

(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
2018 年 10 月 4 日 (04.10.2018)



(10) 国际公布号
WO 2018/176406 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2017/079098
- (22) 国际申请日: 2017 年 3 月 31 日 (31.03.2017)
- (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)。
- (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)。王贤桂(WANG, Xiangui); 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)。林志力(LIN, Zhili); 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)。斯雪明(SI, Xueming); 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)。李恪聃(LI, Kedan); 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)。杨昕(YANG, Xin); 中国广东省南山区西丽镇丽水路深圳大学城北大校区, Guangdong 518055 (CN)。王菡(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)。

- (74) 代理人: 深圳市科吉华烽知识产权事务所(普通合伙)(SZ KINDWOLF 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)。

(54) Title: TOP-LEVEL DOMAIN NAME MANAGEMENT METHOD AND SYSTEM BASED ON ALLIANCE CHAIN

(54) 发明名称: 一种基于联盟链的顶级域名管理方法及系统

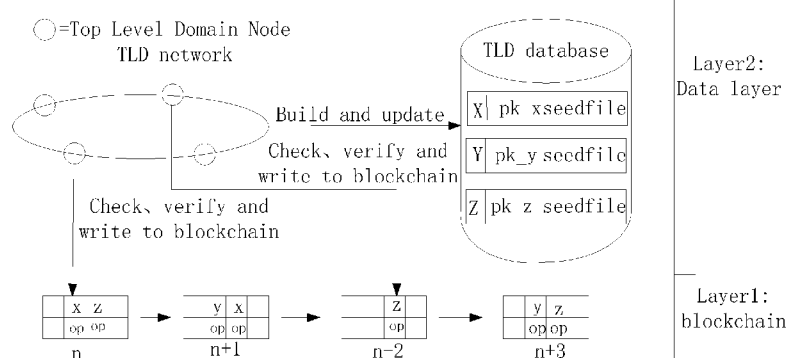


图 3

(57) Abstract: The present invention is applicable to the field of Internet technology improvement, and provides a top-level domain name management method based on a blockchain. The top-level domain name management method comprises the following steps: A. constructing an alliance network in a block chain by using a TLD node; B. layering a system architecture in the alliance network to separate operations from data; and C. by means of a consensus process, enabling the nodes in the alliance network to agree. By means of a more concise and efficient consensus process, the security and reliability of a system can be ensured, and the efficiency of the system is improved; and the structure of the system is layered to ensure the efficiency and portability of the system.

(57) 摘要: 本发明适用于互联网技术改进领域, 提供了一种基于区块链的顶级域名管理方法, 所述顶级域名管理方法包括以下步骤: A、利用TLD节点构成在区块链中的联盟网络; B、在联盟网络中对系统架构进行分层使得操作和数据分离; C、通过共识过程使得联盟网络中的节点达成一致。通过更加简洁高效的共识过程, 保证了系统的安全可靠性, 提高了系统的效率; 对系统结构分层, 保障系统的效率和可移植性。

(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, 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))。

一种基于联盟链的顶级域名管理方法及系统

技术领域

本发明属于互联网技术改进领域，尤其涉及一种基于联盟链的顶级域名管理方法及系统。

5 背景技术

名称在所有计算机系统中都起着重要的作用。它们用来共享资源、唯一标识实体、指向位置等。命名的一个重要结果是可以把名称解析为它所指向的实体。因而，名称解析允许进程访问命名的实体。要解析名称，需要实现命名系统。分布式系统中的命名与非分布式系统中的命名之间的区别在于命名系统实现的方式。而当今的许多应用，如部分文件系统和万维网名称系统都是基于分布式命名系统方案实现的。无论是现今的因特网，还是未来的新型网络，都需要一种基于分布式系统的结构化命名方案来解析参与到网络中的各种实体。域名系统（domain name system，DNS）是因特网使用的命名系统，用来把便于人们使用的机器名字转换为 IP 地址，并且采用具有层次的结构化命名方式，其中除了根域名外层次最高的域名称为顶级域名。

当今使用的最大分布式名称服务之一是因特网的域名系统（domain name system，DNS），DNS 的因特网标准是 RFC 1034，1035。DNS 名称空间采用分层树状结构的命名方法，并使用人类容易记忆和理解名称映射为长度固定为 32 位的 IP 地址（如果是 IPv6 地址，则是定长的 128 位）。在因特网中，任何一个主机或路由器都有一个唯一的层次结构的名称，即域

名 (domain name)。这里“域”是名字空间中一个可被管理的划分,域可以划分为子域,而子域还可以继续被划分,这样就形成了顶级域、二级域、三级域,等等。每个域名之间用点隔开。

因特网的域名系统是一个联机分布式数据库系统,采用客户-服务器

5 方式, DNS 使大多数名字都在本地进行解析,仅少量解析需要在因特网上通信,因此 DNS 系统的查询效率很高,并且单个计算机节点出了故障,也不会妨碍整个 DNS 系统的正常运行。域名服务器程序通常运行在域名服务器上,用于域名到 IP 地址的解析。当某个应用进程需要把主机名解析为 IP 地址时,该应用进程就调用解析程序,并成为 DNS 的一个客户,把待解析的域名放在 DNS 请求报文中,以 UDP 用户数据报方式发给本地域名服务器。本地域名服务器在查找域名后,把对应额 IP 地址放在回答报文中返回。应用进程获得目的主机的 IP 地址后即可进行通信。若本地域名服务器不能回答该请求,则此域名服务器就暂时成为 DNS 中的另一个客户,并向其他域名服务器发出查询请求。

15 各级域名由其上一级的域名管理机构管理,而最高的顶级域名链则由 ICANN 进行管理,这使得 DNS 管理中心化,任何公司、机构需要申请顶级域名时,都要向 ICANN 申请。

因特网上的域名服务器也是按照层次安排的,每个域名服务器都只对域名体系中的一部分进行管辖,所以可以划分为四种不同类型的服务器:

20 根域名服务器、顶级域名服务器、权限域名服务器和本地域名服务器。当一个本地域名服务器无法解析一个域名时,就首先需要求助于根域名服务

器。但目前根域名服务器在世界各地的分布是不合理的，以 2012 年的数据为例，在北美，平均每 375 万个网民可以分摊到一个根域名服务器，而在亚洲，平均超过 2000 万个网民才分摊到一个根域名服务器，这样就会使亚洲的网民域名解析的速度明显地低于北美的，而且当亚洲某个域名服务器出现故障时，就会有 2000 万个网民的域名解析请求受到严重影响，可见这种现象也导致了亚洲的域名解析系统的可靠性更低。

Blockstack 是一个去中心化的 DNS 系统，是以比特币区块链为底层实现的一个开源系统。它将 DNS 功能与公钥基础设施相结合，主要用于新的区块链应用程序。Blockstack 通过分离控制层和数据层，将名称注册、名字的所有者和名称相关的数据分离开来。其中控制层包含区块链层和虚拟链层，数据层分为路由层和存储层，所以 Blockstack 的系统架构其实由四层组成。区块链层占据着最底层，存储了 Blockstack 的一系列操作，并且提供了这些操作写入的顺序一致性，Blockstack 当前采用比特币区块链作为区块链层。虚拟链层在区块链层上定义自身协议，只有 Blockstack 系统软件可以感知到的事务记录。路由层负责将控制层定义的名称映射到实际存储数据的文件上，避免了系统从一开始就采用任意特定的存储服务，从而允许多个存储供应商提供服务。最顶的一层就是存储层，存储实际的“name-value”对数据，包括大容量的数据。Blockstack 采用分层结构，当某一层级出现问题或变更升级时不会影响其他层级的正常运行，并且降低了控制层的传输数据量。Blockstack 基于 Namecoin 的名称操作构建了全局命名系统，而且提出虚拟链的概念，使得系统具有更好的扩展性。Blockstack

还使用了一种基于一致性散列的简化名称验证协议，加速节点验证和新节点的加入。

Blockstack 难以与现有的 DNS 系统兼容。因特网的 DNS 系统采用分层的域名结构，而域名服务器的层次结构也是按照层次安排的。但是

5 Blockstack 并未使用分层的域名结构，域名之间也并没有层级关系。

Blockstack 完全去中心化的设计使得系统难于监管。虽然 Blockstack 可以让用户自由的申请域名，不受任何机构的限制和监管，但是这样的结构会产生许多无人维护的“僵尸”域名，极端的情况下可能成为犯罪的温床，因为你无法知道哪个用户持有域名对应的私钥。顶级域名被认为是真正的企业网络商标，是企业品牌策略战略发展的重要内容，而 Blockstack 抛弃了现有 DNS 的设计理念，顶级域名随意引入，使得顶级域名的意义不复存在。

发明内容

本发明的目的在于提供一种基于联盟链的顶级域名管理方法，旨在解决上述的技术问题。

本发明是这样实现的，一种基于联盟链的顶级域名管理方法，所述顶级域名管理方法包括以下步骤：

- A、利用 TLD 节点构成在区块链中的联盟网络；
- B、在联盟网络中对系统架构进行分层使得操作和数据分离；
- 20 C、通过共识过程使得联盟网络中的节点达成一致。

本发明的进一步技术方案是：所述步骤 A 中 TLD 节点对新加入 TLD 节点的认证包括以下步骤：

A1、新加入 TLD 节点可向 TLD 网络中任意一节点发送注册新的认证节点的消息；

5 A2、将收到的新节点加入消息的节点想所有节点广播该认证消息；

A3、网络中节点根据自身的规则选择同意或反对新加入的节点并将同意或反对的信息广播到其余节点；

A4、任意节点收到半数以上同意加入信息会认为网络同意该节点加入并记录该节点的消息。

10 本发明的进一步技术方案是：所述步骤 C 中联盟网络节点的共识过程包括以下步骤：

C1、每个 TLD 节点根据自己的标准，对每个域名操作进行独立校验；

C2、在预设时间内从 TLD 节点构成的网络中随机选择一个节点作为记账节点；

15 C3、利用选中的 TLD 节点将预设时间内有效的域名操作打包进区块，并广播到其它 TLD 节点和更新 TLD 数据库。

本发明的进一步技术方案是：所述步骤 A 中将系统构架分层为底层和上层，其中底层为嵌入域名操作的区块链，上层为顶层域名相关数据构成的数据层。

本发明的进一步技术方案是：在所述数据层内 TLD 节点通过处理一系列的顶级域名操作更新 TLD database,并将所有的操作同时写入底层的区块链中。

本发明的进一步技术方案是：所述预设时间为 5 分钟。

5 本发明的另一目的在于提供一种基于区块链的顶级域名管理系统，所述顶级域名管理系统包括：

构建联盟网络模块，用于利用 TLD 节点构成在区块链中的联盟网络；

分离模块，用于在联盟网络中对系统架构进行分层使得操作和数据分离；

10 节点一致模块，用于通过共识过程使得联盟网络中的节点达成一致。

本发明的进一步技术方案是：所述构建联盟网络模块中 TLD 节点对新加入 TLD 节点的认证包括：

新注册节点信息发送单元，用于新加入 TLD 节点可向 TLD 网络中任一节点发送注册新的认证节点的消息；

15 广播认证消息单元，用于将收到的新节点加入消息的节点想所有节点广播该认证消息；

网络节点反馈单元，用于网络中节点根据自身的规则选择同意或反对新加入的节点并将同意或反对的信息广播到其余节点；

20 批准加入记录单元，用于任意节点收到半数以上同意加入信息会认为网络同意该节点加入并记录该节点的消息。

本发明的进一步技术方案是：所述节点一致模块中联盟网络节点的共识过程包括：

标准校验单元，用于每个 TLD 节点根据自己的标准，对每个域名操作进行独立校验；

5 记账节点单元，用于在预设时间内从 TLD 节点构成的网络中随机选择一个节点作为记账节点；

打包更新单元，用于利用选中的 TLD 节点将预设时间内有效的域名操作打包进区块，并广播到其它 TLD 节点和更新 TLD 数据库。

本发明的进一步技术方案是：所述分离模块中将系统构架分层为底层
10 和上层，其中底层为嵌入域名操作的区块链，上层为顶层域名相关数据构成的数据层；在所述数据层内 TLD 节点通过处理一系列的顶级域名操作更新 TLD database，并将所有的操作同时写入底层的区块链中；所述预设时间为 5 分钟。

本发明的有益效果是：本发明与因特网的 DNS 的不同之处在于，因
15 特网的 DNS 在域名各层实行中心化的管理，而本发明是基于区块链技术实现的顶级域名管理方案，在选择顶级域名管理者（TLD 节点）和顶级域名的注册上都是去中心化的，即联盟中任意一个或一个小组的 TLD 节点都不能控制整个管理流程。本发明将域名系统分为两层，每个顶级域名有对应的下级域名系统，而下级的域名系统如何设计由顶级域名的持有机构决
20 定，因此下级域名系统可以根据该机构的理念而设计成中心化的或者去中心化的系统。

此外，由于区块链上的信息是公开并且不可更改的，所以被信任的机构甚至是个人都能获取到区块链上的信息并构建相应的种子文件数据库来保存顶级域名与下级域名系统的映射关系。这就意味着，各地区都能根据实际情况搭建相应数量的域名服务器以保证上网速度，而不必受到某些机构的限制。本发明也提出了一个顶级域名链的管理方法，并提出区块头和域名操作的数据结构，使得管理过程的数据流更加明确。

Blockstack 采用完全去中心化的设计架构，使得域名注册等事务难于管理。本发明使用两层结构这样的折中方案解决这个问题。顶级域名链由被认可的联盟成员共同管理而不是有其中一部分成员独揽大权，联盟成员通过制定相应的规则来维护域名系统的合理运行，例如通过制定一系列规则规范顶级域名的申请，从而避免一些毫无意义的顶级域名出现。而各个顶级域名对应的维护机构可以按照自身理念为子域名系统设计不同程度的管理方案，即可以设计成具有严格管理制度的子系统，或者可以设计出如 Blockstack 这样完全去中心化的子系统，因此用户也可以根据自身需要去申请相应的下级域名。

另外，与 Blockstack 相比，本发明可以与现今的 Blockstack 完全兼容，例如联盟可以增加一个“root”的顶级域名，而因特网的 DNS 可直接作为该顶级域名对应的下级域名系统。显然，对应的种子文件其实就是对现有 DNS 系统下的域名解析的接口。通过更加简洁高效的共识过程，保证了系统的安全可靠性，提高了系统的效率；对系统结构分层，保障系统的效率和可移植性。

附图说明

图 1 是本发明实施例提供的基于联盟链的顶级域名管理方法的流程图。

图 2 是本发明实施例提供的基于联盟链的顶级域名管理系统的结构框图。

5 图 3 是本发明实施例提供的基于联盟链的顶级域名管理方法中系统架构图。

图 4 是本发明实施例提供的基于联盟链的顶级域名管理方法中 TLD 数据库示意图。

10 图 5 是本发明实施例提供的基于联盟链的顶级域名管理方法中新加入 TLD 节点示意图。

具体实施方式

图 1 示出了本发明提供的基于联盟链的顶级域名管理方法的流程图，其详述如下：

步骤 S1，利用 TLD 节点构成联盟链的网络；由 TLD 节点构成的联盟
15 链网络，即一组关键 TLD 节点构成的 p2p 网络。TLD 节点主要功能有两个，一是已经加入联盟的节点审核并认证申请加入联盟的节点；二是检查、验证域名操作，提取数据写入到 TLD 数据库中，与此同时将合法的操作写到底层区块链中。考虑到认证的效率和容错性，本方案中新加入 TLD 节点的认证要经历下面四个步骤：步骤 S11，新加入 TLD 节点可向 TLD 网
20 络中任意一节点发送注册新的认证节点的消息；新加入 TLD 的节点可向 TLD 网络中任意一节点发送注册新的认证节点的消息。步骤 S12，将收到

的新节点加入消息的节点想所有节点广播该认证消息；收到新节点加入消息的节点向所有节点广播这条认证消息。步骤 S13，网络中节点根据自身的规则选择同意或反对新加入的节点并将同意或反对的信息广播到其余节点；网络中节点根据自己的规则选择同意或反对新加入的节点，同时将同意和反对的信息广播到其它节点。步骤 S14，任意节点收到半数以上同意加入信息会认为网络同意该节点加入并记录该节点的消息。一个节点收到半数以上同意加入的信息就会认为网络已经同意该节点的加入，记录该节点的消息。

步骤 S2，对系统架构进行分层使得操作和数据分离；将系统架构分为两层，底层为嵌入域名操作的区块链，上层为顶层域名相关数据构成的数据层。一系列的顶级域名节点 TLDN (Top Level Domain Node) 构建一张 p2p 网络共同维护顶级域名，每个节点维护一个记录顶级域名 (TLD)、注册顶级域名的用户的公钥 (Public key)、私钥签名的下级域名系统的种子文件 (Seed file) 的 TLD 数据库。TLD 节点通过处理一系列的顶级域名操作来构建和持续更新这个数据库。这些顶级域名的操作中主要包括顶级域名的注册 (register) 和更新顶级域名对应的种子文件 (update)，如图 3 所示。

TLD 节点通过处理一系列的顶级域名操作来更新 TLD database，所有的操作同时也会被写入底层的区块链中。这些顶级域名的操作包括顶级域名的注册 (register) 和删除 (delete) 其对应的 seedfile 的更新 (update)。

和 Namecoin 系统类似，顶级域名的注册分为预定 (preorder) 和注册 (resister) 两个阶段，也被称为两阶段加密提交协议。preorder 操作宣称要注册一个

顶级域名，但是不会暴露名称，也不会改变数据库。preorder 操作可以防止窃听攻击者竞争成为操作发送者并窃取名称。delete 操作会在 TLD 数据库中删除相关的内容。update 操作会更改顶级域名对应的 seedfile。如图 4 中所示假设了系统中的一些操作，右边为 TLD 数据库中存储的内容。

- 5 步骤 S3，通过共识过程使得联盟链中的节点达到一致；区块链经常被看作一本记录交易的账簿，区块链网路中所有的节点都参与到账簿的维护当中。相比于比特币网络中基于算力的 POW 共识机制，本方案采用了一种更加简便的共识过程使得联盟中的节点达到一致。主要是因为本方案中参与联盟链的算力不足，POW 很容易出现 51%算力攻击问题；另一方面，
- 10 本方案中联盟链都是可信任的节点，不需要 POW 的奖惩机制。本方案中联盟链节点的共识过程主要经历下面三个步骤：步骤 S31、每个 TLD 节点根据自己的标准，对每个域名操作进行独立校验；每个 TLD 节点根据自己的标准，对每个域名操作进行独立校验。步骤 S32，在预设时间内从 TLD 节点构成的网络中随机选择一个节点作为记账节点；每 5 分钟，从 TLD 节点构成的网络中随机选择一个节点，作为记账节点。步骤 S33，利用选中的 TLD 节点将预设时间内有效的域名操作打包进区块，并广播到其它 TLD 节点和更新 TLD 数据库；选中的 TLD 节点将这 5 分钟内有效的域名操作打包进区块，广播到其它 TLD 节点，更新 TLD 数据库。
- 15

- 域名操作和数据结构以及区块链中块的结构对于整个系统来说非常重要，在参考现有的区块链相关应用的前提下，设计适合于本方案的域名操作的数据结构以及区块的机构。TLD 节点根据域名操作的结构验证操作的
- 20

合法性，将有效的域名操作打包加入规定的区块头生成下一个区块。

表一域名操作的结构

长度	字段	描述
32 字节	域名操作 hash	保证域名操作的正确性
128 字节	域名操作发起者的公钥	解密私钥签名的数据，保障安全性
10 个字节	具体的域名操作	Register/delete/update 操作
4 字节	时间戳	域名操作被验证通过的时间点

表二区块头结构

长度	字段	描述
4 字节	版本	版本号，用来跟踪软件的升级
32 字节	前区块的哈希	链中前一区块的哈希值
32 字节	Merkle 根	这个区块中全部操纵构成的 merkle 树的根
4 字节	时间戳	域名操作被验证通过的时间点

图 2 示出了本发明提供的本发明的另一目的在于提供一种基于联盟链

5 的顶级域名管理系统，所述顶级域名管理系统包括：

构建联盟网络模块，用于利用 TLD 节点构成在区块链中的联盟网络；

分离模块，用于在联盟网络中对系统架构进行分层使得操作和数据分

离；

节点一致模块，用于通过共识过程使得联盟网络中的节点达到一致。

10 所述构建联盟链网络模块中 TLD 节点对新加入 TLD 节点的认证包括：

新注册节点信息发送单元，用于新加入 TLD 节点可向 TLD 网络中任意一节点发送注册新的认证节点的消息；

广播认证消息单元，用于将收到的新节点加入消息的节点想所有节点广播该认证消息；

5 网络节点反馈单元，用于网络中节点根据自身的规则选择同意或反对新加入的节点并将同意或反对的信息广播到其余节点；

批准加入记录单元，用于任意节点收到半数以上同意加入信息会认为网络同意该节点加入并记录该节点的消息。

所述节点一致模块中联盟网络节点的共识过程包括：

10 标准校验单元，用于每个 TLD 节点根据自己的标准，对每个域名操作进行独立校验；

记账节点单元，用于在预设时间内从 TLD 节点构成的网络中随机选择一个节点作为记账节点；

打包更新单元吗，用于利用选中的 TLD 节点将预设时间内有效的域名操作打包进区块，并广播到其它 TLD 节点和更新 TLD 数据库。

15 所述分离模块中将系统构架分层为底层和上层，其中底层为嵌入域名操作的区块链，上层为顶层域名相关数据构成的数据层；在所述数据层内 TLD 节点通过处理一系列的顶级域名操作更新 TLD database,并将所有的操作同时写入底层的区块链中；所述预设时间为 5 分钟。

20 本发明基于两层结构设计，提出了一个基于联盟链的顶级域名管理方法，该管理方法使得顶级域名系统的运行在去中心化的同时又得到合适

的管理。本发明中的顶级域名链采用了区块链作为事务记录的数据结构，并且本发明也提出了一种具体的区块头和域名操作的数据结构，更好地体现了去中心化的特性。另外，本发明引入了 TLD 节点的概念来加强顶级域名链的管理。本发明也提出了 TLD 数据库的一种实现方案，说明如何生成

5 从区块链到种子文件的映射。

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、一种基于区块链的顶级域名管理方法，其特征在于，所述顶级域名管理方法包括以下步骤：

A、利用 TLD 节点构成在区块链中的联盟网络；

5 B、在联盟网络中对系统架构进行分层使得操作和数据分离；

C、通过共识过程使得联盟网络中的节点达成一致。

2、根据权利要求 1 所述的顶级域名管理方法，其特征在于，所述步骤 A 中 TLD 节点对新加入 TLD 节点的认证包括以下步骤：

A1、新加入 TLD 节点可向 TLD 网络中任意一节点发送注册新的认证
10 节点的消息；

A2、将收到的新节点加入消息的节点想所有节点广播该认证消息；

A3、网络中节点根据自身的规则选择同意或反对新加入的节点并将同意或反对的信息广播到其余节点；

A4、任意节点收到半数以上同意加入信息会认为网络同意该节点加入
15 并记录该节点的消息。

3、根据权利要求 2 所述的顶级域名管理方法，其特征在于，所述步骤 C 中联盟网络节点的共识过程包括以下步骤：

C1、每个 TLD 节点根据自己的标准，对每个域名操作进行独立校验；

C2、在预设时间内从 TLD 节点构成的网络中随机选择一个节点作为
20 记账节点；

C3、利用选中的 TLD 节点将预设时间内有效的域名操作打包进区块，并广播到其它 TLD 节点和更新 TLD 数据库。

4、根据权利要求 3 所述的顶级域名管理方法，其特征在于，所述步骤 A 中将系统构架分层为底层和上层，其中底层为嵌入域名操作的区块链，
5 上层为顶层域名相关数据构成的数据层。

5、根据权利要求 4 所述的顶级域名管理方法，其特征在于，在所述数据层内 TLD 节点通过处理一系列的顶级域名操作更新 TLD database,并将所有的操作同时写入底层的区块链中。

6、根据权利要求 5 所述的顶级域名管理方法，其特征在于，所述预设
10 时间为 5 分钟。

7、一种基于联盟链的顶级域名管理系统，其特征在于，所述顶级域名管理系统包括：

构建联盟网络模块，用于利用 TLD 节点构成在区块链中的联盟网络；

分离模块，用于在联盟网络中对系统架构进行分层使得操作和数据分
15 离；

节点一致模块，用于通过共识过程使得联盟网络中的节点达到一致。

8、根据权利要求 7 所述的顶级域名管理系统，其特征在于，所述构建联盟链网络模块中 TLD 节点对新加入 TLD 节点的认证包括：

新注册节点信息发送单元，用于新加入 TLD 节点可向 TLD 网络中任
20 意一节点发送注册新的认证节点的消息；

广播认证消息单元，用于将收到的新节点加入消息的节点想所有节点广播该认证消息；

网络节点反馈单元，用于网络中节点根据自身的规则选择同意或反对新加入的节点并将同意或反对的信息广播到其余节点；

5 批准加入记录单元，用于任意节点收到半数以上同意加入信息会认为网络同意该节点加入并记录该节点的消息。

9、根据权利要求 8 所述的顶级域名管理系统，其特征在于，所述节点一致模块中联盟网络节点的共识过程包括：

标准校验单元，用于每个 TLD 节点根据自己的标准，对每个域名操作
10 进行独立校验；

记账节点单元，用于在预设时间内从 TLD 节点构成的网络中随机选择一个节点作为记账节点；

打包更新单元，用于利用选中的 TLD 节点将预设时间内有效的域名操作打包进区块，并广播到其它 TLD 节点和更新 TLD 数据库。

15 10、根据权利要求 9 所述的顶级域名管理系统，其特征在于，所述分离模块中将系统构架分层为底层和上层，其中底层为嵌入域名操作的区块链，上层为顶层域名相关数据构成的数据层；在所述数据层内 TLD 节点通过处理一系列的顶级域名操作更新 TLD database,并将所有的操作同时写入底层的区块链中；所述预设时间为 5 分钟。

20

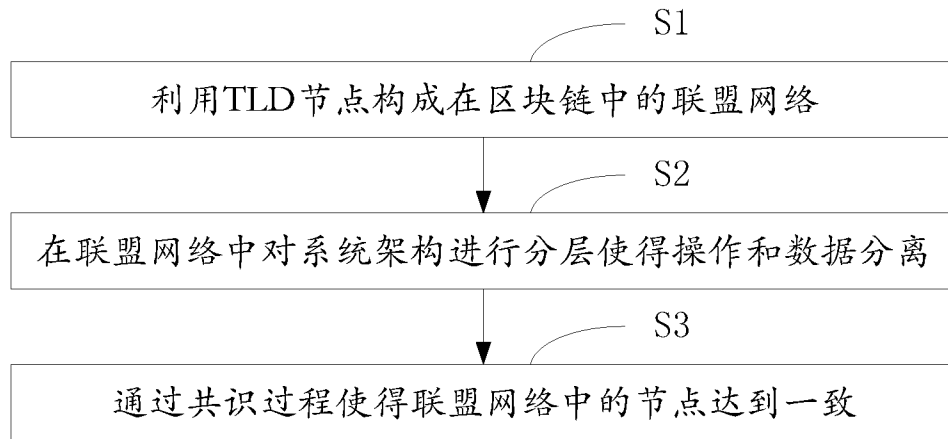


图 1

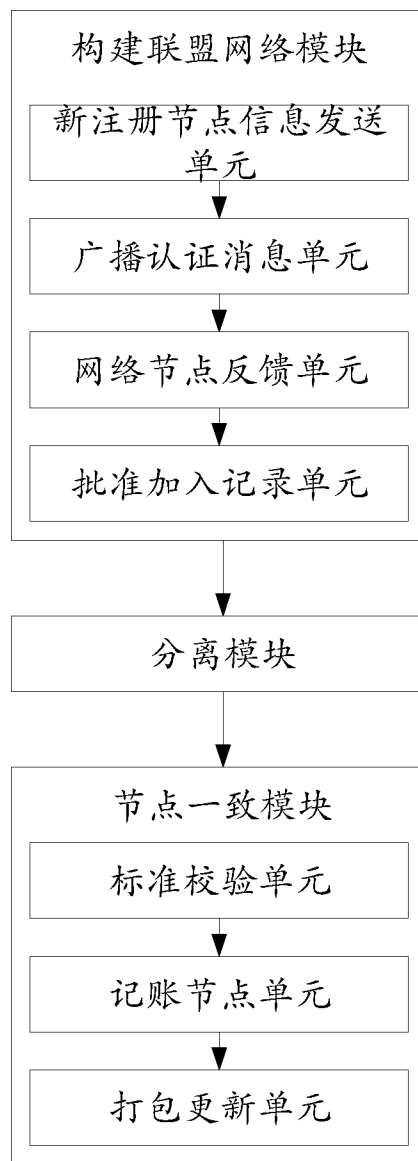


图 2

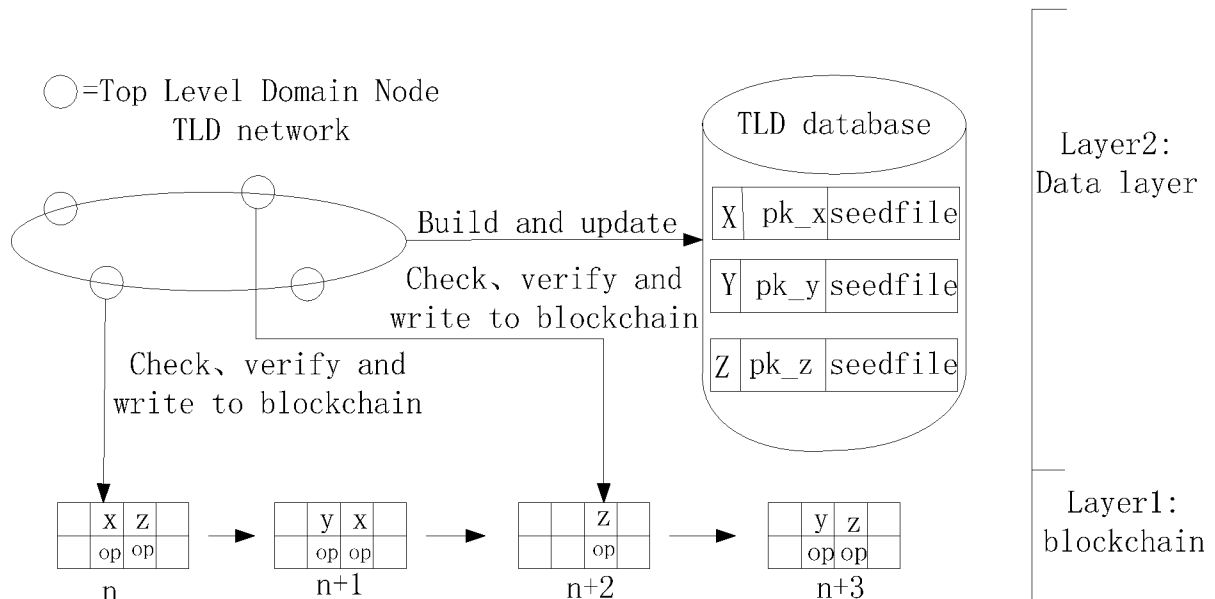


图 3

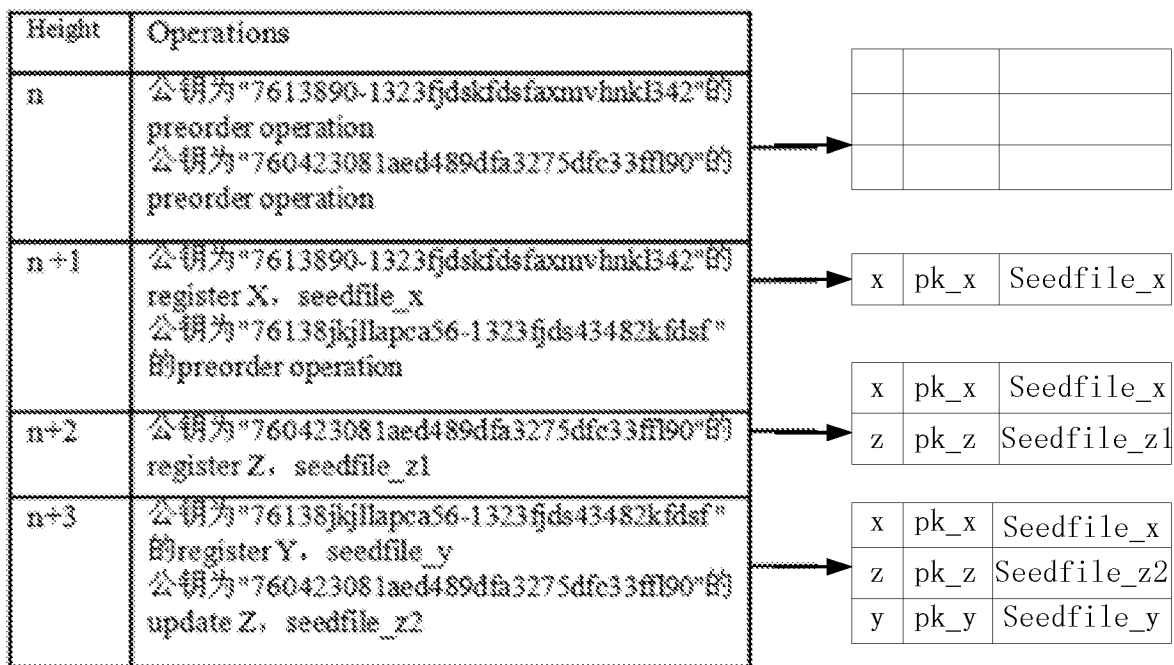


图 4

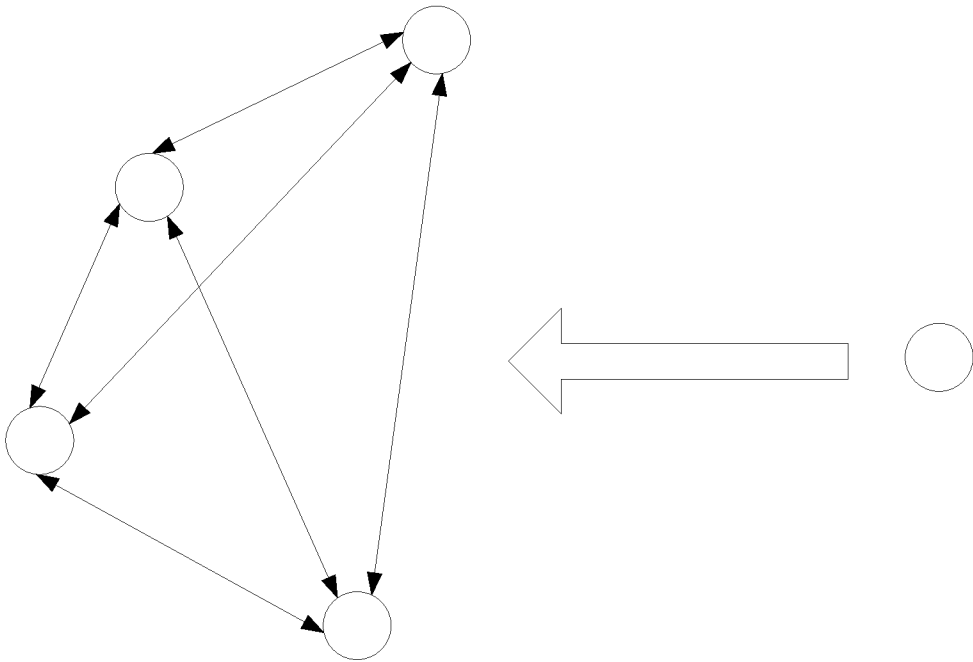


图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/079098

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

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; WPI; EPODOC; GOOGLE; IEEE: 区块链, 顶级域名, 管理, TLD, 联盟网络, 分层, 分离, 共识, 数据库, blockstack, block chain, block stack, top level domain, domain name, database, separat+, layer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2016177026 A1 (ZTE CORP.), 10 November 2016 (10.11.2016), description, page 1, line 19 to page 3, line 27, and figures 1-5	1-10
A	CN 101335618 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 31 December 2008 (31.12.2008), entire document	1-10
A	CN 103347087 A (GUILIN UNIVERSITY OF ELECTRONIC TECHNOLOGY), 09 October 2013 (09.10.2013), entire document	1-10
A	CN 105978697 A (NINGSHENG FINANCE INFORMATION SERVICE (SHANGHAI) CO., LTD.), 28 September 2016 (28.09.2016), entire document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 08 December 2017	Date of mailing of the international search report 03 January 2018
Name and mailing address of the ISA 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 XING, Yunfeng Telephone No. (86-10) 62413374

International application No.
PCT/CN2017/079098

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2017/079098

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

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; WPI; EPODOC; GOOGLE; IEEE; 区块链, 顶级域名, 管理, TLD, 联盟网络, 分层, 分离, 共识, 数据库, blockstack, block chain, block stack, top level domain, domain name, database, separat+, layer

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	WO 2016177026 A1 (中兴通讯股份有限公司) 2016年 11月 10日 (2016 - 11 - 10) 说明书第1页第19行至第3页第27行, 图1-5	1-10
A	CN 101335618 A (南京邮电大学) 2008年 12月 31日 (2008 - 12 - 31) 全文	1-10
A	CN 103347087 A (桂林电子科技大学) 2013年 10月 9日 (2013 - 10 - 09) 全文	1-10
A	CN 105978697 A (宁圣金融信息服务上海有限公司) 2016年 9月 28日 (2016 - 09 - 28) 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

2017年 12月 8日

国际检索报告邮寄日期

2018年 1月 3日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

邢雲峰

传真号 (86-10) 62019451

电话号码 (86-10) 62413374

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/079098

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)
WO	2016177026	A1	2016年 11月 10日	CN	106209947	A	2016年 12月 7日
CN	101335618	A	2008年 12月 31日	无			
CN	103347087	A	2013年 10月 9日	无			
CN	105978697	A	2016年 9月 28日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)