计算机科学
COMPUTER SCIENCE

基于标识与区块链融合的数据安全框架研究

朱军, 张国印, 万静静

引用本文

朱军, 张国印, 万静静. 基于标识与区块链融合的数据安全框架研究[J]. 计算机科学, 2024, 51(6A): 230400056-5.

ZHU Jun, ZHANG Guoyin, WAN Jingjing. Study on Data Security Framework Based on Identity and Blockchain Integration [J]. Computer Science, 2024, 51(6A): 230400056-5.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230400056

基于标识与区块链融合的数据安全框架研究

朱　军[1]　张国印[1]　万静静[2]
1 哈尔滨工程大学计算机科学与技术学院　哈尔滨 150001
2 江苏杰瑞信息科技有限公司　江苏 连云港 222042

摘　要　工业互联网标识解析系统已经成为支撑产业数字化转型的重要新型基础设施。结合目前数据的安全性问题,通过对标识解析架构的梳理,在区块链分布式拓扑结构及其信息安全特性的基础上提出标识与区块链融合的数据安全框架,构建协同模式的安全监管融合的数据安全框架,重点介绍了数据的收集、存储、传输、共享、确权和交易的全流程安全,然后从保密性、完整性、可用性、可追溯性等维度提出标识数据监测的安全指数体系。最后提出数据安全的保护要从固定位置数据的资产保护转变为业务系统数据的加工保护,从关注攻击行为转变为数据生命周期,从防漏洞、补漏洞转变为理数据、管数据的思路上来。

关键词:标识解析;区块链;数据融合;安全指数
中图分类号　TP309

Study on Data Security Framework Based on Identity and Blockchain Integration

ZHU Jun[1],ZHANG Guoyin[1] and WAN Jingjing[2]
1 School of Computer Science and Technology,Harbin Engineering University,Harbin 150001,China
2 Jiangsu JARI Information Technology Co.,LTD,Lianyungang,Jiangsu 222042,China

Abstract　Industrial Internet sign analysis system has become an important new infrastructure to support industrial digital transformation. Combined with the current data security issues,this paper combs the identity parsing architecture and proposes the data security framework of identity and blockchain integration based on the distributed topology of blockchain and its information security features. The collaborative data security framework is the data security framework of supervision amount integration. This paper focuses on the whole process security of data collection,storage,transmission,sharing,right confirmation and transaction. Finally,from the dimensions of confidentiality,integrity,availability,traceability and so on,a security index system of identification data monitoring is proposed. Finally,it is proposed that the protection of data security should be changed from the asset protection of fixed location data to the processing protection of business system data,from the concern of attack behavior to the life cycle of data,and from the idea of preventing and filling loopholes to data management and data management.

Keywords　Identification parsing,Blockchain,Data fusion,Safety index

1　引言

随着互联网技术特别是云计算、物联网、大数据等新一代信息技术的发展和成熟,当前全球工业正在从机械化、电气化、自动化进入数字化、网络化和智能化的新阶段。工业互联网标识解析作为我国新型的基础设施,经过四年多的探索实践,取得了阶段性成效。“武汉、广州、重庆、上海、北京”5 个国家顶级节点和“南京、成都”2 个灾备节点先后建成上线,“5+2”国家顶级节点全面建成,集中打造了自主可控、开放融通、安全可靠的标识解析体系,开启了工业互联网全要素、全产业链、全价值链全面连接的新篇章。四年多来,累计标识注册量突破 2 000 亿个,日解析量 1.2 亿次,服务企业超 20 万家,覆盖 29 个省、自治区、直辖市和 38 个重点行业,已成为推动数字经济创新发展、产业优化升级、生产力整体跃升的重要力量。

在如此大的数据面前,数据的安全、数据协同的监测危机在逐步逼近工业领域。开放互联、新一代信息技术的应用在数据全生命周期管理中引发了更多的数据安全隐患,针对数据层面的攻击方式日渐新型多样,攻击窃取数据的路径增多,工业数据上云、出境等风险加剧,工业数据安全形势复杂严峻。全局性战略性数据安全意识薄弱,数据管理与分类分级防护能力不足,针对性数据安全防护技术手段欠缺,数据安全可信交互共享生态尚未建立,是目前工业数据安全工作亟须解决的重中之重。

2　标识解析体系的数据安全问题

工业互联网标识解析体系是工业互联网网络体系的重要组成部分,是支撑工业互联网互联互通的神经中枢,其作用类似于互联网领域的域名解析系统(Domain Name Systems,DNS)[1]。

工业互联网标识解析体系的核心包括标识编码、标识解析系统和标识数据服务。标识编码是对机器、物品的“身份证”;标识解析系统是利用标识对机器和物品进行唯一性的定位和信息查询,实现全球供应链系统和企业生产系统的精准对接、产品的全生命周期管理;标识数据服务是通过统一的编码实现数据管理和跨企业、跨行业、跨地区、跨国家的数据共享共用。

通信作者:朱军(zhujun15121869283@163.com)

如图 1 所示，我国工业互联网标识解析体系由国际根节点、国家顶级节点、二级节点、企业节点、公共递归解析节点等要素组成。其中，二级节点是指一个行业或者区域内部的标识解析公共服务节点，能够面向行业或区域提供标识编码注册和标识解析服务，以及完成相关的标识业务管理、标识应用对接等。从风险分析视角看，包括架构安全风险分析、身份安全风险分析、数据安全风险分析和运营安全风险分析等；从风险防护视角看，包括行业监管、安全监测、态势感知、威胁预警和响应处置等。

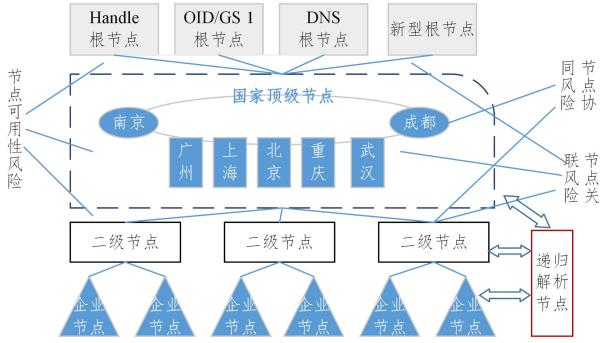

图 1 工业互联网标识体系架构及安全风险

Fig. 1 Industrial Internet identity system architecture and security risks

在此过程中，数据在各个节点进行流转和共享，要保障传输、共享的有效和可信，数据安全的防护必不可少。中国信息通信研究院发布的《数据安全风险分析及应对策略研究报告(2022 年)》显示，2020 年数据泄露加速增长，仅公开报告的全球数据泄漏达 360 亿条，创历史新高。作为数字经济健康发展的重要基石，数据安全的重要性愈发突出，数据安全治理需求愈加明显。2022 年国内外的数据安全事件频频发生，风险系数不断提高。尤其是在近几年中国的数据安全屡遭泄露和攻击，在疫情期间，中国的医药研发中心以及其他相关单位的电脑遭到境外黑客的代码病毒攻击，全国高校研究所以及科研机构遭到黑客攻击等事情，已经是多次出现。

基于目前的情况，国家组建国家数据局，也是把数据安全上升到了国家安全地位，在对数据收集、存储、处理等方面产生了积极推动作用，对数据应用层面的大数据确权、流通和交易产生了积极影响。

如图 2 所示，数据要素价值主要体现在从数据的采集、存储、加工、流通、分析、应用等方面，以来完善、调配市场配置等要素，保障除土地、资本、劳动力、技术等意外的第五种生产要素。

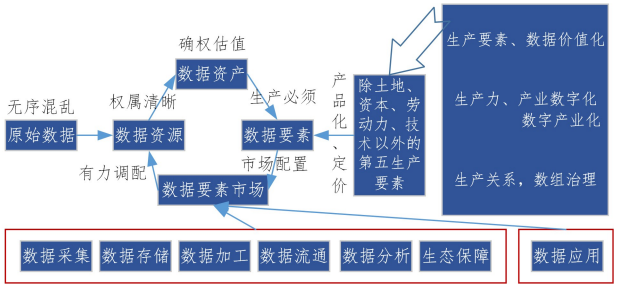

图 2 数据要素价值

Fig. 2 Value of data elements

在国务院发布的《关于构建更加完善的要素市场化配置体制机制的意见》中，数据首次成为新型生产要素被提出，数据要素被确定为数字经济时代的新型生产要素。数据要素是数据价值化的过程，数据价值化的根本保障是数据的可信和安全。

3 融合数据安全监测框架

3.1 标识与区块链融合的设计思路

标识与区块链融合的数据安全设计思路是在数据采集阶段对数据进行标识和加密处理，实现去中心化标识服务框架，达到标识数据源头的可信机制，以及完善标识数据的全生命周期管理方法论，其目是使得标识和区块链融合数据的获取、传输、使用阶段处于可信状态，提高标识解析体系架构的安全指数[2]。

如图 3 所示，标识与区块链融合的设计思路是以数据的源头到数据共享等全生命周期的全流程思路进行，从而完成数据的价值体现。

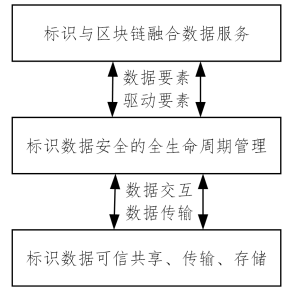

图 3 标识与区块链融合的设计思路

Fig. 3 Design ideas for the integration of identification and blockchain

区块链的去中心化应用机制很好地适用于标识解析体系的顶层架构模式，能实现多网络节点角色和多方关联的管理关系。在节点间协同风险及节点可用风险的把控上实现了标识数据状态账本、分类存储、安全同步的方法论落地。

在标识与区块链融合的设计理念中，标识解析服务框架围绕标识管理定义了角色和关系等要素。标识数据的生命周期管理方法通过融合将其转换为执行账本交互的具体操作，这也成为后续标识数据确权、交易的基础。标识可信存储机制为标识生命周期的管理提供强关联数据作为计算依据[3]，而标识生命周期管理方法使其转化为驱动要素活动的基础。在标识解析体系中，灾备节点是为国家顶级节点的数据做备份，来应对节点的突发事件，进而保障顶级节点、二级节点以及企业节点的数据安全。此外，区块链技术使每个节点都拥有相同的数据，某个节点发生故障并不会影响其他节点的功能，从而保证解析、认证等服务的连续性。

结合工业互联网标识解析体系和区块链技术架构，形成对应映射关系，在底层通过 BID 的形式将数据进行标识，形成了信任机制，对标识数据的解析进行身份鉴权和数据确权，最终在数据的运行监测、测试认证、数据评估等方面进行数据应用。

从数据的连续性以及数据的关联性来看，区块链的共识机制能够有效保障数据在各个节点的一致性和同步性，通过智能合约保障数据的可信，通过分布式的结构管理、治理各个节点数据。

如图 4 所示，数据采用标识的方式从数据的源头进行

标记,结合区块链加密手段,对数据在流转过程中确保其安全,从而保障数据的准确和精确。

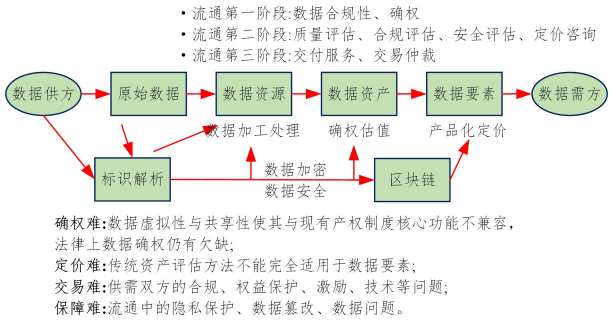

图 4　数据价值化

Fig. 4　Data value

单从数据全生命周期角度考虑,数据从数据的提供方,到数据资源,经过标识成为数据资产,最后流转到市场形成数据交易的整个过程中,数据安全是保障,没有唯一识别的可信数据无法完成数据的价值应用。因此,从原始数据开始,通过标识将数据进行唯一识别,在数据整个流转过程中通过区块链技术进行数据安全加密和处理,实现数据共享[4]的同时保证数据不被篡改和泄露[5]。

系统的总体架构是结合标识解析的三层架构和区块链的防篡改特性进行设计,如图 5 所示。基于标识和区块链的融合数据安全设计思想[6]的重点聚焦于整个标识体系架构的数据安全,构建基于标识体系的区块链网络,贯穿企业节点、二级节点、顶级节点以及递归节点,甚至连接到发挥节点作用的注册、解析客户端,负责标识数据的获取和解析。

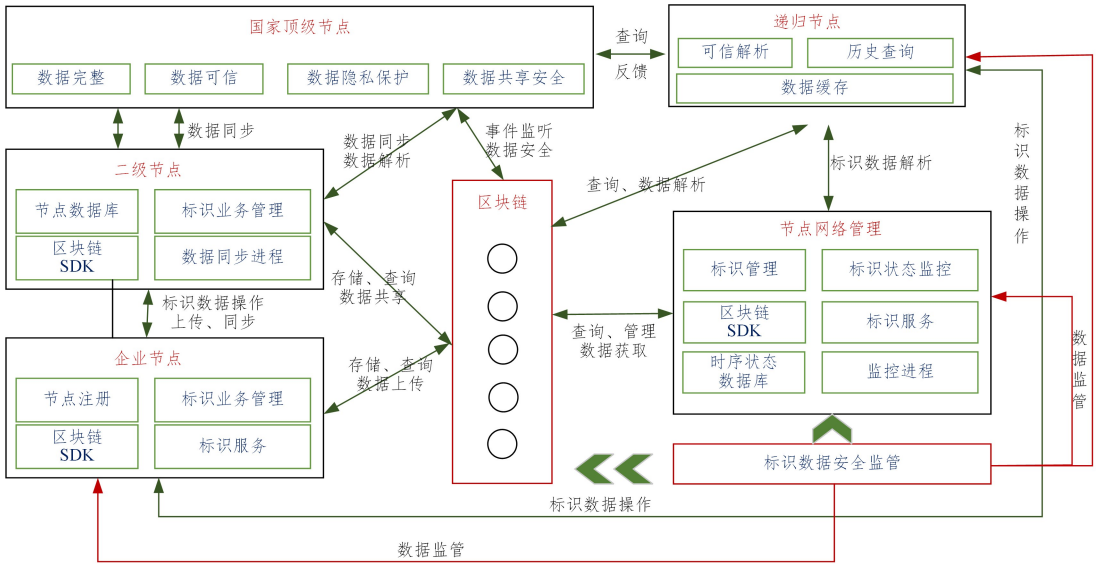

图 5　系统总体架构

Fig. 5　Overall system architecture

3.2　协同式标识数据安全监管

基于标识与区块链融合的分布式协同网络安全监测机制是分别对应一定的监测域(可划分为区域和企业级)。监测域一般是由管理员根据网络情况设计和分配[7]。融合监测中心监控各自监测域内的标识数据对象,记录标识数据安全的相关活动,提供一个日志存储、分析和处理平台,并及时将监测工作成果和资源剩余情况汇报到管理中心。中心检查监测中心的状态反馈,并及时调整监测中心的工作任务。监测域交集的标识对象作为可协调的工作内容,根据监测资源的剩余情况和当前监测工作的完成情况,决定下一时刻监测资源的分配[8],提高监测效率和资源利用率,如图 6 所示。

域内标识数据安全防御方案建立在支撑平台和数据互通之上。支撑平台可由网络平台、专家系统、数据防御系统等环节组成。网络平台是实现网络安全防御的基础,为各安全模块间的交互提供互通的载体。专家系统对环境中的网络安全问题做出判断、解释,提供智能型的决策。数据防御系统对互通数据进行数据加密、防篡改等一系列的安全防护操作[9],以及能够将数据安全隐患及时预警和处置。区块链技术作为整个链条的安全保障技术,实现身份确认、用户权限、秘钥和安全策略等一系列的安全防护,为安全监测服务中心提供稳定、可信的数据库和网络环境[10]。此外,安全响应系统在紧急状况下,能够迅速响应分布式网络环境中的安全隐患和威胁信息,及时发出安全操作指令,指导事件的处置。

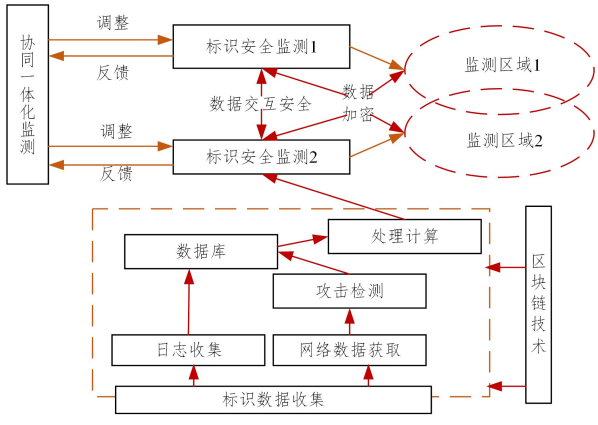

图 6　区域级的协同监测机制

Fig. 6　Regional level collaborative monitoring mechanism

企业级的数据安全监测防护如图 7 所示,主要是从不同网络的角度出发,确保网络之间数据的协同、数据的防篡改和外部攻击。传统的安全防护架构会从安全审计、入侵检测、病毒扫描以及漏洞检查等安全技术角度出发,其目的是监控网络的操作行为,监测网络流量变化和数据信息,及时发现入侵病毒和非法操作等隐患[11]。在此基础上,融入标识+区块链技术,每个网络自成一个节点,节点与节点之间形成一个企业级的

网络架构，使被动的安全防御变为主动的安全预防，从数据本身的唯一性、数据的可信性、数据的防篡改性以及数据在不同网络、不同系统之间流通的加密性上实现了数据安全[12]。

传统的安全防护设备分布在网络安全域中，包括身份认证和数据加密、访问控制、防火墙、安全隔离等设备。安全域是在安全设备及安全策略的统一指导下，根据网络各区域的工作属性、组成设备、所携带的信息性质、使用主体、安全目标等，将网络划分成不同的域，将具有相近安全属性的组成部分归纳在同一域中。区块链网络打破了传统的安全域的问题，从底层数据用标识，并接入区块链网络开始，就已经形成了基于比标识和区块链完整的安全网络，实现了只要数据存在网络中，即属于所说的安全域概念。此外，数据的完整性和机密性问题[13]在区块链网络中也得到了很好的解决。在整个分布式的网络环境中，“标识＋区块链”的安全思想满足了现有的网络安全需求，使得网络中每个安全隐患都能够很好地控制在每个角落，不会影响其他系统或者网络。

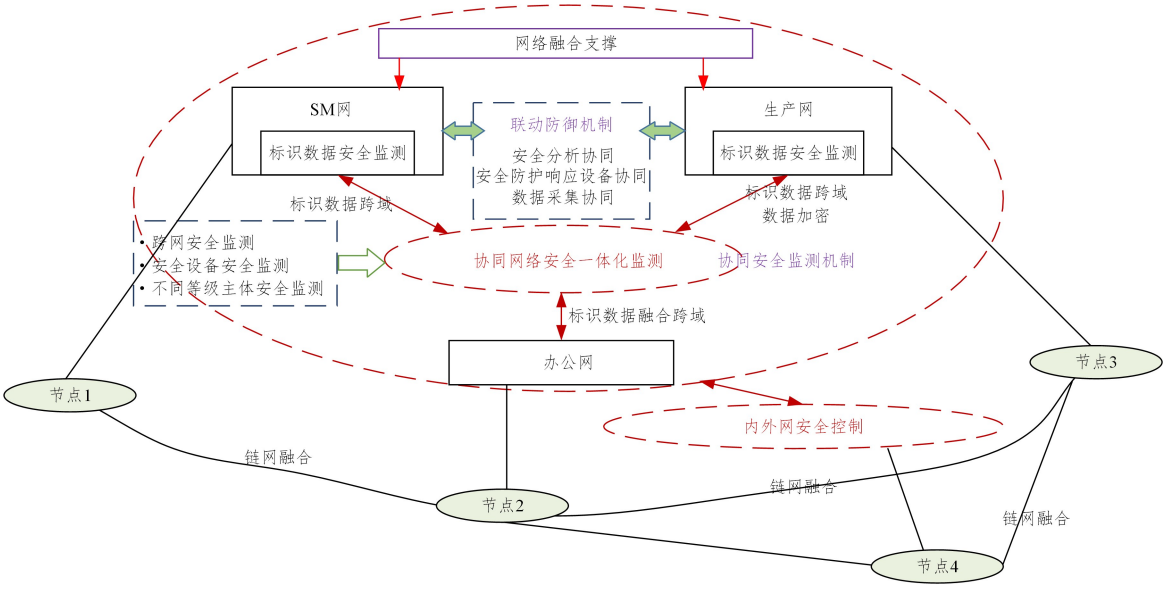

图 7 企业级数据安全监测防护架构

Fig. 7 Enterprise level data security monitoring and protection architecture

数据安全响应协同主要是入侵检测系统与有充分响应能力的网络设备或网络安全设备集成在一起，构成响应和预警互补的综合安全系统。其中包括与防火墙、与交换机、与病毒防御系统、与蜜罐系统等。

数据上标识是为了让数据有唯一的身份信息，在数据交换的过程中与其他文件进行绑定。数据标识应具备数据的唯一性、完整性和不可分离以及不可篡改和可追溯性[14]，通过区块链将其进行有机统一、统一管理和统一管控，实现对数据加密的跟踪和标记。

在数据传输和共享的过程中，为防止数据信息的泄露[15]，对数据信息进行多层加密处理[16]，同时从数据的加密程度对数据的密级进行分级，根据需要对数据进行密级标识。更改密级需要通过审批流程进行操作。在企业生产系统与企业信息系统的互联建设中运用数据密级标识技术[17]，所有需要传输至系统中的数据文件都必须先进行定密[18]，确定数据类型后，传输至数据监测交换平台，且平台只传输具有唯一且不被篡改数据标识的文件或者数据。

3.3 融合数据安全框架的内容

工业互联网标识解析作为工业互联网实现互联互通的“中枢神经”，存储了更多的敏感数据，一旦服务受限或遭遇攻击，将会对国民经济造成重要影响，甚至对国家安全构成一定的威胁。因此在对待标识数据安全方面，会结合最新的区块链技术来障工业互联网标识解析体系面临的新安全风险变化，主要突出表现在架构安全风险、身份安全风险、数据安全风险和运营安全风险 4 个方面。

如图 8 所示，融合数据安全框架的内容利用国密算法、可信上链等技术从架构、身份、数据、运营几个维度进行设计，确保数据在整个流转、互通、共享过程中的安全。

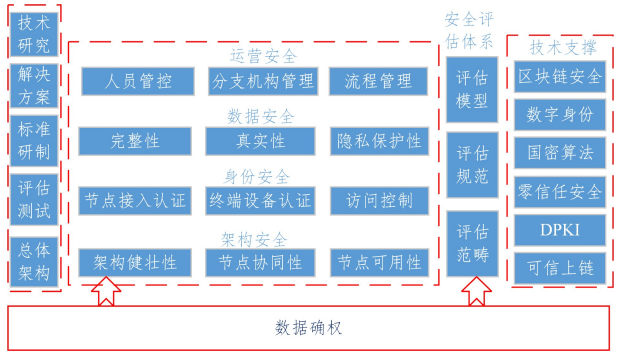

图 8 融合数据安全框架的内容

Fig. 8 Content of fusion data security framework

在数据互通和共享的过程中，数据的确权保护是至关重要的[19]。基于新型基础设施数字身份体系实现数据流通和数据保护，为政府和数据交易提供智能数据确权管理服务，统一把控政务数据、工业数据、产业数据以及供应链数据质量，实现政务数据共享、产业数据互通[20]、经济数据透明等及数据决策功能。依托数据标识、确权标识、隐私计算、链上存证等技术优势，对数据来源进行合规审核，对数据交易活动进行规范管理，明确数据权属，实现数据可信交易等。

3.4 标识数据监测安全指数

针对标识数据安全的风险和挑战，结合工业互联网标识解析目前的体系架构[21]，以及标识在接入、场景、可信以及事件中的评估维度，按照动态性和平台性的原则，构建了标识数据监测安全指数评估体系[22]架构内容。具体如表 1 所列。

表 1　标识数据监测安全指数

Table 1　Identification data monitoring safety index

一级指标	二级指标	三级指标
标识数据安全指数	标识数据安全指数	注册数据正确率
		解析数据正确率
	企业数据接入指数	服务企业数
		服务头部企业数
		企业所属行业分布
		省内外企业占比/本地企业数/本地化率
		集团内外企业占比，外部解析率
		接入企业的活跃数，活跃度
		接入企业增长情况
	标识应用场景风险指数	标识对象评估
		标识软件接口风险
		标识软件类型风险
		应用设备类型指数
		1. 产品/半成品；2. 生产/物流设备；
		3. 自研主动标识载体；4. 5G 相关新产品等
		应用场景的安全防护措施
		应用场景的安全系数
		标识软件数据防护指数
	双链安全评估指数	供应商合规指数
		供应链经营指数
		供应链安全库存指数
		供应链数据安全指数
		产业结构柔性指数
		产业数据安全共性指数
		产业融合度指数
	异常事件指数	注册数据量增幅异常
		解析数据量增幅异常
		标识日志数据外泄指数
		生产经营环节事件预警

结束语　在大数据时代，数据已经渗透到每一个行业，成为重要的生产因素。数据安全是企业生存的根基，而实现数据价值流动的重要前提是数据产生的“安全、可信、确权”。区块链凭借其抗篡改、透明化、分布式的安全特性，成为支撑可信数据有序流动的重要保障，对实现国家及企业数据安全起着至关重要的作用。新型的数据安全思路已经从固定位置数据的资产保护转变为业务系统数据的加工保护，从关注攻击行为转变为数据生命周期，从防漏洞、补漏洞转变为理数据、管数据，因此，数据的安全要从数据源头开始分析到数据流转监测，再到数据风险识别和数据动态监测和审计，一整套的数据全生命周期流程保护。区块链凭借其可信任性、安全性和不可篡改性，使得更多数据得以被释放出来。区块链正在让大数据汹涌而来。

参 考 文 献

[1] CHI C，MA B L，TIAN J. Research on security risk Analysis Model of Industrial Internet Identity Analysis [J]. Information Communication Technology and Policy，2020(10)：23-27.

[2] LI Z P，LIU D P，ZHANG B，et al. Identity parsing technology based on blockchain [J]. Network Security Technology and Application，2023(2)：6-8.

[3] BAI Y M，DENG X F. A safe storage and sharing model of medical data integrating blockchain and cloud storage [J]. Journal of Jiaozuo University，2023，37(1)：75-79.

[4] ZHAO Y X，ZHAO Q，HUANG C，et al. Marine data security sharing system based on blockchain [J]. Marine Development and Management，2023，40(1)：37-43.

[5] CHEN A Q，XIAO Z H，PAN X Y. Analysis of Blockchain security Technology based on data Trusted Sharing [J]. Electronic Technology，2023，52(1)：280-281.

[6] CUI L J. Security Protection of accounting information Big Data under blockchain technology [J]. Marketing，2022(24)：105-107.

[7] ZHAN B. Design of Network privacy data security protection Model based on blockchain [J]. Information and Computer (Theoretical Edition)，2022，34(24)：219-221.

[8] LI Z L. Research on Cloud accounting data Security under the application of blockchain encryption technology [J]. Business News，2022(27)：32-35.

[9] XU J P，HAN J Q，ZHANG X，et al. Research on Traceability of grain and oil Quality Safety based on trusted blockchain and trusted Label [J]. Food Science，2023，44(3)：48-59.

[10] WANG B. Secure storage and analysis of medical device identification based on blockchain technology[D]. Chongqing：Chongqing University of Posts and Telecommunications，2022.

[11] CUI Y，HE B W，SONG X，et al. Research on Identification Analysis Technology of Aerospace Industry for Industrial Internet [C]// Proceedings of the 33rd China Simulation Conference. 2021：683-694.

[12] SU X R，XU X F，GUO W T. Integrated application of identity parsing and blockchain technology in Supply chain management [J]. Science and Technology Industries，2021，21(9)：283-289.

[13] YU J Y. Design and implementation of Identity Resolution Registration Authentication and Trust Resolution Mechanism for Industrial Internet [D]. Beijing：Beijing University of Posts and Telecommunications，2021

[14] ZENG S Q. Design and implementation of Industrial Internet Sign Parsing System based on Blockchain [D]. Beijing：Beijing University of Posts and Telecommunications，2021.

[15] ZHAO H R. Design and implementation of Industrial Internet sign parsing System Performance optimization Scheme based on blockchain [D]. Beijing：Beijing University of Posts and Telecommunications，2021.

[16] WANG L J，LIU J，WANG S，et al. Research on the application of Industrial Internet logo public service based on blockchain [J]. Frontiers of Data and Computing Development，2021，3(1)：60-73.

[17] LIU X J，CAO T C，XIA Y J. Research on Efficient Cross-domain Data Security Sharing of Internet of Vehicles based on Blockchain architecture [J/OL]. Journal of Communications，1-12.

[18] FAN Y. Distributed Logo Design and Analysis of Internet of Things based on blockchain [D]. Beijing：Beijing University of Posts and Telecommunications，2020.

[19] WANG S，YAN M，LIU J，et al. Innovative application mode of scientific data identification technology based on blockchain [J]. Frontiers of Data and Computing Development，2019，1(6)：62-74.

[20] WANG Y M，LI H，WANG H，et al. Research of Blockchain in Industrial Internet logo data management strategy [J]. Computer Engineering and Applications，20，56(7)：1-7.

[21] ZHANG D X. Research on heterogeneous identity equivalence Analysis Technology of Internet of Things based on Blockchain [D]. Chongqing：Chongqing University of Posts and Telecommunications，2018.

[22] LIANG X. Design and Implementation of a Security Module for Service Identification parsing System [D]. Beijing：Beijing Jiaotong University，2009.

ZHU Jun，born in 1987，Ph.D candidate. His main research interests include industrial network security，blockchain，identity analysis，etc.