区块链在域名体系 DNS 中的初步应用研究

蒋兴胜

（西南民族大学计算机科学与技术学院，四川 成都 610000）

摘 要：当前域名体系中，域名名字空间和域名解析依赖的逻辑结构都是单根树，域名的管理机构高度一国化集中，这就隐含着权力滥用的威胁。当权力滥用发生时，顶级域名持有者会面临消失性风险和致盲性风险。针对这一问题，本文提出在现有体系中引入区块链技术组建联盟链，让各国自主根服务器能在链内共享各节点对本国顶级域的权威解析数据。在原根系统出现人为故障时，从联盟链共享的数据区块中获得其他 TLD 权威服务器的 IP 地址完成域名解析，完全化解权力滥用时发生的域名解析风险。

关键词：域名系统；区块链；国家自主根；联盟链

Research of the preliminary application about block chain used in the domain name system

JIANG Xinsheng

（School of Computer Science and Technology, Southwest Minzu University, Chengdu 610000 China）

Abstract：In the current domain name system, the name space and name resolution depends on the logical structure of single tree, and highly country management authority of the domain name , means the abuse of power. When power abuse occurs, the top-level domain name holders will face the disappearing and blinding risks. In order to solve this problem, in this paper, we introduce block chain technology into the existing system to form a chain alliance, where countries, independent root server can be Shared within the chain of each node to the authority of the top-level domain analytical data. When the original root system fault, we can get other TLD authoritative server IP address from league chain Shared data blocks, complete the domain name resolution and completely resolve the power abuse risk.

Key words：the domain name system；block chain; national autonomous root; league chain

0 引 言

访问互联网时，网民容易记住网站的域名，但机器间通信只认 IP 地址。域名与 IP 地址之间的转换就是域名解析，域名解析得由专门的 DNS（domain name system，DNS）服务器完成。互联网早期使用 Hosts 文件解析，各主机通过 FTP 完成更新。现在的 DNS 系统是通过遍布全球的一个分布式数据库来完成域名解析的。

域名的名字空间结构如图 1 所示，是一棵单根树。域名空间被划分为多个区（Zone），如图 2 所示。每个区由权威 DNS 服务器负责解析，如图 3 所示。

域名解析过程如图 4 所示，主机向本地域名服务器发起递归查询，本地域名服务器向根服务器、顶级域名服务器、权限域名服务器等权威服务器发起迭代查询。最后完成域名到 IP 的映射。

作者简介：蒋兴胜（1971–），男，硕士，西南民族大学计算机科学与技术学院实验师，主要研究方向为计算机软件与理论、数据库技术、网络技术等。

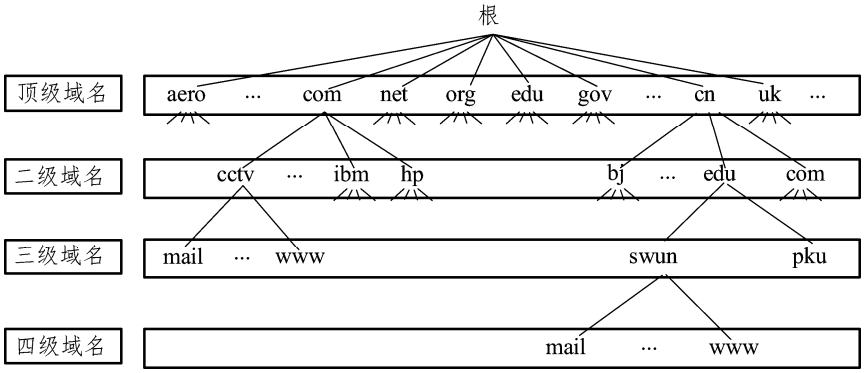

图 1　域名空间

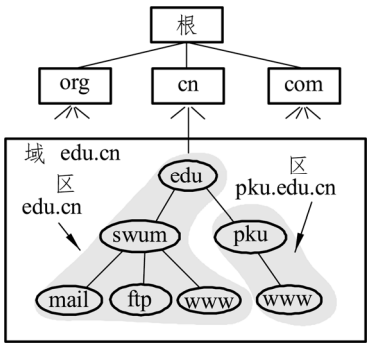

图 2　域名空间的区域划分

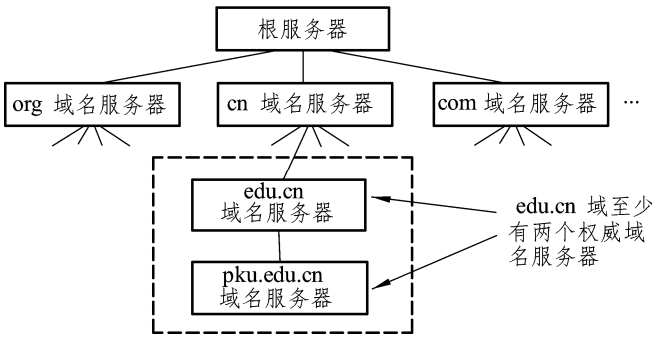

图 3　解析区域数据的 DNS 服务器关系

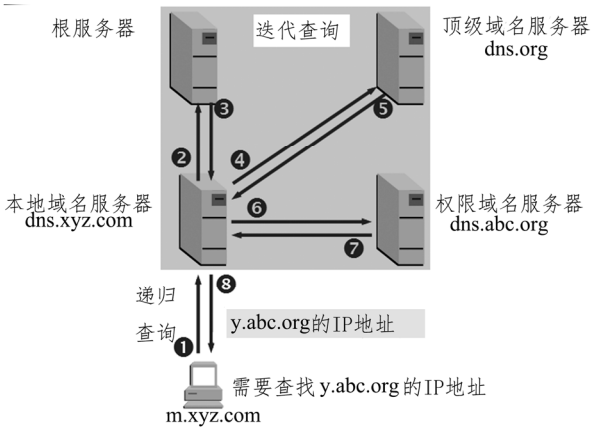

图 4　域名解析的递归及迭代查询过程

一次完整的域名解析需要多层权威服务器参与：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；TLD 服务器负责解析各自顶级域区并提供其管辖区内各权限域名服务器的索引列表；权限域名服务器负责解析它所管辖的域名区域。DNS 域名空间结构、域名分配和解析过程都是严格分层组织。

目前，IP 地址、域名等关键网络资源管理权属于 IANA（Internet Assigned Numbers Authority，互联网数字分配机构）。而 IANA 由美国商务部的下属单位 NTIA（National Telecommunications and Information Administration，国家电信和信息管理局）管辖。NTIA 将 IANA 职能授权给 ICANN（Internet Corporation for Assigned Names and Numbers，美国互联网名称与数字地址分配机构）。ICANN 负责顶级域的注册和授权，拥有根区数据更新的最终审批权；作为根区运营者的 ICANN 附属机构 PTI（Public Technical Identifiers，公共技术标识符

机构），负责处理来自顶级域运营者的根区数据更新申请；作为根区维护者的美国 VeriSign 公司负责根区数据的实际修改，修改后发布到全球的 13 个根服务器及其镜像。这 13 个根服务器中，1 个为主根服务器，其余 12 个为辅根服务器。其地域分布比较集中：美国放置有 9 个根服务器（含主根服务器），英国、瑞典、日本各有一个。

当前域名体系中，域名空间和解析依赖的逻辑结构都是单根树，加之根区这种管理模式，导致其高度中心化特征明显。文献[1]指出这种根中心化结构隐含着权力滥用的威胁，当权力滥用发生时，顶级域名持有者将面临消失性风险和致盲性风险。

（1）消失性风险。

若撤销已授权的特定顶级域名资源，或将其记录从根区文件中删除，将导致该顶级域名从根服务器中消失，网络用户无法访问该顶级域名下网站。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，这是一国互联网被抹掉的风险。

（2）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，将导致递归解析器无法解析域名。若针对一个国家，这就是禁止一国网络用户访问互联网的风险。

综上所述，现有域名体系根区的高度中心化蕴含着权力滥用风险。以网络空间主权的视角，任何已经分配给某国家的顶级域名都应被视为这个国家的网络领土，自己国家域名的解析权理应让自己控制。但从 DNS 现状来看，无论是相关的基础设施还是名字空间的根区数据都是由中心节点控制，顶级域名持有者对此是被动的且缺乏有效的制衡手段。针对这一问题我们提出一个引入区块链技术的联盟链新体系，该方案采用区块链技术共享各国家自主根节点对本国顶级域的权威解析数据，在原根系统出现故障时，能直接从联盟链共享的数据区块中获得其他 TLD 权威服务器的 IP 地址完成域名解析。

1 相关工作

针对域名体系根中心化特点，有以下几种去中心化方案。下面对这些方案做个简要介绍。

（1）本地 DNS 服务器配置根方案：在本地 DNS 服务器上直接做根区解析，实质就是把根服务器设置为本地递归解析器，可以消除递归到根服务器的延迟。

（2）镜像根方案：部分网络运营商建立镜像根，在真正的根服务器之前响应解析器对根的查询请求，可减少查询时延并提高可靠性。

（3）开放根方案：建立一组独立运营的根服务器，仍使用 IANA 根区数据，但不提供 TLD 注册服务，也不创建新的名字空间。可解决根服务器地理分布不均衡问题以及改变根区治理被一国垄断的格局。现有的开放根项目主要有 OSRN[2] 计划和 Yeti[3]计划（又称“雪人计划”）。

（4）全局逻辑根方案：本质上是一种通用根服务器数量扩展方案[4]。在当前 DNS 体系的根区中添加一个称作 UARS（Universal Anycast Root Server，UARS）的全局逻辑根服务器。任何组织都可在自治域内搭建 UARS 服务器，用户通过任播技术实现对特定区域根区解析服务。

（5）另类根方案：建立一个完全独立于当前 IANA 体系的新域名解析系统，建立一个另类名字空间，通常称作“另类域名/山寨域名”。Public-Root[5]方案和 Unified-root[6]方案都使用了新名字空间，兼容原空间，是原空间的超集。此类方案不属于当前 DNS 体系，不满足统一名字空间需求。

前四种方案从本质上是对根区解析服务去中心化，（1）和（2）是一种性能优化方案，（3）和（4）则是建立独立的根服务器，与原根共存。共同点是，根区数据依然来自 IANA，并没有改变 DNS 根中心化结构，权力滥用风险依然存在。对等网思想也被应用于 DNS，此类方案实现了部分 DNS 系统组件去中心化，或针对解析功能，或针对权威服务器，但并未提出完整可替代的根解析体系，因而对根权力滥用的遏制能力有限。

2 引入区块链技术的新设计

2.1 主要思想

各个国家新增一个国家自主根服务器，在原域名系统的Root层增加一个由各国自主根服务器组成的联盟链，链成员间基于区块链技术自愿交换共享顶级域数据。

新设计不改变现有域名空间及域名唯一性，承认 IANA 当前管理模式。TLD 的授权与 TLD 的解析相分离，新设计中仍然由 IANA 负责 TLD 授权，但解析由联盟链或原根完成。由于现有 13 个根服务器与联盟链并存，使得完全依赖于单一权威的域名解析摆脱现状，实现了解析服务的去中心化。新设计既满足了统一域名空间与名字唯一性需求，又实现了对根权威权力的制衡。

2.2 新设计下的系统方案

加入基于区块链技术的联盟链后新的 DNS 结构如图 5 所示，有两个核心的部分：国家自主根和联盟链。

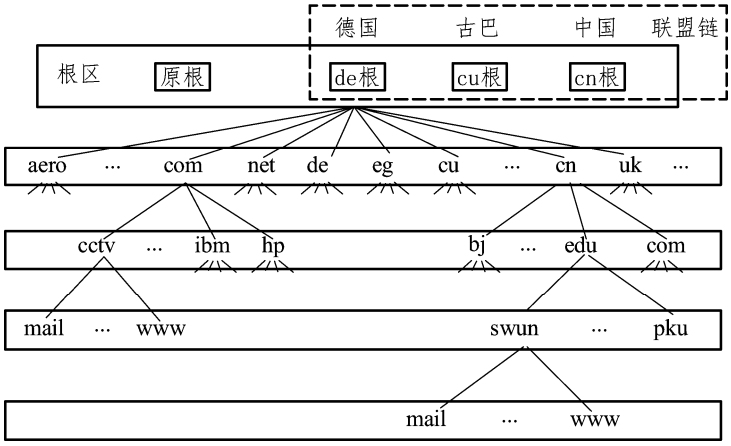

图 5 新设计 DNS 结构

（1）国家自主根是一台特殊的根服务器。

由国家顶级域名的持有者搭建属于自己的国家自主根，如：中国的 cn 根、古巴的 cu 根、德国的 de 根。这些国家根完成解析任务的数据来源于 IANA 的根区数据、本国 TLD 权威报备的根区数据、与其他国家自主根交换来的顶级域数据，国家自主根主要提供对根域的解析功能。

（2）联盟链是由多个国家自主根依据互联协议组建而成的网络。

该网络在本质上是一个分布式的区块链系统[7]。每个国家自主根为网络上的一个节点，每个节点拥有由不可逆椭圆曲线加密函数得出的私钥公钥对，联盟链使用公钥唯一标识每个加入的主体，公钥所绑定的来自 TLD 权威域名信息在国家自主根的数据块中记录，域名拥有者需使用对应私钥签名所持相关域名数据。联盟链内采用类 PBFT 的共识算法进行协商，共同决策新的数据块发布是否有效。在联盟链内超过 2/3 的节点做出判断的情况下，共识算法保证联盟链整体的数据一致性与决策一致性。

新结构下，用户或递归解析器即可使用原根也可使用联盟链内各国家自主根的根区解析服务，可以非常灵活地制定本地信任策略，最大限度地保证 DNS 解析成功。

2.3 防范滥用风险分析

新方案中，假设相关顶级域信息已经成功发布到了国家自主根，而且自主根是稳定安全可靠的，只有原根存在权力滥用问题。以此为假设前提来分析各种风险发生时的域名解析过程[8]。

对于消失性风险，如图 5 所示，假定德国的 de 域从原根服务器中被抹去，中国的递归解析器将无法从原根处得到其信息。如果递归解析器将根指向了中国国家自主根，德国与中国同为联盟链中节点，则两国国家自主根已经交换过各自授

权 ccTLD 信息，此时中国递归服务器就仍可以得到.de 域信息，顺利访问.de 域下域名。这样联盟链中，德国的 ccTLD 并没有消失。迭代解析过程与传统系统架构下类似。

对于致盲性风险，假定原根拒绝对古巴提供服务，对于配置了中国国家根的递归服务器，要解析古巴国家 ccTLD 下域名，与上述“消失性风险”中解析过程雷同，依然可以在联盟链中获得古巴国家 ccTLD 信息，递归解析器一样可以对顶级域.cu 下域名进行解析。

可见，新体系完全具备防范根权威权力滥用的能力。

2.4 新系统的特性

引入区块链技术的新域名体系具有以下特性：

（1）域名空间统一与域名唯一性。

新系统中的国家自主根虽然不直接使用 IANA 提供的根区数据，但它与原 DNS 域名系统一样，都是将 IANA 作为唯一的名字空间管理机构。以 IANA 的域名分配审批结果为权威数据来源，只不过将其写入国家自主根数据块中，作为联盟链验证顶级域名发布合法性的凭证。

（2）数据一致性。

类 PBFT 的共识算法保证 DNS 根区数据在所有国家自主根节点一致。当某个国家自主根发生私钥泄露而被用于伪造攻击时，联盟链内受骗的网络节点能很快发现信息的不一致，从而触发线上线下危机响应处理机制，让事情得到处理而保证了数据的一致性。

（3）相对独立性。

两层意思，一是顶级域的持有者可按照自己意愿决定是否另外组建自己的国家自主根服务器；二是一旦组建了国家自主根加入了联盟链，那么国家自主根的解析数据将不再唯一依赖 IANA，还可以从联盟链内其他对等节点处直接获得。

（4）透明性。

新体系只是对根区进行了处理，采用国家自主根的递归解析器肯定要变化，除此以外其他的 DNS 组件不用改变；新体系无须对当前 DNS 服务器软件做任何改动，对 DNS 协议本身也是透明的。

（5）兼容性与部署的渐进性。

整个新系统与当前的 DNS 不冲突，其域名空间的逻辑结构、管理部门都是保持一致的。新体系的变化只牵涉到域名解析，故其兼容已有的 IANA 域名授权管理结果和现有域名系统。

联盟链中的节点是自由加入的，规模是逐步扩大的，节点数越多，整个系统的风险防范能力越强。

3 结束语

近年来，为解决 DNS 根区中心化问题，许多研究都是尝试通过扩展方案，采用新的域名空间和新的域名分配策略，这失去了与现有域名系统的兼容性。联盟链方案借由区块链技术，在保证名字空间统一性、根区数据一致性的基础上，实现了对原体系根权威权力的制衡，解决了根区数据解析的中心化弊端。

参考文献

[1] FANG B X.“Country Autonomous Root Domain Name Resolution Architecture from the Perfective of CountryCyber Sovereignty”，Information Security and CommunicationPrivacy，no. 12，pp. 35-38（in Chinese），2014.
（方滨兴，“从“国家网络主权”谈基于国家联盟的自治根域名解析体系”，信息安全与通信保密，2014，（12）：35-38。）

[2] BOFFIN M，et al. Open root server network [EB/OL].（2012-05-21）[2018-03-08]. http：//www.orsn.org.

[3] VIXIE P. Yeti DNS project[EB/OL].（2015-01-08）[2018-03-08].http：//www.yeti-dns.org.

[4] LEE X D，YAN Z，VIXIE P. How to scale the DNS root system?[R]. Internet Draft，2015.

[5] Public-Root project [EB/OL].（2003-02-21）[2018-03-08]. http：//public-root.com/tlds.htm.

[6] UnifiedRootproject[EB/OL].（2014-05-24）[2018-03-08]. http：//www.unifiedroot.com.

[7] 庄天舒，刘文峰，李东，等.基于区块链的 DNS 根域名解析体系专题：网络空间安全.[2018-03-09].

[8] 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）.

[9] ZHANG Y，XIA C D，FANG B X，et al. An autonomous openroot resolution architecture for domain name system in the internet[J]. Journal of Cyber Security，2017，2（4）.

自动部署器设计与实现

周绪川，张　基

（西南民族大学计算机科学与技术学院，四川 成都 610041）

摘　要：在一个软件系统的开发和交付工程中，往往要经历多次的部署活动。比如反复的测试环境搭建以及系统交付、升级，通常需要消耗测试或维护人员大量的时间和精力。尤其是部署一个大型系统时，即使每台服务器上部署该系统的过程并不复杂，但因为数量巨大，实施人员在重复大量的简单操作后，容易产生误操作，造成部署步骤和参数设置错误，降低了系统整体的部署质量。设计了一个高适用性、高安全性的自动化部署器，详细说明了其设计思路和安全性手段。根据测试结果，该系统运行稳定，符合系统最初设计目标。

关键词：系统测试；系统部署；自动化部署；安全性

An automatic deployment tool for software development

ZHOU Xuchuan, ZHANG Ji

（School of Computer Science & Technology, Southwest Minzu University, Chengdu 610041 China）

Abstract：There are many deployment activities while a software system has been developed and delivered. It usually takes a lot of time and effort to test and maintain, such as repeated construction of test environment, system delivery and upgrades. Especially when a large system is deployed, the process of deploying the system on a server is not complicated, but implementers are prone to misuse after repeating a large number of simple operations, leading to error of development steps or parameter setting and reducing the quality of the system. This paper designs an automatic deployer that has high applicability and security and introduces design ideas and security means of the automatic deployer. Through the test and operation, the system is proved to be reliable and stable, consistent with the original design goals.

Key words：system test; system deploy; automatic deploy; security

0　引　言

一个系统的开发周期可能包含许多测试和大规模的上线。系统的每一次测试、上线都需要先进行部署活动，包括系统运行环境的搭建、产品的安装等。这些过程通常包含了大量的非智能手工操作，效率和可靠性都较差。不同的公司根据自身产品的特性和规模采用了不同的解决方法：有的公司采用拷贝线上环境修改的方式，对部署人员要求较高；有的公司开发了自有的自动化环境搭建系统，但这类系统往往针对性强、灵活性差。

出于这样的背景，为了提高系统测试和部署的效率，本文设计了一个具有较高通用性和安全性的自动化部署工具 AutoDeploy。该工具能够根

作者简介：周绪川（1972—），通信作者。男，博士，教授，硕士生导师，主要研究方向：软件工程、复杂数据处理；
张基（1996—），通信作者，硕士研究生，研究方向：软件工程。

基金项目：西南民族大学中央高校基本科研业务费专项基金项目，编号 2015NYB12。

据客户端界面的用户选项生成 XML 上线单，并根据上线单自动搭建用户选择的运行环境。AutoDeploy 工具简化了烦琐的环境搭建过程，提高了系统测试和部署效率，解放了工作人员的生产力，使其可以将更多的精力放在领域知识学习和系统开发上，更好地提高系统的质量。

1 系统的分析与设计

1.1 系统结构设计

由于大多数系统的部署需要填写上线步骤，所以本文将 AutoDeploy 设计为一个客户端软件，包括前端界面、后台两部分。其中前端界面涉及用户登录和填写系统环境搭建的各个选项，并以此生成上线单。后台负责根据上线单搭建系统运行环境，并获取系统源代码进行混淆、编译，生成相关文件包，最后将系统部署在指定位置。前端界面与后台通过 XML 文件进行信息交互。

采取这样设计的优势在于将前端界面和后台完全独立开来，后台可以拿出来作为一个单独的工具运行，只要有配置好的 XML 文件，就可以通过控制台命令使后台执行部署功能。

1.2 系统处理流程

本工具在设计时采用了获取上线单—搭建环境—部署的三步处理模式，流程如图 1 所示。

首先是获取上线单。用户登录后，根据前端界面的提示按步骤填写系统部署所需要的各种信息，包括项目名称、项目代码运行环境、服务器配置等。客户端将用户输入的配置信息写入 XML 文件，生成项目上线单。

其次是搭建运行环境。后台读取并解析前端生成的 XML 文件，根据文件中记录的配置信息，在本地配置要部署项目代码所需的编译、运行环境，并搭建相关服务器，为项目的部署做好准备。

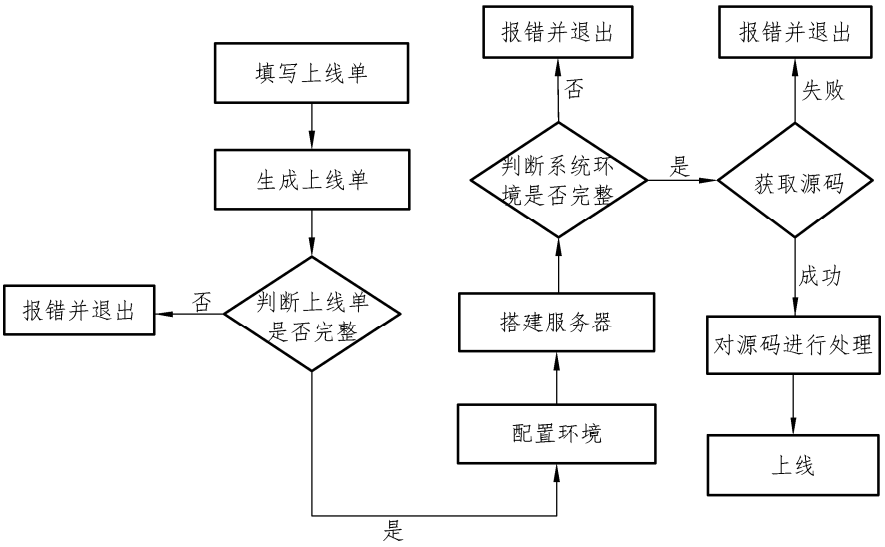

图 1 系统处理流程图

最后是项目部署。后台在完成环境搭建后，会根据项目上线单中的信息，去指定位置将项目源代码下载到本地，并对代码进行混淆、编译、打包，生成 jar 包，最终将项目部署到已经搭建好的服务器上。

1.3 系统前端界面的设计

前端界面的功能是提供选项页面供使用者填写上线相关的信息，然后将信息转换为 XML 文件，存储到指定位置。前端界面的处理顺序如图 2 所示。

为了保护产品安全，工具启动后首先进行权限验证，确保该工具是在指定机器上、规定时间内正常运行，验证通过后才允许用户登录。用户账号类型分为两种，分别是操作员和管理员。成