文章编号：2095-2163(2024)03-0218-05 中图分类号：TP399 文献标志码：A

基于区块链的工业互联网标识解析体系研究

陈大鹏
(湖南工业大学 计算机学院，湖南 株洲 412007)

摘 要：针对现行的标识解析体系多是中心化架构，存在单点故障以及信任问题，阻碍多方交流互通等问题。提出了一种基于区块链的扁平化工业互联网标识解析体系，使用对等节点对外提供解析服务，不设特殊节点，实现完全的扁平化，解决了单点故障问题，促进了多方信任；改进了实用拜占庭算法，根据节点实时状态进行动态选举，最大程度避免选举坏点；使用链下存储方式，避免了区块回溯，把检索时间复杂度从 $O(N)$ 降为 $O(\log N)$。实验结果表明，系统平均吞吐率在写入和解析上分别达到了 1 100 TPS 和 2 000 TPS 左右，空间占用约为 60 Gb/百万条。

关键词：工业互联网；标识解析；区块链；去中心；单点故障

Block chain-based identification and resolution system for industrial Internet of Things

CHEN Dapeng
(College of Computer Science, Hunan University of Technology, Zhuzhou 412007, Hunan, China)

Abstract: The development of Industrial Internet of Things has pushed the importance of the Industrial Internet of Things identification and parsing system to a new height. The current identification and parsing system is mostly centralized, which has the single point of failure and trust issues, hindering communication and interconnection among multiple parties. A blockchain-based flat identification and parsing system for Industrial Internet of Things is proposed, which uses peer-to-peer nodes to provide parsing services, without the need for special nodes, achieving complete flatness and solving the single point of failure problem, promoting mutual trust among multiple parties. The practical Byzantine fault-tolerant algorithm is improved, and dynamic election is carried out according to the real-time status of nodes, minimizing the election of bad nodes. The use of off-chain storage avoids block backtracking, reducing the retrieval time complexity from $O(N)$ to $O(\log N)$. Experimental results show that the system's average throughput reaches about 1 100 TPS and 2 000 TPS for writing and parsing, respectively, and the space occupancy is about 60 Gb per million records.

Key words: Industrial Internet of Things; identification and resolution; blockchain; decentralized; single point failure

0 引 言

工业互联网标识解析体系作为工业互联网[1]的神经中枢，起到了至关重要的作用。通常情况下，可以对工业互联网中出现的大量设备、资源进行有效的标识解析和管理，为数据采集、存储、处理和应用提供了支持。同时，工业互联网标识解析体系还可以实现人、机、物的互联互通，方便了工业系统内各种角色之间的交流和协作。工业互联网标识解析体系作为一个互联互通平台，不同企业、结构均可据此进行资源整合、联合优化，是打破信息孤岛、最大化工业互联网应用价值的重要手段之一[1-3]。

然而，工业互联网标识解析体系多是中心化架构[4]，没有分层管理节点。中心化的管理架构往往存在着单点故障、容易遭受分布式拒绝服务攻击(Distributed Denial of Service , DDoS)[5-6]等问题，系统鲁棒性较低。尤需一提的是，在工业互联互通时代，系统宕机的影响不容小觑。权力集中[7-8]也是中心化架构的弊病之一，中心节点或者根节点被赋予普通节点所没有的特权，这就导致参与各方很难建立信任。

区块链技术[9-11]作为一种新兴的分布式记账和交易机制，善于在不可信网络中构建可信应用。能够弥补中心化方案的局限性，即在一个分布式网络

作者简介：陈大鹏(1998-)，男，硕士研究生，主要研究方向：计算机网络、工业互联网、区块链。Email：lenozzedifigaro@163.com

收稿日期：2023-06-13

中，无需信任第三方机构就能完成数据验证和交换。基于区块链技术的工业互联网标识解析体系可以实现设备身份认证、数据加密、隐私保护等功能，同时也可以有效地防止单点故障和数据篡改。区块链技术通过去中心化和分布式记账方式，确保了数据的安全性和可靠性，是一种极具前景的工业互联网标识解析方案。

区块链的本质是一种去中心化的分布式账本数据库，整合了点对点网络、共识算法、密码学原理、智能合约[12-13]和其他技术。区块链非常适合在不可信的网络中建立可信网络，依托去中心的本质特性，实现零集中管理和控制，从而建立参与各方的相互信任。区块链的结构是一个不断增长的有序块列表，每一块中都记录了前一块的哈希值以及经过加密的交易信息。这种连锁结构使得区块链中的数据是不可篡改的，因为修改任何一个块都会导致其后所有的块被修改。在区块链网络中，所有节点都是平等的，没有哪一方能拥有特权或控制权，因此区块链的数据具有高度的安全性和可信度。同时，由于没有中心化的机构，区块链不会出现单点故障问题，具有天然抵御 DDoS 的特性。

1　工业互联网标识解析体系技术

1.1　对象标识符

对象标识符（Object Identifier，OID）[14-15]体系是由国际标准化组织提出的一种分层树形结构的标识体系，将全球范围内的标识进行了分类和组织，可以对物理或逻辑对象赋予全球唯一性命名。OID 体系被设计为 DNS[16]的一部分，组织机构可以自行添加新节点并实施域内管理。OID 提供 2 种常用的标识机制，分别是点标记法和 OID-国际化资源标识符法（OID Internationalized Resource Identifier，OID-IRI）。

点标记法由点和数字构成，标识符为叶子到树根路径的顺序组合，适合机器阅读和检索，但不适合人类阅读；OID-IRI 使用 Unicode 字符和斜线进行标识，相较于点标记法具有通用可读的优势。OID 的解析流程在 DNS 解析的基础上增加了一个 OID 解析系统（OID Resolution System，ORS），架构模型如图 1 所示，解析流程如下：

（1）客户端向 ORS 发起 OID 标识解析请求；

（2）ORS 把 OID 标识转化为对应的域名；

（3）ORS 再向 DNS 服务器发起解析请求；

（4）DNS 服务器返回对应 NAPTR 记录给 ORS；

（5）ORS 根据 NAPTR 记录将 OID 结果返回到客户端。

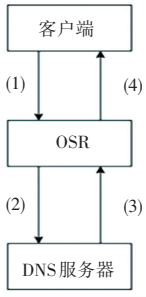

图 1　OID 体系架构模型

Fig. 1　OID system architecture model

1.2　物联网统一标识

物联网统一标识（Entity Code for IoT，Ecode）[17-18]是国内自主研发的一套完整的物联网标识体系，基于 DNS 的域名权限指针（Naming Authority Pointer，NAPTR）资源记录，为工业互联网提供全面的设备标识、数据标识和服务标识解析服务。Ecode 编码分为 3 段。其中，第一段为版本（Version，V），表示 Ecode 使用的版本；第二段为标识体系代码（Numbering System Identifier，NSI），指明标识的解析体系，如 Ecode、OID、Handle 等，是 Ecode 兼容性的基础；第三段则是主码（Master Data Code，MD），其格式和长度取决于 NSI，并由指定该标准的组织机构来定义具体语义。

Ecode 采用类似 DNS 的迭代解析方式，主要有 4 个部件：客户端，发送解析请求的一方，是工业互联网中有解析需求的组件；解析服务器，接受来自客户端的解析请求，拆分出 V、NSI、MD 三段，根据规则转化为标识识别域名并返回给客户端。编码数据结构解析服务器，主要接受客户端发来的标识识别域名，并将其转化为主码域名后返回给客户端；码解析服务器，接受客户端的主码请求，并完成最后的解析。解析流程如图 2 所示。

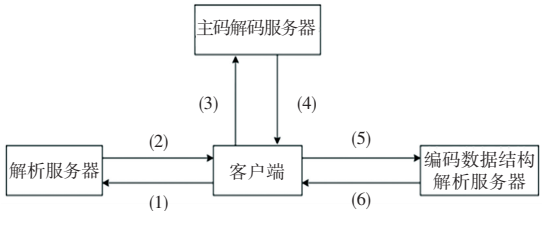

图 2　Ecode 解析流程

Fig. 2　Ecode parsing process

2 基于区块链的解析体系架构设计

基于区块链的工业互联网标识解析体系的基本愿景是一个完全去中心的、简洁高效的、高鲁棒的系统。而与传统解析体系的最大不同则是扁平化的架构设计,系统中只有对等节点,所有对等节点都是相同的。系统可以划分为 3 层,分别是:网络层、共识层、数据层。系统整体架构设计如图 3 所示。由图 3 可知,客户端和所有对等节点构成网络层,对等节点之间通过共识算法交流形成共识层,而数据层则是共识层共同维护的数据库。

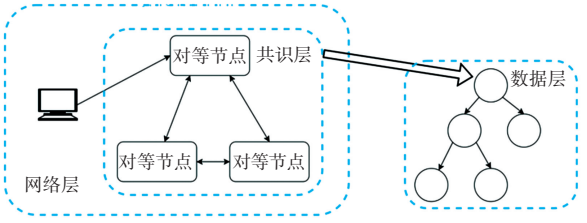

图 3 系统整体架构设计

Fig. 3 Overall system architecture design

2.1 网络层

网络层由解析体系系统中的所有对等节点和客户端构成。其中,客户端是发起解析请求的用户,它可以是工业互联网中的任何一个需要解析的部件。对等节点是整个系统中承担设计实现的实体,每一个对等节点都是相同的,都可以提供解析服务,任何组织或者个人都可以运营一个对等节点。扁平的网络结构决定了对等节点是自由的,还未建立机制来对其在线时间、在线地点和在线方式进行限制。整个网络由这些对等节点和客户端以一种松散的方式组织在一起,不管任何一个对等节点失效,都不会影响整个系统对外提供服务。

2.2 共识层

共识层定义了对等节点之间的交流方式,确保能在分布式网络中达成共识,并能进行可靠的交易和信息传输。共识层使用共同约定的算法和协议,确保网络上所有节点都能就交易内容达成一致,从而保证网络的安全和正确性。每个节点都在共识层上进行操作,从而确保整个区块链系统的一致性和准确性。共识层改进了实用拜占庭容错算法(Practical Byzantine Fault Tolerance,PBFT)[19],进一步加强了网络的安全性和稳健性。

在 PBFT 中,每个节点依次扮演领导者的角色,负责提出和处理请求。然而,这种固定的轮换机制可能导致节点之间的不均衡和性能瓶颈,而改进的 PBFT 就通过引入更灵活的角色选择机制,可以根据节点的负载情况、性能指标、网络延迟等量化数据来动态选择领导者,以实现更好的负载均衡和性能优化。

2.2.1 负载度量指标的选择

要准确评估节点负载,选择适当的负载度量指标是关键。这些指标应该能够捕捉到节点当前的负载情况,并与其他节点进行比较。因此,可以选用以下参数作为度量指标。

(1)CPU 利用率:衡量节点处理器的使用率,可以使用操作系统提供的 CPU 利用率信息或系统监控工具来获取;

(2)内存利用率:衡量节点内存资源的使用情况,包括物理内存和虚拟内存的利用率;

(3)请求队列长度:衡量节点等待处理的请求数量,可通过监控请求队列的长度来获取;

(4)响应时间:衡量节点处理请求所花费的时间,可以通过记录请求的到达时间和完成时间来计算平均响应时间。

2.2.2 负载信息的广播和决策

每个节点使用心跳机制定期触发收集自身的负载信息,并将其广播给其他节点,节点心跳机制的频率可以依照集群规模的大小而做出调整。负载信息可以封装成消息的形式,包含节点的标识和负载度量指标值。节点可以通过点对点通信或者通过共享的状态存储(如分布式数据库或分布式共享内存)将负载信息传递给其他节点。

根据节点的负载信息,采用动态选举策略来选择下一个领导者。该策略综合考虑负载度量指标的值,并根据特定逻辑确定选举结果。如果负载度量指标是连续的,可以选择负载最低的节点作为领导者;如果负载度量指标是离散的,可以将负载分为多个不同的等级或范围,而后根据节点在不同范围内的数量和负载大小来选择领导者;如果负载度量指标是混合的,则分别根据前两者的结果给予 2 个权重进行计算,结果大者当选。

2.3 数据层

数据层用于存储标识系统的实际数据。区块链的公共账本可以作为数据层的实现,但是公共账本检索的最坏情况需要遍历所有区块,平均时间复杂度为 $O(N)$,且任何改动都需要通过新增区块来实现,这都会导致账本异常的臃肿和低效。因此,提出了链下存储方案。把数据以标识为键(key),解析结

果为值(*value*) 组织成一颗树，树的各个节点都是一个星际文件系统（InterPlanetary File System，IFPS）[20]文件，这样一来就只有树根对应的 IFPS 文件的内容标识符（Content Identifier，CID）记录在区块中。数据层结构如图 4 所示。

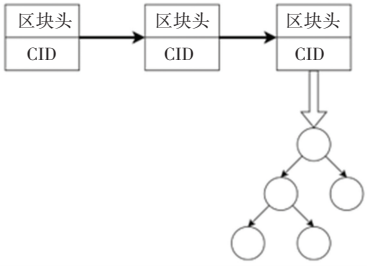

图 4　数据层结构

Fig. 4　Data layer structure

图 4 中，每个区块只记录了当前最新树根的 CID，通过区块中的 CID 可以在 IFPS 中索引树根，而通过树根又可以索引到整颗树。区块头中包含了生成区块的时间戳和前一区块哈希等关键元数据，哈希计算方法如下：

$$hash_i = sha256(hash_{i-1} + blockhead_{i-1} + RootCID_{i-1}) \tag{1}$$

当需要改动数据库时，多个改动可以合并成一次区块提交，这样可以最大限度地简化区块链的公共账本，避免臃肿。在检索时，每次只需要读取最新区块即可，完全避免了区块回溯。在检索树结构时，可采取二分查找算法，时间复杂度降为 $O(\log N)$。

3　实验

为了验证系统的可行性，进行了一系列相关实验。定量考察了系统的吞吐率、空间占用等核心指标，同时搭建了一个拥有 50 个对等节点的系统。实验软硬件环境设置见表 1。

表 1　实验环境设置

Table 1　Environment configuration for the experiment

名称	值	备注
CPU	i5-11300H	
RAM	16 G	
操作系统	Ubuntu	22.04
硬盘	512 G	SSD
编程语言	Golang	1.19
容器环境	Docker	18.09
区块链框架	Hyperledger Fabric	2.2

3.1　吞吐率测试

实验分别在不同数据量的场景下，测试了对等节点的吞吐率，在每个数据量场景下获取所有节点的平均值，实验结果如图 5 所示。

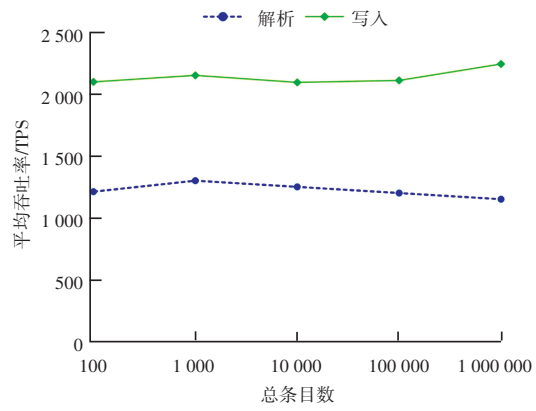

图 5　吞吐率随数据量的变化

Fig. 5　Throughput changes with the variation of data volume

由图 5 可见，吞吐率并不会因为数据量的增加而下降，写入速度达到1 100 TPS左右，检索速率达到2 000 TPS左右，实验结果主要得益于采用了链下存储，避免了区块回溯，降低了时间复杂度。此外，写入和读取之间存在一定速度差的主要原因是写入时有一个共识过程、而读取没有，但考虑到解析体系的使用场景更偏向读取，所以这个速度差是可以接受的。

3.2　空间占用测试

分别在不同数据量的场景下，测试了对等节点的空间占用情况，结果如图 6 所示。

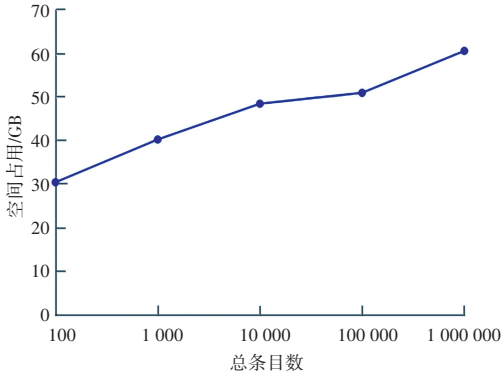

图 6　空间占用随数据量的变化

Fig. 6　Space occupancy changes with the variation of data volume

由图 6 可知，空间占用随着数据量的增加而有所增加，在数据量达到百万级别时，占用了 60 GB 空间，但是相对于其他区块链系统的空间占用来说，处于一个较低的水平。

4 结束语

本文使用区块链构建了一个扁平化的工业互联网标识解析体系,解决了单点故障和权力集中的问题,消除了多方参与时的信任危机。同时还使用了链下存储加 IPFS 的方式,降低了检索时间复杂度,并把空间占用控制在一个较低的水平,是一个可行的工业互联网标识解析体系。

参考文献

[1] 工业互联网产业联盟. 工业互联网体系架构(版本 1.0)[R]. 北京:中国信息通信研究院,2016.

[2] 工业和信息化部. 工业互联网发展行动计划(2018-2020 年)[R]. 北京:工业和信息化部,2018.

[3] 工业互联网产业联盟. 工业互联网安全框架[EB/OL]. [2023-03-01]. https://wenku.baidu.com/view/.

[4] 任语铮, 谢人超, 曾诗钦, 等. 工业互联网标识解析体系综述[J]. 通信学报, 2019, 40(11):138-155.

[5] LEWIS D. The DDoS attack against Dyn one year later[EB/OL]. (2017-10-23)[2023-04-13]. https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later.

[6] MOURA G C M, SCHMIDT R de O, HEIDEMANN J, et al. Anycast vs. DDoS[J/OL]. [2023-03-04]. DOI: https://doi.org/10.1145/2987443.2987446.

[7] FANG B X. Countryautonomous root domain name resolution architecture from the perfective of country cyber sovereignty[J]. Information Security and Communication Privacy, 2014, 12: 35-38.

[8] ZHANG Yu, XIA Zhongda, FANG Binxing, 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.

[9] NAKAMOTO S.Bitcoin: A peer-to-peer electronic cash system[M/OL]. [2023-03-01]. https://bitcoin.org/bitcoin.pdf.

[10] 司冰茹, 肖江, 刘存扬, 等. 区块链网络综述[J]. 软件学报, 2024, 35(2):773-799.

[11] 宋立芳, 韩诗琪, 赵丹. 区块链技术文献综述及管理领域应用展望[J]. 对外经贸, 2023(10):24-27.

[12] 汪永菊, 杜秀娟, 陈浩章. 区块链智能合约技术研究综述[J]. 计算机仿真, 2023, 40(8):1-4,65.

[13] 王丹, 黄松, 王兴亚. 以太坊智能合约测试研究综述[J]. 信息技术与信息化, 2023(10):52-58.

[14] ISO/IEC. Information technology—open systems interconnection—part 1: Object identifier resolution system[S]. USA: ISO/IEC 29168-2, 2011.

[15] ISO/IEC. Information technology—open systems interconnection—part 2: Procedures for the object identifier resolution system operational agency[S]. USA:ISO/IEC 29168-2, 2011.

[16] MOCKAPETRIS P. Domain names - concepts and facilities[EB/OL]. [2023-03-01]. https://datatracker.ietf.org/doc/html/rfc1034.

[17] 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. 物联网标识体系物品编码 Ecode[S]. 北京: GB/T 31866-2015, 2015.

[18] 国家市场监督管理总局, 中国国家标准化管理委员会. 物联网标识体系 Ecode 解析规范[S]. 北京: GB/T 36605-2018, 2018.

[19] MIGUEL C, BARBARA L. Practical Byzantinefault tolerance[C]// Proceedings of the Third Symposium on Operating Systems Design and Implementation. New Orleans,USA:dblp, 1999:1-14.

[20] REITER M. A secure group membership protocol[C]//Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, USA:IEEE, 1994: 176-189.