

面向跨域可信的泛中心化区块链 DNS 架构研究

雷凯^{1,2}, 束方兴^{1,2}, 黄磊^{1,2}, 章奇超^{1,2}

(1. 北京大学深圳市内容中心网络与区块链重点实验室, 广东 深圳 518055;

2. 北京大学互联网研究院(深圳), 广东 深圳 518055)

摘要: DNS 系统是重要的互联网基础设施, 采用中心化层级式结构, 在根区存在中心化现象, 导致单点故障风险、中心权利滥用风险等缺陷。设计新的泛中心化 DNS 架构将使域名系统从依赖中心的单一信任域, 变为多个以顶级域名为根相互平行的信任域, 存在跨域可信的研究挑战。围绕跨域可信架构的设计, 在架构设计层面采用控制与解析分离的思想, 提出双区块链 DNS 架构; 在数据层面的跨域验证方面设计了基于单向累加器的验证方案, 将传统验证过程 $O(N)$ 的时间复杂度降为接近 $O(1)$; 在关键技术的性能层面, 结合 DPoS 机制与 BFT 算法提出 CDBFT 算法, 平均吞吐量可以达到 736 TPS (transaction per second)。并用理论推导和实验验证了架构在安全、性能及可扩展性方面具有优势。

关键词: DNS; 区块链; 单向累加器; 跨域可信; 共识机制

中图分类号: TP311.1

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020024

Research on cross-domain trustable blockchain based decentralized DNS architecture

LEI Kai^{1,2}, SHU Fangxing^{1,2}, HUANG Lei^{1,2}, ZHANG Qichao^{1,2}

1. Shenzhen Key Lab for Information Centric Networking & Blockchain Technology,
School of Electronics and Computer Engineering, Peking University, Shenzhen 518055, China

2. Internet Research Institute, Peking University, Shenzhen 518055, China

Abstract: The domain name system (DNS) is an important internet infrastructure. However, current DNS utilizes centralized hierarchical structure with severe dependence on root server, which causes defects such as the risk of single-point failure and the abuse of central rights. Designing new decentralized DNS mainly focuses on transforming the domain name system from a single trust domain which relies on the center to multiple trust domains with the top-level domain name as the root parallel to each other, but also faces cross-domain credible

收稿日期: 2020-01-17; 修回日期: 2020-02-12

通信作者: 雷凯, leik@pkusz.edu.cn

基金项目: 深圳市科技创新基金资助项目 (No.ZDSYS201802051831427)

Foundation Item: The Science and Technology Innovation Project of Shenzhen (No.ZDSYS201802051831427)

论文引用格式: 雷凯, 束方兴, 黄磊, 等. 面向跨域可信的泛中心化区块链 DNS 架构研究[J]. 网络与信息安全学报, 2020, 6(2): 19-34.

LEI K, SHU F X, HUANG L, et al. Research on cross-domain trustable blockchain based decentralized DNS architecture[J]. Chinese Journal of Network and Information Security, 2020, 6(2): 19-34.

challenges. To design a cross-domain trusted architecture, the concept of separating control and analysis was adopted, and a dual-blockchain DNS architecture was proposed. At data layer, a novel cross-domain verification was designed based on a one-way accumulator verification scheme, with the time complexity of the verification process $O(N)$ reducing to $O(1)$ nearly. The CDBFT algorithm was proposed by combining the DPoS mechanism and the BFT algorithm, whose average throughput reaches 736 TPS. The theoretical derivation and experimental results have demonstrated the advantages of this new DNS architecture on security, performance, and scalability.

Key words: DNS, blockchain, one-way accumulator, cross-domain trustable, consensus mechanism

1 引言

DNS 系统是重要的互联网基础设施,被用来在用户可读的域名和机器可以寻址的 IP 地址之间建立映射,提供查询和解析服务,由层次化域名空间、域名服务器和解析器 3 个部分组成。

目前的 DNS 系统采用中心化层级式结构,通过从根区开始的自顶向下的方式进行数据解析、认证、审批以及授权等操作。这样的流程和结构使所有顶级域名的注册、数据更新、管理、解析以及整个 DNSSEC (DNS security extensions) 体系都对根区中心节点和根服务器存在严重的依赖^[1],造成 DNS 根区严重的中心化现象,导致单点故障风险、中心权利滥用风险^[2]等缺陷。摆脱传统中心化 DNS 架构导致的问题,设计新的分布式去中心化 DNS 架构成为互联网研究人员关注的重要方向。关于去中心化 DNS 系统的研究,早期受限于 Zooko 不可能三角猜想^[3]的限制,相关探索大多局限于域名数据的解析层面,如通过分布式哈希表 (DHT, distributed hash table) 进行域名数据缓存,提供去中心化的解析方案^[4]。而域名数据的管理、授权、注册等操作仍然由中心完成,并没有解决当摆脱中心后各平行信任域间域名数据的跨域信任问题,无法从根本上解决 DNS 系统中心化的情况。直到区块链技术的出现^[5],区块链作为一种新兴的分布式计算范式,具有去信任化、可审计、不可篡改、集体维护、可编程等特点,受到学术界与产业界的广泛关注^[6-8]。并发现利用区块链技术可以突破 Zooko 不可能三角猜想的限制,构建各平行域之间不依赖中心的跨域信任。2013 年,Namecoin^[9]诞生,它作为首个基于比特币为底层平台的完全去中心化域名系统,打破了 Zooko 不可能三角猜想的限制,同时实现了域名系统的去中心化、名字唯一、

命名用户可读。但 Namecoin 存在跨域数据验证效率低、系统事务处理吞吐率低、域名管理困难、功能单一等问题,无法与现有域名系统兼容,需要在浏览器安装特定的插件才可以使用,实用性无法满足网络发展对域名系统的要求。

为解决现有域名系统在架构设计上的不足,本文采用泛中心化的设计思想进行 DNS 架构设计。在泛中心化的架构中,整个网络域名系统从一个整体依赖单一中心的信任域,变为多个以顶级域名为根相互平行的信任域,因此在新的架构中跨域可信成为重要问题。针对泛中心化 DNS 架构中的跨域可信问题,本文基于区块链技术,采用控制与解析分离的思想提出了新的泛中心化 DNS 架构。在泛中心化的 DNS 架构中,通过将传统 DNS 系统中各域对中心的信任,转换为在区块链技术中对数学公理以及程序算法的信任,摆脱了对单一中心的信任依赖。围绕如何设计高效、可扩展、安全的跨域可信架构,本文分别从系统主体架构设计层面、数据层面的跨域验证及安全可信方面,以及跨域可信系统关键技术性能层面进行研究。本文的主要贡献如下。

1) 在系统主体架构设计层面,为构建良好的可扩展性与系统性能,本文采用控制与解析分离的思想,设计了双区块链结构的 DNS 根区架构。通过将根区分为根区域域名管理层以及根区数据解析分发层,分别由顶级域名持有者搭建服务器组成的联盟链和开放的公链系统构成,使两类区块链系统在不同层面发挥优势。通过在管理控制层采用联盟链,设置节点加入的准入门槛,避免了公链系统完全暴露所导致的高安全风险问题。同时,在联盟链采用较高吞吐率的共识算法提高系统性能,降低分叉概率、提高安全性和系统事务处理的吞吐率。在数据解析分发层采用公链系统,利用公链的开放性和高可扩展性调动充分的节点

加入网络进行域名数据的分发，为系统带来良好的可扩展性。

2) 在数据层面的跨域验证方面，为提高跨域可信系统的数据验证性能，针对传统去中心化域名系统中数据验证需要遍历链上区块数据，导致验证时延开销大，影响系统效率和可扩展性的问题。本文引入基于单向密码累加器的验证方案，将传统遍历验证过程 $O(N)$ 的时间复杂度降低为接近 $O(1)$ ，提升域名数据的跨域验证效率和可扩展性。

3) 在数据层面的安全可信方面，为维护泛中心化 DNS 架构中跨域数据安全可信，避免不同信任域主体签发恶意内容，破坏泛中心化 DNS 架构的跨域可信，本文设计了恶意内容的防御方案。包括对恶意内容的规避方法以及基于反馈机制的发布者信任度评级模型。通过规避恶意内容，智能合约对低信任度节点进行多种限制，威慑恶意内容发布行为。

4) 在跨域可信系统关键技术的性能层面，为实现高效的跨域可信系统性能，以及可扩展性需求，本文为顶级域名管理层的联盟区块链系统设计了结合 DPoS (delegated proof of stake) 机制与 BFT (Byzantine fault tolerance) 算法的 CDBFT (credit-based delegated Byzantine fault tolerance) 共识算法。通过基于信任值的 DPoS 代理选取，相较于传统 BFT 类算法，CDBFT 拥有更好的安全与可扩展性。并通过实验评测验证了算法的性能，平均吞吐量可以达到 736 TPS。

最后，本文通过理论推导和实验评测结果，验证了本文提出的架构在安全、性能以及可扩展性方面具有优势。

2 研究背景介绍

2.1 区块链的技术特点

区块链技术是一种采用链式区块结构或者 DAG^[10] 结构进行验证与数据存储，通过共识算法实现分布式网络中各节点账本状态一致，基于密码学技术确保数据安全与隐私，通过智能合约脚本进行编程的分布式计算范式。从技术栈分层的角度来看，区块链可以分为 5 层，如图 1 所示，自下而上分别是数据层、网络层、共识层、合约层和应用层^[11-14]。



图 1 区块链技术架构

Figure 1 Technology architecture of blockchain

在数据层采用特定的数据结构、哈希函数和密码学技术对交易数据进行记录和封装，通过时间戳及哈希指向确保区块按时序相连。网络层用来设定区块链网络的组网模式、通信协议和数据验证机制等因素^[15]。共识层用来规定分布式账本的集体维护规则，确保所有节点所认可和存储的信息准确并一致^[16]。合约层用来设置区块链系统运行中的脚本代码以及智能合约，从而实现区块链系统灵活的编程和数据操作功能。应用层表示底层技术平台所支撑的各种业务场景或具体应用，如数字支付场景或供应链管理 (DAPP)。

基于以上各层技术的有机结合与相互加持，使区块链具有去信任化、去中心化、集体维护、不可篡改、可审计、可编程等特点。其中，去信任化是指在交易过程中交易双方并不需要有任何了解，同时无须设立共同依赖的第三方可信实体，可以直接通过区块链技术保障完成交易。信任问题是网络技术与应用中的重要问题，目前多数系统采用中心化架构设计，存在单点故障风险、中心作恶风险、不同系统或信任域之间构建信任困难等问题。区块链技术采用去中心化的方式对数据进行验证、冗余存储及集体维护，并且通过对密码学算法和共识机制的使用，使原本需要依赖可信第三方的信任构建转为对数学公理与机器程序的信任。因此，基于区块链技术设计跨域可信架构在跨域信任的安全性、可靠性以及可扩展性方面具有优势。

2.2 基于区块链技术的域名系统研究现状

2.2.1 国外研究现状

(1) Namecoin

2013 年，Namecoin^[9] 作为首个基于比特币为底层平台的去中心化域名系统诞生，通过去中心

化的方式设置和记录域名数据,第一次出现了可以突破 Zooko 不可能三角猜想^[3]限制的域名系统架构,成功构建了能够同时满足去中心化、唯一性以及用户可读 3 个要求的域名系统。但 Namecoin 存在结构简单、域名管理困难、功能单一、系统性能差等问题。同时,Namecoin 无法与现有域名系统兼容,用户使用前需要在浏览器中安装特定的插件。并且因为 Namecoin 系统是比特币系统的一个分叉,所以在继承比特币系统优点的同时继承了很多原有比特币系统的问题^[17]。例如,Namecoin 的系统吞吐能力较低,需要耗费大量的算力进行系统维护,使 Namecoin 很难进一步推广,且实用性无法满足网络发展对域名系统的要求。

(2) Blockstack

2016 年,Namecoin 的主要团队,设计了新的去中心化域名系统 Blockstack^[17],底层依然基于比特币来构建信任。但 Blockstack 通过构建虚拟链的方式大大扩展了之前 Namecoin 系统的功能以及可用性。Blockstack 采用了 4 层结构的系统设计模式,自底向上分别是:第一层是比特币区块链层,该层只负责构建去中心化的信任锚,为整个系统提供分布式的信任支撑;第二层是基于状态机机制搭建的虚拟链,用来实现域名系统的注册、域名交易、地址更新等操作,并将操作数据的散列存储在底层区块链中;第三层是路由存储层,采用 DHT 进行构建,存储域名数据的查询路径;第四层是存储层,基于 Amazon S3 等云存储搭建,用于存储域名的各类资源记录数据。但由于 Blockstack 在底层仍然基于比特币,所以系统性能存在瓶颈现象,并且有文献^[18]监测指出出现过特定的某周时间出现过最大矿池的算力占据了系统 75%,存在中心权利过大的风险。另一方面,当在用户需要进行域名数据验证操作时,Blockstack 开销大、速度慢,同时由于缺少构建跨域可信机制的设计,难以形成跨域可信的域名数据管理机制,系统中存在大量僵尸域名,影响了系统的可用性。

2.2.2 国内研究现状

国内关于分布式 DNS 的研究起步略晚于国外,同时在设计新的互联网域名系统的过程中缺少关于跨域可信问题的研究。2017 年,哈尔滨工业大学的刘井强^[19]提出了构建一种私有 DNS 根

系统的构想,并通过虚拟化技术构建虚拟网络对方案进行了模拟。通过创建私有的 DNS 根系统,虽然可以确保在网络中,国家主权的独立性不会受到中心权威节点的影响,但由于私有网络带来的互联网分裂,在数据共享和协议兼容方面存在不足,使该方案在实用性方面还需要进一步地探索。针对中心化域名系统所存在的权力滥用风险,张宇等^[20]提出了一种新的自主开放根解析体系,在与现有 DNS 兼容的同时,通过解耦授权与解析的机制设定对中心化结构下的中心权力进行制衡,同时提出组建国家根联盟的思想,通过国家根内部的自治以及合作化解中心权力滥用风险问题。在张宇等^[20]方案的基础上,庄天舒等^[21]在 2018 年提出了组建“根联盟”共同管理根区数据的思路,采用区块链技术解决各个根节点在数据交换过程中出现的数据不一致问题,使根区数据可以摆脱对中心的依赖。但该方案没有解决泛中心化根区设计后各个域之间跨域信任的问题,并缺少可扩展性良好、安全可信的根区数据解析和分发方案设计。同时,该方案虽然提出联盟链内部采用类 PBFT 算法进行共识,但如何解决 PBFT 算法^[22]的可扩展性问题^[23],使之能够满足构建 DNS 根区的可扩展性要求,还缺少具体的措施。

2.3 单向累加器的原理与特点

为了实现系统中域名数据的高效跨域验证,本文提出了基于单向累加器的高效跨域数据验证方案,因此本节介绍单向累加器(one way accumulator)的原理与特点。单向累加器首先由 Benaloh 和 De-Mare^[24]提出,是一种特殊的单向哈希函数,满足单向哈希函数的可计算性与单向性,同时具有准交换性(quasi-commutative)。单向哈希函数为一个有限哈希函数的集合,任意元素 $h_l: X_l \times Y_l \rightarrow Z_l$ 满足以下特性。

1) 可计算性:即存在一个多项式 P 和整数 l , 对 $\forall x \in X_l, y \in Y_l$, $h_l(x, y)$ 可以在多项式时间 $P(l, |x|, |y|)$ 内计算得到。

2) 单向性:指不存在多项式 P ,可以得到一个概率多项式的时间算法能够对所有 l (l 足够大), 对于确定的 $(x, y) \in X_l \times Y_l$ 和 $y \in Y_l$, 发现 $x' \in X_l$ 使 x' 满足 $h_l(x, y) = h_l(x', y')$ 的概率大于 $\frac{1}{p(l)}$ 。

3) 准交换性：对于 $h_l : X_l \times Y_l \rightarrow X_l$ 满足

对 $\forall x \in X_l, y_1, y_2 \in Y_l$, 有

$$h_l(h_l(x, y_1), y_2) = h_l(h_l(x, y_2), y_1) \quad (1)$$

其中, $h_l(x, y)$ 被称为元素 $y \in Y_l$ 的累加值, 对于集合 $Y' = \{y_1, y_2, \dots, y_m\}$ 而言, 得到累加值为 $h_l(x, Y') = h_l(h_l(\dots h_l(x, y_1), y_2), \dots, y_{m-1}), y_m)$ 。

与一般的单向哈希函数不同, 准交换性可以确保在同一个集合中, 采用不同的序列进行累加计算所得到的结果相同。因此, 单向累加器可以被用来为集合中的元素生成元素存在性证明 (witness)。单向累加器有不同的实现方案, 按单向函数族的选取来区分, 可以分为基于组合学和基于数论的单向累加器两种, 元素验证的时间复杂度不大于 $O(n)$ 。

单向累加器的单向性可以使 $\forall x \in X_l, y \in Y_l, y' \in Y_l$ 在一个多项式时间内尝试发现一个 $x' \in X_l$ 满足 $h_l(x, y) = h_l(x', y')$ 是困难的。即单向累加器可以表示成一组函数集合

$$ACC = \{Setup, Dig, Proof, Verf\}$$

其中

1) Setup: 参数 $parm$ 的生成器, 输入安全因子 λ , 输出参数 $parm$, 可以表示为

$$parm \leftarrow Setup(1^\lambda) \quad (2)$$

2) Dig: 待累加的数据元素集合, $M = \{y_1, y_2, \dots, y_l\}$, 其中 $y_i \in Y_{parm}$, a 表示累加值。

$$a \leftarrow Dig(parm, M) \quad (3)$$

同时, 单向累加器需要具备 3 种功能^[25] 集成员证明、非集成员证明和动态操作。其中, 集成员证明是指有效地为集合 $\{E\}$ 中任何元素 e 生成 $e \in \{E\}$ 的证明, 非集成员证明是指证明某一元素不在集合 $\{E\}$ 中; 动态操作指可以动态更新集合 $\{E\}$ 并对集合元素生成新的对应证明。在本文的集元素验证方案中, 采用了基于 RSA (Rivest-Shamir-Adleman) 假设的单向累加器设计方案。

3 基于双链与单向累加器的泛中心化区块链 DNS 架构设计

为解决现有域名系统在架构设计上的不足, 本文采用泛中心化思想进行域名系统根区设计, 提出基于双链与单向累加器的泛中心化区块链 DNS 架构。如图 2 所示, 在泛中心化域名系统中通过顶级域名持有者搭建服务器构成根区联盟。

在泛中心化架构中域名系统不再依赖单一信任中心, 整个网络域名系统从一个整体依赖单一中心的信任域, 变为多个以顶级域名为根相互平

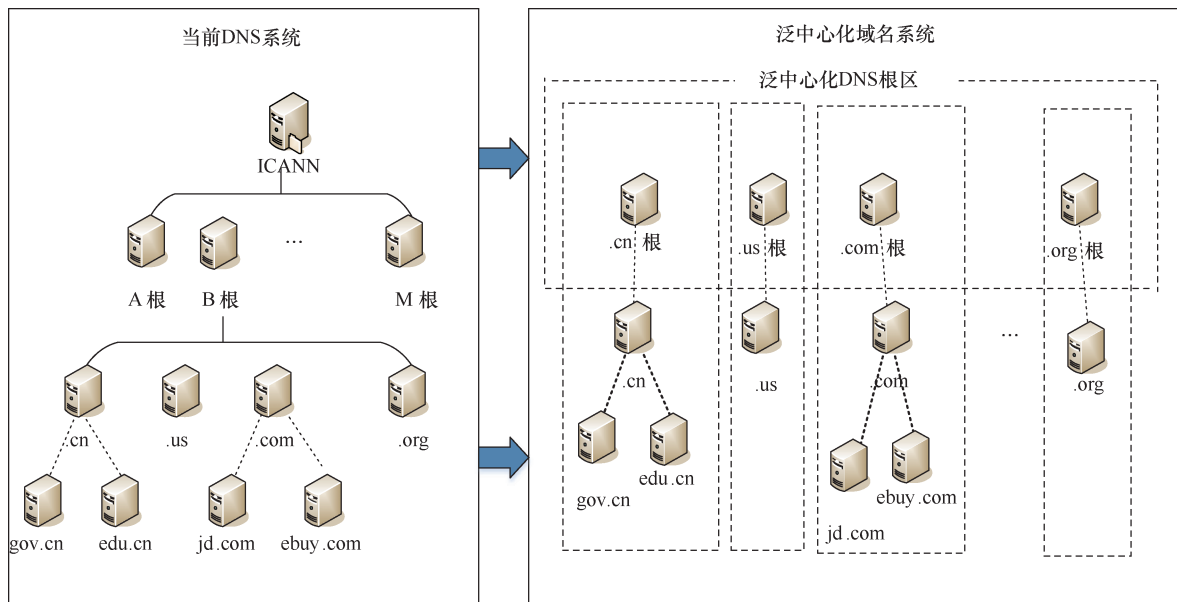


图2 泛中心化域名系统
Figure 2 Decentralized domain name system

行的信任域,因此在新的架构中跨域可信成为重要问题。针对泛中心化域名系统中的跨域可信问题,围绕如何设计高效、可扩展、安全的跨域可信架构,本文分别从系统主体架构设计层面、数据层面的跨域验证及安全可信两个方面,以及跨域可信系统关键技术的性能层面进行研究。

在系统主体架构设计层面,本文采用控制与解析分离的思想,通过融合联盟链的低分叉、高安全、高事务处理吞吐率的特点^[26-27],以及公链系统的开放、系统健壮性好、可扩展性强的特点,设计了高可扩展的双区块链 DNS 根区系统架构。针对数据层面的跨域验证及安全可信两个方面,本文设计了基于单向累加器的跨域数据验证方案,将跨域数据验证所需的时间复杂度从传统验证方式的 $O(N)$ 优化到近似常数的 $O(1)$ 。同时为避免泛中心化架构下的恶意内容签发,本文设计了包括恶意内容规避以及基于反馈机制的发布者信任度评级模型在内的恶意内容防御方案。最后,在跨域可信系统关键技术的性能层面,为满足顶级域名管理层的联盟链性能及可扩展性要求,提出结合 DPoS 机制与 BFT 算法的高效联盟链共识方案。

3.1 双链结构的泛中心化 DNS 根区架构设计

基于控制与解析分离的思想,本文对泛中心化 DNS 根区架构设计采用双区块链结构。如图 3 所示,将 DNS 根区分为基于联盟链的顶级域名管理控制层,以及根区数据解析分发层。

通过双链结构的 DNS 根区架构设计,可以结合联盟链以及公链系统的优势,使两类区块链系统在不同层面发挥优势。在顶级域名管理层采用联盟链,具备一定的节点加入准入门槛,避免公链系统完全暴露、易受到攻击的安全风险,同时联盟链可以采用较高吞吐率的共识算法提高系统性能并降低分叉概率,而无须进行巨大的算力消耗来维持系统。另外,在数据的解析、分发及缓存过程中采用成熟公链系统搭建根区数据解析分发层,可以吸引充分的节点加入网络进行域名数据的分发以及解析,为系统带来良好的可扩展性。

顶级域名管理层的参与方包括持有顶级域名的国家、组织和个人,由参与方的服务器共同构成的联盟链网络组成根区域域名管理层。该层负责根区域域名的注册、解析数据设置、域名交易转移、

域名管理等工作。数据分发层采用开放的公链区块链系统进行搭建,负责顶级域名数据的缓存及解析分发工作。在控制层联盟链上通过共识确定域名操作事务,之后由打包节点进一步分发到下层公链中进行数据的分发,而公链网络中的节点只负责确认和验证下发数据是否合规,将合规的域名数据记录在区块中进行全网的同步。

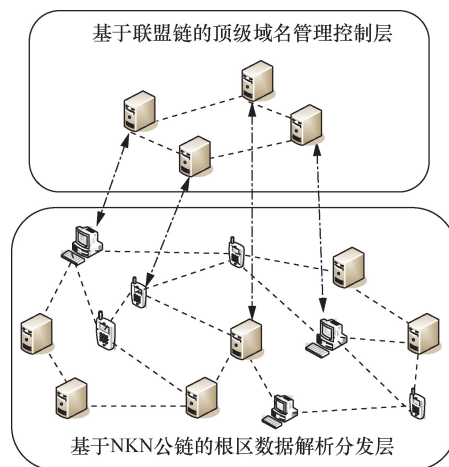


图3 控制与解析分离的双链 DNS 根区架构
Figure 3 Double-chain DNS root zone architecture with separate control and resolution

3.1.1 根区管理控制层

在根区管理控制层,本文采用通过顶级域名持有者(包括国家、组织机构、个人)组建“根联盟”实现根区共同管理的思想^[20]。与目前的根区服务器并存,每个顶级域名的持有者搭建自主的根服务器参与构建联盟链,没有参加根联盟的顶级域名持有者(TLD owner, top level domain owner)可以通过委托其他参与者管理,或者由联盟链共识指定某些参与者先行代为管理。在系统的启动阶段通过现有域名系统公钥以及 CA 证书的合法性来标识联盟链的各参与实体。顶级域名持有者通过私钥签发相应顶级域内的域名数据信息并广播到区块链网络中,通过打包节点验证,并经过共识机制的集体确认后,联盟链网络中的其他节点记录相应区块,如图 4 所示。

3.1.2 根区数据解析分发层

在数据分发层,本文提出基于 NKN^[15](new kind of network)公链,搭建开放的根区数据解析分发层,对顶级域名数据进行缓存与解析分发工作。

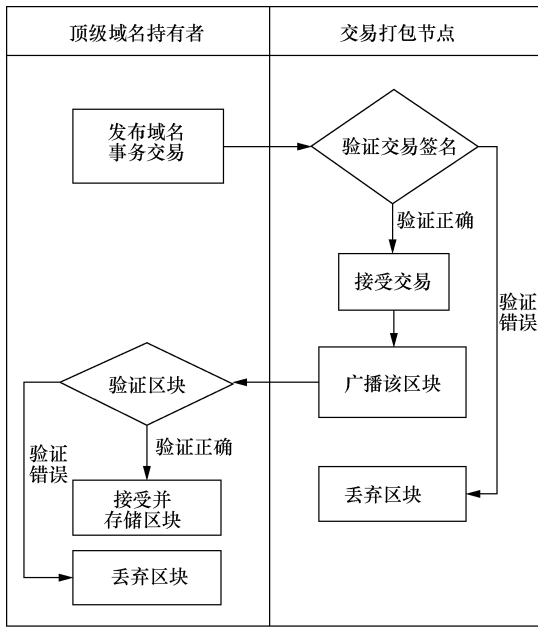


图4 域名数据签发流程

Figure 4 The issuing process of domain name data

NKN 采用区块链技术加持的网络连接协议，通过引入区块链的激励机制鼓励网络用户共享网络连接与带宽。采用基于 MOCA (major vote cellular automata) 的共识机制，为 NKN 系统带来了良好的可扩展性，2020 年 1 月 NKN 官网数据^[28]显示有超过 10 000 的全节点参与主网共识，数量仅次于比特币和以太坊。良好的可扩展性与强大的传输能力，使 NKN 成为良好的去中心化根区数据分发平台。

基于 NKN 的开放与强大的传输能力，通过在 NKN 网络上构建发布订阅 (pub/sub) 服务，实现域名解析数据的分发。解析服务器或普通用户的机器都可以加入 NKN 网络，订阅自己缓存过的或者可能有用户会访问的根区数据。从而当顶级域名持有者的数据发生更新时，将数据发布在 NKN 网络中时，订阅相关数据的解析器就可以相对实时地获得自己所需要的根区数据。根区的顶级域名持有者可以根据共识确定自己的域名更新，并把该记录发布到 NKN 网络的发布订阅系统中，从而使域名持有者可以真正拥有并管理自己的域名数据。

3.2 基于单向累加器的跨域数据验证方案

在不依赖单一中心的泛中心化 DNS 架构中，维护各个平行顶级域之间的跨域可信是确保网络

域名系统域名数据安全、可信的重要前提与保证。本文通过区块链技术，为不同的顶级域名持有实体构建了泛中心化的跨域可信桥梁。但在传统基于区块链的域名系统中，对域名数据进行验证时需要基于 UTXO (unspent transaction output) 的数据结构进行遍历运算，时间复杂度为 $O(N)$ 。然而，随着域名系统的使用，域名键值对及证书信息数据会不断增加，使遍历运算的开销不断增长。跨域验证的延迟将会随数据增长而增加，导致系统验证效率下降，制约根区管理层联盟链系统以及数据解析分发层的验证效率和可扩展性。

为了解决泛中心化 DNS 架构中域名数据的验证效率低的问题，本文设计了基于 RSA 假设的单向累加器验证方案。通过引入单向累加器，将传统时间复杂度为 $O(N)$ 的验证方式优化到近似常数的 $O(1)$ ，提高了系统的验证效率及可扩展性。

本文所提出的单向累加器基于 Baric 和 Pfitzmann 的单向累加器^[24]实现。其中，将使用到单向累加器的以下 4 个多项式算法。

1) $AccGen(1^k) \rightarrow a_0$: 初始化空累加器生成一个初始累加值 a_0 。

2) $AccAdd(a, y) \rightarrow (a', w)$: 在累加器状态值为 a 时加入待累加元素 y ，输出为累加计算后的状态值 a' 和元素存在性证明 w (witness)。

3) $AccWitAdd(w, y) \rightarrow w'$: 输入待累加元素 y 以及存在性证明 w ，输出新的元素存在性证明 w' 。

4) $AccVer(a, y, w) \rightarrow b \in \{0, 1\}$: 输入累加器状态值 a 、待验证元素 y 和 y 属于累加器的存在性证明 w ，若 y 属于累加器，则返回 1；否则返回 0。

在联盟链中的顶级域名持有者通过自己的私钥为所属域内的域名事务进行数据签发，包括顶级域名服务器的 A 记录、 NS 记录、 MX 记录等相关数据，以及自己域名和下属权威域名的名字公钥键值对 $\langle name, pk \rangle$ 数据。将以上数据发布到管理层区块链网络中，打包共识节点对以上签名进行验证，通过验证的使用单向累加器进行累加运算—— $AccAdd(a, y) \rightarrow (a', w)$ ，生成元素存在性证明 w ，以及新的全局累加器状态 a' 。每个区块需要在记录的键值对完成累加后，将最新的累加器

状态值打包记录到该区块中。成员存在性证明 w 以及新的域名数据记录和累加器状态值下发到数据分发层区块链网络。用户在请求域名数据时同时下发键值对 $\langle name, pk \rangle$ 及存在性证明 w 。当用户或者其他域的实体需要验证跨域数据时, 只需读取本地下载的域名数据键值对 $\langle name, pk \rangle$ 以及存在性证明 w , 然后从当前网络中请求最新的累加器状态值, 通过累加器运算 $AccVer(a, \langle name, pk \rangle, w) \rightarrow b$, 以 $O(1)$ 的时间复杂度即可完成域名数据键值对 $\langle name, pk \rangle$ 的有效性验证, 其中, $b=1$ 时表示验证通过。对域名数据的具体操作方案如下。

(1) 域名注册

当参与根区联盟链的顶级域名持有者需要在本顶级域下注册新的权威域名并签发证书时, 则向链上发布交易。

$$T_{regi} = (\langle name, pk_{name}, register \rangle = (pk, \delta)) \quad (4)$$

其中, $name$ 为需要新签发证书的域名, pk_{name} 为 $name$ 域名持有者对应的公钥, pk 表示签发该权威域名数据的顶级域名持有者的公钥, $\delta = (sk, \langle name, pk_{name} \rangle)$ 是顶级域名持有者私钥的签名。挖矿节点收到后需要校验, 当满足:

- ① $name$ 符合域名规则要求;
- ② $ver(pk, \delta, \langle name, pk_{name} \rangle) = 1$ 。

同时满足以上两个条件时认为注册有效, 其中域名规则为现行域名系统对权威域名注册的要求, 包括唯一性、长度符合要求、字符符合要求, 以及从属于正确的顶级域名下等。否则, 忽略此交易。

有效注册之后需要主动更新全局的单向累加器值 a_g , 确认新注册域名的合法性。

$$(a'_g, w) \leftarrow AccAdd(a_g, name) \quad (5)$$

其算法伪代码如图 5 所示。

(2) 域名数据更新

当需要进行域名数据更新时, 相应的累加器状态也需要进行更新。域名持有者希望用新的公钥 pk^{new} 替换旧的公钥 pk^{old} , 可以通过顶级域名管理层的相应顶级域名参与方发布域名数据更新交易到区块链中。

$T_{up} = (name, update, values = (pk^{old}, pk^{new}, \delta_1, \delta_2, aux))$ 其中, $\delta_1 = sign(sk^{old}, (name, pk^{new}))$ 是域名所有者使

用旧私钥 sk^{old} 为 $name$ 和新的公钥 pk^{new} 的签名, $\delta_2 = sign(sk^{new}, name)$ 是所有者使用新的私钥 sk^{new} 对 $name$ 的签名; aux 字段包含辅助信息 (如累加器的陷门函数 t_f), 可以用于当 sk 泄露时撤销密钥对。

```

AccAdd(accu_state, x)
1)  if elements contain x :
2)  return accu_state
3)  else:
4)  hash-
      Prime, nonce ← hashToPrime(x, ACCUMULATED_PRIME
      _SIZE)
5)  accu_state ← accu_state.modPow(hashPrime, N)
6)  put x, nonce into elements
7)  return accu_state, nonce

```

图 5 注册算法伪代码

Figure 5 Pseudo code of registration algorithm

当区块链网络中的“矿工”收到 T_{up} 时, 检查以下条件是否满足:

- ① $name$ 是否对应交易中的 pk^{old} ;
- ② $ver(pk^{old}, \delta_1, (name, pk^{new})) = 1$;
- ③ $ver(pk^{new}, \delta_2, name) = 1$ 。

若无法同时满足以上 3 条, 则忽略此交易。

(3) 数据验证

在传统的基于区块链域名系统中, 由于区块顺序附加 (append-only) 的特点, 需要完整遍历链上的区块数据才能确定域名的有效性, 需要的时间复杂度为 $O(N)$, 即正比于网络中域名记录的数量。为了提高数据验证效率、降低时间复杂度, 本文提出了基于密码学的单向累加器的身份验证方案。

域名验证功能通过键值对参数 $\langle name, pk \rangle$ 和一同存储的元素存在性证明 w , 结合获取最新的全局累加器状态值 a_g , 通过下述条件

$$AccVer(a_g, \langle name, pk \rangle, w) = 1 \quad (6)$$

判断等式是否成立, 进行数据验证。

由于区块链网络中任意节点都可以获取全局累加器 a_g 的值, 因此每个节点都可以作为验证节点。当需要验证某一顶级或权威域名的公钥是否合规时, 只需读取链上的最新累加器状态进行验证运算, 即可验证该名字公钥键值对

的合规性。

3.3 恶意内容防御方案设计

在泛中心化 DNS 架构中, 顶级域名的持有者不会受到其他第三方或中心的影响, 可以完全拥有域名数据的控制权。同时, 由于区块链的不可篡改性以及对域名数据的可信验证依赖于对域名数据签名的验证, 因此当有域名持有者进行了恶意域名数据的签发并通过验证被记录在链上时, 如果没有防御方案, 将会给泛中心化域名系统带来信任与安全风险。例如, 在 Namecoin 中因为缺少相关机制设置, 而且域名一旦成功注册便无法删除, 导致其成为搭建暗网与“僵尸”网络的新“温床”。

为提高泛中心化 DNS 架构中域名数据的安全可信性, 避免不同信任域主体主动或被动地签发恶意内容, 破坏泛中心化 DNS 架构的跨域可信, 本文设计了恶意内容的防御方案。恶意内容防御方案包括两部分: 第一部分是用户可以在发现恶意内容后, 通过恶意内容规避来避免再次请求到该恶意内容; 第二部分是基于反馈机制的发布者信任度评价模型, 通过智能合约对低信任度节点进行多种限制, 威慑恶意内容发布行为。

恶意内容主要包括 3 类: ① 错误数据, 当正常的域名解析请求收到错误数据, 无法访问正确的服务器; ② 恶意域名, 作为顶级域名持有者, 在授权域内签发恶意域名数据, 违反网络域名规范; ③ 虚假指向数据, 如当域名 A 为了攻击域名 B 的正常服务, 用 A 的密钥签发域名 A 的名字地址映射时, 将 $name_A$ 指向 $name_B$ 的服务器地址, 使域名 B 的服务器查询流量突然增大而影响正常解析服务。这样的数据被称为虚假指向数据, 并没有指向真实对应的域名服务器地址。

主动或被动情况指: ① 域名持有者的密钥被盗取或者遗失, 使攻击者掌握了域名数据的签发权利; ② 域名持有者主动作恶签发恶意内容。

3.3.1 恶意内容规避方案

本文提出恶意内容规避方案, 通过 NKHB (name-key-hash binding rules) 规则将域名数据记录的名字、公钥以及域名数据发布者所签发内容的哈希值进行绑定, 通过基于反馈的恶意内容分辨机制判断恶意内容, 并进行高效规避以确保跨域数据访问安全可信。考虑到域名解析数据需要

持续频繁的更新, 而密钥更新的频率相对较低, 同时简单的共识判定难以识别恶意内容。因此, 为降低单向累加器的计算开销提高系统效率, 平衡系统的效率与安全开销, 只将 $\langle name, pk \rangle$ 进行累加运算生成累加证明, 并设计了基于 NKHB 的恶意内容的规避方案。

具体方案为当域名请求者在进行域名数据的请求后发现所请求到的数据是恶意内容, 可以向数据解析层公链网络中发布该信息, 上报该内容的 DISTRUST 交易。该交易的结构为 $\langle DISTRUST, name, pk, hash, Signature \rangle$, 表示有用户对某个域名数据不信任。一般来说, 被不信任的交易提及的次数越多, 说明该域名内容为恶意内容的可能性越大, 但也存在恶意上报过多不信任信息的可能, 因此需要对上报的 DISTRUST 交易信息进行恶意内容判定。当数据解析层的共识节点读取到该 DISTRUST 交易时将其上报给管理层节点。管理层节点将该交易在联盟链中进行广播, 链上共识节点对该交易信息中的内容进行验证, 并判断是否为恶意内容, 恶意内容判定流程如图 6 所示。

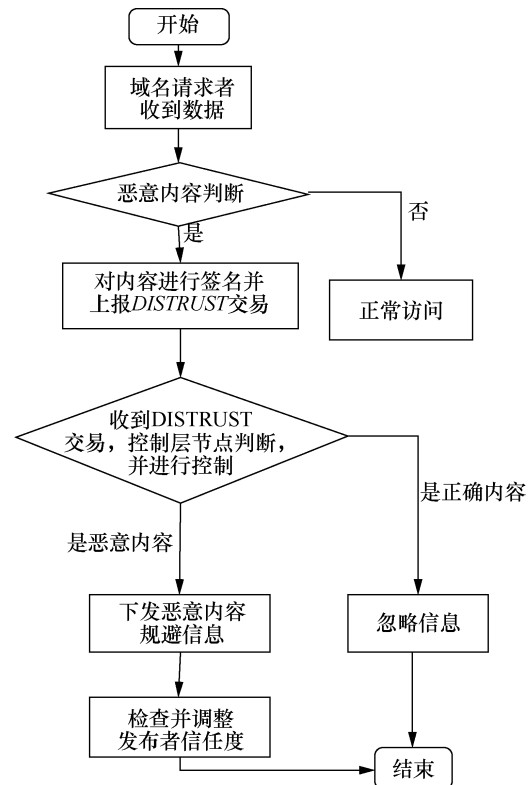


图6 恶意内容判定流程
Figure 6 Malicious content determination process

当 DISTRUST 交易上报的信息被确定为恶意内容后,管理层将会基于 NKHB 规则下发对该内容的规避信息。其他解析器收到规避信息后更新本地的缓存,将符合内容哈希的域名数据标记为恶意,不再返回给任何对该数据的请求者,为用户规避该恶意数据,直到收到新的域名数据 $\langle \text{Name}, \text{Key}, \text{Hash} \rangle$ 键值对中的 Hash 与之前被标记为恶意的域名数据不同,才会重新缓存新的域名数据,并开始响应新的对该域名的查询请求。

3.3.2 基于反馈机制的信任评价模型

为了对泛中心化 DNS 架构中的域名持有者进行正向的信任激励,避免随意签发恶意内容破坏域名数据跨域可信,威胁域名系统安全,本文提出基于反馈机制的发布者信任度评价模型,通过智能合约对低信任度节点进行多种限制,威慑恶意内容发布行为。

对恶意内容的识别和判断是进行信任评价的前提,本文采用 3.3.1 节中的恶意内容发现与判定机制,通过向管理层联盟链上反馈恶意内容,并经过链上多个“矿工”节点的验证与共识确定是否属于恶意内容发布。如果共识确认该域名持有者发布了恶意内容,则降低该发布者的信任度,如果没有认定为恶意内容则忽略此次反馈。

基于对恶意内容的反馈机制,本文提出如下信任度评级模型。

设定所有控制层联盟链的顶级域持有者的初始信任度为 1,则区块高度为 h 时顶级域 A 持有者的信任度为 $T_A(h)=1$ 。假定通过共识判定,顶级域 A 持有者签发了恶意内容,则对其信任度降低为

$$T_A(h+1)=x^n T_A(h) \quad n \in \mathbb{Z}, x \in (0,0.5) \quad (7)$$

n 表示该内容发布者被控告,并认定签发恶意内容的次数, x 为可调参数。

如果通过共识判定,顶级域 A 持有者没有签发恶意内容,则忽略此次反馈。同时信誉值低于 1 的联盟链参与者,可以随着时间推移,正确签发的数据增多而逐步提升信誉值,但需要确保在这个阶段中不再有被确认的恶意内容签发行为。具体为

$$T(h+m)=\min(1, y^m \cdot T(h)) \quad m \in \mathbb{Z}, y \in (1,1.01) \quad (8)$$

m 表示在新增的 m 区块高度期间内,该内容发布者正确签发域名数据,没有被确认的恶意内容发布, y 为可调参数。

对信任度的评价可以作为泛中心化 DNS 架构中域名数据管理层对联盟链参与者权限的设置参考,通过限制低信任度节点对联盟链域名数据打包、共识参与、域名数据签发等权限,减轻主动或被动的恶意内容发布,加强泛中心化 DNS 架构域名数据的跨域可信,提高系统安全。

3.4 CDBFT 共识算法设计

目前主流的共识算法包括 PoW (proof of work)、PoS (proof of stake)、PBFT (practical Byzantine fault tolerance) 等,其中以 PoW 和 PoS 为代表的共识算法有较好的可扩展性,可以承受至多 50% 的算力攻击,具有良好的健壮性,但存在 TPS 较低、性能不足的缺陷,适用于对健壮性和可扩展性要求较高的公链区块链网络^[29]。以 PBFT 为代表的类 BFT 算法,通过节点间的消息广播传递投票信息,最终使节点间形成共识状态。此类 BFT 算法^[30]具有较好的 TPS 性能,事务处理吞吐率高,同时具备较强的一致性维护能力,产生分叉的概率低。但类 BFT 算法只能容忍小于 $\frac{1}{3}$ 的拜

占庭节点,同时由于通信时间复杂度为 $O(N^2)$,随着共识参与节点数量的增加产生指数增长的通信开销,导致共识效率下降。可以看出,类 BFT 算法在健壮性和可扩展性方面较弱,因此,常被应用于节点数量规模较小的联盟链系统。

在本文所提出的基于区块链泛中心化 DNS 架构方案中,共识算法作为关键技术需要具备良好的性能,在可扩展性、吞吐率、延迟、分叉概率方面有较高要求,传统的共识方案难以直接应用。因此,本文设计了结合 DPoS 机制与 BFT 算法的 CDBFT 共识算法。借鉴 DPoS 机制结合 3.3 节的节点信誉评级模型,基于节点的信誉值进行代理节点选取,由代理节点进行数据的打包和校验,每个代理节点可以在固定的时间内产生区块。同时借鉴 BFT 算法,应用基于门限值的多重签名机制,未被验证的区块需要得到超过 $\frac{2}{3}$ 代理节点的确认,才能成为被确认的区块,被网络中的其他节点所接受。因为传统的基于 Shamir 方案的门

限多重签名方法存在初始化密钥被攻击者冒充的风险，在 CDBFT 算法中采用了基于有限域上离散对数问题设计的门限签名方案，提高了 CDBFT 算法的安全性。

CDBFT 算法需要从网络中选取 N 个代理 ($D_1, D_2, \dots, D_n$)，设置固定的时间片 ΔT ，代理的选取可以依据不同节点的信任值进行，信任值较高的节点有更高概率被选为代理。每个代理可以根据当前的时间戳 **timestamp** 确定该时间段内负责打包数据的代理，具体计算公式如下。

$$Delegated_Id = (\text{timestamp} / \Delta T) \bmod N \quad (9)$$

例如，当前时间片由 D_1 进行区块打包，具体流程如图 7 所示， D_1 将本地需要打包的数据组成事务列表，并填充区块头，未被验证的区块被称为 **unverified block**，表示为 B_u 。 D_1 发送 B_u 到其他被选出的代理节点，其他代理节点收到后对该区块的合法性进行验证，如果接受该区块，则生成自己的签名信息，并返回给 D_1 ；当有超过 $\left\lfloor (N-1) \cdot \frac{2}{3} \right\rfloor + 1$ 数量的有效签名返回时，则认为该区块通过了共识，生成多重签名，并将该多重签名信息加入区块 B_u 中，此时 B_u 区块状态变为已验证区块 (**verified block**) B_v ； D_1 广播区块到联盟链网络中，其他节点验证该区块成功后记录保存。

其中，交易的合法性验证需要满足 4 个条件：
① 该交易的签名信息正确；② 该交易中的格式正确，符合系统规范，如交易的时间戳不能大于当前时间；③ 交易中包含的脚本能正确运行；④ 该笔交易未曾出现在历史区块中。如果以上 4 点满足，则可认为该交易合法。具体交易合法性验证的算法的伪代码如图 8 所示。

代理组对 B_u 区块完成验证后首先生成的是单个用户签名，然后通过区块打包节点来产生多重签名，构成 B_v 区块。在其他区块链项目中也有各类多重签名技术的使用。例如，在比特币的脚本中，可以通过使用类似于多重签名方案的服务 (2-of-3 Multisig)，使交易流程更加安全和方便，满足多方交易应用场景中的需求。门限签名技术被分为两种：门限多重签名技术与门限群签名技术，大多数门限签名方案基于 Shamir 的秘

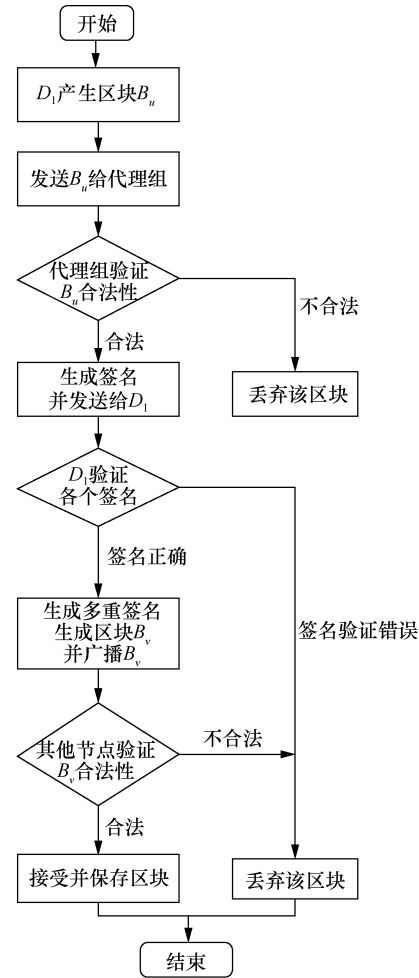


图7 CDBFT 算法流程
Figure 7 CDBFT algorithm flow

```

Transaction Verify(Tx)
1)  Function: Transaction_Verify(Tx)
2)  if Sign(Tx) then
3)    if Writen_Correctly(Tx) then
4)      if Excuted_Correctly(Tx) then
5)        if Not_Exist_in_Blockchain(Tx) then
6)          return true
7)        return false
8)    end function

```

图8 交易的合法性验证伪代码
Figure 8 Pseudocode of transaction validity verification

密共享方案^[31]。其中， (k,n) 门限秘密共享是把秘密切分为 n 个份额后发送至不同的秘密共享参与者，后续秘密的恢复需要集中至少 k 个参与者才能完成。但基于 Shamir 方案的初始化密钥

存在被攻击者冒充的风险,因此,本文采用基于有限域上的离散对数问题设计门限密钥方案。

(1) 初始化阶段

初始化阶段首先通过代理成员 D_A 构建尚未验证的区块 B_u , 并将 B_u 广播至其他节点。在联盟链系统中其他成员的公钥信息以及所使用的安全哈希函数 H 都可以公开查验, 其中有 $PK_i = g^{sk_i} \bmod p$, sk_i 为代理的私钥。

(2) 生成单代理签名

D_i 收到来自 D_A 的区块 B_u , 首先验证其交易的合法性。通过后对 B_u 的头部进行签名。 D_i 选取任意的 $k_i \in [1, p-1]$, 进行 $r_i = g^{k_i} \bmod p$, 其中 g 也是公开可查询的。得到 D_i 对 B_u 头部信息的签名。

$$s_i = H(B_{\text{head}}) \cdot x_i - r_i k_i \bmod \phi(p) \quad (10)$$

将消息 $(B_{\text{head}}, (S_i, r_i))$ 打包发到 D_A 。

(3) 生成多重代理签名

代理 D_A 收到来自不同成员的单个签名 $(B_{\text{head}}, (S_i, r_i))$, 首先对收到的签名进行验证, 公式为

$$r_i^{r_i} g^{S_i} = PK_i^{H(B_{\text{head}})} \bmod p \quad (11)$$

签名验证错误则丢弃该消息, 只针对验证正确的签名进行计数, 如果高于共识验证门限 $\left\lfloor (N-1) \cdot \frac{2}{3} \right\rfloor + 1$, 则开始生成多重代理签名。

已知 m 个签名的代理公钥为 PK_i , 其中 $i \in [1, m]$, 产生此 m 个签名的签名公钥为 r_i , 可得

$$R = \prod_{i=1}^m r_i^{r_i} \bmod p \quad (12)$$

然后通过收到不同成员的有效单个签名 S_i 可得多重签名为

$$S = R \cdot \sum_{i=1}^m S_i \bmod \phi(p) \quad (13)$$

则 (S, R) 为 D_A 所生成的多重代理签名, D_A 将此多重签名打包至生成的验证通过区块 B_v 中。

(4) 验证多重签名

其他节点收到 B_v , 对签名的正确性进行验证: 首先验证 D_A 的签名是否正确, 然后对多重代理签名 (S, R) 进行验证。在验证多重签名 (S, R) 时需要获取 m 个代理签名的公钥, 可以直接在链上获取后计算

$$Y = \prod_{i=1}^m PK_i \bmod p \quad (14)$$

最后节点验证

$$R^R g^S = Y^{RH(B_{\text{head}})} \bmod p \quad (15)$$

如果等式成立, 则验证成功, 认可该区块的合法性并在本地记录该区块。

(5) 基于有限域上离散对数问题的多重签名方案正确性证明

已知 p 是一个使在 $GF(p)$ 上计算离散对数不可行的大素数, g 为 $GF(p)$ 的本原元, H 表示公开可查的安全哈希函数。

$$\begin{cases} r_i = g^{k_i} \bmod p \\ y_i = g^{x_i} \bmod p \\ S_i = H(B_{\text{head}}) \cdot x_i - r_i k_i \bmod \phi(p) \end{cases} \quad (16)$$

得到下列式子成立, 其中 S_i 为单个代理所生成的签名。

$$r_i^{r_i} g^{S_i} = g^{r_i k_i} g^{H(B_{\text{head}})x_i - r_i k_i} = g^{H(B_{\text{head}})x_i} = y_i^{H(B_{\text{head}})} \bmod p \quad (17)$$

可知单个代理的签名验证公式正确。

同时, 由下列等式

$$\begin{cases} r_i = g^{k_i} \bmod p \\ R = \prod_{j=1}^m r_j^{r_j} \bmod p \\ S_i = H(B_v) \cdot x_i - r_i k_i \bmod \phi(p) \end{cases} \quad (18)$$

可以得到

$$\begin{aligned} & S + R \sum_{j=1}^m r_j k_j \\ &= R \sum_{j=1}^m (H(B_{\text{head}})x_j - r_j k_j) + R \sum_{j=1}^m r_j k_j \bmod \phi(p) \\ &= R \sum_{j=1}^m H(B_{\text{head}})x_j \bmod \phi(p) \end{aligned} \quad (19)$$

其中, $X_j, K_j (1 \leq j \leq m)$ 表示 PK_j 对应的签名代理的参数。因此,

$$g^{(S + R \sum_{j=1}^m r_j k_j) \bmod \phi(p)} \bmod p = g^{R \sum_{j=1}^m (H(B_{\text{head}})x_j \bmod \phi(p)) \bmod p} \bmod p \quad (20)$$

最后, 根据式(21)

$$\begin{aligned} R^R g^S &= \left(\prod_{j=1}^m r_j^{r_j} \bmod p \right)^R g^S \\ &= \left(\prod_{j=1}^m g^{r_j k_j} \right)^R g^S \bmod p \\ &= \left(\prod_{j=1}^m g^{R r_j k_j} \right) g^S \bmod p \\ &= g^{R \sum_{j=1}^m H(B_{\text{head}})x_j \bmod \phi(p)} \bmod p \\ &= Y^{RH(B_{\text{head}})} \bmod p \end{aligned} \quad (21)$$

可以证得,本文采用的基于有限域上的离散对数问题进行的多重签名验证算法的正确性成立。

4 实验评测

4.1 基于单向累加器的跨域数据验证方案评测

本文采用基于以太坊和 Docker 容器的实验方案对系统进行测评。从系统功能、验证效率以及可扩展性 3 个方面进行实验评测。采用的硬件平台为 4 台服务器, CPU 型号为 Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40 GHz, 内存配置为 32 GB DDR3 1600 MHz, 硬盘容量为 1 TB, 服务器之间采用吉比特网卡进行连接。在测试中, 本文采用基于联盟链的机制, 并通过随机算法选取共识节点, 以降低共识所需要的时间开销。

本文定义泛中心化域名系统的可扩展性为随着加入区块链系统的顶级域数量增加以及每个顶级域名下所管理的权威域名数量的增加时, 域名合规性验证的时延变化。本文的测试平台通过 GnuPG 加密套件进行大量密钥的生成并随机与不同的域名绑定。

随着名字密钥对数量的增加, 传统基于 UTXO 的域名验证系统需要通过遍历的查询来进行实体验证, 验证的时延呈线性增加, 时间复杂度为 $O(N)$ 。而在本文基于单向累加器的泛中心化域名数据验证方案中, 验证 $\langle name, pk, w \rangle$ 所需要的时间复杂度为 $O(1)$ 不会随密钥键值对数量的增加而影响, 接近常数。本次测试为随顶级域数量的增加, 在验证过程中产生的时延测试, 测试中设定每个顶级域下设 1 000 个 $\langle name, pk, w \rangle$ 名字密钥键值对。与基于传统区块链的验证系统 Certcoin^[16] 进行对比, 结果如图 9 所示。

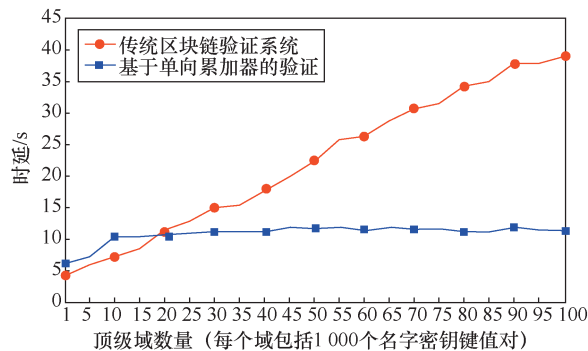


图9 跨域数据验证时延
Figure 9 Cross-domain data validation delay

为了测试随顶级域数量 (M) 以及每个域内权威域名数量 (N) 的增加跨域验证的时延变化, 本文利用 Docker 容器技术生成了 5 个、15 个、25 个不同的顶级域, 并测试了随 M 和 N 变化的时延趋势, 对比系统和前面实验一样为 Certcoin。结果如图 10 所示。

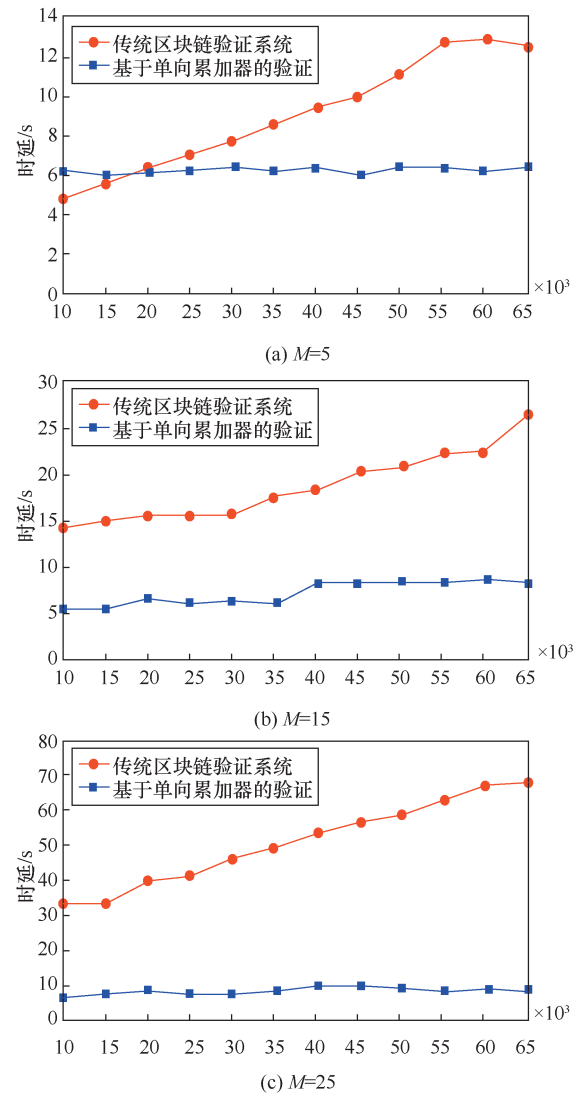


图10 随顶级域数量 (M) 以及权威域名数量 (N) 变化的时延
Figure 10 Delays with the number of top-level domains (M) and the number of authoritative domains (N)

通过图 10 可以看出, 随着顶级域数量的增加, 本文基于单向累加器的跨域可信验证方案时延仍然能够控制在 10 s 以内, 而传统区块链系统会逐渐超过 1 min, 这对于具有验证实时性要求的场景来说是难以适用的。通过以上对功能和可扩展性的测试可以看出, 本文的跨域验证方案在跨

域验证的效率方面具有明显优势,可以在顶级域名以及权威域名不断增加的状态下保持较为平稳的验证性能。实验结果表明,本文方案具备跨域验证的功能,并且与传统区块链系统相比在性能和可扩展性方面有较好的提升。

4.2 CDBFT 共识算法性能评测

针对提出的 CDBFT 共识算法,本文进行了性能评测并与主流区块链共识算法进行对比,使用 6 台主机搭建网络,运行环境为 Ubuntu16.04,代理节点数设置为 3 个,普通节点数量设置为 3 个。性能评测中主要考虑以下指标。

(1) 系统吞吐量:指每秒可以响应的事务处理数量,该指标与系统性能表现呈正相关。本文使用 TPS 作为系统吞吐量的测试指标,其中

$$TPS_{\Delta t} = \frac{Total_Transactions_{\Delta t}}{\Delta t} \quad (22)$$

Δt 表示区块产生的时间间隔, $Total_Transactions$ 表示 Δt 时间间隔内打包确认的事务数量。

(2) 交易确认时延:指系统中一个交易事务从被发出到完成打包确认所需要的时间,包括交易传播时延 $Tx_Broadcast_{\Delta t}$ 、区块传播时延 $Block_Broadcast_{\Delta t}$ 以及共识确认时延 $Consensus_{\Delta t}$,交易确认时延的公式如下。

$$Tx_Delay = T_{confirm} - T_{Tx_generate} = Tx_Broadcast_{\Delta t} + Block_Broadcast_{\Delta t} + Consensus_{\Delta t} \quad (23)$$

首先,对本文所使用的基于有限域上离散对数问题的多重签名方案进行评测,结果显示,对区块头的签名时约为 239 ms,验证时间需要 16 ms。

在算法测试过程中,为获得较好的 TPS 表现,本文通过不同的产块时间等待产生 10 个合法区块,收集 5 次的测试记录,计算 TPS 和交易确认时延,然后获得平均的 TPS 和交易确认时延结果。

如图 11 所示,比特币采用 POW 算法,每秒只有 7 笔的吞吐量,以太坊的共识机制与比特币类似,其吞吐量每秒只有 25 笔,Bitshare^[22]采用了 DPoS 共识机制,TPS 可以达到 483,相比以上主流平台,CDBFT 的 TPS 可以实现较高的系统吞吐量,达到 736,CDBFT 算法具备高效性。

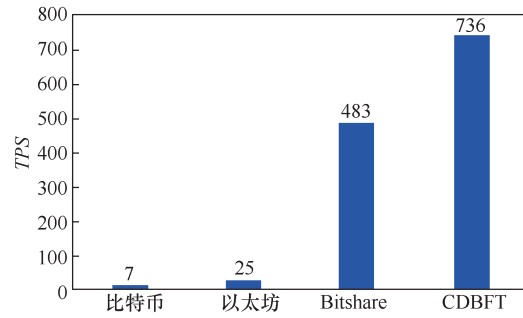


图 11 CDBFT 算法与主流平台的 TPS 对比

Figure 11 TPS Comparison between CDBFT with mainstream platform

通过图 12 的对比可以看出,主流平台(如比特币)的出块间隔为 10 min,并需要 6 次实现区块的确定。以太坊的出块间隔为 25 s,区块确认时间需要 15 min,莱特币出块间隔为 2.5 min,但需要 70 min 才可以实现确认。本文将 CDBFT 算法的出块间隔配置为 6 s,确认时间大约需要 12 s,对比主流的平台实现了较低的时延和确认时间。通过以上测评可以看出,相比目前主流平台的共识机制,CDBFT 算法具备良好的系统吞吐量以及较低的交易确认时延。

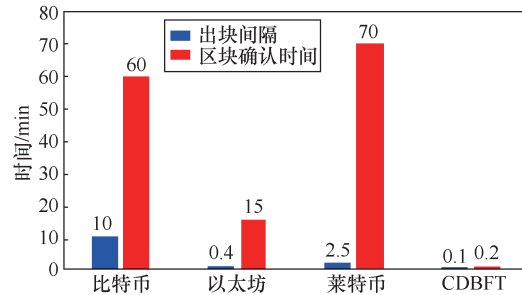


图 12 出块间隔与区块确认时间对比

Figure 12 Block interval and confirmation time

5 研究分析

针对泛中心化 DNS 架构中的跨域可信问题,本文围绕如何设计高效、可扩展、安全的跨域可信架构,分别从系统主体架构设计层面、数据层面的跨域验证及安全可信两个方面,以及跨域可信系统关键技术性能层面进行研究。

在系统主体架构设计层面,采用控制与解析分离的思想,提出了新的泛中心化 DNS 架构。新 DNS 架构中将根区分为根区域名管理层以及根区数据解析分发层,分别使用联盟链和公链在不同层面发挥优势。在管理控制层采用了联盟区块

链,设置节点加入的准入门槛,避免了公链系统完全暴露所导致的高安全风险问题。同时,在联盟链采用较高吞吐率的共识算法,提高系统事务处理吞吐率,降低分叉概率提高安全性。在数据解析分发层,采用公链区块链系统,利用公链的开放性和高可扩展性调动充分多的节点加入网络进行域名数据的分发,使系统整体的安全性和可扩展性得到提高。

在数据层面的跨域验证方面,为了提高域名数据的跨域验证效率,增强系统的可扩展性,本文设计了基于 RSA 假设的单向累加器验证方案。通过单向累加器的引入,可以将传统时间复杂度为 $O(N)$ 的验证方式优化到近似常数的 $O(1)$ 。并通过实验对方案进行性能以及可扩展性评测,证明可以有效提高系统跨域验证效率。

在数据层面的安全可信方面,为增强泛中心化 DNS 架构中域名数据的安全可信,避免不同信任域主体签发恶意内容,破坏泛中心化 DNS 架构的跨域可信,本文设计了恶意内容防御方案。该方案包括对恶意内容的规避,以及基于反馈机制的发布者信任度评级模型。通过规避恶意内容,防止恶意内容扩大影响范围。通过基于反馈机制的发布者信任度评级模型,结合智能合约对低信任度节点进行多种限制,威慑恶意内容发布行为。

在跨域可信系统关键技术的性能层面,为满足顶级域名管理层联盟区块链的性能及可扩展性需要,本文设计了高效的 CDBFT 共识算法。该算法融合了 DPoS 机制与 BFT 算法,通过基于信任值的 DPoS 代理选取,相较传统 BFT 类算法, CDBFT 拥有更好的安全与可扩展性,并通过实验评测验证了算法的性能,平均吞吐量可以达到 736 TPS。

最后,本文通过理论推导和实验评测,验证了所提出架构在安全、性能以及可扩展性方面具有优势。

6 结束语

本文针对泛中心化 DNS 系统架构设计中的跨域可信问题提出了基于双链与单向累加器的泛中心化区块链 DNS 架构。未来可就该架构进行完整的系统实现,并在大规模网络环境下对性能、

可扩展性以及安全性等方面进行充分测试。关于共识算法未来可在通信机制优化以及视图切换^[32]等方面开展进一步研究,提升算法的可扩展性和吞吐量。

参考文献:

- [1] 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. Study on the development of the DNS root system[J]. Chinese Journal of Network and Information Security, 2017, 3(3): 1-12.
- [2] 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[J]. 信息安全与通信保密, 2014(12): 35-38.
FANG B X. Country autonomous root domain name resolution architecture from the perspective of country cyber sovereignty[J]. Information Security and Communication Privacy, 2014(12): 35-38.
- [3] KAMINSKY D. Spelunking the triangle: exploring Aaron Swartz's take on Zooko's triangle[EB]. 2011.
- [4] RAMASUBRAMANIAN V, SIRER E G. The design and implementation of a next generation name service for the Internet[C]//ACM Sigcomm. 2004.
- [5] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [R]. 2008.
- [6] BARNABY C, AWAIS R. Trust beyond computation alone: human aspects of trust in blockchain technologies[C]//ACM 41st ICSE 2019. 2019: 21-30.
- [7] ABRAHAM I, CHAN T H, DOLEV D, et al. Communication complexity of Byzantine agreement, revisited[C]//Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing (PODC 2019). 2019: 317-326.
- [8] DONG X L, AMAL A, JIANBING N, et al. Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3527-3537.
- [9] Namecoin[EB].
- [10] LI C, LI P, XU W, et al. Scaling Nakamoto consensus to thousands of transactions per second[EB].
- [11] CHAN T H, PASS R, SHI E. PaLa: a simple partially synchronous Blockchain[J]. IACR Cryptology ePrint Archive, 2018.
- [12] PASS R, SHI E. Rethinking large-scale consensus[C]//Proceedings of 30th IEEE Computer Security Foundations Symposium (CSF 2017). 2017: 115-129.
- [13] 章峰,史博轩,蒋文保. 区块链关键技术及应用研究综述[J]. 网络与信息安全学报, 2018, 4(4): 22-29.
ZHANG F, SHI B X, JIANG W B. Review of key technology and its application of blockchain[J]. Chinese Journal of Network and Information Security, 2018, 4(4): 22-29.
- [14] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned Block-chains[C]//Proceedings of the Thirteenth EuroSys Conference (EuroSys 2018). 2018: 1-15.

- [15] NKN Lab. NKN: a scalable self-evolving and self-incentivized decentralized network[EB].
- [16] FROMKNECHT C, VELICANU D, YAKOUBOV S. Certcoin: a namecoin based decentralized authentication system 6.857 class project[EB]. 2014.
- [17] HU W H, AO M, SHI L, et al. Review of blockchain-based DNS alternatives[J]. Chinese Journal of Network and Information Security. 2017, 3(3): 71-77.
- [18] ALI M, JUDE N, et al. Blockstack: design and implementation of a global naming system with Blockchains[C]//USENIX Annual Technical Conference. 2016: 181-194
- [19] 刘井强. 基于私有根域名的 DNS 解析实验系统设计与实现[D]. 哈尔滨: 哈尔滨工业大学, 2017.
LIU J Q. Design and implementation of DNS resolution test system based on private root domain[D]. Harbin: Harbin Institute of Technology, 2017.
- [20] 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): 57-69.
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): 57-69.
- [21] 庄天舒, 刘文峰, 李东. 基于区块链的 DNS 根域名解析体系. 电信科学, 2018(3): 17-22.
ZHUANG T S, LIU W F, LI D. DNS root domain name analysis system based on blockchain[J]. Telecommunications Science, 2018(3): 17-22.
- [22] PASS R, SHI E. Hybrid consensus: efficient consensus in the permission less model[C]//Proceedings of 31st International Symposium on Distributed Computing (ISDC 2017). 2017: 1-16.
- [23] ABRAHAM I, MALKHI D, SPIEGELMAN A. Validated asynchronous Byzantine agreement with optimal resilience and asymptotically optimal time and word communication[EB].
- [24] BENALOH J, DE-MARE M. One-way accumulators: a decentralized alternative to digital signatures[C]//Advances in Cryptology-EUROCRYPT'93. Berlin, Heidelberg: Springer. 1993: 274-285.
- [25] NIKE B, PFITZMANN B. Collision-free accumulators and fail-stop signature schemes without trees [C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer. 1997.
- [26] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. Omni-Ledger: a secure, scale-out, decentralized ledger via sharding[C]//Proceedings of 2018 IEEE Symposium on Security and Privacy (S&P 2018). 2018: 583-598.
- [27] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 17-30.
- [28] New Kind of Network [EB].
- [29] GARAY J A, KIAYIAS A. SoK: a consensus taxonomy in the Blockchain era[J]. ACR Cryptology ePrint Archive, 2018(5): 26-37.
- [30] ABRAHAM I, MALKHI D, SPIEGELMAN A. Validated asynchronous Byzantine agreement with optimal resilience and asymptotically optimal time and word communication[EB].
- [31] SAPIRSHTAIN A, SOMPOLINSKY Y, ZOHAR A. Optimal selfish mining strategies in Bitcoin [C]//Financial Cryptography and Data Security 2016. 2016: 515-532.
- [32] MATHIEU B, SERGE P, PIERRE P, et al. STeward: SDN and blockchain-based trust evaluation for automated risk management on IoT devices[C]//IEEE Infocom 2019-WKSHPS. 2019.

[作者简介]



雷凯 (1976—), 男, 湖南长沙人, 博士, 北京大学副教授, 主要研究方向为信息中心网络、区块链、联邦学习与知识图谱。



束方兴 (1990—), 男, 宁夏银川人, 北京大学硕士生, 主要研究方向为区块链系统。



黄磊 (1993—), 男, 江苏扬州人, 北京大学硕士生, 主要研究方向为分布式系统和区块链系统。



章奇超 (1994—), 男, 浙江杭州人, 北京大学硕士生, 主要研究方向为区块链系统。