



专题：网络空间安全

基于区块链的 DNS 根域名解析体系

庄天舒¹, 刘文峰², 李东^{2,3}

- (1. 长春大学计算机科学技术学院, 吉林 长春 130022;
2. 哈尔滨工业大学计算机科学与技术学院, 黑龙江 哈尔滨 150001;
3. 电子科技大学广东电子信息工程研究院, 广东 东莞 523808)

摘要: 互联网域名系统的中心化解析体系蕴含无法避免的权力滥用风险, 即一个顶级域可能从根区中被删除。通过分析当前根区中心化方面的工作, 指出大多数解决方案主要是在当前根区之外部署新的根解析服务, 而并未实现对根区数据去中心化。提出一种对根区数据去中心化的方案, 通过国家根之间点对点联盟实现根区数据分发与解析的去中心化。本方案将信任从点对点转变为集体, 在具备自主、开放、平等、透明等特征的同时, 通过区块链技术实现了对根区数据的分布式共识, 从而保障根区数据一致性。

关键词: 域名系统; 区块链; 去中心化

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018125

DNS root domain name analysis system based on block chain

ZHUANG Tianshu¹, LIU Wenfeng², LI Dong^{2,3}

1. College of Computer Science and Technology, Changchun University, Changchun 130022, China
2. School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China
3. UESTC Guangdong Institute of Electronic Information Engineering, Dongguan 523808, China

Abstract: The centralized resolution system of the domain name system (DNS) implies an unavoidable risk of abuse of power, a top-level domain may be deleted from the root zone. By analyzing the related work on the root zone decentralization, the most were mainly to deploy new root resolution services outside the current root servers, but not to decentralize the root zone data. A scheme to decentralize the root zone data was proposed, and the decentralization of root zone data distribution and analysis were achieved through a peer-to-peer coalition between national roots. Trust from peer-to-peer to collective, with features such as autonomy, openness, equality, and transparency, and implements a distributed consensus on root zone data through blockchain technology were transformed by the program, thereby ensuring root zone data consistency.

Key words: domain name system, blockchain, decentralization

收稿日期: 2018-01-20; 修回日期: 2018-03-09

通信作者: 刘文峰, 15b903031@hit.edu.cn

基金项目: 东莞市引进创新科研团队计划基金资助项目 (No.201636000100038)

Foundation Item: Dongguan Innovative Research Team Program (No.201636000100038)



1 引言

域名系统 (domain name system, DNS) 作为关键互联网基础设施, 为大量互联网应用提供了域名到 IP 地址的解析服务。一次完整的域名解析需要多个层级的权威服务器参与, 根服务器负责解析根区并提供顶级域名 (top level domain, TLD) 服务器的索引列表。网络使用者无论是选择基于 PC 的有线网络互连, 还是选择以 4G、5G 技术^[1-3]为主的无线网络互连, 都需要借助域名系统将所连接目标的域名转化为 IP 地址后发起通信。在当前域名体系中, 根的中心化特征体现在以下 3 个方面。

(1) 结构方面

域名的名字空间结构和解析依赖结构都是单根树, 根域是名字空间的顶点, 根服务器是域名解析的起点。

(2) 管理方面

根区管理属于互联网数字分配机构 (internet assigned numbers authority, IANA) 的职能。目前, 互联网名称和数字地址分配机构 (internet corporation for authorized names and numbers, ICANN) 作为根区管理者, 负责根区更新的最终审批; 公共技术标识符机构 (public technical identifiers, PTI, ICANN 附属机构), 作为根区运营者, 负责处理来自顶级域运营者的根区更新申请; 威瑞信公司 (VeriSign), 作为根区维护者, 负责根区数据的更新与发布。

(3) 机制方面

所有递归解析器软件中的根服务器配置 (称为 “root hint”) 包含 13 个根服务器的 IP 地址, DNS 安全扩展 (DNS security extension, DNSSEC) 协议的信任锚都配置为根的密钥签名密钥 (key signing key, KSK) 的公钥。

高度中心化的特征使当前域名体系蕴含着权力滥用的威胁, 当权力滥用发生时, 顶级域名持有者面临消失性风险和致盲性风险。

(3) 消失性风险

已授权的顶级域名资源被撤销, 或从根区文件中被删除, 导致该顶级域名在根服务器中消失, 用户无法访问该顶级域名及其子域名。如果一个国家代码顶级域名 (country code top level domain, ccTLD) 被删除, 则该国域名下的域名体系也随之崩溃。

(4) 致盲性风险

根服务器或根镜像的运营者拒绝为特定范围内的递归解析器提供解析服务, 由于域名解析结构具有中心化特征, 根服务器拒绝服务将导致递归解析器无法解析域名。若递归解析器软件的默认配置不做更改, 用户无法使用这些被 “致盲” 的递归解析器从 13 个根服务器之外获取 TLD 信息。

综上所述, 根域名解析体系的高度中心化蕴含着权力滥用风险。从国家网络主权的角度来看, 任何已经分配给国家的顶级域名都是国家网络疆域的一部分, 本国域名的解析权理应由自己控制。但从域名系统现状来看, 无论是基础设施还是根区数据都由中心节点控制, 顶级域名持有者对此缺乏有效的制衡手段。本文针对这一问题提出一个基于区块链的根域名解析体系, 该方案在原有工作^[4]的基础上, 采用区块链技术解决了各根节点在数据交换过程中出现的数据不一致问题。

2 相关工作

2.1 根的去中心化

根的去中心化方案不同程度地降低了解析器对根服务器的依赖程度, 下面对这些方案做简要介绍。

(1) 递归根方案^[5]

本质是让解析器实现根服务器的功能。在该方案中, 允许解析器使用本地回环 (loopback) 地址提供对根区的解析服务, 由于根区解析服务只绑定在回环地址上, 因而该服务只对解析器本机

有效。递归根方案就给递归解析器附加了一个只给自己使用的根服务器,根区数据还是来源于IANA。

(2) 伪装根方案

本质是伪装成根服务器应答的流量劫持技术。伪装根方案有多种实现方式,无论通过哪种技术实现,其目标都是要在真正的根服务器之前响应对根的查询请求。该方案的初衷是用来降低用户查询时延,多由网络运营商实施。

(3) 开放根方案

本质是一组独立运营的根服务器,这组根服务器使用IANA的根区数据为用户提供根区解析。开放根与现有根服务器的区别之一在于,其IP地址并不在递归服务器软件缺省配置中。现有的开放根项目主要有OSRN^[6]计划和Yeti^[7]计划(又称“雪人计划”)。

(4) 全球根方案

本质上是一种通用根服务器数量扩展方案^[8]。通过任播技术,该方案可以将全球现有的13个根服务器扩展到更大规模。该方案在根区中添加一个称作UARS(universal anycast root server)的全局逻辑根服务器,网络运营商可在自治域内搭建属于自己的根服务器,用户则通过任播技术访问自治域内的根服务器。

(5) 另类根方案

这类方案尝试建立一个完全独立于当前域名系统的新域名解析体系,并尝试建立新的、平行的名字空间。新的名字空间或继承原有名字空间中的域名分配结果,或完全抛弃已有域名,采用全新的域名分配机制,因此另类根方案中使用的域名也被称为“另类域名/山寨域名”。公共根(public-root)^[9]方案和统一根(unified-root)^[10]方案都使用了新名字空间,该名字空间兼容原来的名字空间,是原名字空间的超集。

2.2 NameCoin

NameCoin^[11]是基于区块链技术实现的去中心

化的域名体系。NameCoin中不存在类似“ICANN”的域名分配机构,而是采用“先占先得”的方式分配“.bit”域下的域名,即一个域名会分配给最早申请该域名并被记入公开账簿的申请者。NameCoin的共识采用类似比特币的工作量证明机制来实现,因此,算力决定了域名分配的权力。

NameCoin也存在以下局限性,使得其设计难以直接应用于根的去中心化。

- 恶意抢注:先占先得的域名分配机制会造成恶意抢注,无法保证具有天然归属特性的国家代码顶级域名被正确分配。
- 兼容性问题:现有的递归解析器无法解析.bit域名,用户需要第三方插件实现解析。

3 设计目标

3.1 域名空间统一与域名唯一性

新的根域名体系使用与原域名体系相同的名字空间,并确保域名的唯一性。统一的域名空间是互联网作为一个整体的关键,分裂的名字空间阻碍互联互通,同时也带来了域名仿冒的风险。域名唯一性是DNS最基本的功能与安全属性。

在本文第2.1节所述的域名系统去中心化方案中,绝大多数的方案要么直接使用原根数据,解决不了根区数据由单节点控制的弊端;要么另辟蹊径,重新使用新的名字空间和新的名字分配机制,但会导致新旧体系中的域名不兼容。参考文献[11]中的方案在设计时考虑到这一设计目标,需要所有参与根联盟的根节点自发遵守,根联盟内部的蓄意破坏者可以打破这一目标。

3.2 根区数据一致性

由多互联根共同管理数据后,保证各互联根得到的数据一致。互联根1.0方案采用点对点的方式在联盟内建立信任,建立互信的互联根交换顶级域数据,共同管理根区。这种信任机制和数据交换机制容易使互联根间数据不一致,造成不一致的因素有很多,攻击行为、信任现状都可能造



成联盟内的根服务器数据不一致。

(1) 攻击行为

例如，中国国家顶级域名（CN）的互联根被攻击，并造成私钥泄露，攻击者伪造 CN 顶级域数据向其他根发布数据更新。其他根服务器对 CN 遭受攻击的状况毫不知情，接收了 CN 的新顶级域数据。遭到欺骗的根并没有意识到自己与其他 5 个互联根的根区数据已经不同，联盟内的互联根间出现数据不一致。

(2) 信任现状

根服务器尚未在所有节点间建立信任关系。假设英国顶级域名（UK）仅与俄罗斯顶级域名（RU）建立点对点信任关系，所以 UK 根只能与 RU 根互换顶级域数据，而 RU 根域香港域名（HK）根、韩国域名（KR）根、德国域名（DE）根均建立了点对点的信任关系，因而可以得到它们的数据。UK 根与 RU 根因建立信任的对象数量不同导致根区数据不同，联盟内的互联根间出现数据不一致。

本方案是基于参考文献[11]的一种改进方案，提出了一个基于“根联盟”概念的自主根域名解析体系。不同于本文第 2 节所述的中心化方案和现有域名体系^[12]，本方案从根服务器和根区数据两个方面都实现了对根的去中心化，这两方面相辅相成，缺一不可。如果根服务器没有去中心化，即使根区数据管理实现去中心化，解析过程还是要依赖现有根服务器；同理，如果根区数据管理没有去中心化，即使搭建了新的根服务器，解析过程还要依赖 IANA 管理的根区数据。

3.3 核心思想

基于区块链的新方案的核心思想是在根服务器和根区数据两个方面都实现了对根的去中心化。本方案仍然采用了组建“根联盟”实现共同管理根区数据的思路^[13]，与原方案有相同的体系结构，增加了保障根区数据管理结果一致性的措施。在本方案中，根联盟内通过共识算法（类 PBFT

算法）协商根区管理过程，保证协商出的根区数据达成一致。出于共识算法自身具有的特性，根联盟内允许出现少量的故障节点和恶意节点。当根联盟内的大部分节点正常运转时，根联盟整体的数据一致性就能得到保证。

3.4 方案概览

基于区块链的互联根域名解析体系有两个核心部分组成：自主根和根联盟，该体系结构与原方案类似。

(1) 自主根是一台特殊的根服务器

所有顶级域名的持有者都可以搭建属于自己的自主根，这些根服务器与当前域名系统中的根服务器并存。递归解析器可以自主选择使用两者中的任何一个作为域名解析的起点。在该体系中，自主根除了提供对根域的解析功能外，还负责与其他自主根交换顶级域数据。

(2) 根联盟是由多个自主根依据互联协议组建而成的网络

从技术上来讲，该网络在本质上是一个分布式的区块链系统。根联盟是一个平等、开放的互联体系，所有顶级域的持有者都可以随时选择加入或退出根联盟。根联盟使用公钥唯一标识每个加入根联盟的主体，公钥所绑定的域名信息在自主根名片中记录，域名的持有者需使用对应私钥将所持域名的相关数据进行签名。联盟内采用类 PBFT 的共识算法进行协商，共同决策新的数据发布是否有效。在联盟内超过 2/3 的节点做出正确决策的情况下，共识算法保证联盟整体的决策一致性。

3.5 根区数据发布

所有顶级域持有者分别向根联盟发布所持有的顶级域名信息并接受其他成员的决策，根联盟使集体内的所有决策达成共识，实现所有成员共同管理根区数据且数据一致。根区管理方案由以下 4 个关键步骤组成。

步骤 1 通知阶段：国家根向根联盟就所持的顶级域名发起数据更新。

步骤 2 同意阶段：数据更新申请在根联盟内广播，由所有其他国家根对数据更新内容的合法性做检查，其他国家根对通过检查的更新请求签名为“同意”并回复给发起者。发起更新请求的国家根收集足够数量的“同意”并将这些“同意”合并为“联名同意背书”后广播；若发起更新请求的国家根没有收集到足够数量的“同意”，则默认此次顶级域数据更新行为被根联盟否决，终止后续操作。

步骤 3 更新阶段：收到“联名同意背书”的其他国家根向发起请求的国家根回复“承诺”，承诺按照其申请内容更新数据。发起更新请求的国家根收集足够数量的“承诺”并将这些“承诺”合并为“联名承诺背书”后广播。

步骤 4 确认阶段：收到“联名更新承诺”的其他国家根更新根区数据并返回更新结果。

经过上述 4 个步骤，根区数据可以在所有国家根共同管理的情况下达成一致。其中步骤 2 和步骤 3 是关键，步骤 2 完成意味着根联盟对数据更新申请达成共识，步骤 3 完成意味着根联盟对承诺数据更新达成共识。4 个步骤完成后，联盟对一次数据更新请求达成共识，对这次更新请求的管理过程结束。

3.6 新体系特性

基于区块链的互联根体系具有以下特性。

(1) 域名空间统一与域名唯一性

新体系虽然不使用 IANA 提供的根区数据，但新体系与当前域名系统一样，都遵循 IANA 作为唯一的名字空间管理机构。新体系以 IANA 的域名分配结果为基准，将其写入自主根名片中，作为根联盟验证顶级域发布合法与否的依据。

(2) 数据一致性

共识算法保证根区数据在所有根节点一致。当某个互联根发生私钥泄露且被用于伪造攻击时，受骗的根可以很快发现信息与其他根不一致，从而触发线下应急响应。基于区块链的域名体系

依赖的是集体共识，不同于双边共识，所有加入根联盟的互联根都相信其他根节点组成的集体，因而该体系并不存在因信任关系导致的数据不一致。

(3) 自主性

所有顶级域的持有者按照自主意愿建立根服务器，且自主根不依赖 IANA 数据运转。

(4) 透明性与兼容性

整个系统与当前的 DNS 互不冲突；新体系只涉及域名解析，兼容已有的 IANA 域名授权管理结果；根联盟体系对除采用国家根的递归解析器外其他 DNS 组件透明；新体系无需对当前 DNS 服务器软件做任何改动，对 DNS 协议本身透明。

(5) 渐进部署

新体系支持渐进式部署，根联盟的规模可以随着自主根的建立逐步扩大，直至覆盖所有顶级域名。

4 结束语

近年来，大量研究尝试通过扩展方案和去中心化方案弱化根服务体系的中心化现状^[14]，但在互联根方案^[15]之前，绝大多数的去中心化研究要么无法解决根区数据依赖 IANA 的现状，要么直接放弃兼容性，采用新的域名空间和新的域名分配策略。互联根方案是在保证域名空间统一性的基础上的域名系统去中心化方案，本文在互联根方案的基础上，提出基于区块链的互联根体系。该体系在继承互联根方案特性的基础上，借由区块链技术的特性消除各互联根之间的数据不一致问题，确保所有的互联根都提供一致的域名解析服务。

参考文献：

- [1] 卢卫, 陆希玉. 4G 时代移动互联网的发展趋势[J]. 电信科学, 2014, 30(5): 51-54.
LU W, LU X Y. Mobile internet trends in 4G era [J]. Telecommunications Science, 2014, 30(5): 51-54.
- [2] 林金桐, 许晓东. 第五代移动互联网[J]. 电信科学, 2015, 31(5): 7-14.
LIN J T, XU X D. The 5th generation of mobile internet[J].



- Telecommunications Science, 2015, 31(5): 7-14.
- [3] 刘云璐, 杨光, 杨宁, 等. 面向 5G 的多网融合研究[J]. 电信科学, 2015, 31(5): 63-67.
- LIU Y L, YANG G, YANG N, et al. Study on multi-RAT coordination in 5G [J]. Telecommunications Science, 2015, 31(5): 63-67.
- [4] 张宇, 夏重达, 方滨兴, 等. 一个自主开放的互联网根域名解析体系[J]. 信息安全学报, 2017, 2(4).
- ZHANG Y, XIA C D, FANG B X, et al. An autonomous open root resolution architecture for domain name system in the internet[J]. Journal of Cyber Security, 2017, 2(4).
- [5] KUMARI W, HOFFMAN P. Decreasing access time to root servers by running one on loopback[S]. 2015.
- [6] BOFFIN M, et al. Open root server network[EB/OL]. (2012-05-21)[2018-03-08]. <http://www.orsn.org>.
- [7] VIXIE P. Yeti DNS project[EB/OL]. (2015-01-08)[2018-03-08]. <http://www.yeti-dns.org>.
- [8] LEE X D, YAN Z, VIXIE P. How to scale the DNS root system?[R]. Internet Draft, 2015.
- [9] Public-Root project [EB/OL]. (2003-02-21)[2018-03-08]. <http://public-root.com/tlds.htm>.
- [10] UnifiedRoot project[EB/OL]. (2014-05-24)[2018-03-08]. <http://www.unifiedroot.com>.
- [11] Namecoin project[EB/OL]. (2018-02-21)[2018-03-08]. <https://namecoin.org>.
- [12] CASTRO M O T D. Practical byzantine fault tolerance[M]. Cambridge: Massachusetts Institute of Technology, 2000.
- [13] SCHWARTZ D, YOUNGS N, BRITTO A. The ripple protocol consensus algorithm[R]. 2014.
- [14] JAKOBSSON B M, JUELS A. Proofs of work and bread pudding protocols: US 7356696 B1[P]. 2008.
- [15] Proof-of-stake consensus algorithm[EB/OL]. (2018-03-04)

[2018-03-08]. <https://en.wikipedia.org/wiki/Proof-of-stake>.

- [16] 延志伟, 耿光刚, 李洪涛, 等. DNS 根服务体系的发展研究[J]. 网络与信息安全学报, 2017, 3(3): 1-12.

YAN Z W, GENG G G, LI H T, et al. Study on the development of the DNS root system[J]. Chinese Journal of Network and Information Security, 2017, 3(3): 1-12.

[作者简介]



庄天舒 (1983-), 女, 长春大学计算机科学技术学院讲师, 主要研究方向为计算机程序设计特殊教育、网络安全、未来网络体系等。



刘文峰 (1992-), 男, 哈尔滨工业大学计算机科学与技术学院博士生, 主要研究方向为网络体系结构、网络安全等。



李东 (1967-), 男, 电子科技大学广东电子信息工程研究院教授, 主要研究方向为网络信息安全技术、并行计算、计算机体系结构、计算机图形学等。