(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

(43) 国际公布日
2020 年 11 月 5 日 (05.11.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/220627 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/114985

(22) 国际申请日: 2019 年 11 月 1 日 (01.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910354377.X 2019年4月29日 (29.04.2019) CN

(71) 申请人: 清 华 大 学 (TSINGHUA UNIVERSITY) [CN/CN]; 中 国 北 京 市 海 淀 区 清 华 园, Beijing 100084 (CN)。

(72) 发明人: 徐 恪 (XU, Ke); 中 国 北 京 市 海 淀 区 清 华 园, Beijing 100084 (CN)。 吕 亮 (LV, Liang); 中 国 北 京 市 海 淀 区 清 华 园, Beijing 100084 (CN)。 吴 波 (WU, Bo); 中 国 北 京 市 海 淀 区 清 华 园, Beijing 100084 (CN)。 谭 崎 (TAN, Qi); 中 国 北 京 市 海 淀 区 清 华 园, Beijing 100084 (CN)。 赵 乙 (ZHAO, Yi); 中 国 北 京 市 海 淀 区 清华园, Beijing 100084 (CN)。

(74) 代理人: 北 京 清 亦 华 知 识 产 权 代 理 事 务 所 (普 通 合 伙) (TSINGYIHUA INTELLECTUAL PROPERTY LLC); 中国北京市海淀区清华园清华大学照澜院商业楼301室, Beijing 100084 (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,

(54) **Title:** METHOD AND DEVICE FOR STRONG CROSS-DOMAIN LOGIC ISOLATION AND SECURE ACCESS CONTROL IN INTERNET OF THINGS SCENARIO

(54) **发明名称:** 物联网场景下跨域逻辑强隔离与安全访问控制方法及装置

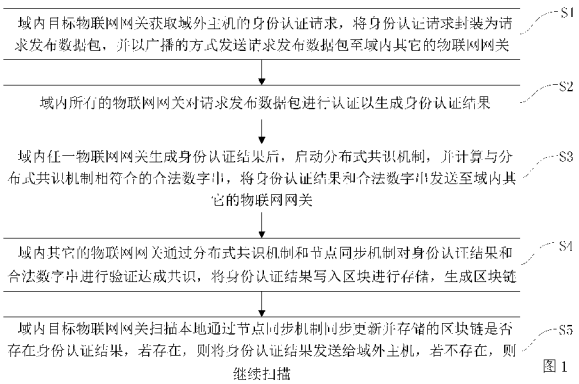

图 1

S1 An intra-domain target Internet of Things gateway acquires an identity authentication request from an extra-domain host, encapsulates the identity authentication request into a request publishing data packet, and sends, in a broadcast manner, the request publishing data packet to other intra-domain Internet of Things gateways

S2 All intra-domain Internet of Things gateways verify the request publishing data packet to generate an identity authentication result

S3 Any intra-domain Internet of Things gateway, after generating the identity authentication result, starts a distributed consensus mechanism, computes a valid numerical string consistent with the distributed consensus mechanism, and sends the identity authentication result and the valid numerical string to the other intra-domain Internet of Things gateways

S4 The other intra-domain Internet of Things gateways verify the identity authentication result and the valid numerical string by means of the distributed consensus mechanism and a node synchronization mechanism to reach a consensus, write the identity authentication result into blocks for storage, to generate a block chain

S5 A target intra-domain Internet of Things gateway scans to determine whether there is an identity authentication result in the block chain updated and stored locally by means of the node synchronization mechanism, and if so, sends the identity authentication result to the extra-domain host, and if not, continues to scan

(57) **Abstract:** The present application feedback discloses a method and a device for strong cross-domain logic isolation and secure access control in an Internet of Things scenario. The method comprises: after a certain Internet of Things gateway receives an identity authentication request, the gateway broadcasting the request to other intra-domain Internet of Things gateways; after receiving the identity authentication request, the intra-domain Internet of Things gateways starting to independently verify whether the identity

WO 2020/220627 A1

[见续页]

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, 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))。

authentication request is valid; after a certain Internet of Things gateway obtains an identity authentication result, starting a distributed consensus mechanism; the intra-domain Internet of Things gateways reaching a consensus on the authentication result by means of the distributed consensus mechanism, and then the identity authentication result being written into blocks for storage, and these blocks forming a block chain. Thus, intra-domain Internet of Things gateways perform access control by means of a distributed consensus mechanism, realizing strong cross-domain logic isolation, and effectively improving the security of an Internet of Things system, and an identity authentication result is stored in blocks in a block chain, achieving the characteristics of openness, transparency and traceability.

(57) 摘要：本申请反馈公开了一种物联网场景下跨域逻辑强隔离与安全访问控制方法及装置，其中，该方法包括：当某台物联网网关接收到身份认证请求后，该网关将此请求广播到域内的其它物联网网关上；域内的物联网网关接收到身份认证请求后，开始独立验证是否该身份认证请求是否合法；某台物联网网关得出身份认证结果后，启动分布式共识机制；域内的物联网网关通过分布式共识机制对认证结果达成共识，而后身份认证结果被写入区块存储起来，这些区块形成区块链。由此，域内的物联网网关以分布式共识机制进行访问控制，实现跨域逻辑强隔离，有效提升了物联网系统的安全性，并且身份认证结果存储在区块链中的区块上，具有公开透明和可追溯的特性。

物联网场景下跨域逻辑强隔离与安全访问控制方法及装置

相关申请的交叉引用

本申请要求清华大学于 2019 年 04 月 29 日提交的、发明名称为“物联网场景下跨域逻辑强隔离与安全访问控制方法及装置”的、中国专利申请号“201910354377.X”的优先权。

技术领域

本申请反馈属于网络空间安全技术领域，特别涉及一种物联网场景下跨域逻辑强隔离与安全访问控制方法及装置。

背景技术

访问控制技术是网络空间安全领域的重要研究内容，该技术旨在防止对任何资源进行的未授权访问，确保计算机系统在合法的范围内使用。根据国际电信联盟的定义，物联网主要解决物品与物品、物品与人、人与人之间的互联。在物联网（Internet of Things）场景中，物联网节点通常算力有限，难以完成复杂的计算操作和访问控制，所以被劫持的风险很高；物联网节点数量大，如果物联网节点被劫持，黑客可以借助物联网节点在数量上的优势实施 DDoS(Distributed Denial of Service，分布式拒绝服务)攻击，极大危害网络安全；物联网节点与人类生活息息相关，因此物联网节点通常记录了人们的隐私数据，若被劫持，可能会造成严重的隐私泄漏。瑞士苏黎世大学的 Mattern 团队曾经总结了从互联网到物联网的转变过程中可能会面临的一系列安全问题，其中尤为强调了访问控制问题。因此，研究物联网场景下的访问控制机制具有重要意义。

近年来，随着物联网的广泛应用，物联网场景中有大量关于访问控制方面的研究。目前，物联网中的访问控制解决方案大致从两个层面开展工作。第一，是从协议和框架（Protocols and Frameworks）层面入手，代表性工作包括 XACML（Extensible Access Control Markup Language）、OAUTH（Access control solutions based on Open Authorization protocol）、UMA（User-Managed Access）等；第二，是从模型(Models)层面入手，代表性工作包括 RBAC（Role-Based Access Control）、ABAC（Attribute-Based Access Control）、CAPBAC（Capability-based access control）、UCON（usage control）、ORBAC（Organizational-Based Access Control）等。尽管这些方案从各个层面上增强了物联网系统的安全性，但是从宏观来看，在上述解决方案中，访问控制通常由单一认证节点（比如物联网网关）完成，并且

通常假设这个认证节点是可信的、安全的。这导致一个问题：如果该认证节点被劫持，该域内的所有物联网设备和用户数据就处于风险之中；尽管在某些解决方案中，域内可以部署多个认证节点，但是这些认证节点之间通常互为备份，这仅为提升系统可靠性考虑，只要多个认证节点中有一个认证节点被劫持，即可极大威胁身份认证安全，并无法有效提升系统安全性。此外，尽管相对于物联网节点来说，物联网网关具备较多的计算资源，但是仍然无法支持复杂的身份认证过程，总是假设认证节点是安全的或者可信的是不现实的，所以上述采用单认证节点的访问控制方案安全性仍有提升空间。

发明内容

本申请反馈旨在至少在一定程度上解决相关技术中的技术问题之一。

为此，本申请反馈的一个目的在于提出一种物联网场景下跨域逻辑强隔离与安全访问控制方法，该方法克服单认证节点方案存在的弊端，具有高安全性、透明和可追溯等特点。

本申请反馈的另一个目的在于提出一种物联网场景下跨域逻辑强隔离与安全访问控制装置。

为达到上述目的，本申请反馈一方面实施例提出了一种物联网场景下跨域逻辑强隔离与安全访问控制方法，包括：

S1，域内目标物联网网关获取域外主机的身份认证请求，将所述身份认证请求封装为请求发布数据包，并以广播的方式发送所述请求发布数据包至域内其它的物联网网关；

S2，域内所有的物联网网关对所述请求发布数据包进行认证以生成身份认证结果；

S3，域内任一物联网网关生成所述身份认证结果后，启动分布式共识机制，并计算与所述分布式共识机制相符合的合法数字串，将所述身份认证结果和所述合法数字串发送至域内其它的物联网网关；

S4，域内其它的物联网网关通过所述分布式共识机制和节点同步机制对所述身份认证结果和所述合法数字串进行验证达成共识，将所述身份认证结果写入区块进行存储，生成区块链；

S5，所述域内目标物联网网关扫描本地通过所述节点同步机制同步更新并存储的所述区块链是否存在所述身份认证结果，若存在，则将所述身份认证结果发送给所述域外主机，若不存在，则继续扫描。

本申请反馈实施例的物联网场景下跨域逻辑强隔离与安全访问控制方法，当某台物联网网关接收到身份认证请求后，将此认证请求发布给域内的其它物联网网关，域内的物联网网关分别对此发送此请求的主机进行身份认证，并以分布式共识机制对身份认证的结果达成共识。由此，域内的物联网网关以分布式共识机制进行访问控制，实现跨域逻辑强隔

离，有效提升了物联网系统的安全性，并且身份认证结果以区块形式存储，便于检索查阅，具有公开透明和可追溯的特性。

另外，根据本申请反馈上述实施例的物联网场景下跨域逻辑强隔离与安全访问控制方法还可以具有以下附加的技术特征：

进一步地，所述域内所有的物联网网关对所述请求发布数据包进行认证生成身份认证结果，包括：

域内所有的物联网网关接收到所述请求发布数据包后，提取所述请求发布数据包中的身份信息，并根据本地存储的合法身份证书对所述身份信息进行认证生成身份认证结果。

进一步地，所述 S3，还包括：所述域内任一物联网网关生成所述身份认证结果后，若在计算出与所述分布式共识机制相符合的合法数字串之前，域内另一物联网网关计算出所述身份认证结果和所述合法数字串，则由另一域内物联网网关启动所述分布式共识机制，将所述身份认证结果和所述合法数字串发送至域内其它的物联网网关。

进一步地，所述 S4，进一步包括：

S41，域内所有的物联网网关验证接收到的所述身份认证结果与本物联网网关生成的认证结果是否相同，若不同，则不认可所述身份认证结果，丢弃所述身份认证结果，执行 S42，若相同，则执行 S43；

S42，计算与所述分布式共识机制相符合的所述合法数字串，计算完成后，启动所述分布式共识机制，将本物联网网关的认证结果和所述合法数字串发送至域内所有的物联网网关，执行 S41；

S43，验证所述合法数字串是否符合所述分布式共识机制规定的条件，若不符合，则执行 S42，若符合，通过所述分布式共识机制和所述节点同步机制对所述身份认证结果和所述合法数字串达成共识，将所述身份认证结果写入区块进行存储，生成所述区块链。

进一步地，所述节点同步机制为域内所有的物联网网关在对所述身份认证结果和所述合法数字串进行验证时，域内所有的物联网网关的区块链进行信息交互，将所述区块链进行同步存储。

为达到上述目的，本申请反馈另一方面实施例提出了一种物联网场景下跨域逻辑强隔离与安全访问控制装置，包括：

获取模块，用于域内目标物联网网关获取域外主机的身份认证请求，将所述身份认证请求封装为请求发布数据包，并以广播的方式发送所述请求发布数据包至域内其它的物联网网关；

生成模块，用于域内所有的物联网网关对所述请求发布数据包进行认证以生成身份认证结果；

发送模块，用于域内任一物联网网关生成所述身份认证结果后，启动分布式共识机制，并计算与所述分布式共识机制相符合的合法数字串，将所述身份认证结果和所述合法数字串发送至域内其它的物联网网关；

验证模块，用于域内其它的物联网网关通过所述分布式共识机制和节点同步机制对所述身份认证结果和所述合法数字串进行验证达成共识，将所述身份认证结果写入区块进行存储，生成区块链；

扫描模块，用于所述域内目标物联网网关扫描本地通过所述节点同步机制同步更新并存储的所述区块链是否存在所述身份认证结果，若存在，则将所述身份认证结果发送给所述域外主机，若不存在，则继续扫描。

本申请反馈实施例的物联网场景下跨域逻辑强隔离与安全访问控制装置，当某台物联网网关接收到身份认证请求后，将此认证请求发布给域内的其它物联网网关，域内的物联网网关分别对此发送此请求的主机进行身份认证，并以分布式共识机制对身份认证的结果达成共识。由此，域内的物联网网关以分布式共识机制进行访问控制，实现跨域逻辑强隔离，有效提升了物联网系统的安全性，并且身份认证结果以区块形式存储，便于检索查阅，具有公开透明和可追溯的特性。

另外，根据本申请反馈上述实施例的物联网场景下跨域逻辑强隔离与安全访问控制装置还可以具有以下附加的技术特征：

进一步地，所述生成模块，具体用于，

域内所有的物联网网关接收到所述请求发布数据包后，提取所述请求发布数据包中的身份信息，并根据本地存储的合法身份证书对所述身份信息进行认证生成身份认证结果。

进一步地，所述发送模块，还用于，

所述域内任一物联网网关生成所述身份认证结果后，若在计算出与所述分布式共识机制相符合的合法数字串之前，域内另一物联网网关计算出所述身份认证结果和所述合法数字串，则由另一域内物联网网关启动所述分布式共识机制，将所述身份认证结果和所述合法数字串发送至域内其它的物联网网关。

进一步地，包括身份认证单元、计算单元和数字串验证单元；

所述身份认证单元，用于域内所有的物联网网关验证接收到的所述身份认证结果与本物联网网关生成的认证结果是否相同，若不同，则不认可所述身份认证结果，丢弃所述身份认证结果，执行所述计算单元，若相同，则执行所述数字串验证单元；

所述计算单元，用于计算与所述分布式共识机制相符合的所述合法数字串，计算完成后，启动所述分布式共识机制，将本物联网网关的认证结果和所述合法数字串发送至域内所有的物联网网关，执行所述身份认证单元；

所述数字串验证单元，用于验证所述合法数字串是否符合所述分布式共识机制规定的条件，若不符合，则执行所述计算单元，若符合，通过所述分布式共识机制和所述节点同步机制对所述身份认证结果和所述合法数字串达成共识，将所述身份认证结果写入区块进行存储，生成所述区块链。

进一步地，所述节点同步机制为域内所有的物联网网关在对所述身份认证结果和所述合法数字串进行验证时，域内所有的物联网网关的区块链进行信息交互，将所述区块链进行同步存储。

本申请反馈附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本申请反馈的实践了解到。

附图说明

本申请反馈上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

图 1 为根据本申请反馈一个实施例的物联网场景下跨域逻辑强隔离与安全访问控制方法流程图；

图 2 为根据本申请反馈一个实施例的物联网网关发送的请求发布数据包结构示意图；

图 3 为根据本申请反馈一个实施例的广播身份认证结果数据包的示意图；

图 4 为根据本申请反馈另一个实施例的物联网场景下跨域逻辑强隔离与安全访问控制方法流程图；

图 5 为根据本申请反馈一个实施例的记录身份认证结果的区块链结构示意图；

图 6 为根据本申请反馈一个实施例的物联网场景下跨域逻辑强隔离与安全访问控制方法的系统结构图；

图 7 为根据本申请反馈又一个实施例的物联网场景下跨域逻辑强隔离与安全访问控制方法流程图；

图 8 为根据本申请反馈一个实施例的物联网场景下跨域逻辑强隔离与安全访问控制装置结构示意图。

具体实施方式

下面详细描述本申请反馈的实施例，实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本申请反馈，而不能理解为对本申请反馈的限制。

下面参照附图描述根据本申请反馈实施例提出的物联网场景下跨域逻辑强隔离与

安全访问控制方法及装置。

首先将参照附图描述根据本申请反馈实施例提出的物联网场景下跨域逻辑强隔离与安全访问控制方法。

图 1 为根据本申请反馈一个实施例的物联网场景下跨域逻辑强隔离与安全访问控制方法流程图。

如图 1 所示，该物联网场景下跨域逻辑强隔离与安全访问控制方法包括以下步骤：

步骤 S1，域内目标物联网网关获取域外主机的身份认证请求，将身份认证请求封装为请求发布数据包，并以广播的方式发送请求发布数据包至域内其它的物联网网关。

具体地，域内的物联网网关自组成网，域内的某台物联网网关收到域外的主机的身份认证请求后，将身份认证请求中携带的信息封装到请求发布数据包中，并以广播的方式将请求发布数据包发送给域内的其它的物联网网关，共享该身份认证请求的信息。

比如，域内物联网有 A、B、C、D 和 E 共 5 个网关组成，网关 A 收到一个身份认证请求 R，将 R 中携带的信息进行封装后发送给 B、C、D 和 E，5 个网关共同对该身份认证请求 R 进行处理。

如图 2 所示，展示了物联网网关发送的请求发布数据包结构，其中，时间戳 Timestamp 字段 128 位，表示本消息发送的时刻；消息类型 MsgType 字段 64 位，表明消息类型；ID 字段 128 位，填写发送本消息的物联网网关的独有编码；认证信息 AuthInfo 字段 4096 位，填写身份认证信息。

步骤 S2，域内所有的物联网网关对请求发布数据包进行认证以生成身份认证结果。

具体地，域内其它的物联网网关收到域内目标物联网网关发送的携带身份认证请求信息的请求发布数据包后，通过预先设定的方式对请求发布数据包进行认证，生成身份认证结果。

对请求数据包进行认证有多种方式，作为一种可能实现的方式，域内所有的物联网网关可以在接收到请求发布数据包后，提取请求发布数据包中的身份信息，并根据本地存储的合法身份证书对身份信息进行认证生成身份认证结果。

需要说明的是，域内所有的物联网网关都对请求发布数据包进行认证，生成身份认证结果，多个身份认证结果可以相同，也可以不相同。并且每个物联网网关的计算速度不同，多个物联网网关先后计算出多个身份认证结果。

比如，根据上述的实施例，A、B、C、D 和 E，5 个物联网网关都对请求发布数据包进行认证，生成对应的 5 个身份认证结果，5 个身份认证结果可以相同，也可以不相同。

步骤 S3，域内任一物联网网关生成身份认证结果后，启动分布式共识机制，并计算与

分布式共识机制相符合的合法数字串，将身份认证结果和合法数字串发送至域内其它的物联网网关。

具体地，由于物联网网关的计算速度有差异，因此，首先计算出身份认证结果的域内任一物联网网关，启动分布式共识机制将计算出的身份认证结果在域内广播至域内除自身外的其它物联网网关，在广播身份认证结果之前，还要计算与分布式共识机制相符合的合法数字串，将身份认证结果和合法数字串一同在域内广播至其它的物联网网关。

需要说明的是，域内任一物联网网关生成身份认证结果后，若在计算出与分布式共识机制相符合的合法数字串之前，域内另一物联网网关先计算出身份认证结果和合法数字串，则由另一域内物联网网关启动所述分布式共识机制，将身份认证结果和所述合法数字串发送至域内其它的物联网网关。

可以理解的是，域内所有的物联网网关都在计算身份认证结果与分布式共识机制相符的合法数字串，首先计算出二者的物联网网关才可以将身份认证结果和合法数字串发送至其它物联网网关。

举例而言，根据上述的实施例， 比如，A、B、C、D 和 E，5 个物联网网关都生成身份认证结果，其中，C 首先生成身份认证结果，再计算合法数字串，在 C 完成合法数字串的计算时，其它 4 个物联网网关都没有完成合法数字串的计算，则 C 启动分布式机制，将 C 生成的身份认证结果和合法数字串在域内以广播的方式发送给 A、B、D 和 E，4 个物联网网关。

又如，A、B、C、D 和 E，5 个物联网网关都生成身份认证结果，其中，C 首先生成身份认证结果，在 C 计算合法数字串的过程中，E 生成身份认证结果后，在 C 之前计算出符合分布式共识机制的合法数字串，则 E 启动分布式共识机制，将 E 生成的身份认证结果和合法数字串在域内以广播的方式发送给 A、B、C 和 D，4 个物联网网关。

如图 3 所示，展示了认证完成且得出合法数字串的物联网网关发送的广播数据包结构，广播数据包中包括身份认证结果和合法数字串，其中，时间戳 Timestamp 字段 128 位，表示本消息发送的时刻；消息类型 MsgType 字段 64 位，表明消息类型；ID 字段 128 位，填写发送本消息的物联网网关的独有编码；数字字串 NumString 字段 1024 位，填写本物联网网关得到的符合分布式共识机制规定的合法数字串；认证结果 AuthResult 字段长度可变，最短不低于 128 位，最长不超过 3776 位，填写本物联网网关得到的身份认证结果。

步骤 S4，域内其它的物联网网关通过分布式共识机制和节点同步机制对身份认证结果和合法数字串进行验证达成共识，将身份认证结果写入区块进行存储，生成区块链。

可以理解的是，在每个物联网网关内都存在身份认证结果和合法数字串后，通过分布式共识机制和节点同步机制对二者进行验证，验证通过后才认可身份认证结果。

其中，分布式共识机制有很多种，具体使用哪种分布式共识机制不做限定，区块链也有自身的节点同步机制，节点之间通过节点同步机制可以将各自存储的区块链统一起来，不同的区块链系统的同步机制可能有所不同，具体使用哪种节点同步机制不做限定，比如可以使用比特币区块链中的初始化区块下载（Initial Block Download，IBD）同步机制，也可使用其它节点同步机制。

作为一种可能实现的方式，分布式共识机制采用工作量证明的方式（Proof of Work，PoW），如图 4 所示，步骤 S4 具体包括：

S41，域内所有的物联网网关验证接收到的身份认证结果与本物联网网关生成的认证结果是否相同，若不同，则不认可身份认证结果，丢弃身份认证结果，执行 S42，若相同，则执行 S43；

S42，计算与分布式共识机制相符合的合法数字串，计算完成后，启动分布式共识机制，将本物联网网关的认证结果和合法数字串发送至域内所有的物联网网关，执行 S41；

S43，验证合法数字串是否符合分布式共识机制规定的条件，若不符合，则执行 S42，若符合，通过分布式共识机制和节点同步机制对身份认证结果和合法数字串达成共识，将身份认证结果写入区块进行存储，生成区块链。

具体地，和通常的 PoW（工作量证明）分布式共识机制相比，当某个物联网网关计算出 PoW 所需的合法数字串后，该网关需要将其得到的身份认证结果和该合法数字串一同在域内广播。其它物联网网关接收到该广播后，首先核对该广播数据包中的身份认证结果是否与本网关得到的身份认证结果相同，若不同，则直接丢弃该数据包；若相同，则验证合法数字串是否符合 PoW 规定的条件。只有广播数据包中的身份认证结果与本网关得到的身份认证结果相同并且广播数据包携带的合法数字串符合特定条件时，本物联网网关才认可身份认证结果和合法数字串对应的物联网网关生成新的区块，最终将其链接到域内的区块链中。

举例而言，根据上述的实施例，A、B、D、E 收到 C 发送的身份认证结果和合法数字串后，进行验证，比如，A 验证 C 发送的身份认证结果与本网关生成的身份认证结果是否相同，若相同，则再验证合法数字串，若合法数字串也符合要求，则认可 C 将该身份认证结果写入区块，存入区块链，并结束合法数字串的计算；若 A 验证 C 发送的身份认证结果与本网关生成的身份认证结果不相同，则丢弃该身份认证结果，继续计算合法数字串，计算完成后启动分布式共识机制，过程如上述的实施例，不做赘述；若 A 验证 C 发送的身份认证结果与本网关生成的身份认证结果相同，但合法数字串不符合要求，则计算合法数字串，计算完成后启动分布式共识机制，过程如上述实施例，不做赘述。B、D 和 E 同理进行验证，不做赘述。

需要说明的是，域内所有的物联网网关在对身份认证结果和合法数字串进行验证时，域内所有的物联网网关的区块链进行信息交互，将区块链进行同步存储，由此，可以对身份认证结果达成共识，生成区块，写入区块链。

如图 5 所示，展示了记录身份认证结果的区块链结构示意图，其中，前一区块 ID、当前区块 ID、时间戳和随机数都是当前主流区块链系统中区块结构的固有内容，其中前一区块 ID 表示本区块所链接的前一区块的 ID，当前区块 ID 表示本区块的 ID，每个区块的 ID 都是全网唯一的；时间戳表示本区块生成的时刻，随机数是生成本区块的物联网网关得出的符合 PoW 规定的数字串。DataRecord 部分记录了与身份认证相关的数据记录，这些数据记录可以是网络状态、主机信息和身份认证的日志记录等。区块链中的数据记录对于域内的物联网网关而言是公开透明的，且一旦写入区块链就无法被篡改。

步骤 S5，域内目标物联网网关扫描本地通过节点同步机制同步更新并存储的区块链是否存在身份认证结果，若存在，则将身份认证结果发送给域外主机，若不存在，则继续扫描。

具体地，在进行验证的过程中，接收到身份认证请求的物联网网关持续扫描本地通过节点同步机制同步更新并存储的区块链，当确认区块链中的区块上包含对身份认证请求的认证结果后，将区块中的身份认证结果反馈给发送身份认证该请求的域外主机。

可以理解的是，不同的分布式共识机制和节点同步机制在生成区块链时有所差异，作为一种可能实现的方式，比如，若采用比特币区块链的分布式共识机制以及比特币区块链的节点同步机制，在扫描时，如果含有该身份认证结果的区块已经在链上并且其该区块后已经链接了 6 个其它区块，则说明该身份认证结果已经被域内的大多数网关认可，则将身份认证结果返回给发送身份认证请求的域外网关；否则，持续扫描区块链。

进一步地，域内的物联网网关互联成网，共享本域内所有合法主机的身份证书，克服当前物联网场景中，单物联网网关访问控制机制在安全性不足方面的问题，具有高安全性、公开透明和可追溯的特点。

如图 6 所示，用户（域外主机）向物联网网关发起身份认证请求，域内的物联网网关通过分布式共识机制对身份认证结果达成共识，并将认证结果以区块链的形式存储起来。

在上述实施例中，采用工作量证明（Power of Work）机制达成共识，即物联网网关利用散列算法计算进行大量尝试，生成一串难于计算但易于验证的数字。所谓难于计算，是指物联网网关通常需要经过大量计算才能计算出一个符合条件的数字串；所谓易于验证，是指其它物联网网关可以很容易的验证这个数字串是否符合特定的条件。在这个过程中，因为需要不断尝试不同的随机数，物联网网关需要付出一定的计算资源才能得到符合条件的字符串进而形成新区块，并链接至区块链中。物联网网关的工作量越大（计算时间越长、

计算次数越多），就越有可能计算生成新的区块，保证了入侵者只有劫持超过 50%的计算资源才有可能篡改身份认证结果。另外，所有成功链接至区块链中的区块都是不可篡改的，也都是所有物联网网关公开可见且获得所有物联网网关认可的。

以一个具体实施例对物联网场景下跨域逻辑强隔离与安全访问控制方法详细说明，如图 7 所示，物联网网关 1 接收到某主机 H 发送的身份认证请求 R。物联网网关 1 将身份认证请求 R 中携带的身份信息封装到请求发布数据包中，并将该请求发布数据包发送给域内的其它物联网网关。

域内的物联网网关接收到请求发布数据包后，提取数据包内携带的身份信息，并根据本地存储的合法身份证书对该身份信息进行认证。

当物联网网关得到认证结果后，即开始启动分布式共识机制。假设物联网网关采用工作量证明（Proof of Work，PoW）作为分布式共识机制。假设物联网网关 3 最先计算得到符合 PoW 规定的合法数字串。

当物联网网关 3 计算出 PoW 所需的合法数字串后，该网关将其得到的身份认证结果和该数字串封装在广播数据包中，发送给域内的其它物联网网关。其余物联网网关接收到该广播后，首先核对广播数据包中的身份认证结果是否与本网关得到的身份认证结果相同，若不同，则直接丢弃该数据包，同时继续计算数字串，进行分布式共识机制；若相同，则验证数字串是否符合 PoW 规定的条件；若不符合条件，则继续计算数字串，进行分布式共识机制；只有广播数据包中的身份认证结果与本网关得到的身份认证结果相同并且广播数据包携带的数字串符合特定条件时，本物联网网关才认可由物联网网关 3 生成新的区块，停止计算符合条件的数字串，该区块最终链接到域内的区块链中。

在此过程中，接收到身份认证请求的物联网网关 1 持续扫描域内的区块链，当确认区块链中的区块上包含对身份认证请求 R 的认证结果后，将区块中的身份认证结果反馈给 R 的发送者。

根据上述的实施例，物联网场景下跨域逻辑强隔离与安全访问控制方法面向物联网场景，将传统访问控制方案中的单个节点进行认证的模式，扩展为由域中的所有物联网网关通过分布式共识机制完成认证。理论上，只有当域中超过 50%的计算资源都被劫持时，才会导致域内的物联网设备受到安全威胁。实现了跨域强逻辑隔离，有效提升了系统安全性。

根据本申请反馈实施例提出的物联网场景下跨域逻辑强隔离与安全访问控制方法，当某台物联网网关接收到身份认证请求后，将此认证请求发布给域内的其它物联网网关，域内的物联网网关分别对此发送此请求的主机进行身份认证，并以分布式共识机制对身份认证的结果达成共识。由此，域内的物联网网关以分布式共识机制进行访问控制，实现跨域逻辑强隔离，有效提升了物联网系统的安全性，并且身份认证结果以区块形式存储，便于

检索查阅，具有公开透明和可追溯的特性。

其次参照附图描述根据本申请反馈实施例提出的物联网场景下跨域逻辑强隔离与安全访问控制装置。

图 8 为根据本申请反馈一个实施例的物联网场景下跨域逻辑强隔离与安全访问控制装置结构示意图。

如图 8 所示，该物联网场景下跨域逻辑强隔离与安全访问控制装置包括：获取模块 100、生成模块 200、发送模块 300、验证模块 400 和扫描模块 500。

其中，获取模块 100，用于域内目标物联网网关获取域外主机的身份认证请求，将身份认证请求封装为请求发布数据包，并以广播的方式发送请求发布数据包至域内其它的物联网网关。

生成模块 200，用于域内所有的物联网网关对请求发布数据包进行认证以生成身份认证结果。

发送模块 300，用于域内任一物联网网关生成身份认证结果后，启动分布式共识机制，并计算与分布式共识机制相符合的合法数字串，将身份认证结果和合法数字串发送至域内其它的物联网网关。

验证模块 400，用于域内其它的物联网网关通过分布式共识机制和节点同步机制对身份认证结果和合法数字串进行验证达成共识，将身份认证结果写入区块进行存储，生成区块链。

扫描模块 500，用于域内目标物联网网关扫描本地通过节点同步机制同步更新并存储的区块链是否存在身份认证结果，若存在，则将身份认证结果发送给域外主机，若不存在，则继续扫描。

该装置克服了单认证节点方案存在的弊端，具有高安全性、透明和可追溯等特点。

进一步地，生成模块，具体用于，

域内所有的物联网网关接收到请求发布数据包后，提取请求发布数据包中的身份信息，并根据本地存储的合法身份证书对身份信息进行认证生成身份认证结果。

进一步地，发送模块，还用于，

域内任一物联网网关生成身份认证结果后，若在计算出与分布式共识机制相符合的合法数字串之前，域内另一物联网网关计算出身份认证结果和合法数字串，则由另一域内物联网网关启动分布式共识机制，将身份认证结果和合法数字串发送至域内其它的物联网网关。

进一步地，包括身份认证单元、计算单元和数字串验证单元；

身份认证单元，用于域内所有的物联网网关验证接收到的身份认证结果与本物联网网

关生成的认证结果是否相同，若不同，则不认可身份认证结果，丢弃身份认证结果，执行计算单元，若相同，则执行数字串验证单元；

计算单元，用于计算与分布式共识机制相符合的合法数字串，计算完成后，启动分布式共识机制，将本物联网网关的认证结果和合法数字串发送至域内所有的物联网网关，执行身份认证单元；

数字串验证单元，用于验证合法数字串是否符合分布式共识机制规定的条件，若不符合，则执行计算单元，若符合，通过分布式共识机制和节点同步机制对身份认证结果和合法数字串达成共识，将身份认证结果写入区块进行存储，生成区块链

进一步地，节点同步机制为域内所有的物联网网关在对身份认证结果和合法数字串进行验证时，域内所有的物联网网关的区块链进行信息交互，将区块链进行同步存储。

需要说明的是，前述对物联网场景下跨域逻辑强隔离与安全访问控制方法实施例的解释说明也适用于该实施例的装置，此处不再赘述。

根据本申请反馈实施例提出的物联网场景下跨域逻辑强隔离与安全访问控制装置，当某台物联网网关接收到身份认证请求后，将此认证请求发布给域内的其它物联网网关，域内的物联网网关分别对此发送此请求的主机进行身份认证，并以分布式共识机制对身份认证的结果达成共识。由此，域内的物联网网关以分布式共识机制进行访问控制，实现跨域逻辑强隔离，有效提升了物联网系统的安全性，并且身份认证结果以区块形式存储，便于检索查阅，具有公开透明和可追溯的特性。

在本申请反馈的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“长度”、“宽度”、“厚度”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”“内”、“外”、“顺时针”、“逆时针”、“轴向”、“径向”、“周向”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本申请反馈和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本申请反馈的限制。

此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本申请反馈的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

在本申请反馈中，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”、“固定”等术语应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或成一体；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通或两个元件的相互作用关系，除非另有明确的限定。对于本领域的普通

技术人员而言，可以根据具体情况理解上述术语在本申请反馈中的具体含义。

在本申请反馈中，除非另有明确的规定和限定，第一特征在第二特征 “上”或“下”可以是第一和第二特征直接接触，或第一和第二特征通过中间媒介间接接触。而且，第一特征在第二特征“之上”、“上方”和“上面”可是第一特征在第二特征正上方或斜上方，或仅仅表示第一特征水平高度高于第二特征。第一特征在第二特征“之下”、“下方”和“下面”可以是第一特征在第二特征正下方或斜下方，或仅仅表示第一特征水平高度小于第二特征。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、 “示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请反馈的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

尽管上面已经示出和描述了本申请反馈的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本申请反馈的限制，本领域的普通技术人员在本申请反馈的范围内可以对上述实施例进行变化、修改、替换和变型。

权利要求书

1、一种物联网场景下跨域逻辑强隔离与安全访问控制方法，其特征在于，包括以下步骤：

S1，域内目标物联网网关获取域外主机的身份认证请求，将所述身份认证请求封装为请求发布数据包，并以广播的方式发送所述请求发布数据包至域内其它的物联网网关；

S2，域内所有的物联网网关对所述请求发布数据包进行认证以生成身份认证结果；

S3，域内任一物联网网关生成所述身份认证结果后，启动分布式共识机制，并计算与所述分布式共识机制相符合的合法数字串，将所述身份认证结果和所述合法数字串发送至域内其它的物联网网关；

S4，域内其它的物联网网关通过所述分布式共识机制和节点同步机制对所述身份认证结果和所述合法数字串进行验证达成共识，将所述身份认证结果写入区块进行存储，生成区块链；

S5，所述域内目标物联网网关扫描本地通过所述节点同步机制同步更新并存储的所述区块链是否存在所述身份认证结果，若存在，则将所述身份认证结果发送给所述域外主机，若不存在，则继续扫描。

2、根据权利要求 1 所述的方法，其特征在于，所述域内所有的物联网网关对所述请求发布数据包进行认证生成身份认证结果，包括：

域内所有的物联网网关接收到所述请求发布数据包后，提取所述请求发布数据包中的身份信息，并根据本地存储的合法身份证书对所述身份信息进行认证生成身份认证结果。

3、根据权利要求 1 所述的方法，其特征在于，所述 S3，还包括：所述域内任一物联网网关生成所述身份认证结果后，若在计算出与所述分布式共识机制相符合的合法数字串之前，域内另一物联网网关计算出所述身份认证结果和所述合法数字串，则由另一域内物联网网关启动所述分布式共识机制，将所述身份认证结果和所述合法数字串发送至域内其它的物联网网关。

4、根据权利要求 1 所述的方法，其特征在于，所述 S4，进一步包括：

S41，域内所有的物联网网关验证接收到的所述身份认证结果与本物联网网关生成的认证结果是否相同，若不同，则不认可所述身份认证结果，丢弃所述身份认证结果，执行 S42，若相同，则执行 S43；

S42，计算与所述分布式共识机制相符合的所述合法数字串，计算完成后，启动所述分布式共识机制，将本物联网网关的认证结果和所述合法数字串发送至域内所有的物联网网关，执行 S41；

S43，验证所述合法数字串是否符合所述分布式共识机制规定的条件，若不符合，则执行 S42，若符合，通过所述分布式共识机制和所述节点同步机制对所述身份认证结果和所述合法数字串达成共识，将所述身份认证结果写入区块进行存储，生成所述区块链。

5、根据权利要求 4 所述的方法，其特征在于，所述节点同步机制为域内所有的物联网网关在对所述身份认证结果和所述合法数字串进行验证时，域内所有的物联网网关的区块链进行信息交互，将所述区块链进行同步存储。

6、一种物联网场景下跨域逻辑强隔离与安全访问控制装置，其特征在于，包括：

获取模块，用于域内目标物联网网关获取域外主机的身份认证请求，将所述身份认证请求封装为请求发布数据包，并以广播的方式发送所述请求发布数据包至域内其它的物联网网关；

生成模块，用于域内所有的物联网网关对所述请求发布数据包进行认证以生成身份认证结果；

发送模块，用于域内任一物联网网关生成所述身份认证结果后，启动分布式共识机制，并计算与所述分布式共识机制相符合的合法数字串，将所述身份认证结果和所述合法数字串发送至域内其它的物联网网关；

验证模块，用于域内其它的物联网网关通过所述分布式共识机制和节点同步机制对所述身份认证结果和所述合法数字串进行验证达成共识，将所述身份认证结果写入区块进行存储，生成区块链；

扫描模块，用于所述域内目标物联网网关扫描本地通过所述节点同步机制同步更新并存储的所述区块链是否存在所述身份认证结果，若存在，则将所述身份认证结果发送给所述域外主机，若不存在，则继续扫描。

7、根据权利要求 6 所述的装置，其特征在于，所述生成模块，具体用于，

域内所有的物联网网关接收到所述请求发布数据包后，提取所述请求发布数据包中的身份信息，并根据本地存储的合法身份证书对所述身份信息进行认证生成身份认证结果。

8、根据权利要求 6 所述的装置，其特征在于，所述发送模块，还用于，

所述域内任一物联网网关生成所述身份认证结果后，若在计算出与所述分布式共识机制相符合的合法数字串之前，域内另一物联网网关计算出所述身份认证结果和所述合法数字串，则由另一域内物联网网关启动所述分布式共识机制，将所述身份认证结果和所述合法数字串发送至域内其它的物联网网关。

9、根据权利要求 6 所述的装置，其特征在于，所述验证模块，包括身份认证单元、计算单元和数字串验证单元；

所述身份认证单元，用于域内所有的物联网网关验证接收到的所述身份认证结果与本

物联网网关生成的认证结果是否相同，若不同，则不认可所述身份认证结果，丢弃所述身份认证结果，执行所述计算单元，若相同，则执行所述数字串验证单元；

所述计算单元，用于计算与所述分布式共识机制相符合的所述合法数字串，计算完成后，启动所述分布式共识机制，将本物联网网关的认证结果和所述合法数字串发送至域内所有的物联网网关，执行所述身份认证单元；

所述数字串验证单元，用于验证所述合法数字串是否符合所述分布式共识机制规定的条件，若不符合，则执行所述计算单元，若符合，通过所述分布式共识机制和所述节点同步机制对所述身份认证结果和所述合法数字串达成共识，将所述身份认证结果写入区块进行存储，生成所述区块链。

10、根据权利要求 9 所述的装置，其特征在于，所述节点同步机制为域内所有的物联网网关在对所述身份认证结果和所述合法数字串进行验证时，域内所有的物联网网关的区块链进行信息交互，将所述区块链进行同步存储。

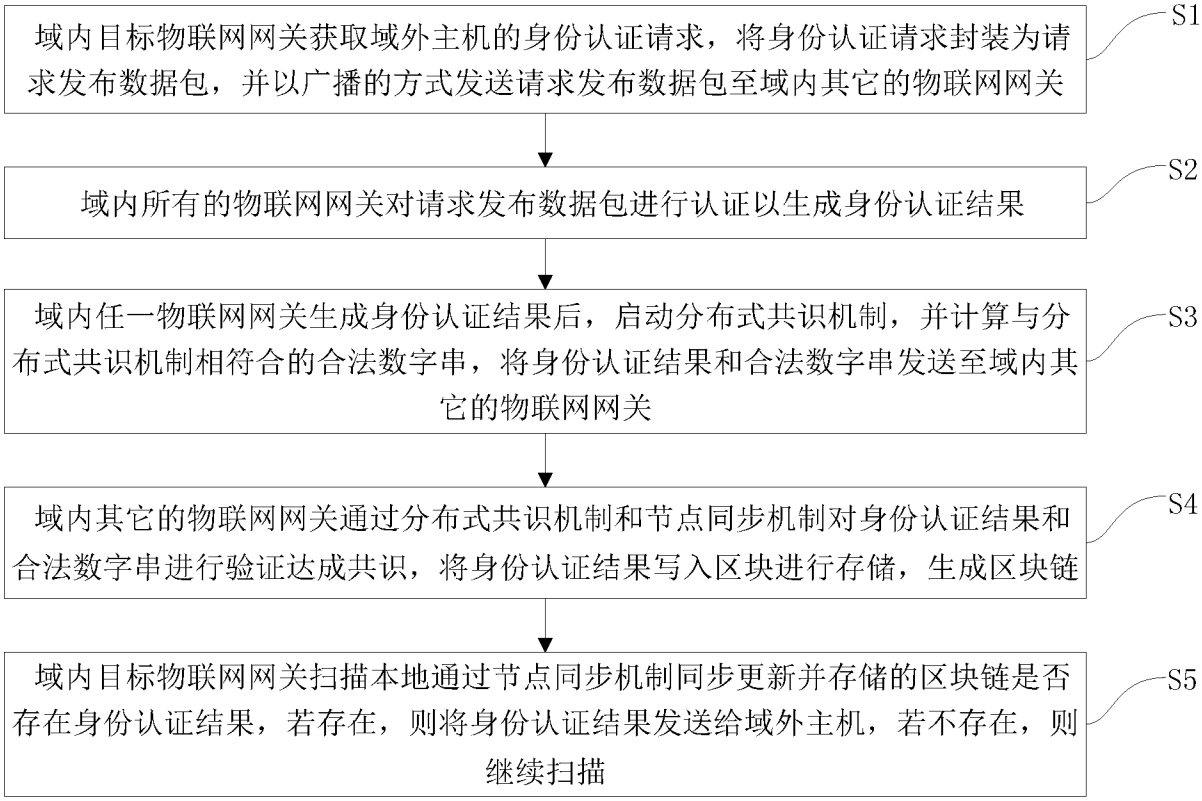
域内目标物联网网关获取域外主机的身份认证请求，将身份认证请求封装为请求发布数据包，并以广播的方式发送请求发布数据包至域内其它的物联网网关
S1
域内所有的物联网网关对请求发布数据包进行认证以生成身份认证结果
S2
域内任一物联网网关生成身份认证结果后，启动分布式共识机制，并计算与分布式共识机制相符合的合法数字串，将身份认证结果和合法数字串发送至域内其它的物联网网关
S3
域内其它的物联网网关通过分布式共识机制和节点同步机制对身份认证结果和合法数字串进行验证达成共识，将身份认证结果写入区块进行存储，生成区块链
S4
域内目标物联网网关扫描本地通过节点同步机制同步更新并存储的区块链是否存在身份认证结果，若存在，则将身份认证结果发送给域外主机，若不存在，则继续扫描
S5

图 1

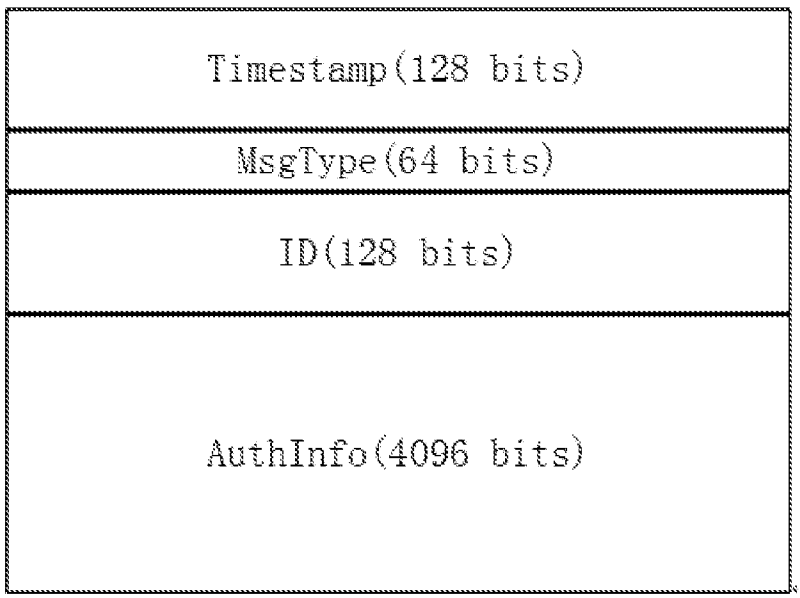
Timestamp(128 bits)
MsgType(64 bits)
ID(128 bits)
AuthInfo(4096 bits)

图 2

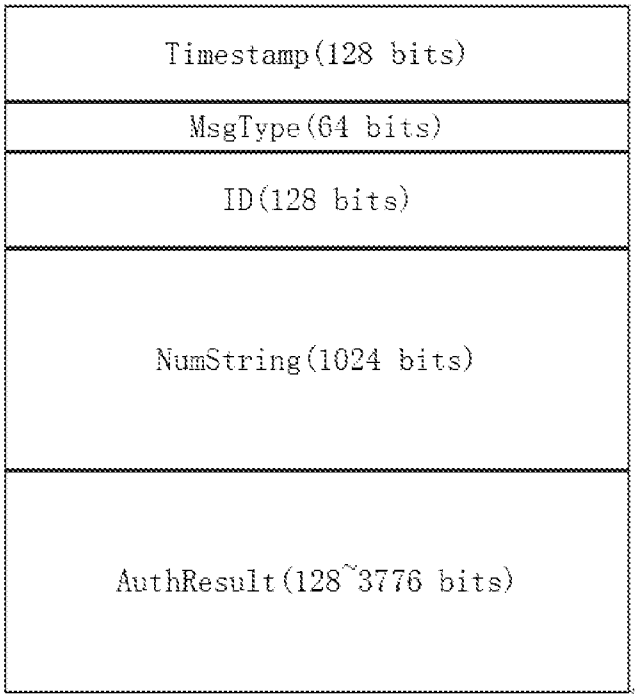
Timestamp(128 bits)
MsgType(64 bits)
ID(128 bits)
NumString(1024 bits)
AuthResult(128~3776 bits)

图 3

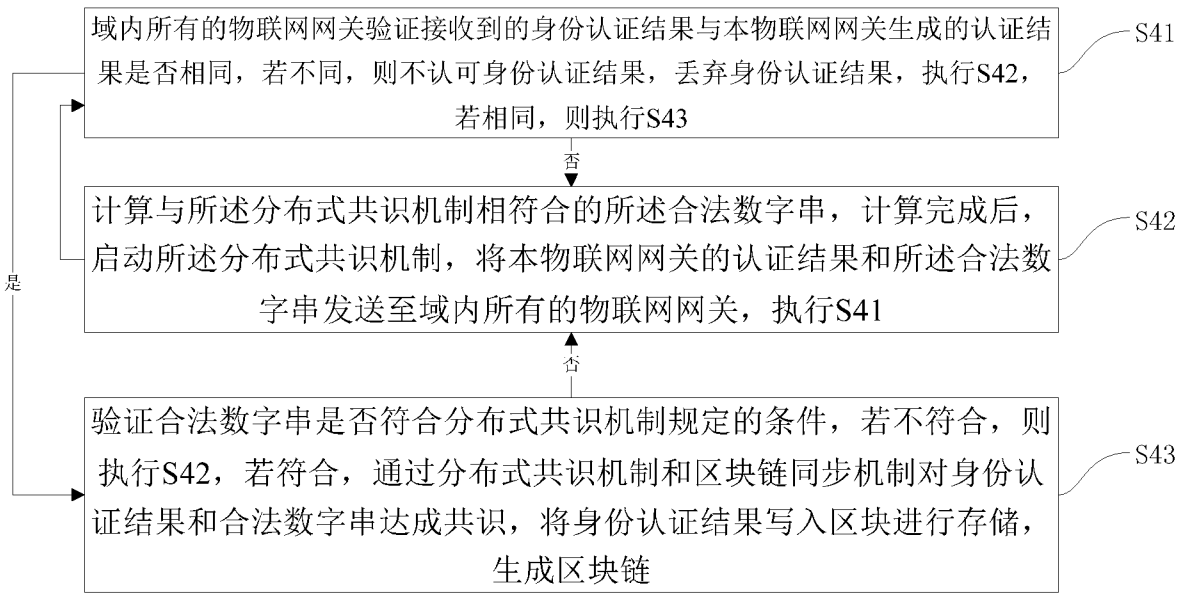
域内所有的物联网网关验证接收到的身份认证结果与本物联网网关生成的认证结果是否相同，若不同，则不认可身份认证结果，丢弃身份认证结果，执行S42，若相同，则执行S43
S41
否
计算与所述分布式共识机制相符合的所述合法数字串，计算完成后，启动所述分布式共识机制，将本物联网网关的认证结果和所述合法数字串发送至域内所有的物联网网关，执行S41
S42
是
否
验证合法数字串是否符合分布式共识机制规定的条件，若不符合，则执行S42，若符合，通过分布式共识机制和区块链同步机制对身份认证结果和合法数字串达成共识，将身份认证结果写入区块进行存储，生成区块链
S43

图 4

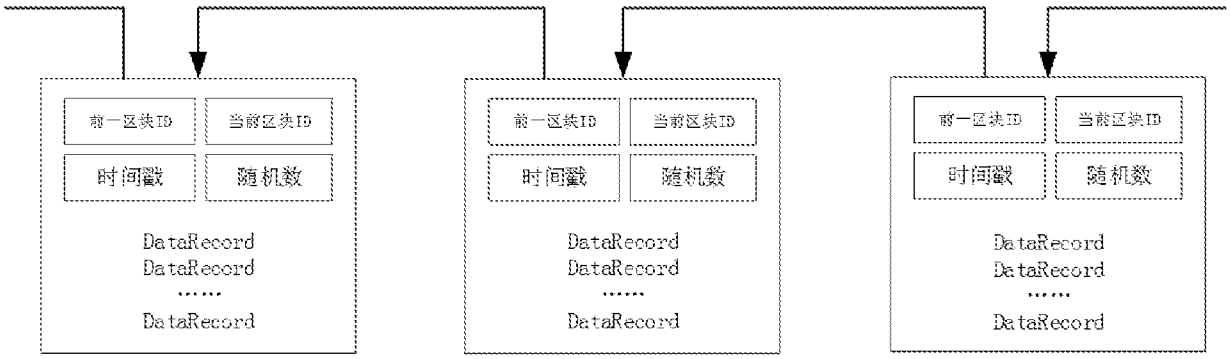
前一区块ID
当前区块ID
时间戳
随机数
DataRecord
DataRecord
……
DataRecord
前一区块ID
当前区块ID
时间戳
随机数
DataRecord
DataRecord
……
DataRecord
前一区块ID
当前区块ID
时间戳
随机数
DataRecord
DataRecord
……
DataRecord

图 5

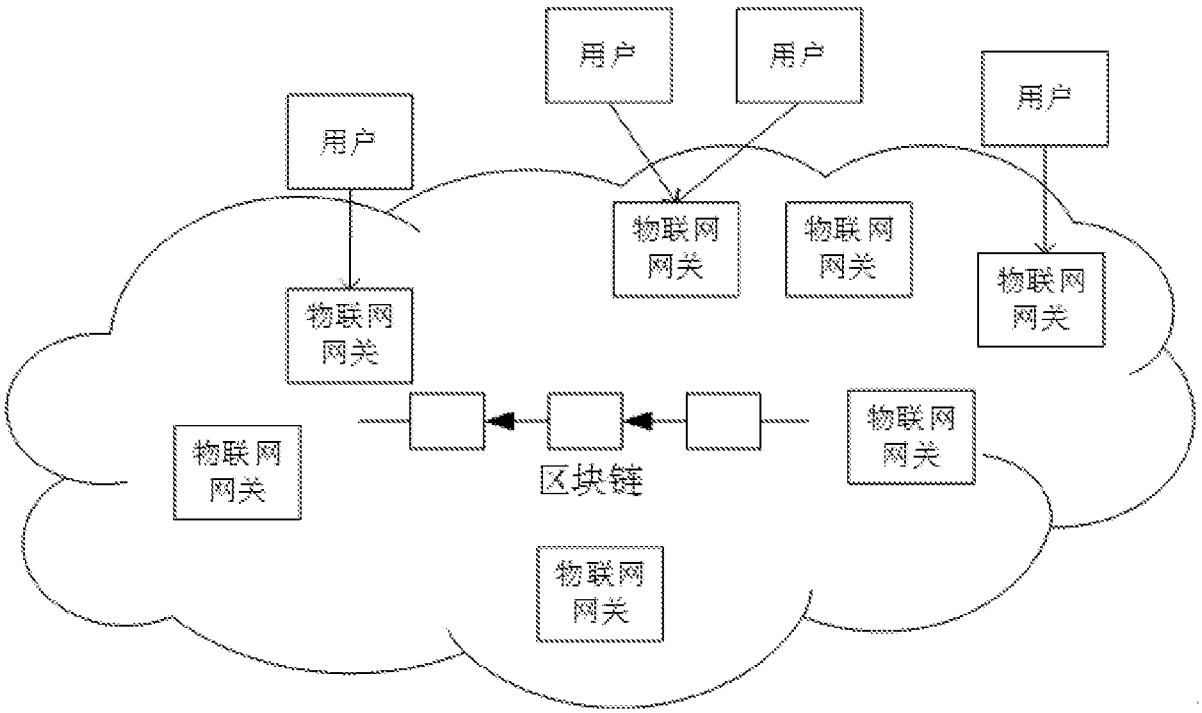
用户
用户
用户
用户
物联网网关
物联网网关
物联网网关
物联网网关
物联网网关
物联网网关
区块链

图 6

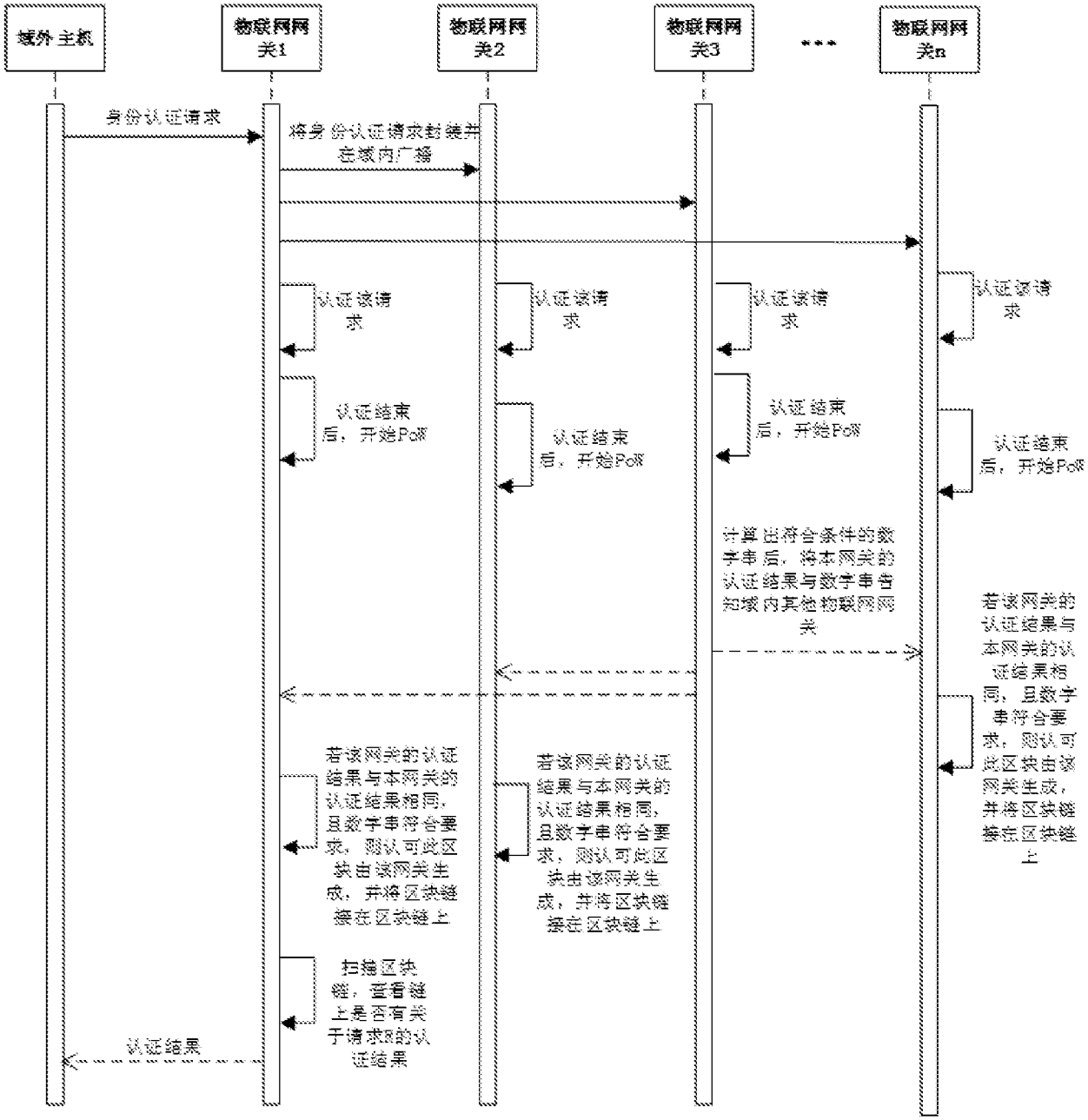
域外主机
物联网网关1
物联网网关2
物联网网关3
...
物联网网关n
身份认证请求
将身份认证请求封装并在域内广播
认证该请求
认证结束后，开始PoW
计算出符合条件的数字串后，将本网关的认证结果与数字串告知域内其他物联网网关
若该网关的认证结果与本网关的认证结果相同，且数字串符合要求，则认可此区块由该网关生成，并将区块链接在区块链上
扫描区块链，查看链上是否有关于请求R的认证结果
认证结果

图 7

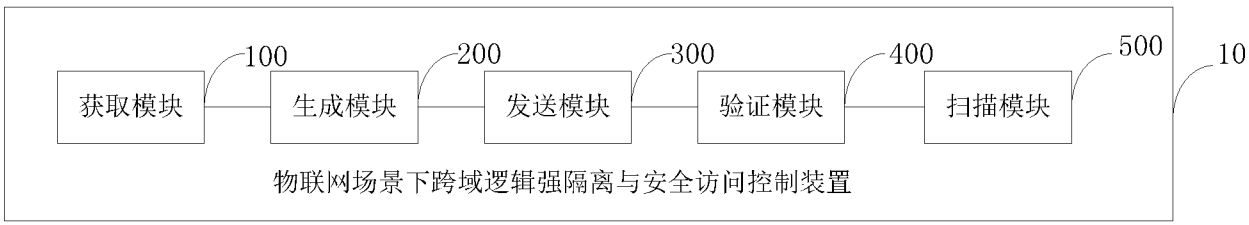
100
200
300
400
500
10
获取模块
生成模块
发送模块
验证模块
扫描模块
物联网场景下跨域逻辑强隔离与安全访问控制装置

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/114985

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)

H04W; 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)

WPI, EPODOC, CNKI, CNPAT: 分布, 域, 共识, 组播, 广播, IOT, 物联网, 区块链, 认证, consensus, broadcast, groupcast, blockchain, block chain, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109981689 A (TSINGHUA UNIVERSITY) 05 July 2019 (2019-07-05) decription, paragraphs [0004]-[0040], and claims 1-10	1-10
X	CN 109495516 A (STATE GRID JIANGSU ELECTRIC POWER CO., LTD. WUXI POWER SUPPLY CO.) 19 March 2019 (2019-03-19) description, paragraph [0016]	1-10
A	CN 108964924 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 07 December 2018 (2018-12-07) entire document	1-10
A	US 2018302222 A1 (SAMSUNG ELECTRONICS CO., LTD.) 18 October 2018 (2018-10-18) entire document	1-10
A	US 2018225661 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC) 09 August 2018 (2018-08-09) entire document	1-10

☐ 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	Date of mailing of the international search report
09 January 2020	**01 February 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/114985

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109981689 A	05 July 2019	None	
CN 109495516 A	19 March 2019	None	
CN 108964924 A	07 December 2018	None	
US 2018302222 A1	18 October 2018	WO 2018194368 A1	25 October 2018
US 2018225661 A1	09 August 2018	US 2018227275 A1	09 August 2018
		CN 110268691 A	20 September 2019
		CN 110249333 A	17 September 2019
		EP 3580905 A1	18 December 2019
		US 2018225448 A1	09 August 2018
		CN 110300973 A	01 October 2019
		EP 3580682 A1	18 December 2019
		EP 3580683 A1	18 December 2019
		WO 2018148069 A1	16 August 2018
		WO 2018148068 A1	16 August 2018
		WO 2018148067 A1	16 August 2018

国际检索报告

国际申请号
PCT/CN2019/114985

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)

H04W; 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））

WPI, EPODOC, CNKI, CNPAT:分布，域,共识,组播,广播,IOT，物联网,区块链,认证,consensus，broadcast，groupcast,blockchain,block chain,authentication

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 109981689 A (清华大学) 2019年 7月 5日 (2019-07-05) 说明书第[0004]-[0040]段，权利要求1-10	1-10
X	CN 109495516 A (国网江苏省电力有限公司无锡供电分公司) 2019年 3月 19日 (2019-03-19) 说明书第[0016]段	1-10
A	CN 108964924 A (腾讯科技深圳有限公司) 2018年 12月 7日 (2018-12-07) 全文	1-10
A	US 2018302222 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2018年 10月 18日 (2018-10-18) 全文	1-10
A	US 2018225661 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC) 2018年 8月 9日 (2018-08-09) 全文	1-10

☐ 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	国际检索报告邮寄日期
2020年 1月 9日	2020年 2月 1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	受权官员 陈红英 电话号码 86-(10)-53961636

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/114985

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	109981689	A	2019年 7月 5日	无			
CN	109495516	A	2019年 3月 19日	无			
CN	108964924	A	2018年 12月 7日	无			
US	2018302222	A1	2018年 10月 18日	WO	2018194368	A1	2018年 10月 25日
US	2018225661	A1	2018年 8月 9日	US	2018227275	A1	2018年 8月 9日
				CN	110268691	A	2019年 9月 20日
				CN	110249333	A	2019年 9月 17日
				EP	3580905	A1	2019年 12月 18日
				US	2018225448	A1	2018年 8月 9日
				CN	110300973	A	2019年 10月 1日
				EP	3580682	A1	2019年 12月 18日
				EP	3580683	A1	2019年 12月 18日
				WO	2018148069	A1	2018年 8月 16日
				WO	2018148068	A1	2018年 8月 16日
				WO	2018148067	A1	2018年 8月 16日