计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20160991
54(4):742-749,2017

基于区块链的数据安全共享网络体系研究

王继业[1] 高灵超[2] 董爱强[2] 郭少勇[3] 陈 晖[3] 魏 欣[3]
[1](国家电网公司 北京 100031)
[2](北京中电普华信息技术有限公司 北京 100192)
[3](网络与交换技术国家重点实验室(北京邮电大学) 北京 100876)
(syguo@bupt.edu.cn)

Block Chain Based Data Security Sharing Network Architecture Research

Wang Jiye[1], Gao Lingchao[2], Dong Aiqiang[2], Guo Shaoyong[3], Chen Hui[3], and Wei Xin[3]
[1](*State Grid Corporation of China*, *Beijing* 100031)
[2](*Beijing China-Power Information Technology Co. Ltd.*, *Beijing* 100192)
[3](*State Key Laboratory of Networking and Switching Technology* (*Beijing University of Posts and Telecommunications*), *Beijing* 100876)

Abstract For the process of internal and external data sharing in energy Internet enterprises, there are centralized deployment, non-uniqueness identification, and theft or tampering to affect the efficiency of data asset sharing. Based on the character of decentralization, peer-to-peer and difficult-to-change, we construct data security sharing network architecture base on block chain to support exchange information for internal and inter-enterprise. It is to achieve a trusted network environment with the distributed storage. Firstly, we propose a block chain based data security sharing network architecture, including decentralized data unified naming technology, authorized data distributed storage and data distribution protocol. Secondly, an open data index naming structure (ODIN) is designed, including single-level basic ODIN and multi-level extended ODIN. And then ODIN operation mechanism is described. Thirdly, we design the decentralized DNS (domain name sever) resolution module with ODIN. Then the part of system function is realized. And we analyze its performance.

Key words energy Internet; block chain; security; sharing; open data index naming (ODIN)

摘 要 针对能源互联网企业内部与外间的数据共享过程中,存在集中部署访问受限、标识不唯一、易被窃取或篡改隐患等问题,影响到数据作为资产进行统一安全共享的效率.为此,结合区块链的去中心化、自主对等、难以更改的技术特征,构建基于区块链的数据安全共享网络体系,主要包括去集中化数据统一命名技术及服务、授权数据分布式高效存储和支持自主对等的数据高效分发协议.其次,设计了开放式数据索引命名结构,含一级基础ODIN和多级扩展ODIN,且阐述了开放数据索引命名运行机制.再次,基于ODIN技术,设计了基于ODIN的去中心化DNS的域名协议模块,为数据间P2P安全可信共

收稿日期:2016-12-20;**修回日期**:2017-01-23
基金项目:国家科技支撑计划基金项目(2015BAG10B00);国家电网公司科技项目(5211DS17002D);中央高校基本科研业务费专项资金项目
This work was supported by the National Key Technology Research and Development Program of China (2015BAG10B00), the State Grid Corporation of Science and Technology Project (5211DS17002D), and the Fundamental Research Funds for the Central Universities.
通信作者:高灵超(gaolingchao@sgitg.sgcc.com.cn)

享奠定基础.最后,针对基于ODIN的去中心DNS的功能进行验证,为实现企业内部及企业间的数据安全共享构建了一种可信网络环境.

关键词 能源互联网;区块链;安全;共享;开放式数据索引命名技术

中图法分类号 TP391

“能源互联网”是以电力系统为核心,以互联网及其他前沿信息技术为基础,以分布式可再生能源为主要一次能源,与天然气网络、交通网络等其他系统深入结合而形成的新的能源利用体系.能源互联网应提供一种在供需双方之间建立快速、可信、自动的能源交易模式,帮助供需双方高效建立和完成交易[1-2].但现有能源互联网解决方案中,大多利用中心化的管理控制机构完成.但能源互联网体系庞大,中心化管理机构任务繁重,某些情况下去中心化具有更高的效率,如家庭光伏电站的剩余电量提供给某邻居家电器使用,在双方可信的基础上可以直接完成交易,从而具有更高的效率.需要为构建一种可信的对等数据共享平台,支撑能源互联网的高效快速交易[2-3].

而区块链作为一种构建去中心化的分布式存储的对等可信数据网络的技术,是以比特币为代表的数字加密货币体系的核心支撑技术,为构建可信、点对点数据安全共享提供技术基础.区块链技术具有高度透明、去中心化、去信任、集体维护(不可更改)、匿名等性质,能够通过运用数据加密、时间戳、分布式共识和经济激励等手段,在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点数据共享、协调与协作,为解决中心化机构普遍存在的高成本、低效率和数据存储不安全等问题提供了解决途径[3].区块链仅提供了一种安全可信的共识交易的基础平台,仍缺乏适应于能源互联网中多业务形态的数据共享的技术[4-6].在能源互联网中,如何融合区块链与物联网、信息系统、业务形态,解决网络、系统与业务间的去中心化的数据安全共享的问题,满足能源互联网的需求,成为了当前急需解决的问题[7-9].

因此,本文结合区块链的特征,构建一种基于区块链的数据安全共享网络体系,主要包括去集中化数据统一命名技术、授权数据分布式存储与高效分发协议等内容,以实现去中心化域名解析.本文提出开放式命名索引技术,并将其应用于区块链中,解决数据作为资产的安全统一标识的问题,并在此基础上构建了基于区块链的去中心化的DNS域名服务解析机制,解决了集中式的DNS受控可信的问题.

1 基于区块链的数据安全共享网络体系

本节构建了一种基于区块链的数据安全共享网络体系,如图1所示.该体系依托于现有的互联网架构,承载联盟链或私有链,将数据作为资产进行统一标识,利用区块链将数据进行分布式存储,通过设计高效分发协议,实现数据在提供者与消费者间自主对等的信息中心网络(peer to peer information centric network, P2P ICN).具体内容如下:

1) 去集中化数据统一命名技术及服务

结合企业数据的规范和统一资源标识符(URI)规范,基于共享信息模型(shared information data/model, SID)建模,提出开放式数据索引命名技术(open data index naming, ODIN),为网络环境下自主命名标识和交换数据内容索引提供一种开放性系

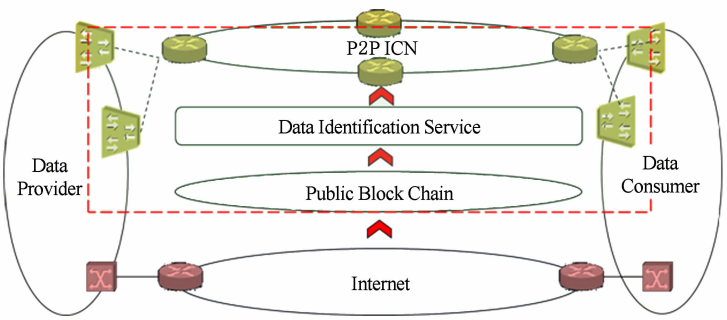

Fig. 1 Block chain based data security sharing network architecture

图1 基于区块链的数据安全共享网络体系

统,为自主开放、安全可信的数据内容管理和知识产权管理提供了一个可扩展的数据统一命名标识体系,为数据提供者与消费者间共享奠定基础[10].

2) 授权数据分布式高效存储

以区块链为数据承载基础,当数据接入时,将其作为一种资产,并对其进行授权加密实现控制访问权限的约束.同时,结合业务特征与需求,在去中心化的网络边缘进行分布式存储,数据缓存管理和缓存策略的问题也成为基于区块链的数据间安全共享的一个难题.

3) 支持自主对等的数据高效分发协议

基于区块链的数据共享本质上就是为了实现一种 P2P 的数据对等共享网络,即 P2P ICN.其中,数据安全传输过程包括基于开放式数据索引命名的底层标识符解析过程、基于名字寻址过程与数据传输过程,典型的例子如:构建去中心化的 DNS 域名解析服务,以实现数据的对等可信传输.

2 去集中化数据统一命名技术

2.1 开放数据索引命名结构设计

本节设计了一种开放式数据索引命名机制 ODIN,该机制是一种层次化的命名规则[11],类似于 SID.为了融合已有单独的链及新增链的扩展,本文将 ODIN 命名方式分为一级基础 ODIN 和多级扩展 ODIN 两种,如图 2 所示.一级基础 ODIN 解决主链之间的数据命名标识的问题;多级扩展 ODIN 是解决私有链或扩展链内部数据命名标识的问题,以便实现数据的分布式缓存且提高账本的同步效率.接下来将分别介绍二者的命名规则.

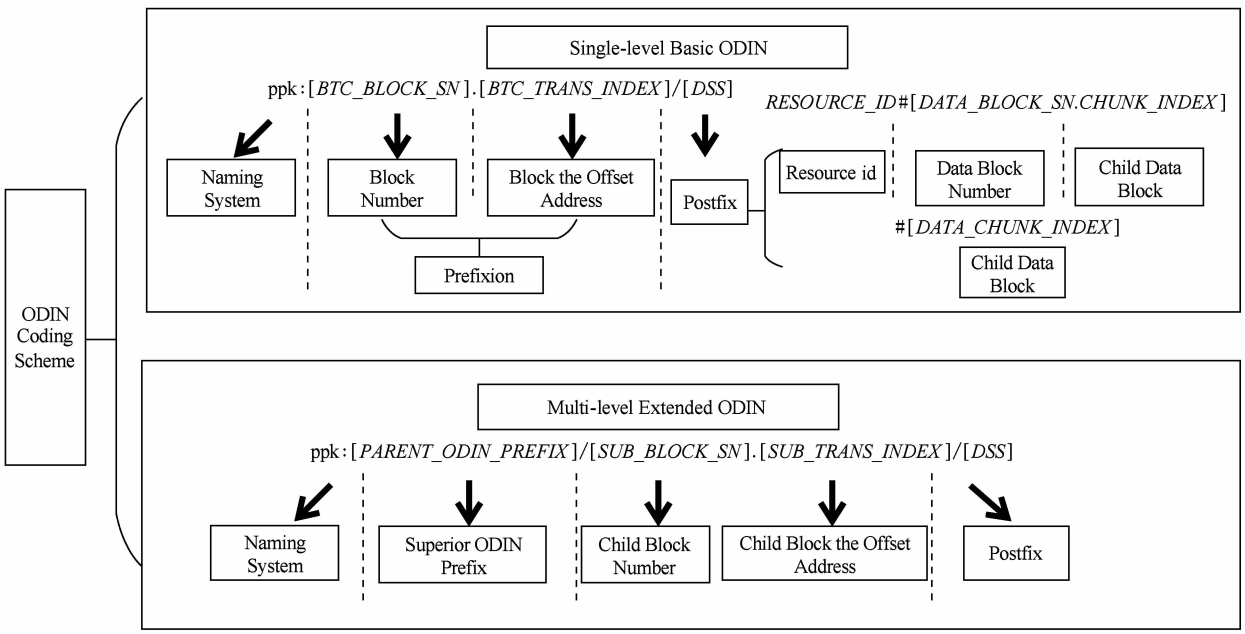

Fig. 2 ODIN naming structure

图 2 ODIN 命名结构图

2.1.1 一级基础 ODIN

一级 ODIN 的标准结构式为

ppk:[*BTC_BLOCK_SN*].[*BTC_TRANS_INDEX*]/[*DSS*]

后缀的标准结构式可扩展为 2 种:

RESOURCE_ID #[*DATA_BLOCK_SN.CHUNK_INDEX*] 或 #[*DATA_CHUNK_INDEX*].

2 种命名方式的区别在于前者引入了资源标识(*RESOURCE_ID*)并通过数据所在区块编号(*DATA_BLOCK_SN*)和子数据块在区块内的索引(*CHUNK_INDEX*)这样一个二级的标识对每一个数据块进行标识;而后者则是通过将所有区块的子数据块进行统一编号后,对数据所在的子数据块[*DATA_CHUNK_INDEX*]进行标识.这里需要注意的是,后缀为命名中可以省略的部分,结构式中'#'字符及其后续部分也可省略,缺省情况下默认为区块内的第 1 个子数据块.

此外,一级基础 ODIN 可以采用短编码的方式表示,标准结构式为

ppk:[*REG_ORDER_INDEX*]/[*DSS*].

与前一种命名的唯一区别在于将前者前缀中的

登记记录的二级索引替换为该记录在全部 ODIN 注册记录中以注册时间早晚排序的数字索引值(*REG_ORDER_INDEX*).

下面列举出一些合法的一级 ODIN 命名:

ppk:351474.430/21.35/

ppk:351474.430/21.35/ISBN2890321345#

ppk:351474.430/21.35/ISBN2890321345#1.0

2.1.2 多级扩展 ODIN

以一级 ODIN 为基础,注册者可以利用自有的区块链来扩展自定义二级 ODIN,并将二级 ODIN 注册记录批量打包后形成的新区块的 HASH 关键字写入上一级骨干区块链获得合法验证并确保唯一性.以此类推,可以形成更多级的 ODIN 标识.

多级 ODIN 的标准结构式为

ppk:[*PARENT_ODIN_PREFIX*]/[*SUB_BLOCK_SN*].[*SUB_TRANS_INDEX*]/[*DSS*]

其中,[*PARENT_ODIN_PREFIX*]为对应上级 *ODIN* 的前缀.[*SUB_BLOCK_SN*]和[*SUB_TRANS_INDEX*]为对应子级 ODIN 在上级自定义区块链上的登记记录所在区块和区块内记录位置的阿拉伯数字编号.后缀[*DSS*](data suffix string)由上级 ODIN 注册者可选并自行给出的具体数据内容定位标识,需要自主确保具有唯一性,命名方案同上.

此外,多级 ODIN 自定义结构式为

ppk:[*PARENT_ODIN_PREFIX*]/[*SUB_TRANS_ID*]/[*DSS*]

[*SUB_TRANS_ID*]为该 ODIN 记录在子级区块链上的唯一标识,由所属上级 ODIN 标识注册者来定义,可以是流水编号,也可以是唯一取值的字符串,需自行保证能与标准结构式区分开且不能包含"/"和"#"这 2 个字符.

下面列举出一些合法的多级 ODIN 命名:

ppk:351474.430/22/

ppk:1/22/ISBN2890321345

ppk:1/22/ISBN2890321345#2.1

ppk:1/china/books/

ppk:1/china/books/#

ppk:1/china/books/ISBN2890321345-P218#

2.2 开放数据索引命名服务运行机制

ODIN 技术对数据统一命名,并通过 ODIN 数据库接口提供相关服务,每个 ODIN 操作都将按照特定的协议规范被编码后广播到公有链平台,得到共识后加入区块,存入公有链.

ODIN 技术是在网络环境下标识和交换数据内容索引的一种开放性系统,它遵从 URI 规范与 SID 建模思想,为基于数字加密货币区块链的自主开放、安全可信的数据内容管理和知识产权管理提供了一个可扩展的框架.主要特点包括自主性、安全性、唯一性和永久性,具体体现为:

1) 自主性.ODIN 标识符是基于去中心化的区块链技术,并由申请者自主生成并管理的一种命名标识技术,其生成和管理规则是完全开放的,没有中心化的控制机构.除了拥有管理密钥的申请者之外,其他组织和个人都无权控制和篡改.

2) 安全性.每一个 ODIN 标识符的拥有者都对应拥有一对非对称加密技术的公私钥,可以通过私钥对自主发布的数据内容进行签名,接受数据内容的个体可以通过公钥进行验证,以确保收到的数据是来源可信和不被篡改的.

3) 唯一性.结合公有区块链,ODIN 标识符能对任何数据内容对象(如文本、图片、声音、数据、影像、软件等)的开放访问索引进行唯一标识,使数据内容对象能被人们准确地识别和提取.

4) 永久性.ODIN 标识符一旦生成就将永久不变,不随其所标识的数据内容对象的持有者或存储地址等属性的变更而改变.

ODIN 技术的运行机制如图 3 所示.

开放数据索引命名服务运行机制主要包括 2 步;

1) 每个有意开放数据的个体(data owner)可以通过开源的 ODIN 注册客户端来自主注册获得一个 ODIN 号(成为 ODIN 注册者,即 ODIN Register),以此为前缀可以为其开放的每一份数据资源编制一个包含本身 ODIN 前缀的且增加了后缀的 ODIN 标识串,并将该 ODIN 标识串索引到数据资源的元数据和 URL 上,这样 ODIN 就成为数据资源的一部分,始终与该数字资源共存;

2) 已被开放的这些数据资源的 ODIN 记录、元数据及其 URL 信息可以 JSON 编码的形式保存在该 ODIN 注册者的数据库内,这些被集中存贮起来的资源就形成一个 ODIN 资源标识库.

当用户根据 ODIN 标识串寻找一个数据资源或有关这一资源的相关信息时,查询请求就会通过开源的 ODIN 解析库在区块链上进行定位,然后被传送到该 ODIN 注册者所登记的访问点(access point, AP)上进行解析并得到该数据资源的元数据描述和实际数据 URL 链接.ODIN 注册者可以完全

开放数据资源访问权,也可以通过适当的自定义机制让用户获取数据资源访问权,如通过订购、资源传递、按浏览付费或者预印本付费等方式获得,为日后的授权数据认证奠定基础.

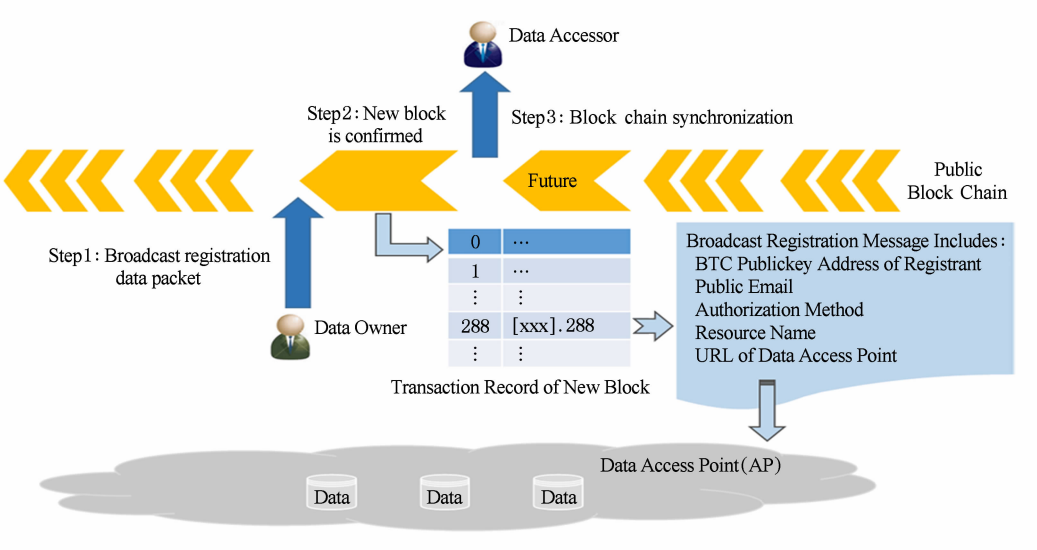

Fig. 3 ODIN operation mechanism

图 3 ODIN 运行机制示意图

3 基于 ODIN 的去中心化 DNS 域名解析

ODIN 标识运行机制,为数据资产提供了统一命名的技术手段. 每个数据便可以当做一个数据提供服务来进行请求,而 ODIN 便是类似于域名解析的地址. 为此,通过 ODIN 标识访问数据块的过程,便形成了一种基于 ODIN 的去中心化的 DNS 域名解析过程[6],如图 4 所示,具体的解析流程如下:

步骤 1. 数据请求者向 ODIN 客户端发出以 ODIN 为标识的 DNS 请求.

步骤 2. 客户端收到后首先就本块中的数据库检索此域名,若检索不到即向最近的存有完整区块的节点请求检索,仍检索不到则说明该域名不合法.

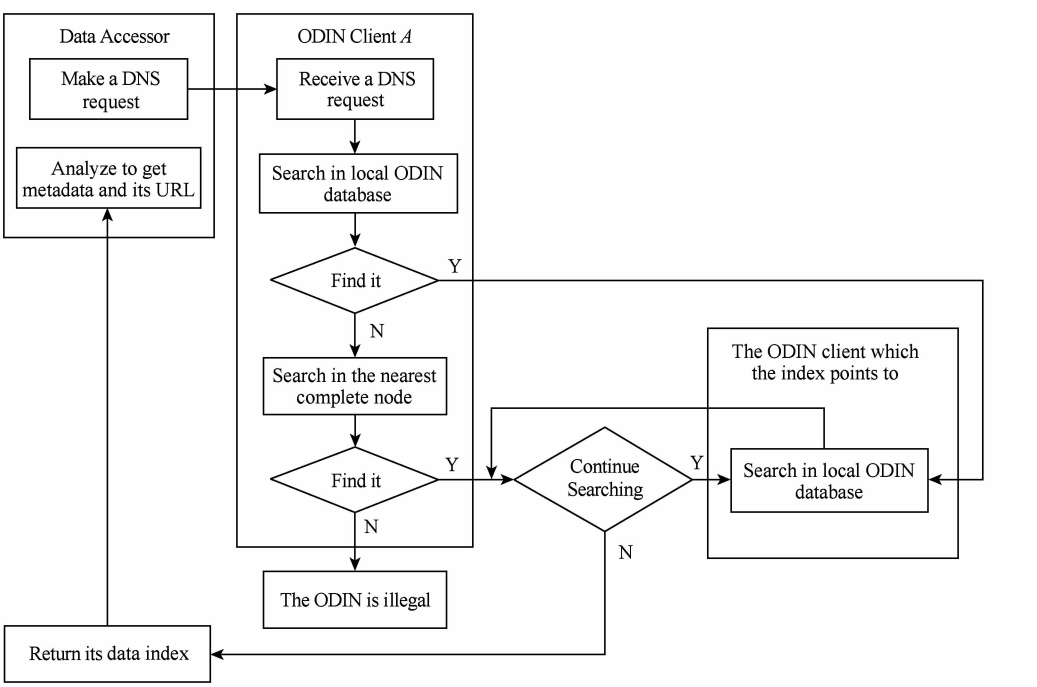

Fig. 4 ODIN based decentralized DNS domain name resolution process

图 4 基于 ODIN 的去中心化 DNS 域名解析流程

若检索到域名,则向其指向的数据源所在 ODIN 客户端检索下一级域名,直到不能检索为止.

步骤 3,将最终得到的索引数据返回给数据请求者,请求者对其解析,得到元数据及 URL,再利用 P2P 的对等传输协议访问数据.

4 实现与验证

本节基于工作组先前的工作基础[10],利用 5 台服务器搭建扩展链,并与公有链相链接构成实验环境,将一级 ODIN 标识注册在公有链上,多级扩展 ODIN 存储在扩展链上进行原型系统验证,并针对域名解析效率进行了统计分析.

4.1 基于区块链的 ODIN 注册过程

如图 5 所示,ODIN 既支持开放式的命名方式,也对命名提出了部分约束条约,以实现 ODIN 域名的注册与管理,如图 5 中步骤 1 与步骤 2,以支持本地化的 ODIN 注册、管理与共享. 其他人可以根据查询已有的 ODIN 命名标识,该标识便可以当做域名,供人查询与解析,以实现去中心化的可信的 DNS 域名解析能力.

4.2 基于 ODIN 的去中心化 DNS 域名解析

如图 6 所示,呈现基于 ODIN 的去中心化 DNS 域名解析成功访问内容的视图,其他数据便可以依托于此标识进行安全验证,确保本标识下的数据来源可信.

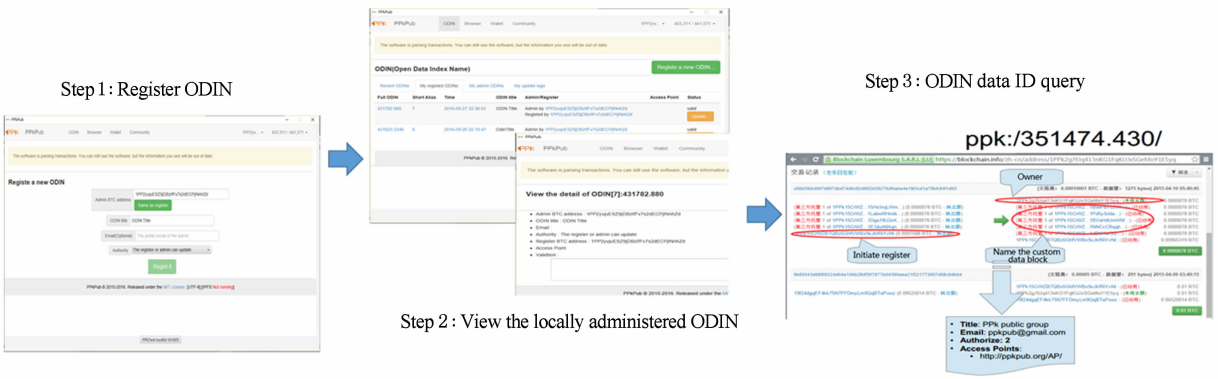

Fig. 5 ODIN registration process based on block chain

图 5 基于区块链的 ODIN 注册过程

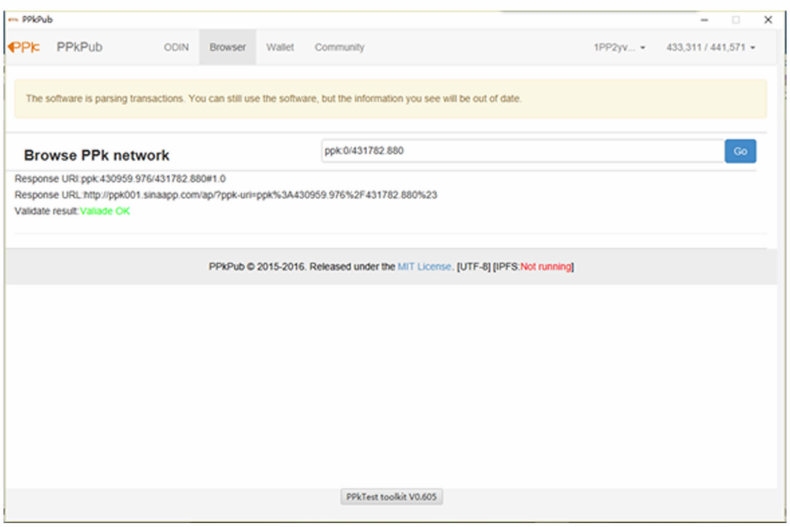

Fig. 6 ODIN based decentralized DNS domain name resolution

图 6 基于 ODIN 的去中心化 DNS 域名解析

同时,本文也根据用户量与 DNS 解析的访问效率进行了时间验证,当用户逐步增大,以 ODIN 为基础的 DNS 域名增长时,随着用户的增长,访问时间也越来越大,但是可以发现用户量与 DNS 域名之间是有平衡点的,即当一定用户量缓存域名时,域名在一定量内访问效率较高,一旦超过这个平衡,效率

呈现下降趋势. 如图 7 所示,区块数对解析速度的影响,一开始随着用户增加,查询速度增长较快,之后增长放缓,有一定波动;解析用时始终在 200 ms 以内.

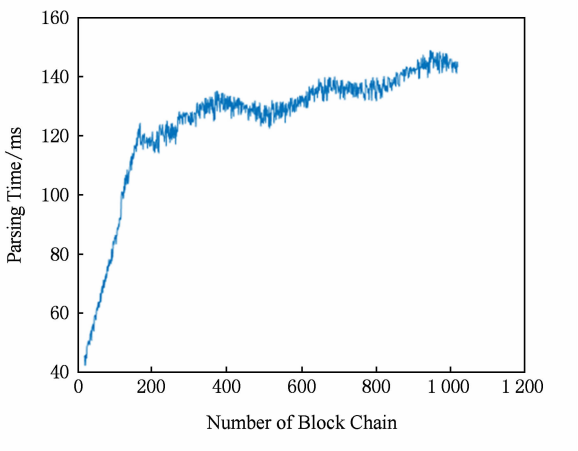

Fig. 7 The influence between users block and parsing speed

图 7 DNS 域名与用户块间解析速度

5 总 结

本文结合区块链的去中心化、自主对等难以更改的技术特征,1)提出基于区块链的数据安全共享网络体系,主要包括去集中化数据统一命名技术及服务、授权数据分布式高效存储和支持自主对等的数据高效分发协议;2)设计了开放式数据索引命名结构,含一级基础 ODIN 和多级扩展 ODIN,且阐述了开放数据索引命名运行机制;3)基于 ODIN 技术,设计了基于 ODIN 的去中心化 DNS 的域名协议模块;4)针对部分功能进行验证并进行性能的分析. 下一步工作中,将针对数据分布式存储及域名解析效率进行优化.

参 考 文 献

[1] Cao Junwei, Yang Mingbo, Zhang Dehua, et al. Energy Internet—Information and energy infrastructure integration [J]. Southern Power System Technology, 2014, 8(4): 1-10 (in Chinese)
(曹军威, 杨明博, 张德华, 等. 能源互联网——信息与能源的基础设施一体化[J]. 南方电网技术, 2014, 8(4): 1-10)

[2] Dennis R, Owen G. Rep on the block: A next generation reputation system based on the blockchain [C] //Proc of the 10th Int Conf for Internet Technology and Secured Transactions (ICITST). Piscataway, NJ: IEEE, 2015: 131-138

[3] Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using blockchain for medical data access and permission management [C] //Proc of Int Conf on Open and Big Data (OBD). Piscataway, NJ: IEEE, 2016: 25-30

[4] Yuan Yong, Wang Feiyue. The development status and prospects of blockchain technology [J]. Acta Automatica Sinica, 2016, 42(4): 481-494 (in Chinese)
(袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494)

[5] Swan M. Blockchain thinking: The brain as a DAC (decentralized autonomous organization) [C/OL] //Proc of Texas Bitcoin Conf. 2015: 27-29. [2017-03-02]. http://inpluslab. sysu. edu. cn/files/Paper/SmartContract/Blockchains _ And_Smart_Contracts_For_The_Internet_Of_Things. pdf

[6] Huckle S, Bhattacharya R, White M, et al. Internet of things, blockchain and shared economy applications [J]. Procedia Computer Science, 2016, 98: 461-466

[7] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of things [J]. IEEE Access, 2016, 4: 2292-2303

[8] Crosby M, Pattanayak P, Verma S, et al. Blockchain technology: Beyond bitcoin [J]. Applied Innovation, 2016, 2: 6-10

[9] Kishigami J, Fujimura S, Watanabe H, et al. The blockchain-based digital content distribution system [C] //Proc of the 5th IEEE Big Data and Cloud Computing (BDCloud). Piscataway, NJ: IEEE, 2015: 187-190

[10] PPK Open Club. Introduction of ODIN [EB/OL]. [2016-11-17]. http://www. ppkpub. org/ppk _ odin _ cn. html (in Chinese)
(PPk 开放小组. ODIN 标识简介[EB/OL]. [2016-11-17]. http://www. ppkpub. org/ppk_odin_cn. html)

[11] Zou Jun, Zhang Haining, Tang Yi, et al. The Blockchain Technical Guide [M]. BeiJing: China Machine Press, 2016 (in Chinese)
(邹均, 张海宁, 唐屹, 等. 区块链技术指南[M]. 北京: 机械工业出版社, 2016)

Wang Jiye, born in 1964. Professor-level senior engineer. His main research interests include information, management of power systems, smart grid and the next generation energy system.

Gao Lingchao, born in 1971. Senior engineer. His main research interests include information management of power systems, smart grid and the next generation energy system.

Dong Aiqiang, born in 1979. Senior engineer. His main research interests include power enterprise informatization and information integration work.

Guo Shaoyong, born in 1985. PhD. Lecturer of State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China. His current research interests include smart grid, network management and terminal management.

Chen Hui, born in 1978. His current research interests include promoting the blockchain and network communications technology innovation and application development by developing open source projects.

Wei Xin, born in 1996. Master candidate of State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China. Her current research interests include network management and smart grid.

2017 年《计算机研究与发展》专题(正刊)征文通知

——车联网关键技术与应用研究

随着传感器和无线通信等技术的发展,车联网作为物联网和移动互联网发展的代表性产物,成为现代智能交通的重要组成部分.车联网在提高交通运行效率和减少环境污染的同时,还能够提供辅助安全驾驶和安全消息广播等措施来保障生命财产安全,此外车载导航、娱乐和 Internet 接入等服务改善了驾驶体验.尽管我国的车联网研究起步稍晚,但近几年得到了政府、企业和研究机构的大力支持和高度重视.2013 年,工信部电信研究院和中国移动研究院联合发布《车联网产业发展白皮书》;2014 年,国务院出台《关于促进智慧城市健康发展的指导意见》,将智慧交通上升到国家战略;2016 年,工信部批准国家智能网联汽车(上海)试点示范区封闭测试区在上海国际汽车城正式开园,同时国家重大专项 LTE-V 车联网专用通信标准化项目启动.在学术界,车联网已经成为一个备受关注的新兴研究领域,对其关键技术的研究有利于推进智慧交通的建设步伐.

《计算机研究与发展》拟于 2017 年 11 月出版"车联网关键技术与应用研究"专题,讨论车联网领域最新的突破性进展,交流车联网领域新的学术思想和方法,展望车联网前沿技术未来的发展趋势.欢迎相关领域的专家学者和科研人员踊跃投稿.现将专题论文征集有关事项通知如下.

征文内容

本专题包括(但不限于)下列主题:

- 车联网移动通信与接入技术
- 车联网智能交通控制
- 车联网消息安全与隐私保护
- 车联网协同控制(例如协助下载、协作式安全应用)
- 车联网移动模型与性能评估
- 车联网资源调度与路径规划
- 车联网紧急消息广播
- 车联网各层协议(例如 MAC 层协议、路由算法等)

投稿要求

1) 论文应属于作者的科研成果,数据真实可靠,具有重要的学术价值与推广应用价值,未在国内外公开发行的刊物或会议上发表或宣读过,不存在一稿多投问题.作者在投稿时,需向编辑部提交版权转让协议.
2) 论文应包括题目、作者信息、摘要、关键词、正文和参考文献,论文一律用 Word 排版,论文格式请参考《计算机研究与发展》近期文章.
3) 论文需附通讯作者的联系方式、联系地址、及 E-mail 信息.
4) 论文请通过期刊网站(http://crad.ict.ac.cn)进行投稿,并在作者留言中注明"车联网 2017 专题"(否则按自由来稿处理).

重要日期

征文截稿日期:2017 年 5 月 31 日
录用通知日期:2017 年 7 月 18 日
最终稿提交日期:2017 年 7 月 25 日
出版日期:2017 年 11 月

特邀编委

吴黎兵 教授 武汉大学 wu@whu.edu.cn
郭得科 教授 国防科学技术大学 dekeguo@nudt.edu.cn
蒋洪波 教授 华中科技大学 hongbojiang@hust.edu.cn

联系方式

编 辑 部:crad@ict.ac.cn,010-62620696,010-62600350
通信地址:北京 2704 信箱《计算机研究与发展》编辑部
邮政编码:100190