

(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 6 月 11 日 (11.06.2020)



(10) 国际公布号
WO 2020/113546 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

河南省郑州市文化路俭学街 7 号,
Henan 450000 (CN).

(21) 国际申请号: PCT/CN2018/119724

(22) 国际申请日: 2018 年 12 月 7 日 (07.12.2018)

(25) 申请语言: 中文

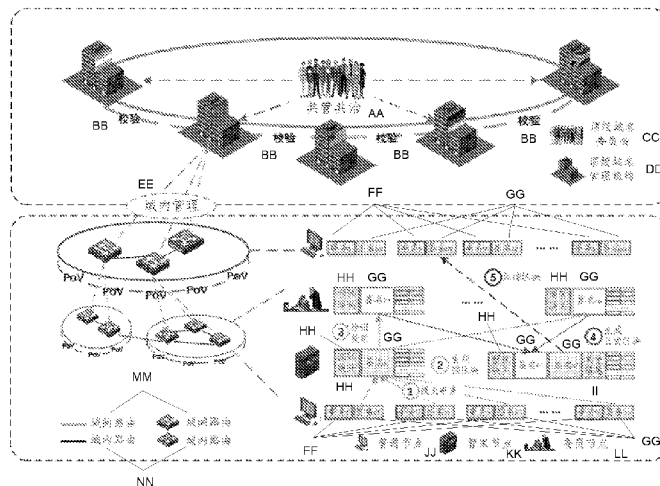
(26) 公布语言: 中文

(71) 申请人: 北京大学深圳研究生院(PEKING UNIVERSITY SHENZHEN GRADUATE SCHOOL) [CN/CN]; 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。国家数字交换系统工程技术研究中心(CHINA NATIONAL DIGITAL SWITCHING SYSTEM ENGINEERING & TECHNOLOGICAL R&D CENTER) [CN/CN]; 中国

(72) 发明人: 李挥(LI, Hui); 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。王茜(WANG, Han); 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。邬江兴(WU, Jiangxing); 中国河南省郑州市文化路俭学街 7 号, Henan 450000 (CN)。朱伏生(ZHU, Fusheng); 中国广东省广州市连新路广东省科技厅大楼 801 室(广东省新一代通信与网络创新研究院), Guangdong 510000 (CN)。伊鹏(YI, Peng); 中国河南省郑州市文化路俭学街 7 号(国家数字交换系统工程技术研究中心), Henan 450000 (CN)。安辉耀(AN, Huiyao); 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055

(54) Title: PRIVACY PROTECTION AND IDENTITY MANAGEMENT METHOD AND SYSTEM FOR MULTI-MODE IDENTIFIER NETWORK

(54) 发明名称: 一种用于多模标识网络隐私保护与身份管理的方法及系统



- AA Co-management
- BB Authentication
- CC Top-level domain name committee
- DD Top-level domain name registry
- EE Intra-domain management
- FF Transaction
- GG Signature
- HH Pre-block header
- II Other information
- JJ Ordinary node
- KK Manager node
- LL Member node
- MM Inter-domain router
- NN Intra-domain router
- 1 Transaction submission
- 2 Pre-block generation
- 3 Vote verification
- 4 Formal block generation
- 5 Block compression

图 2

(57) Abstract: The present invention is applicable to the technical field of blockchains. Provided is a privacy protection and identity management method for a multi-mode identifier network. The method comprises: S1, utilizing blockchain technology to register network identifiers, forming a multi-mode identifier network, and performing domain division to construct a hierarchical blockchain system; S2, employing a group/ring signature mechanism to combine, according to differences in the identification of respective nodes in the multi-mode identifier network, respective node signatures into a signature tree structure; and S3, performing authentication on a

(CN)。张昕淳(ZHANG, Xinchun); 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。王子贤(WANG, Zixian); 中国广东省深圳市南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。

(74) 代理人: 深圳市科吉华烽知识产权事务所(普通合伙)(SZ KINDWALF INTELLECTUAL PROPERTY FIRM); 中国广东省深圳市南山区深南西路深南花园裙楼A区四层402室, Guangdong 518057 (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, 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))。

given higher-level node signature in the signature tree structure to realize authentication of a lower-level node signature by taking said signature as a root in the signature tree structure. The present invention employs a group/ring signature technique to realize identity privacy protection for members. A manager node and ordinary nodes form a group so as to generate an upper-level group signature for multiple transactions. At the same time, the manager node and member nodes also form a ring so as to create an upper-level ring signature for multiple voting messages.

(57) 摘要: 本发明适用于区块链技术领域, 提供了用于多模标识网络隐私保护与身份管理的方法, 包括: S1、利用区块链技术对网络标识进行注册, 形成多模标识网络并进行域划分构建层级化区块链系统; S2、在多模标识网络中根据各节点的身份不同通过层次化群/环签名机制将各节点签名共同组成树型签名结构; S3、网络仅验证树形签名结构的上级节点签名从而实现以该签名为根的下级节点签名树验证。采用群/环签名技术实现成员身份的隐私保护。管家节点与普通节点建立群, 生成多个事务的上级群签名; 同时与委员节点建立环, 生成多个投票消息的上级环签名。

一种用于多模标识网络隐私保护与身份管理的方法及系统

技术领域

本发明属于区块链技术领域，尤其涉及用于多模标识网络隐私保护与身份管理的方法。

5 背景技术

多模标识网络是针对现有互联网控制能力过于集中、缺乏国际性的多边共管共治等本质缺陷而提出的新型开放式网络架构，具体指不同体系结构的网络共同部署多路由标识协同路由寻址的网络环境。例如在传统网络中部署内容网络，如果数据可以在这两种网络间穿梭，便形成了一个由两种网络体系组成的、内容标识和地址标识共同寻址的多模网络环境。通过
10 利用不同网络的优势协同工作，多模标识网络能够提升当前互联网的基础传输能力，加强网络资源的利用率，丰富网络层功能。更重要的是，多模标识网络降低了现有互联网体系对地址标识的依赖性和局限性，为互联网的多边共管共治提供可能。

15 2008年10月，一位化名为“中本聪”的密码学研究者公开发表了一篇关于比特币的论文，描述了一种无需第三方可信机构介入的点对点电子货币系统，首次提出了区块链的概念。区块链，即一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。区块链技术本质上是一种防篡改的、共
20 享的分布式账本，网络中的所有成员节点共同维护账本，基于密码学技术而非外部信任，能够用链式数据结构完整地记录全部交易信息。因此，区块链拥有三大显著特征：去中心化、不可篡改和去信任化。在某些区块链

应用场景中，需要引入身份控制，这就形成了联盟链。联盟链是指若干个机构共同参与记账的区块链，每个机构运行一个或多个节点，联盟成员之间通过对多中心的互信来达成共识。链上块的创建由预选的记账节点共同决定，而只允许普通成员节点进行读写、记录和发送交易。与公有链不同，

- 5 联盟链被认为是“部分去中心”的，在某种程度上只属于联盟内部的成员所有，链上的数据仅限联盟里的机构和成员才有权限进行访问。联盟链的部分去中心化特性恰好契合了多模标识网络的多边共管共治理念。且相比于公有链，联盟链在高可用、高性能、可编程和隐私保护上更有优势。

- 在区块链系统中，每一条数据交易都需要签名，以保证信息的完整性
- 10 和真实性。一个简单的数字签名机制是，若服务器 A 向服务器 B 发送一条消息，为了向 B 证明这条消息只有 A 才能发出，A 用私钥将消息 M 加密成一个签名 S，B 收到消息 M 和签名 S 后，用 A 公钥解密 S 并比对解密后的消息和 M，若相同即可证明签名有效。在实际的系统中通常要求保密性，一般在数字签名机制中结合散列算法。发送方 A 用一个 Hash 函数从消息
- 15 中生成消息摘要，然后用自己的私钥将这个摘要加密为签名，和消息一起发送给接收方 B。接收方首先用与 A 相同的 Hash 函数从接收到的消息中计算出消息摘要，再用 A 的公钥来对附加的签名进行解密。比较这两个摘要，若相同则可确认签名属于 A。

- 可见，基于数字签名的身份管理和隐私保护机制是确保联盟链事务安
- 20 全可靠的关键核心技术，是联盟链能够进一步良性循环发展的必要条件。
- 然而，现有的面向区块链的隐私保护和身份管理方法与标识网络的可扩展层次化结构的匹配度不高，且存在着规模较大和高验证复杂度的问题，无

法支持高通量的大规模网络。

2013 年 8 月份, Christina Garman 等人提出了去中心化的匿名凭证系统用来解决互联网身份隐私认证问题。在传统的解决方案中, 证书授权中心、DNS 设施或者像谷歌在内的登录提供者等大型组织在互联网认证过程中扮演了非常重要的角色。然而, 这些中心化的大型组织非常容易成为攻击者攻击的对象, 并且一旦这些组织出现异常, 容易泄露用户的隐私。Garman 等人提出建立由多节点构成的区块链组织来为用户提供身份证明的生成与验证服务, 并且借助一定的加密算法实现匿名性, 更好地保护了用户隐私。匿名凭证允许用户证明其拥有某个组织颁发的凭证, 且不泄露任何其他个人隐私。在标准安全定义下, 即使验证者和凭证发行者串通, 他们也无法确定凭证被谁发布及何时将被使用。

由于 Garman 在方案的构造中使用了比较昂贵的“双层离散对数证明”, 生成的凭证规模较大且验证速度较慢, 无法满足实际应用的需求。此外, 该方案仅仅能实现对于身份隐私的保护, 却无法对于身份进行有效的管理, 无法满足多模标识网络的实际需要。

门罗币是于 2014 年 4 月份创建的开源加密货币, 使用环签名技术来保护用户的匿名性和交易的隐私保护, 即 RingCT 协议。

环签名是一类数字签名方案, 它允许环内某一成员在不透露自身身份的情况下代表环内所有成员签署消息。普通的环签名提供无条件的匿名性, 验证者无法判断两个签名是否来自于同一位成员。然而, 在某些情况下这种完备的匿名性并不适用, 可关联环签名技术应运而生。可关联环签名的特征是, 给定任意两个可关联环签名, 验证者知道它们是否由同一签名者

生成，但对签名者的身份一无所知，除非验证者与签名者处于同一环上。

在门罗币系统中，每个用户可能拥有一些不同的账户，其中每个账户由一个一次性地址和币组成，与一个可授权支出的账户密钥相关联。在每一笔交易中，用户可以使用相应的密钥花费自己的账户。

5 RingCT 协议主要由两个阶段组成：

1) 消费者生成环机密交易：

消费者首先确定多个输入和输出账户，使得它们的累计余额相等，再分别对每笔交易的输入组建环并进行签名。

2) 接收者验证环机密交易：

10 矿工一旦接收到区块链网络中的交易，则利用消息和签名共同验证交易的有效性，并将有效交易打包进新的区块。

门罗币采用的保护机制虽然对于隐私保护有了很好的解决，但是无法实现对参与节点身份的有效管理和行为的有效追踪，这在存在管理参与方行为需求的多模标识场景中是无法接受的。

15 发明内容

本发明的目的在于提供用于多模标识网络隐私保护与身份管理的方法，旨在解决针对所有参与方在同域内的情况，或者依赖于第三方可信机构提供的服务，不具备可追溯性，也无法适用于多模标识网络的层次化联盟链结构的问题。

20 本发明是这样实现的，用于多模标识网络隐私保护与身份管理的方法，所述方法包括以下步骤：

S1、利用区块链技术对网络标识进行注册，形成多模标识网络并进行

域划分构建层级化区块链系统；

S2、在多模标识网络中根据各节点的身份不同通过层次化群/环签名机制将各节点签名共同组成树型签名结构；

5 S3、网络仅验证树形签名结构的上级节点签名从而实现以该签名为根的下级节点签名树验证。

本发明的进一步技术方案是：所述步骤 S3 中每个上级节点管理一组下级节点作为叶子节点，每个上级节点签名下级节点签名结合生成且包含了下级的全部信息。

10 本发明的进一步技术方案是：所述步骤 S2 中根据各个节点签名的所属和作用将其分化为投票环签名和普通群签名两类签名树。

本发明的进一步技术方案是：所述步骤 S2 中层次化群/环签名机制包括以下步骤：

S21、底层域内任意普通节点生成事务并附上签名 S ，管家节点监听域内事务并将有效事务放入事务池中；

15 S22、值班管家节点定期取事务封装成预区块，与事务所属普通节点组成群生成新的上级群签名 S' 并与预区块一并发送给域内所有委员节点和管家节点；

S23、委员节点收到预区块后验证其事务和管家签名 S' 并判断是否同意生成对应的正式区块，若同意生成正式区块，则将自己的可关联环签名
20 P 和时间戳作为投票消息发回给值班管家节点并执行下一步，若不同意，则直接丢弃；

S24、在区块截止生成时间之前，判断值班管家收集到同域委员节点的签名和时间戳数量是否大于预设值，若大于预设值，则值班管家节点与这些签名所属委员节点组成环并生成新的上级环签名 P' ，将其加在预区块头后生成正式区块头，和区块体、时间戳、签名 S' 一起向全域发布并执行下一步，若小于预设值或超过截止时间，则本轮值班管家不生成区块；

S25、委员节点接收到正式区块后验证区块内的签名 P' 和 S' 并将有效区块包含的事务从事务池中删除。

本发明的进一步技术方案是：所述步骤 S21 中还包括以下步骤：

S211、底层域内任意普通节点还接收域内事务并验证事务内容和签名是否正确，若正确，则向域内其他节点转发该事务，若不正确，则直接丢弃。

本发明的进一步技术方案是：所述步骤 S25 还包括以下步骤：

S251、判断接收区块的委员节点是否处于顶层域，若不处于顶层域，则提取区块为一条事务，根据后附的管家签名 S' 生成新的上级群签名 S'' ，作为上一层域的普通节点提交该事务，其他上级节点继续验证签名 P' 和 S'' ，若接收委员节点处于顶层域，则执行下一步；

S252、判断收到正式区块的委员节点数量是否大于设定值，若大于设定值，则此区块进入合法状态拥有最终确认性，若小于设定值，则此区块无效。

本发明的进一步技术方案是：所述预设值大于等于 50%；所述设定值大于等于 50%。

本发明的另一目的在于提供一种于多模标识网络的隐私保护与身份管理系统，所述用于多模标识网络的隐私保护与身份管理系统包括

5 多模标识网络生成模块，用于利用区块链技术对网络标识进行注册，形成多模标识网络并进行域划分构建层级化区块链系统；

层次化签名模块，用于在多模标识网络中根据各节点的身份不同通过层次化群/环签名机制将各节点签名共同组成树型签名结构；

验证模块，用于网络仅验证树形签名结构的上级节点签名从而实现以
10 该签名为根的下级节点签名树验证。

本发明的进一步技术方案是：所述验证模块中每个上级节点管理一组下级节点作为叶子节点，每个上级节点签名由下级节点签名结合生成且包含了下级节点签名的全部信息。

本发明的进一步技术方案是：所述层次化签名模块中根据各个节点签名的所属和作用将其分化为投票环签名和普通群签名两类签名树。
15

本发明的进一步技术方案是：所述层次化签名模块中层次化群/环签名机制包括

监听节点签名生成单元，用于底层域内任意普通节点生成事务并附上签名 S ，管家节点监听域内事务并将有效事务放入事务池中；

20 预区块生成单元，用于值班管家节点定期取事务封装成预区块，与事务所属普通节点组成群生成新的上级群签名 S' 并与预区块一并发送给域内所有委员节点和管家节点；

第一判断单元,用于委员节点收到预区块后验证其事务和管家签名 S' 并判断是否同意生成对应的正式区块,若同意生成正式区块,则将自己的可关联环签名 P 和时间戳作为投票消息发回给值班管家节点并执行第二判断单元,若不同意,则直接丢弃;

- 5 第二判断单元,用于在区块截止生成时间之前,值班管家判断收集到同域委员节点的签名和时间戳数量是否大于预设值,若大于预设值,则值班管家节点与这些签名所属委员节点组成环并生成新的上级环签名 P' ,将其加在预区块头后生成正式区块头,和区块体、时间戳、签名 S' 一起向全域发布并执行签名验证单元,若小于预设值或超过截止时间,则本轮值班管家不生成区块;
- 10

签名验证单元,用于委员节点接收到正式区块后验证区块内的签名 P' 和 S' 并将有效区块包含的事务从事务池中删除。

- 本发明的进一步技术方案是:所述监听节点签名生成单元中还包括实务正确判断单元,用那个与底层域内任意普通节点还接收域内事务并验证事务内容和签名是否正确,若正确,则向域内其他节点转发该事务,若不正确,则直接丢弃。
- 15

本发明的进一步技术方案是:所述签名验证单元还包括

- 第三判断单元,用于判断接收区块的委员节点是否处于顶层域,若不处于顶层域,则提取区块为一条事务,根据后附的管家签名 S' 生成新的上级群签名 S'' ,作为上一层域的普通节点提交该事务,其他上级节点继续
- 20

验证签名 P' 和 S'' ，若接收委员节点处于顶层域，则执行第四判断单元；

第四判断单元，用于判断收到正式区块的委员节点数量是否大于设定值，若大于设定值，则此区块进入合法状态拥有最终确认性，若小于设定值，则此区块无效。

- 5 本发明的进一步技术方案是：所述预设值大于等于 50%；所述设定值大于等于 50%。

本发明的有益效果是：采用群/环签名技术实现成员身份的隐私保护。管家节点与普通节点建立群，生成多个事务的上级群签名；同时与委员节点建立环，生成多个投票消息的上级环签名。普通节点在接收到签名消息
10 后，只能确定消息的内容而不能知道消息的处理流程，从而兼顾权限控制和区块链的公开透明特性。

下级域中的委员节点同时也是上级域中的普通节点，负责为下级域中的事务向上层域提起请求。在跨域节点中加入层次化签名设计可以实现身份追踪，从而更好地管理成员和区块事务。

- 15 群主可以对于一个群内的成员进行管理，识别消息的具体来源，从而保证群内的成员不能恶意发送消息而接受不到相应的惩罚。在多模标识网络中，管家与普通节点间的群建立与维护过程对于网络的正常运转具有重要意义，防止了不正当节点对网络的扰动。

附图说明

- 20 图 1 是本发明实施例提供的层次化签名树结构身份模型示意图。

图 2 是本发明实施例提供的新型联盟链架构下的层次化签名机制示意图。

具体实施方式

如图 1-2 所示, 本发明提供的用于多模标识网络隐私保护与身份管理的方法, 其详述如下:

步骤 S1, 利用区块链技术对网络标识进行注册, 形成多模标识网络并
5 进行域划分构建层级化区块链系统, 并通过 PoV 投票共识算法对每个网络域进行管理。

步骤 S2, 在多模标识网络中根据各节点的身份不同通过层次化群/环签名机制将各节点签名共同组成树型签名结构; 根据各个节点签名的所属和作用将其分化为投票环签名和普通群签名两类签名树。

10 步骤 S3, 网络仅验证树形签名结构的上级节点签名从而实现以该签名为根的下级节点签名树验证。每个上级节点管理一组下级节点作为叶子节点, 每个上级节点签名由下级节点签名结合生成且包含了下级节点签名的全部信息, 对上级签名的验证也包含了对以该签名为根的树的验证。

与普通的群/环签名要求相似, 在只拿到签名和验证公钥的情况下, 任
15 何第三方都不能追踪签名所属者的身份。此外, 层次化的群签名方案的安全性要求群管理员只能追踪其叶子节点的签名者身份, 并不能打开其他群组下的成员所产生的签名。通过在不同层级、不同身份的节点之间建立群组关系, 上级节点的群管理员可以快速定位到问题群, 并识别相应的恶意用户。

20 一种用于多模标识网络的隐私保护与身份管理方法, 根据多模标识联盟链网络的结构化特性, 设计了一套层次化签名方案。通过利用群/环签名的匿名性和可监管优势, 本发明实现了不同层次间节点身份的充分隐匿与

同一层次内身份的有效管理，更好地满足了多模标识网络对安全和管理的需求。

在本发明中，域内节点按身份由低到高分普通节点、管家节点和委员节点，同一节点可以兼任多个身份，如图 1 所示。其中，普通节点只享有知情权和提案权，无法参与共识过程。管家节点拥有生产区块的权利。委员节点拥有验证区块和推荐、验证、评价管家节点并参与上一级共识的权利。下层域的委员节点同时也在上一层域担任身份。

由于多模网络的节点分工不同，本发明考虑使用层次化的群/环签名机制。网络中的节点签名共同形成树型结构，每个上级节点管理一组下级节点作为其叶子节点。上级签名由下级签名结合生成，包含了下级的全部信息，对上级签名的验证也包含了对以该签名为根的树的验证。与普通的群/环签名要求相似，在只拿到签名和验证公钥的情况下，任何第三方都不能追踪产生签名的签名者的身份。此外，层次化的群签名方案的安全性要求群管理员只能追踪其叶子节点的签名者身份，并不能打开其他群组下的成员所产生的签名。通过在不同层级、不同身份的节点之间建立群组关系，上级节点的群管理员可以快速定位到问题群，并识别相应的恶意用户。

针对于层次化签名方案的特点，本发明使用如下区块结构：

Pre – Block			
Pre – Header		Body	
Hash	当前区块的唯一标志符，由值班管家对Pre – Header除了Hash之外的部分加密后用SHA-256 散列而成。	$\{tx\}$ $= \{tx_0, tx_1, \dots, tx_i\}$	事务列表
Pre – Hash	上一区块的Hash值，是区块		

	链链式数据结构的重要属性。		
Height (h)	当前区块的高度值，也可简称为 h 。创世区块的高度值为0。		
Height_LastSpe (hs)	离当前区块最近的一个特殊区块的高度值，也简称为 hs 。若 $h = hs$ ，说明此区块为特殊区块，一般每隔 B_w 个区块会出现一个特殊区块，即 $h - hs \leq B_w$ 。		
M	当前区块耗费多少个值班周期生成，也意味着本轮共识共有 $M - 1$ 个区块为无效区块。		
Puk (addr)	封装当前区块的值班管家的公钥，也是节点的地址addr，用于证明当前区块的记账归属权和统计管家节点的最终收益。		
Merkle_Root	默克尔根，由事务数据两两哈希生成，用于校验所有事务的原始性和真实性，配合Pre-Hash成为区块链链式结构不可篡改特性的重要属性。		
...	自定义属性部分，如 T_b 为生成区块的值班周期， N_b 为选出的管家节点数量， N_{bc} 为管家候选人数量， N_c 为委员节点数量。		

Block			
Final – Header		Body	
Pre – Header	包含Pre – Header的一切属性。	$\{tx\}$ $= \{tx_0, tx_1, \dots, tx_i\}$	事务列表
pre_header_ring_sign {(C_time, C_sign)}	委员节点返回的签名列表的上级环签名，其中C_time为签名时刻委员处理器的时间戳，在一定程度上影响区块最终生成时间；C_sign为委员节点使用私钥对 Pre – Header 和 C_time拼接的字符串哈希后加密的过程。		
R	使用 RandomNum 算法得到的随机函数，决定下一区块的值班管家编号。		
time	当前区块生成的时间。		

具体签名流程如图 2 所示。

- 1) 底层域内任意普通节点产生事务并附上签名 S ，同时也接收域内事务，验证事务内容和签名的正确性，若正确则向域内其他节点转发该事务。管家节点监听域内事务，并将有效的事务放入事务池中。
- 5 2) 值班管家节点定期从事务池中取出一些事务，封装成预区块，与这些事务所属的普通节点组成群，生成新的上级群签名 S' ，和预区块一起发送给域内所有委员节点和管家节点。管家节点在收到新的上级群签名 S' 和预区块后，将其进行备份。
- 3) 委员节点收到预区块后，验证预区块内的事务和管家签名 S' ，若

同意本区块生成则将自己的可关联环签名 P 和时间戳作为投票消息发回给值班管家节点。

4) 在区块截止生成时间之前,若值班管家已经收集到大于预设值数量的同域委员节点的签名和时间戳,则与这些签名所属的委员节点组成环,

- 5 生成新的上级环签名 P' ,值班管家将新的签名 P' 加在预区块头后生成正式区块头,和区块体、签名 S' 一起向全域发布。若小于预设值或超过截止时间,则本轮共识不生成区块。在该过程中,根据应用环境不同,值班管家收到的委员节点的签名和时间戳的数量值也不同,可能是大于50%的委员节点,也可能是60%委员节点或70%委员节点或80%委员节点或85%委员节点或90%委员节点等。

5) 当委员节点接收到正式区块后,验证区块内的签名 P' 和 S' ,将有效区块包含的事务从事务池中删除。若此时委员节点不处于顶层域,提取区块为一条事务,根据后附的管家签名 S' 生成新的上级群签名 S'' ,作为上一层域的普通节点提交该事务。其他上级节点继续验证签名 P' 和 S'' 。

- 15 若此时委员节点处于顶层域,当有大于设定值数量的委员节点确认收到后,此区块进入合法状态,拥有最终确认性。在收到委员节点确认中,确认数量可能是半数委员节点或60%委员节点或70%委员节点或80%委员节点或85%委员节点或90%委员节点等。根据应用场景的不同和应用环境可以在任意选择上述的数值作为确认点。

- 20 本发明的另一目的在于提供一种于多模标识网络的隐私保护与身份管

理系统，所述用于多模标识网络的隐私保护与身份管理系统包括

多模标识网络生成模块，用于利用区块链技术对网络标识进行注册，形成多模标识网络并进行域划分构建层级化区块链系统；

层次化签名模块，用于在多模标识网络中根据各节点的身份不同通过

5 层次化群/环签名机制将各节点签名共同组成树型签名结构；

验证模块，用于网络仅验证树形签名结构的上级节点签名从而实现以该签名为根的下级节点签名树验证。

所述验证模块中每个上级节点管理一组下级节点作为叶子节点，每个上级节点签名由下级节点签名结合生成且包含了下级节点签名的全部信息。

10 所述层次化签名模块中根据各个节点签名的所属和作用将其分化为投票环签名和普通群签名两类签名树。

所述层次化签名模块中层次化群/环签名机制包括

监听节点签名生成单元，用于底层域内任意普通节点生成事务并附上签名 S ，管家节点监听域内事务并将有效事务放入事务池中；

15 预区块生成单元，用于值班管家节点定期取事务封装成预区块，与事务所属普通节点组成群生成新的上级群签名 S' 并与预区块一并发送给域内所有委员节点和管家节点；

第一判断单元，用于委员节点收到预区块后验证其事务和管家签名 S' 并判断是否同意生成对应的正式区块，若同意生成正式区块，则将自己的可关联环签名 P 和时间戳作为投票消息发回给值班管家节点并执行第二判断单元，若不同意，则直接丢弃；

20

第二判断单元, 用于在区块截止生成时间之前, 值班管家判断收集到同域委员节点的签名和时间戳数量是否大于预设值, 若大于预设值, 则值班管家节点与这些签名所属委员节点组成环并生成新的上级环签名 P' , 将其加在预区块头后生成正式区块头, 和区块体、时间戳、签名 S' 一起向全域发布并执行签名验证单元, 若小于预设值或超过截止时间, 则本轮值班管家不生成区块;

签名验证单元, 用于委员节点接收到正式区块后验证区块内的签名 P' 和 S' 并将有效区块包含的事务从事务池中删除。

所述监听节点签名生成单元中还包括

- 10 实务正确判断单元, 用那个与底层域内任意普通节点还接收域内事务并验证事务内容和签名是否正确, 若正确, 则向域内其他节点转发该事务, 若不正确, 则直接丢弃。

所述签名验证单元还包括

- 15 第三判断单元, 用于判断接收区块的委员节点是否处于顶层域, 若不处于顶层域, 则提取区块为一条事务, 根据后附的管家签名 S' 生成新的上级群签名 S'' , 作为上一层域的普通节点提交该事务, 其他上级节点继续验证签名 P' 和 S'' , 若接收委员节点处于顶层域, 则执行第四判断单元;

- 20 第四判断单元, 用于判断收到正式区块的委员节点数量是否大于设定值, 若大于设定值, 则此区块进入合法状态拥有最终确认性, 若小于设定值, 则此区块无效。

所述预设值大于等于 50%；所述设定值大于等于 50%。

采用群/环签名技术实现成员身份的隐私保护。管家节点与普通节点建立群，生成多个事务的上级群签名；同时与委员节点建立环，生成多个投票消息的上级环签名。普通节点在接收到签名消息后，只能确定消息的内容而不能知道消息的处理流程，从而兼顾权限控制和区块链的公开透明特性。

下级域中的委员节点同时也是上级域中的普通节点，负责为下级域中的事务向上层域提起请求。在跨域节点中加入层次化签名设计可以实现身份追踪，从而更好地管理成员和区块事务。

群主可以对于一个群内的成员进行管理，识别消息的具体来源，从而保证群内的成员不能恶意发送消息而接受不到相应的惩罚。在多模标识网络中，管家与普通节点间的群建立与维护过程对于网络的正常运转具有重要意义，防止了不正当节点对网络的扰动。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1、一种用于多模标识网络的隐私保护与身份管理方法，其特征在于，所述用于多模标识网络的隐私保护与身份管理方法包括以下步骤：

S1、利用区块链技术对网络标识进行注册，形成多模标识网络并进行域划分构建层级化区块链系统；

5 S2、在多模标识网络中根据各节点的身份不同通过层次化群/环签名机制将各节点签名共同组成树型签名结构；

S3、网络仅验证树形签名结构的上级节点签名从而实现以该签名为根的下级节点签名树验证。

2、根据权利要求1所述的用于多模标识网络隐私保护与身份管理的方法，其特征在于，所述步骤S3中每个上级节点管理一组下级节点作为叶子节点，每个上级节点签名由下级节点签名结合生成且包含了下级节点签名的全部信息。

3、根据权利要求2所述的用于多模标识网络隐私保护与身份管理的方法，其特征在于，所述步骤S2中根据各个节点签名的所属和作用将其分化为投票环签名和普通群签名两类签名树。

4、根据权利要求3所述的用于多模标识网络隐私保护与身份管理的方法，其特征在于，所述步骤S2中层次化群/环签名机制包括以下步骤：

S21、底层域内任意普通节点生成事务并附上签名 S ，管家节点监听域内事务并将有效事务放入事务池中；

20 S22、值班管家节点定期取事务封装成预区块，与事务所属普通节点组成群生成新的上级群签名 S' 并与预区块一并发送给域内所有委员节点和管家节点；

S23、委员节点收到预区块后验证其事务和管家签名 S' 并判断是否同意生成对应的正式区块，若同意生成正式区块，则将自己的可关联环签名 P 和时间戳作为投票消息发回给值班管家节点并执行下一步，若不同意，则直接丢弃；

5 S24、在区块截止生成时间之前，值班管家判断收集到同域委员节点的签名和时间戳数量是否大于预设值，若大于预设值，则值班管家节点与这些签名所属委员节点组成环并生成新的上级环签名 P' ，将其加在预区块头后生成正式区块头，和区块体、时间戳、签名 S' 一起向全域发布并执行下一步，若小于预设值或超过截止时间，则本轮值班管家不生成区块；

10 S25、委员节点接收到正式区块后验证区块内的签名 P' 和 S' 并将有效区块包含的事务从事务池中删除。

5、根据权利要求4所述的用于多模标识网络隐私保护与身份管理的方法，其特征在于，所述步骤S21中还包括以下步骤：

15 S211、底层域内任意普通节点还接收域内事务并验证事务内容和签名是否正确，若正确，则向域内其他节点转发该事务，若不正确，则直接丢弃。

6、根据权利要求5所述的用于多模标识网络隐私保护与身份管理的方法，其特征在于，所述步骤S25还包括以下步骤：

20 S251、判断接收区块的委员节点是否处于顶层域，若不处于顶层域，则提取区块为一条事务，根据后附的管家签名 S' 生成新的上级群签名 S'' ，

作为上一层域的普通节点提交该事务，其他上级节点继续验证签名 P' 和 S'' ，若接收委员节点处于顶层域，则执行下一步；

S252、判断收到正式区块的委员节点数量是否大于设定值，若大于设定值，则此区块进入合法状态拥有最终确认性，若小于设定值，则此区块

5 无效。

7、根据权利要求4-7任一项所述的用于多模标识网络隐私保护与身份管理的方法，其特征在于，所述预设值大于等于50%；所述设定值大于等于50%。

8、一种用于多模标识网络的隐私保护与身份管理系统，其特征在于，
10 所述用于多模标识网络的隐私保护与身份管理系统包括

多模标识网络生成模块，用于利用区块链技术对网络标识进行注册，形成多模标识网络并进行域划分构建层级化区块链系统；

层次化签名模块，用于在多模标识网络中根据各节点的身份不同通过层次化群/环签名机制将各节点签名共同组成树型签名结构；

15 验证模块，用于网络仅验证树形签名结构的上级节点签名从而实现以该签名为根的下级节点签名树验证。

9、根据权利要求8所述的用于多模标识网络隐私保护与身份管理的系统，其特征在于，所述验证模块中每个上级节点管理一组下级节点作为叶子节点，每个上级节点签名由下级节点签名结合生成且包含了下级节点签名的全部信息。
20

10、根据权利要求9所述的用于多模标识网络隐私保护与身份管理的系统，其特征在于，所述层次化签名模块中根据各个节点签名的所属和作

用将其分化为投票环签名和普通群签名两类签名树。

11、根据权利要求 10 所述的用于多模标识网络隐私保护与身份管理的系统，其特征在于，所述层次化签名模块中层次化群/环签名机制包括

监听节点签名生成单元，用于底层域内任意普通节点生成事务并附上

5 签名 S ，管家节点监听域内事务并将有效事务放入事务池中；

预区块生成单元，用于值班管家节点定期取事务封装成预区块，与事务所属普通节点组成群生成新的上级群签名 S' 并与预区块一并发送给域内所有委员节点和管家节点；

第一判断单元，用于委员节点收到预区块后验证其事务和管家签名 S'

10 并判断是否同意生成对应的正式区块，若同意生成正式区块，则将自己的可关联环签名 P 和时间戳作为投票消息发回给值班管家节点并执行第二判断单元，若不同意，则直接丢弃；

第二判断单元，用于在区块截止生成时间之前，值班管家判断收集到同域委员节点的签名和时间戳数量是否大于预设值，若大于预设值，则值

15 班管家节点与这些签名所属委员节点组成环并生成新的上级环签名 P' ，将其加在预区块头后生成正式区块头，和区块体、时间戳、签名 S' 一起向全域发布并执行签名验证单元，若小于预设值或超过截止时间，则本轮值班管家不生成区块；

签名验证单元，用于委员节点接收到正式区块后验证区块内的签名 P'

20 和 S' 并将有效区块包含的事务从事务池中删除。

12、根据权利要求 11 所述的用于多模标识网络隐私保护与身份管理的系统，其特征在于，所述监听节点签名生成单元中还包括

实务正确判断单元，用那个与底层域内任意普通节点还接收域内事务并验证事务内容和签名是否正确，若正确，则向域内其他节点转发该事务，

5 若不正确，则直接丢弃。

13、根据权利要求 12 所述的用于多模标识网络隐私保护与身份管理的系统，其特征在于，所述签名验证单元还包括

第三判断单元，用于判断接收区块的委员节点是否处于顶层域，若不处于顶层域，则提取区块为一条事务，根据后附的管家签名 S' 生成新的上

10 级群签名 S'' ，作为上一层域的普通节点提交该事务，其他上级节点继续验证签名 P' 和 S'' ，若接收委员节点处于顶层域，则执行第四判断单元；

第四判断单元，用于判断收到正式区块的委员节点数量是否大于设定值，若大于设定值，则此区块进入合法状态拥有最终确认性，若小于设定值，则此区块无效。

15 14、根据权利要求 11-13 任一项所述的用于多模标识网络隐私保护与身份管理的系统，其特征在于，所述预设值大于等于 50%；所述设定值大于等于 50%。

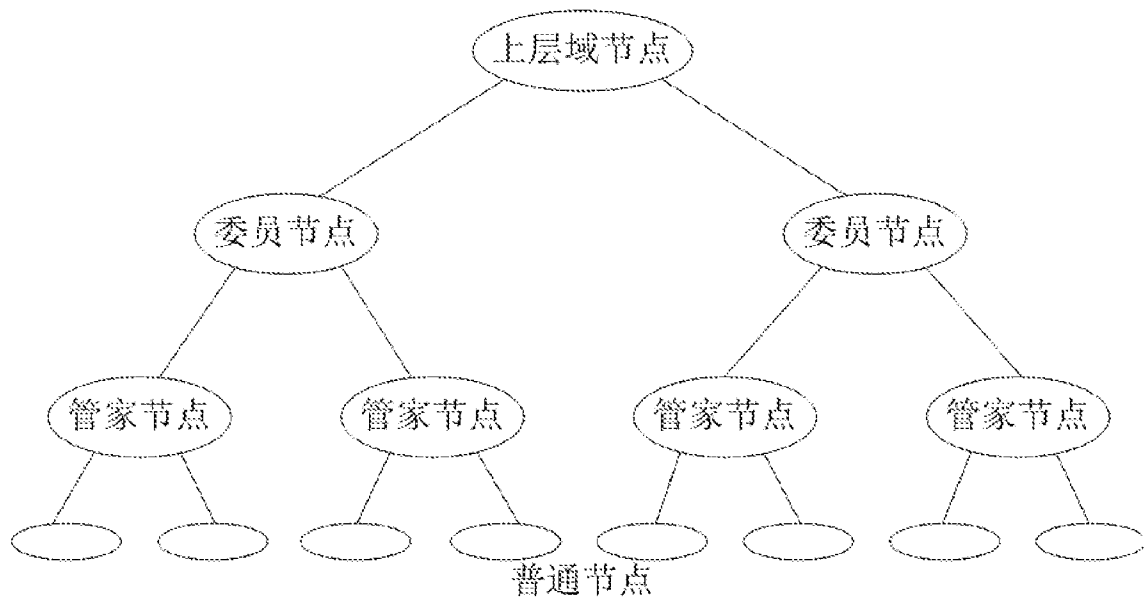


图 1

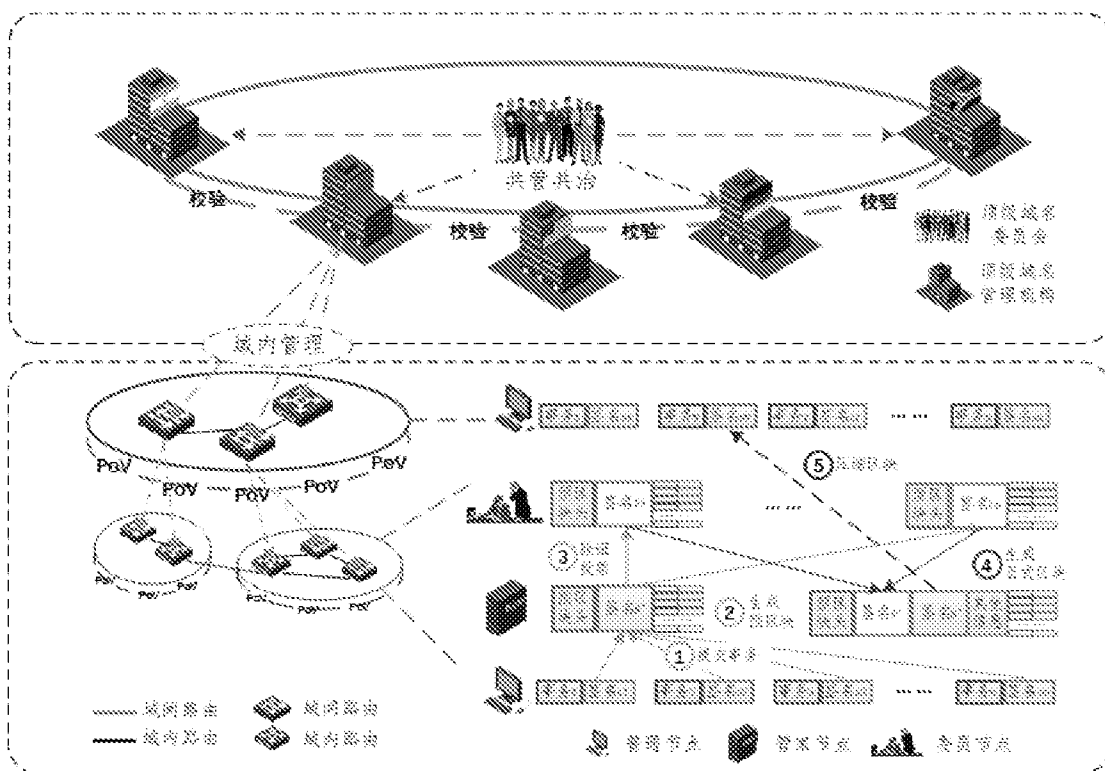


图 2

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/119724

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; G06F

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: 区块链, 签名, 身份, 隐私, 标识, 层次化, 群, 环签名, 去中心化, 多模, 树形, 数字签名树, 多模标识网络, blockchain, block w chain, signature, identity, privacy, preserving, hierarchical, cluster, ring, centralization, digital, tree,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 108259438 A (CHINA MOBILE (SUZHOU) SOFTWARE TECHNOLOGY CO., LTD. et al.) 06 July 2018 (2018-07-06) description, paragraphs [0040]-[0066]	1-14
A	CN 102055769 A (BEIJING INSTITUTE OF TECHNOLOGY) 11 May 2011 (2011-05-11) entire document	1-14
A	CN 101325481 A (CHENGDU WESTONE INFORMATION INDUSTRY INC.) 17 December 2008 (2008-12-17) entire document	1-14
A	US 2018341775 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 29 November 2018 (2018-11-29) entire document	1-14

☐ 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

26 August 2019

Date of mailing of the international search report

10 September 2019

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/119724

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	108259438	A	06 July 2018	None	
CN	102055769	A	11 May 2011	None	
CN	101325481	A	17 December 2008	None	
US	2018341775	A1	29 November 2018	None	

国际检索报告

国际申请号

PCT/CN2018/119724

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; G06F

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; EPDOC; CNKI; CNPAT: 区块链, 签名, 身份, 隐私, 标识, 层次化, 群, 环签名, 去中心化, 多模, 树形, 数字签名树, 多模标识网络, blockchain, block w chain, signature, identity, privacy, preserving, hierarchical, cluster, ring, centralization, digital, tree,

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	CN 108259438 A (中移苏州软件技术有限公司 等) 2018年 7月 6日 (2018 - 07 - 06) 说明书第[0040]-[0066]段	1-14
A	CN 102055769 A (北京理工大学) 2011年 5月 11日 (2011 - 05 - 11) 全文	1-14
A	CN 101325481 A (成都卫士通信息产业股份有限公司) 2008年 12月 17日 (2008 - 12 - 17) 全文	1-14
A	US 2018341775 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2018年 11月 29日 (2018 - 11 - 29) 全文	1-14

☐ 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

2019年 8月 26日

国际检索报告邮寄日期

2019年 9月 10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

徐泉

电话号码 86-(010)-53961794

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/119724

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	108259438	A	2018年 7月 6日	无	
CN	102055769	A	2011年 5月 11日	无	
CN	101325481	A	2008年 12月 17日	无	
US	2018341775	A1	2018年 11月 29日	无	