中是否存在所述第二区块链节点的扩展项信息中联盟链组织的标识。
- [0062] 这一步骤用于验证第一区块链节点和第二区块链节点是否属于相同的联盟链组织。
- [0063] S1033，若所述创世块中存储的预设组织成员列表中不存在所述第二区块链节点的扩展项信息中联盟链组织的标识，则判断所述通信请求对应的节点行为是否符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为。
- [0064] 这一步骤用于验证第二区块链节点当前发起的请求行为是否符合其自身的节点行为。例如，假设区块链节点B的节点类型为收款交易，但是区块链节点B向区块链节点A发起的是支付交易，那么区块链节点B的行为与其节点类型不符，则不允许交易。
- [0065] 可选的，所述判断所述通信请求对应的节点行为是否符合所述第二区块链节点

的扩展项信息中区块链节点的类型对应的节点行为，包括：

[0066] 获取所述第二区块链节点的扩展项信息中区块链节点的类型对应的行为列表，并获取所述通信请求中包含的请求码。

[0067] 查找所述行为列表中是否存在所述请求码。

[0068] 若所述行为列表中存在所述请求码，则判定所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为。

[0069] 示例性的，假设区块链节点B发起支付交易，支付交易对应的请求信息为002，而区块链节点B的行为列表中只有001，说明区块链节点B不允许发起支付交易。

[0070] S1034，若所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为，则对所述第二区块链节点的身份认证通过。

[0071] 到这一步，完成了第一区块链节点对第二区块链节点的身份认证，即完成了第二重认证。

[0072] 步骤S104，若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。

[0073] 本申请实施例通过第一区块链节点向联盟链中的创世块提交身份标识数据并请求加入联盟链，以实现创世块对第一区块链节点的认证；在创世块认证通过后，监测联盟链中第二区块链节点的通信请求，并根据第二区块链节点的身份标识数据对第二区块链节点进行身份认证，以实现第一区块链节点对第二区块链节点的认证；认证通过后向第二区块链节点返回数据。通过上述方法，经过双重认证才能实现第一区块链节点与第二区块链节点之间的数据交互，有效提高了基于联盟链的身份认证方法的可靠性。

[0074] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对本申请实施例的实施过程构成任何限定。

[0075] 图2是本申请实施例提供的基于联盟链的身份认证装置的示意图，为了便于说明，仅示出与本申请实施例相关的部分。

[0076] 图2所示的基于联盟链的身份认证装置可以是内置于现有的终端设备内的软件

单元、硬件单元、或软硬结合的单元，也可以作为独立的挂件集成到所述终端设备中，还可以作为独立的终端设备存在。

[0077] 所述基于联盟链的身份认证装置2包括：

[0078] 提交单元21，用于向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据所述身份标识数据对所述第一区块链节点进行身份认证，并在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中。

[0079] 监测单元22，用于若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求。

[0080] 认证单元23，用于如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证。

[0081] 返回单元24，用于若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。

[0082] 其中，所述身份标识数据为区块链节点的数字证书中的扩展项信息。

[0083] 所述扩展项信息包括：

[0084] 联盟链的名称、联盟链组织的标识、区块链节点的名称和区块链节点的类型。

[0085] 可选的，所述认证单元23包括：

[0086] 第一验证模块，用于验证所述第二区块链节点的扩展项信息中联盟链的名称是否与所述第一区块链节点的扩展项信息中联盟链的名称相同。

[0087] 第二验证模块，用于若所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同，则验证所述创世块中存储的预设组织成员列表中是否存在所述第二区块链节点的扩展项信息中联盟链组织的标识。

[0088] 第三验证模块，用于若所述创世块中存储的预设组织成员列表中不存在所述第二区块链节点的扩展项信息中联盟链组织的标识，则判断所述通信请求对应的节点行为是否符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的

节点行为。

[0089] 第一通过模块，用于若所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为，则对所述第二区块链节点的身份认证通过。

[0090] 可选的，所述第一验证模块包括：

[0091] 转换子模块，用于将所述第一区块链节点的扩展项信息中联盟链的名称转换为第一字符串，并将所述第二区块链节点的扩展项信息中联盟链的名称转换为第二字符串。

[0092] 比对子模块，用于分别将所述第一字符串中的每个字符与所述第二字符串中对应的字符进行比对。

[0093] 第一判定子模块，用于若所述第一字符串的每个字符与所述第二字符串中对应的字符相同，则判定所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同。

[0094] 可选的，所述第三验证子模块包括：

[0095] 获取子模块，用于获取所述第二区块链节点的扩展项信息中区块链节点的类型对应的行为列表，并获取所述通信请求中包含的请求码。

[0096] 查找子模块，用于查找所述行为列表中是否存在所述请求码。

[0097] 第二判定子模块，用于若所述行为列表中存在所述请求码，则判定所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为。

[0098] 可选的，所述提交单元21包括：

[0099] 第一判断模块，用于判断该身份标识数据中联盟链的名称是否与所述创世块对应的联盟链的名称相同。

[0100] 第二判断模块，用于若所述身份标识数据中联盟链的名称与所述创世块对应的联盟链的名称相同，则判断所述创世块中存储的预设组织成员列表中是否存在该身份标识数据中联盟链组织的标识。

[0101] 第二通过模块，用于若所述创世块中存储的预设组织成员列表中存在该身份标识数据中联盟链组织的标识，则对所述第一区块链节点的身份认证通过。

[0102] 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。

[0103] 图3是本申请实施例提供的终端设备的示意图。如图3所示，该实施例的终端设备3包括：处理器30、存储器31以及存储在所述存储器31中并可在所述处理器30上运行的计算机可读指令32。所述处理器30执行所述计算机可读指令32时实现上述各个基于联盟链的身份认证方法实施例中的步骤，例如图1所示的步骤S101至S104。或者，所述处理器30执行所述计算机可读指令32时实现上述各装置实施例中各模块/单元的功能，例如图2所示模块21至24的功能。

[0104] 示例性的，所述计算机可读指令32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31中，并由所述处理器30执行，以完成本申请。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可读指令的指令段，该指令段用于描述所述32在所述终端设备3中的执行过程。例如，所述计算机可读指令32可以被分割成提交单元、监测单元、认证单元、返回单元，各单元具体功能如下：

[0105] 提交单元，用于向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据所述身份标识数据对所述第一区块链节点进行身份认证，并在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中。

[0106] 监测单元，用于若接收到所述创世块返回的认证通过信息，则监测是否接收到

第二区块链节点的通信请求。

[0107] 认证单元，用于如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证。

[0108] 返回单元，用于若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。

[0109] 其中，所述身份标识数据为区块链节点的数字证书中的扩展项信息。

[0110] 所述扩展项信息包括：

[0111] 联盟链的名称、联盟链组织的标识、区块链节点的名称和区块链节点的类型。

[0112] 可选的，所述认证单元包括：

[0113] 第一验证模块，用于验证所述第二区块链节点的扩展项信息中联盟链的名称是否与所述第一区块链节点的扩展项信息中联盟链的名称相同。

[0114] 第二验证模块，用于若所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同，则验证所述创世块中存储的预设组织成员列表中是否存在所述第二区块链节点的扩展项信息中联盟链组织的标识。

[0115] 第三验证模块，用于若所述创世块中存储的预设组织成员列表中不存在所述第二区块链节点的扩展项信息中联盟链组织的标识，则判断所述通信请求对应的节点行为是否符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为。

[0116] 第一通过模块，用于若所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为，则对所述第二区块链节点的身份认证通过。

[0117] 可选的，所述第一验证模块包括：

[0118] 转换子模块，用于将所述第一区块链节点的扩展项信息中联盟链的名称转换为第一字符串，并将所述第二区块链节点的扩展项信息中联盟链的名称转换为第二字符串。

[0119] 比对子模块，用于分别将所述第一字符串中的每个字符与所述第二字符串中对

应的字符进行比对。

[0120] 第一判定子模块，用于若所述第一字符串的每个字符与所述第二字符串中对应的字符相同，则判定所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同。

[0121] 可选的，所述第三验证子模块包括：

[0122] 获取子模块，用于获取所述第二区块链节点的扩展项信息中区块链节点的类型对应的行为列表，并获取所述通信请求中包含的请求码。

[0123] 查找子模块，用于查找所述行为列表中是否存在所述请求码。

[0124] 第二判定子模块，用于若所述行为列表中存在所述请求码，则判定所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为。

[0125] 可选的，所述提交单元包括：

[0126] 第一判断模块，用于判断该身份标识数据中联盟链的名称是否与所述创世块对应的联盟链的名称相同。

[0127] 第二判断模块，用于若所述身份标识数据中联盟链的名称与所述创世块对应的联盟链的名称相同，则判断所述创世块中存储的预设组织成员列表中是否存在该身份标识数据中联盟链组织的标识。

[0128] 第二通过模块，用于若所述创世块中存储的预设组织成员列表中存在该身份标识数据中联盟链组织的标识，则对所述第一区块链节点的身份认证通过。

[0129] 所述终端设备3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。所述终端设备可包括，但不仅限于，处理器30、存储器31。本领域技术人员可以理解，图3仅仅是终端设备3的示例，并不构成对终端设备3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，例如所述终端设备还可以包括输入输出设备、网络接入设备、总线等。

[0130] 所称处理器30可以是中央处理单元(Central Processing Unit, CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor, DSP)、专用集成电路(Application Specific Integrated Circuit, ASIC)、现成可编程门阵列(Field-Programmable Gate Array, 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。

[0131] 所述存储器31可以是所述终端设备3的内部存储单元，例如终端设备3的硬盘或内存。所述存储器31也可以是所述终端设备3的外部存储设备，例如所述终端设备3上配备的插接式硬盘，智能存储卡（Smart Media Card, SMC），安全数字（Secure Digital, SD）卡，闪存卡（Flash Card）等。进一步地，所述存储器31还可以既包括所述终端设备3的内部存储单元也包括外部存储设备。所述存储器31用于存储所述计算机可读指令以及所述终端设备所需的其它程序和数据。所述存储器31还可以用于暂时地存储已经输出或者将要输出的数据。

[0132] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中未详述或记载的部分，可以参见其它实施例的相关描述。

[0133] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

[0134] 在本申请所提供的实施例中，应该理解到，所揭露的装置/终端设备和方法，可以通过其它的方式实现。例如，以上所描述的装置/终端设备实施例仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以通过一些接口，装置或单元的间接耦合或通讯连接，可以是电性，机械或其它的形式。

[0135] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0136] 另外，在本申请各个实施例中的各功能单元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。

[0137] 所述集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请实现上述实施例方法中的全部或部分流程，也可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一计算机可读存储介质中，该计算机可读指令在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机可读指令包括计算机可读指令代码，所述计算机可读指令代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机可读指令代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器（ROM， Read-Only Memory）、随机存取存储器（RAM， Random Access Memory）、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括是电载波信号和电信信号。

[0138] 以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权利要求书

- [权利要求 1] 一种基于联盟链的身份认证方法，其特征在于，应用于第一区块链节点，所述方法包括：
- 向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据所述身份标识数据对所述第一区块链节点进行身份认证，并在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中；
- 若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求；
- 如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证；
- 若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。
- [权利要求 2] 如权利要求1所述的基于联盟链的身份认证方法，其特征在于，所述身份标识数据为区块链节点的数字证书中的扩展项信息；
- 所述扩展项信息包括：
- 联盟链的名称、联盟链组织的标识、区块链节点的名称和区块链节点的类型。
- [权利要求 3] 如权利要求2所述的基于联盟链的身份认证方法，其特征在于，所述根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证，包括：
- 验证所述第二区块链节点的扩展项信息中联盟链的名称是否与所述第一区块链节点的扩展项信息中联盟链的名称相同；
- 若所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同，则验证所述创世块中存储

的预设组织成员列表中是否存在所述第二区块链节点的扩展项信息中联盟链组织的标识；

若所述创世块中存储的预设组织成员列表中存在所述第二区块链节点的扩展项信息中联盟链组织的标识，则判断所述通信请求对应的节点行为是否符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为；

若所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为，则对所述第二区块链节点的身份认证通过。

[权利要求 4]

如权利要求3所述的基于联盟链的身份认证方法，其特征在于，所述验证所述第二区块链节点的扩展项信息中联盟链的名称是否与所述第一区块链节点的扩展项信息中联盟链的名称相同，包括：

将所述第一区块链节点的扩展项信息中联盟链的名称转换为第一字符串，并将所述第二区块链节点的扩展项信息中联盟链的名称转换为第二字符串；

分别将所述第一字符串中的每个字符与所述第二字符串中对应的字符进行比对；

若所述第一字符串的每个字符与所述第二字符串中对应的字符相同，则判定所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同。

[权利要求 5]

如权利要求3所述的基于联盟链的身份认证方法，其特征在于，所述判断所述通信请求对应的节点行为是否符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为，包括：

获取所述第二区块链节点的扩展项信息中区块链节点的类型对应的行为列表，并获取所述通信请求中包含的请求码；

查找所述行为列表中是否存在所述请求码；

若所述行为列表中存在所述请求码，则判定所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应

的节点行为。

- [权利要求 6] 如权利要求2所述的基于联盟链的身份认证方法，其特征在于，所述创世块根据该身份标识数据对所述第一区块链节点进行身份认证，包括：
- 判断该身份标识数据中联盟链的名称是否与所述创世块对应的联盟链的名称相同；
- 若所述身份标识数据中联盟链的名称与所述创世块对应的联盟链的名称相同，则判断所述创世块中存储的预设组织成员列表中是否存在该身份标识数据中联盟链组织的标识；
- 若所述创世块中存储的预设组织成员列表中存在该身份标识数据中联盟链组织的标识，则对所述第一区块链节点的身份认证通过。
- [权利要求 7] 一种基于联盟链的身份认证装置，其特征在于，所述装置包括：
- 提交单元，用于向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据所述身份标识数据对所述第一区块链节点进行身份认证，并在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中；
- 监测单元，用于若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求；
- 认证单元，用于如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证；
- 返回单元，用于若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。
- [权利要求 8] 如权利要求7所述的基于联盟链的身份认证装置，其特征在于，所述身份标识数据为区块链节点的数字证书中的扩展项信息；
- 所述扩展项信息包括：

联盟链的名称、联盟链组织的标识、区块链节点的名称和区块链节点的类型。

[权利要求 9]

如权利要求8所述的基于联盟链的身份认证装置，其特征在于，所述认证单元包括：

第一验证模块，用于验证所述第二区块链节点的扩展项信息中联盟链的名称是否与所述第一区块链节点的扩展项信息中联盟链的名称相同；

第二验证模块，用于若所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同，则验证所述创世块中存储的预设组织成员列表中是否存在所述第二区块链节点的扩展项信息中联盟链组织的标识；

第三验证模块，用于若所述创世块中存储的预设组织成员列表中不存在所述第二区块链节点的扩展项信息中联盟链组织的标识，则判断所述通信请求对应的节点行为是否符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为；

第一通过模块，用于若所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为，则对所述第二区块链节点的身份认证通过。

[权利要求 10]

如权利要求9所述的基于联盟链的身份认证装置，其特征在于，所述第一验证模块包括：

转换子模块，用于将所述第一区块链节点的扩展项信息中联盟链的名称转换为第一字符串，并将所述第二区块链节点的扩展项信息中联盟链的名称转换为第二字符串；

比对子模块，用于分别将所述第一字符串中的每个字符与所述第二字符串中对应的字符进行比对；

第一判定子模块，用于若所述第一字符串的每个字符与所述第二字符串中对应的字符相同，则判定所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同

。

[权利要求 11]

如权利要求9所述的基于联盟链的身份认证装置，其特征在于，所述第三验证子模块包括：

获取子模块，用于获取所述第二区块链节点的扩展项信息中区块链节点的类型对应的行为列表，并获取所述通信请求中包含的请求码；

查找子模块，用于查找所述行为列表中是否存在所述请求码；

第二判定子模块，用于若所述行为列表中不存在所述请求码，则判定所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为。

[权利要求 12]

如权利要求8所述的基于联盟链的身份认证装置，其特征在于，所述提交单元包括：

第一判断模块，用于判断该身份标识数据中联盟链的名称是否与所述创世块对应的联盟链的名称相同；

第二判断模块，用于若所述身份标识数据中联盟链的名称与所述创世块对应的联盟链的名称相同，则判断所述创世块中存储的预设组织成员列表中是否存在该身份标识数据中联盟链组织的标识；

第二通过模块，用于若所述创世块中存储的预设组织成员列表中不存在该身份标识数据中联盟链组织的标识，则对所述第一区块链节点的身份认证通过。

[权利要求 13]

一种计算机可读存储介质，所述计算机可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被处理器执行时实现如下步骤：

向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据该身份标识数据对所述第一区块链节点进行身份认证、在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中

；

若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求；

如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证；

若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。

[权利要求 14] 如权利要求13所述的计算机可读存储介质，其特征在于，所述身份标识数据为区块链节点的数字证书中的扩展项信息；

所述扩展项信息包括：

联盟链的名称、联盟链组织的标识、区块链节点的名称、区块链节点的类型。

[权利要求 15] 一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

向联盟链中的创世块提交所述第一区块链节点的身份标识数据和加入请求，所述加入请求用于指示所述创世块根据该身份标识数据对所述第一区块链节点进行身份认证、在身份认证通过后向所述区块链节点返回认证通过信息，所述认证通过信息用于表示所述创世块已经根据所述身份标识数据将所述第一区块链节点加入到相应的联盟链组织中；

若接收到所述创世块返回的认证通过信息，则监测是否接收到第二区块链节点的通信请求；

如果接收到第二区块链节点的通信请求，则从所述通信请求中获取所述第二区块链节点的身份标识数据，并根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证；

若对所述第二区块链节点的身份认证通过，则将与所述通信请求对应的数据返回给所述第二区块链节点。

- [权利要求 16] 如权利要求15所述的终端设备，其特征在于，所述身份标识数据为区块链节点的数字证书中的扩展项信息；
所述扩展项信息包括：
联盟链的名称、联盟链组织的标识、区块链节点的名称、区块链节点的类型。
- [权利要求 17] 如权利要求16所述的终端设备，其特征在于，所述根据所述第二区块链节点的身份标识数据对所述第二区块链节点进行身份认证，包括：
验证所述第二区块链节点的扩展项信息中联盟链的名称是否与所述第一区块链节点的扩展项信息中联盟链的名称相同；
若所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同，则验证所述创世块中存储的预设组织成员列表中是否存在所述第二区块链节点的扩展项信息中联盟链组织的标识；
若所述创世块中存储的预设组织成员列表中存在所述第二区块链节点的扩展项信息中联盟链组织的标识，则判断所述通信请求对应的节点行为是否符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为；
若所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为，则对所述第二区块链节点的身份认证通过。
- [权利要求 18] 如权利要求17所述的终端设备，其特征在于，所述验证所述第二区块链节点的扩展项信息中联盟链的名称是否与所述第一区块链节点的扩展项信息中联盟链的名称相同，包括：
将所述第一区块链节点的扩展项信息中联盟链的名称转换为第一字符串，并将所述第二区块链节点的扩展项信息中联盟链的名称转换为第二字符串；
分别将所述第一字符串中的每个字符与所述第二字符串中对应的字符进行比对；

若所述第一字符串的每个字符与所述第二字符串中对应的字符相同，则判定所述第二区块链节点的扩展项信息中联盟链的名称与所述第一区块链节点的扩展项信息中联盟链的名称相同。

[权利要求 19] 如权利要求17所述的终端设备，其特征在于，所述判断所述通信请求对应的节点行为是否符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为，包括：
获取所述第二区块链节点的扩展项信息中区块链节点的类型对应的行为列表，并获取所述通信请求中包含的请求码；
查找所述行为列表中是否存在所述请求码；
若所述行为列表中存在所述请求码，则判定所述通信请求对应的节点行为符合所述第二区块链节点的扩展项信息中区块链节点的类型对应的节点行为。

[权利要求 20] 如权利要求16所述的终端设备，其特征在于，所述创世块根据该身份标识数据对所述第一区块链节点进行身份认证，包括：
判断该身份标识数据中联盟链的名称是否与所述创世块对应的联盟链的名称相同；
若所述身份标识数据中联盟链的名称与所述创世块对应的联盟链的名称相同，则判断所述创世块中存储的预设组织成员列表中是否存在该身份标识数据中联盟链组织的标识；
若所述创世块中存储的预设组织成员列表中存在该身份标识数据中联盟链组织的标识，则对所述第一区块链节点的身份认证通过。

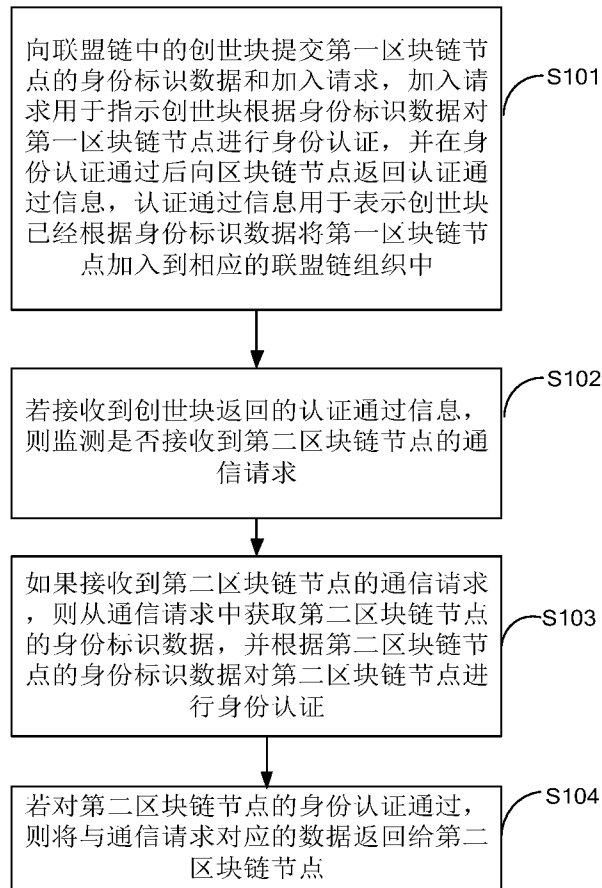


图 1

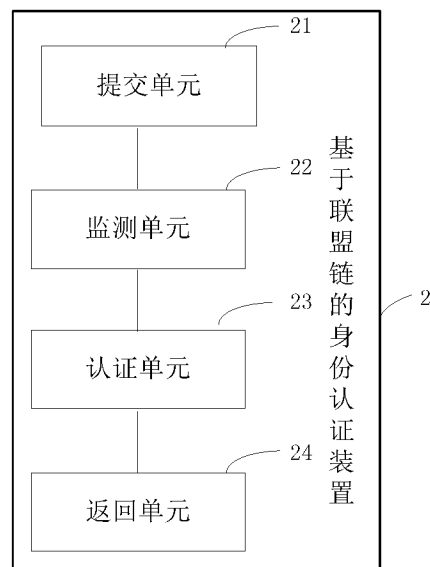


图 2

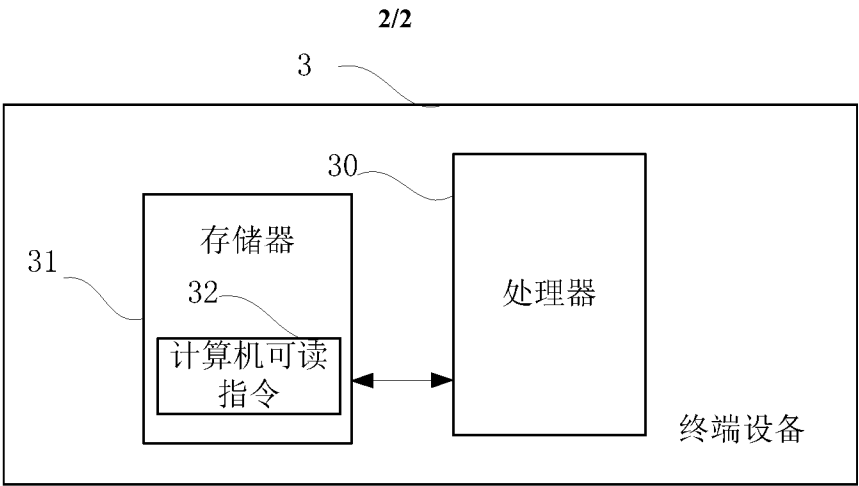


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/122453

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, EPODOC, WPI, IEEE: 身份, 认证, 核实, 创世块, 联盟链, 区块链, 许可链, 公钥, 私钥, 名称, 成员, 列表, 扩展信息, 交易行为, 字符串, 组织, 节点, 请求码, identity, authentication, verification, creation block, alliance chain, block chain, permission chain, public key, private key, name, member, list, extension information, transaction behavior, character string, organization, node and request code

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109815657 A (ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) 28 May 2019 (2019-05-28) description, paragraphs 0001-0137	1-20
X	CN 106789920 A (SHENZHEN QIANHAI WEIZHONG BANK CO., LTD.) 31 May 2017 (2017-05-31) description, paragraphs 0002, 0047-0087, and 0098-0104, and figures 1-5	1, 2, 6-8, 12-16, 20
A	CN 108416589 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 17 August 2018 (2018-08-17) entire document	1-20
A	CN 108389130 A (HEIFEI UNIVERSITY) 10 August 2018 (2018-08-10) entire document	1-20
A	US 2005114447 A1 (CAMERON, K. et al.) 26 May 2005 (2005-05-26) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance
 “E” earlier application or patent but published on or after the international filing date
 “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 “O” document referring to an oral disclosure, use, exhibition or other means
 “P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 “&” document member of the same patent family

Date of the actual completion of the international search

19 January 2020

Date of mailing of the international search report

06 February 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/122453

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	张健毅等 (ZHANG, Jianyi et al.). "基于区块链的可监管数字货币模型 (A Regulatable Digital Currency Model Based on Blockchain)" <i>计算机研究与发展 (Journal of Computer Research and Development)</i> , 15 October 2018 (2018-10-15), entire document	1-20
A	WANG, Wentong et al. "BlockCAM: A Blockchain-based Cross-domain Authentication Model" <i>2018 IEEE Third International Conference on Data Science in Cyberspace</i> , 19 July 2018 (2018-07-19), entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/122453

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	109815657	A	28 May 2019	None	
CN	106789920	A	31 May 2017	None	
CN	108416589	A	17 August 2018	None	
CN	108389130	A	10 August 2018	None	
US	2005114447	A1	26 May 2005	None	

国际检索报告

国际申请号

PCT/CN2019/122453

A. 主题的分类 H04L 29/06 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L; G06Q 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNKI, CNPAT, EPDOC, WPI, IEEE: 身份, 认证, 核实, 创世块, 联盟链, 区块链, 许可链, 公钥, 私钥, 名称, 成员, 列表, 扩展信息, 交易行为, 字符串, 组织, 节点, 请求码, identity, authentication, verification, creation block, alliance chain, block chain, permission chain, public key, private key, name, member, list, extension information, transaction behavior, character string, organization, node and request code		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 109815657 A (深圳壹账通智能科技有限公司) 2019年 5月 28日 (2019 - 05 - 28) 说明书第0001-0137段	1-20
X	CN 106789920 A (深圳前海微众银行股份有限公司) 2017年 5月 31日 (2017 - 05 - 31) 说明书第0002、0047-0087、0098-0104段, 附图1-5	1-2, 6-8, 12-16, 20
A	CN 108416589 A (深圳前海微众银行股份有限公司) 2018年 8月 17日 (2018 - 08 - 17) 全文	1-20
A	CN 108389130 A (合肥学院) 2018年 8月 10日 (2018 - 08 - 10) 全文	1-20
A	US 2005114447 A1 (CAMERON, Kim等) 2005年 5月 26日 (2005 - 05 - 26) 全文	1-20
A	张健毅等. “基于区块链的可监管数字货币模型” 计算机研究与发展, 2018年 10月 15日 (2018 - 10 - 15), 全文	1-20
☒ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2020年 1月 19日		国际检索报告邮寄日期 2020年 2月 6日
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		授权官员 于雷 电话号码 86-10-53961719

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	WANG, Wentong等. "BlockCAM: A Blockchain-based Cross-domain Authentication Model" 2018 IEEE Third International Conference on Data Science in Cyberspace, 2018年 7月 19日 (2018 - 07 - 19), 全文	1-20

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/122453

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	109815657	A	2019年 5月 28日	无	
CN	106789920	A	2017年 5月 31日	无	
CN	108416589	A	2018年 8月 17日	无	
CN	108389130	A	2018年 8月 10日	无	
US	2005114447	A1	2005年 5月 26日	无	