国家工业信息安全发展研究中心
CHINA INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

区块链与数据安全治理白皮书

（2021）

cic 工信安全

2021 年 4 月

版权说明

本白皮书版权属于各参编单位共有，受法律保护。转载、摘编或利用其它方式使用白皮书文字或者观点的，应注明“来源：《区块链与数据安全治理白皮书》（2021 版）”。违反上述声明者，各参编单位将追究其相关法律责任。

牵头编写单位：国家工业信息安全发展研究中心

联合编写单位：深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、北京邮电大学、北方工业大学、北京天融信网络安全技术有限公司、中汽院汽车技术有限公司、北京市盈科律师事务所、北京韬安律师事务所、北京安华金和科技有限公司、《中国中医药报》社有限公司、武汉东湖大数据交易中心股份有限公司、山东省电子信息产品检验院（中国赛宝（山东）实验室）、西安纸贵互联网科技有限公司、杭州趣链科技有限公司、深圳法大大网络科技有限公司、长春吉大正元信息技术股份有限公司、全链通有限公司

参编人员：潘妍、李卫、郭晓栋、余宇舟、许智鑫、吴平平、邵兵、刘江、钟力、唐会芳、石瑞生、兰丽娜、何云华、艾龙、谢雄、周开宇、温子瑜、王娜、王军、王立岩、唐力、武东、沈冠楠、杜乐、张睿、王新霞、杨文韬、杨珍、虞博名、庄子骏、刘岱、韩璇、刘思辰

前　言

区块链与数据安全治理的结合应用是电信、互联网、金融、医疗、政务、交通等多个行业在信息化、数字化、智能化转型过程产生的新议题、新实践。随着信息技术的快速发展，云计算、大数据、物联网、移动互联网、人工智能等新技术、新应用广泛普及，数据的海量汇聚推动了数字经济的快速发展。数据已成为数字经济时代的关键生产要素，数据的核心价值已成为国内外各界关注的焦点。与此同时，数据安全治理工作正面临前所未有的新挑战、新机遇。

首先，全球数据安全形势愈发严峻，给国家安全、企业秘密和个人隐私等带来严重安全威胁。由网络攻击、数据窃取和非法交易形成的网络黑市，已经逐步成为大规模、有组织的集团性犯罪平台，甚至成为某些国家黑客主导的高度成熟经济组织发展的温床。当前，全球数据黑产的规模已达数千亿美元。数据安全不仅对企业和个人造成巨大的经济损失，也给各国的政治安全和社会稳定带来了复杂的不良影响。

其次，全球数据安全立法和监管不断加强。各国数据保护相关法律法规持续升级，相继制定专门的数据安全和个人信息保护法，确立数据保护和个人信息收集使用的严格规则，对企业数据安全合规提出了更高的要求。我国《网络安全法》将个人信息保护纳入网络安全保护的范畴，《数据安

全法（草案）》《个人信息保护法（草案）》等围绕数据安全治理的相关配套法规和标准相继出台，数据合规正成为企业的法定义务。

最后，全球产业对数据的开发利用亟需数据安全治理保障。随着大数据与各个行业的紧密结合以及在生产生活的各个领域广泛应用，数据安全治理已成为有效发掘和实现数据价值的重要前提。通过数据安全治理，企业能够将数据资源梳理为具有价值的数据资产，并将数据资产作为正确决策的重要依据。产业亟需通过数据安全治理来应对数据泄露、数据滥用、数据篡改、数据孤岛等多种管理和技术风险。

区块链技术的应用可为数据安全治理工作提供新思路。利用区块链技术，数据安全治理工作能够在数据全生命周期形成模块化的数据安全管理平台和工具，便于相关主体对数据的安全保护和开发使用。区块链采用的分布式账本技术解决了数据共享的效率问题，能够保证数据的不可篡改性和可追溯性，解决了数据安全可信问题。此外，有关部门可在区块链技术基础上配置监管策略，掌握数据态势，做好数据安全风险防控。

数字经济时代，需要加快区块链技术同各行业各领域数据安全治理工作的融合应用。在保证数据安全可信、公开透明和有效监管的基础上，更大程度地加强企业之间的合作和数据共享，真正发挥数据的价值。

目 录

第一章 区块链与数据安全治理白皮书概述

一、编制背景

当前，数据已成为数字经济时代下的核心生产要素，数据应用正加速渗透到经济社会的各个领域，成为促进资源优化配置、提高全生产要素效率、推动产业转型升级、培育经济新动能的重要力量。然而，复杂的数据应用技术、高风险的数据海量汇聚、不完善的数据产业生态正在对数据安全治理工作提出新的挑战，亟待国家、行业、企业等多维度的主体积极参与，共同解决。为更好地汇聚产业各方力量，聚焦数据安全治理核心问题，推动数据安全产业发展，区块链技术与数据安全工业和信息化部重点实验室成立了“数据安全治理工作组”，在工作组的框架下定期出台面向行业的“数据安全治理”主题系列白皮书。

二、编制目标

本白皮书旨在梳理区块链与数据安全治理的政策法规、技术标准和产业现状，研究总结区块链与数据安全治理结合的技术可行性，探索建立利用区块链助力数据安全治理的应用方案，提出下一步的工作建议与思路。本白皮书主要围绕以下内容展开：一是区块链与数据安全治理的背景现状，包括在法律政策、技术标准、行业应用等方面取得的现有成效；

二是区块链与数据安全治理的综合分析，包括数据安全问题的痛难点、区块链与数据安全治理的关联性以及二者结合的可行性；三是区块链与数据安全治理在各行业、各领域进行有效结合的应用方案；四是区块链与数据安全治理相关产业的发展建议与展望。期冀本白皮书能够为部门决策和行业发展提供参考建议，推动数据安全治理工作有序开展。

三、特别申明

（一）研究范围

本白皮书提出的“数据安全治理”是指各行业、各领域为解决数据安全问题而采用的一系列方法、工具、手段，通过安全使用数据实现业务目标的行为。研究聚焦于相关机构在数据安全治理工作中有效应用区块链技术的路径和方案，以解决三类主要目标任务：数据安全合规，为符合国家政策、法律法规、强制性标准等要求，以降低违法违规风险为目标所做的数据安全工作；数据安全保护，为提升信息系统的安全防护能力，降低系统脆弱性和被恶意攻击的风险，确保数据的保密性、完整性、可用性，以降低技术层面的安全风险为目标所做的数据安全工作；数据安全管理，为提升数据管理能力、数据安全能力、数据治理能力的成熟度，从组织建设、制度流程、技术工具、人员能力等维度入手，以更好发挥数据作用为目标所做的数据安全工作。

（二）研究内容

本白皮书主要观点和内容仅代表编制组目前对区块链与数据安全治理的研究和思考，欢迎业界专家指导和提出意见，共同推进白皮书不断更新与完善。

CIC 工信安全

第二章 区块链与数据安全治理现状

一、法律政策

（一）数据安全治理相关法律政策

1. 国内法律政策

我国在数据安全治理领域已初步形成了由法律、政策、法规规章、规范性文件及相关政策文件组成的多层次法律政策体系。

在法律层面，我国颁布并施行了《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国电子商务法》《中华人民共和国密码法》《中华人民共和国民法典》等多部法律。目前，《中华人民共和国数据安全法（草案）》已于2020年6月28日提请十三届全国人大常委会第二十次会议审议，《中华人民共和国个人信息保护法（草案）》也于2020年10月21日公布并公开征求社会意见。两部法律草案分别从不同角度不同程度对个人信息和数据保护做了相关规定。

在政策层面，国务院于2015年7月发布《关于运用大数据加强对市场主体服务和监管的若干意见》，建议在数据开放的市场下，利用大数据以及现代信息技术提升政府对大数据的运用能力，完善政府服务和监管体系，提高政府数据

治理水平。同年 8 月，国务院印发《促进大数据发展行动纲要》，指出加快政府数据开放共享、推动资源整合、提升治理能力的主要任务，要求推动产业创新发展，培育新兴业态，助力经济转型，强化安全保障，提高管理水平，促进健康发展。2020 年 4 月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，提出加快培育数据要素市场，优化经济治理基础数据库，提高数据资源整合利用。

在法规规章层面，由《电信和互联网用户个人信息保护规定》《计算机信息系统安全保护条例》《互联网信息服务管理办法》等文件初步形成了数据安全治理监管体系。国家互联网信息办公室于 2019 年陆续发布了《数据安全管理办法（征求意见稿）》和《个人信息出境安全评估办法（征求意见稿）》，并审议通过了《儿童个人信息网络保护规定》。

总体来说，我国对数据安全治理高度重视，诸多立法、政策齐头并进，为数据及其安全治理落地实践提供了全面的保障措施。

2. 国外法律政策

数据安全已引起全球各个国家的高度重视，各国政府和组织近几年相继颁布数据安全治理相关的法规和政策，如《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）、《非个人数据自由流动条例》（Regulation on

the Free Flow of Non-personal Data）、《欧洲数据战略》（A European Strategy for data）、《2018 年加州消费者隐私法》（California Consumer Privacy Act）等。

2018 年 5 月正式生效的 GDPR 对全球数据治理生态产生了深刻影响，尤其是规定了欧盟境外主体在特定条件下也必须遵循 GDPR 相关规范，而处罚标准可能会让企业面临“上限 2000 万欧元或全年营业额的 4%（取高者）”的罚款。数字经济的全球化迫使包括中国在内的企业主体在进行数据治理战略部署和开展跨境数据运营业务时，不得不考虑和评估 GDPR 的约束和实际影响力。

欧盟委员会于 2017 年 9 月提出“促进非个人数据在欧盟境内自由流动”的立法建议。2018 年 10 月，欧洲议会投票通过《非个人数据自由流动条例》。其后，欧盟委员会于 2020 年发布《欧洲数据战略》，提出将就影响数据敏捷性经济体系中各主体关系的议题探讨立法的必要性。2020 年 6 月，欧盟委员会向欧洲议会和欧盟理事会提交《数据保护是增强公民赋权和欧盟实现数字化转型的基础—GDPR 实施两周年》报告。同年 6 月，欧洲数据保护监管机构（EDPS）发布《EDPS 战略计划（2020-2024）—塑造更安全的数字未来》。

此外，美国、日本、韩国、加拿大、澳大利亚等发达国家和巴西、印度等发展中国家也在数据治理进程中表现出极大热情，在指导各自境内企业或组织保障个人信息和数据安

全的同时，皆在全球化数字经济中尽可能地将自身利益最大化。总体来说，全球政策法律环境由前期的以信息自由、数据共享为核心，逐步发展到以个人信息及隐私保护为重点，并向全面的数据治理扩张，为数据安全治理及其法治化提供法律和政策保障。

（二）区块链相关法律政策

党中央和政府部门高度关注区块链。2019 年 10 月 25 日，在中央政治局十八次集体学习中，习近平总书记强调，构建区块链产业生态，加快区块链和人工智能、大数据、物联网等前沿信息技术的深度融合，推动集成创新和融合应用。

此前，国家层面已陆续出台了系列风险防控和发展政策。2013 年 12 月，为了防范比特币全球投资浪潮高涨带来的金融风险，央行等五部委联合发布《关于防范比特币风险的通知》。2016 年 12 月，区块链技术列入“十三五”国家信息化规划。

在产业促进方面，2016 年工信部发布《中国区块链技术和应用发展白皮书（2016）》，将区块链定义为分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，首次提出了我国区块链技术发展的标准路线图。2018 年 3 月 23 日，工信部发布《2018 年信息化和软件服务业标准化工作要点》，提出推动组建全国区块链和分布式记账技术标准化委员会。

在学科建设方面，国务院办公厅于2017年1月20日发布的《关于创新管理优化服务培育壮大经济发展新动能加快新旧动能接续转换的意见》，提出要创新体制机制，突破院所和学科管理限制，在人工智能、区块链、能源互联网、智能制造、大数据应用、基因工程、数字创意等交叉融合领域，构建若干产业创新中心和创新网络。

在行业监管方面，2019年1月10日，国家互联网信息办公室发布《区块链信息服务管理规定》，并于2月15日正式施行。规定指出区块链信息服务提供者和使用者不得利用区块链信息服务从事危害国家安全、扰乱社会秩序、侵犯他人合法权益等法律行政法规禁止的活动。规定对我国区块链行业发展做出了规范限制，意味着我国正式迎来对于区块链信息服务的“监管时代”。

尽管在法律法规方面，我国对区块链技术的立法稍显薄弱，但区块链作为一项底层技术，其法律体系仍离不开当前计算机及信息技术相关的基础法律体系。因此，在区块链的规范应用中，在遵循《区块链信息服务管理规定》相关要求的同时，还应当遵循《中华人民共和国网络安全法》《电子商务法》《电子签名法》《计算机信息系统安全保护条例》《互联网信息服务管理办法》等基础性法律法规的规定。

（三）区块链与数据安全治理相关法律政策

在法律法规层面，区块链作为一项底层技术，在具体的

应用场景中有望实现数据安全合规的目标。《数据安全法（草案）》中提出要建立数据安全保护体系，这将促使数据安全与区块链的结合以赋能数据确权与数据流通。虽然适用于数据安全治理领域的相关法律法规尚未直接规范区块链技术领域，但因数据安全治理所追求的法律目标与区块链领域所追求的技术目标存在相似之处，故在一定程度上，区块链技术的落地应用，同样离不开对数据安全治理领域相关法律法规的遵循和使用。

在地方政策层面，北京、山东、江西、福建等地积极提出区块链与政务结合的具体落地措施，通过新一代信息技术提升政务服务水平，重构社会信用体系。2020 年 6 月，北京市政府发布《北京市加快新型基础设施建设行动方案 2020-2022 年》，提出建设政务区块链支撑服务平台，推进建立数据特区和数据专区，建设数据交易平台。同月，北京市政府办公厅发布《北京市区块链创新发展行动计划（2020-2022 年）》，提出将围绕数据安全、监管合规的医疗卫生管理体系建设需求，探索打造区块链技术应用场景。疫情期间，济南市政府部门会同相关厂商研发上线的“身份健康码”，以区块链服务平台作为支撑，通过数字身份合约和数据存证服务，有效保障“身份健康码”及人员数据安全和授权使用服务。

二、技术标准

（一）数据安全治理标准

1. 国内技术标准

目前，我国正处于持续推动数据安全治理标准化的发展阶段。2018 年 3 月，国标 GB/T 36073-2018《数据管理能力成熟度评估模型》正式发布。2018 年 6 月，中国电子工业标准化技术协会信息技术服务分会（ITSS 分会）正式发布国标 GB/T 34960.5-2018《信息技术服务治理 第 5 部分：数据治理规范》。2019 年 8 月，国标 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》正式发布。2020 年 2 月，全国金融标准化技术委员会发布金融行业标准 JR/T 0177-2020《证券期货业投资者权益相关数据的内容和格式》。2020 年 11 月，全国 APP 个人信息保护监管会共发布 18 项 APP 个人信息保护团体标准，为 APP 侵害用户权益专项整治工作提供依据和支撑。2020 年 12 月，工信部正式发布《电信和互联网行业数据安全标准体系建设指南》。

根据国家标准化管理委员会和全国信息安全标准化技术委员会的标准化工作要点，近几年将优先开展大数据安全参考框架的研制、完善个人信息安全相关标准研制、推进数据交换共享相关安全标准研制、加快数据出境安全相关标准研制以及启动重点领域大数据安全标准研制等工作。

2. 国际技术标准

我国积极参与数据安全领域的国际技术标准制定工作。2014 年，中国电子工业标准化技术协会信息技术服务分会（ITSS 分会）启动了数据安全标准预研工作，并向 SC40/WG1 提交了《数据治理白皮书》（英文版）和数据治理研究技术报告。2015 年 5 月，在巴西 SC40 全会上，中国代表团正式提出“数据治理国际标准”新工作项目建议并获通过。会议决定将数据治理国际标准分为两个部分：第一部分，由我国成员体申请立项和研制的 ISO/IEC38505-1《ISO/IEC 38500 在数据治理中的应用》于 2017 年 3 月获国际标准化组织批准，成为国际上第一个数据治理国际标准；第二部分，由我国专家主导研制的第二个数据治理领域的重要国际标准——ISO/IEC TR 38505-2《数据治理对数据管理的影响》于 2018 年 5 月获批发布。2020 年 10 月，我国专家担任编辑的国际标准 ISO/IEC 20547-4: 2020《信息技术 大数据参考架构 第 4 部分：安全与隐私保护》正式发布。

（二）区块链技术标准

1. 国内技术标准

中国区块链标准化工作于 2016 年底启动，与国际标准化基本同步。2016 年 10 月，工信部发布《中国区块链技术和应用发展白皮书》，首次提出我国区块链标准化路线图。同时结合区块链应用场景和技术架构，提出了区块链标准体系框架建议。2017 年 5 月 17 日，工信部发布《区块链参考

架构》，通过阐述区块链的用户视图和功能视图，对区块链的主要参与者和核心功能组件进行了详细规定，系统地描述了区块链的生态系统。2017 年 12 月 12 日，工信部发布《区块链数据格式规范》，规定了区块链技术相关的数据结构、数据分类及其相互关系和数据元的数据格式要求等，为区块链系统建设提供了数据参考。2019 年 11 月 4 日，工信部在《2018 年信息化和软件服务业标准化工作要点》中提出将推动成立全国区块链和分布式记账技术标准化委员会，体系化推进标准制定工作，加快制定关键急需标准，构建标准体系，积极对接 ISO、ITU 等国际组织，积极参与国际标准化工作。目前，《中国区块链技术和应用发展白皮书》《区块链参考架构》《区块链数据格式规范》都已经作为标准化文件贡献到国际标准中。

我国区块链标准化工作可分为：密码算法和签名标准、底层框架技术标准、技术应用标准和测评认证标准等。截至 2020 年 6 月底，在密码算法及电子签名标准领域，相关国密算法标准约 20 项、密码算法规范约 5 项、数字签名标准约 29 项；在区块链底层框架及技术应用标准领域，涉及底层框架技术方面团体标准 8 项、在研标准 3 项，区块链应用方面团体标准 24 项、行业专业应用标准 8 项。2020 年 10 月，国家互联网应急中心牵头推进的行业标准《区块链技术架构安全要求》正式发布并实施；该标准规定了区块链技术架构应

满足的安全要求，包括共识机制安全、智能合约安全、账本安全等。

在行业标准方面，中国人民银行正式发布《金融分布式账本规范》（JR/T 0184-2020），对金融分布式账本技术的基础硬件、基础软件、密码算法、节点通信、账本数据、共识协议、智能合约、身份管理、隐私保护、监管支撑、运维要求和治理机制等方面的安全技术规范进行了详细说明，有效保障金融行业信息安全能力，推动“区块链+金融”朝着更加规范的方向发展。

2. 国际技术标准

从国外来看，国际制定区块链标准的相关机构主要有ISO/TC307、IEEE、ITU、W3C 等组织。其中，ISO/TC 307 已发布相关标准 3 项，在研 12 项。IEEE 在研 13 项。ITU 已发布 5 项，在研 15 项。

ISO（国际标准化组织）在 2016 年 9 月成立了区块链和分布式记账技术委员会（ISO/TC 307），并成立 5 个研究组（参考架构、用例、安全、身份、智能合约），制定全球区块链标准和相关支持协议。目前该组织共提出 15 项区块链标准及相关规范、报告，多为基础标准相关的内容，如术语和概念、参考架构、合规性智能合约等。ISO 已发布《ISO 22739:2020 区块链及分布式账本技术：术语》《ISO 22739:2020 区块链及分布式账本技术：隐私和个人身份信息

保护注意事项》《ISO/TR 23455:2019 区块链及分布式账本技术：区块链中的智能合约和分布式账本技术系统的概述及其交互》等三项区块链标准。

IEEE（电气电子工程师学会）成立区块链工作组 P2418，重点针对区块链在 IoT 场景下的标准开展研究，确定未来区块链在 IoT 场景下接口对接标准。截至目前，已研究、制定 13 项国际区块链标准，其中有 11 项属于业务和应用领域，涉及交通、医疗、政务等领域。

ITU（国际电信联盟）是负责确立国际无线电和电信的管理制度和标准的国际组织。中国是 ITU-T 区块链技术标准化工作的重要推进力量，牵头负责分布式账本的总体需求、参考架构、安全、评估体系及其在物联网中的应用研究。ITU-T 在区块链方向已开展了 20 个项目的研究，已发布《F.751.0 分布式账本系统技术要求》《F.751.1 分布式账本技术的评估标准》《F.751.2 分布式账本技术参考框架》《X.1400 分布式账本技术的术语和定义》《X.1404 分布式账本的安全保证》等 5 项标准。

（三）区块链与数据安全治理相关标准

1. 国内技术标准

在国家标准层面，2019 年 7 月 1 日，工信部发布的《电信和互联网行业提升网络数据安全保护能力专项行动方案》提出要出台《网络数据安全标准体系建设指南》，加快完善

行业网络数据安全标准体系。2020 年 12 月 17 日，工信部办公厅正式印发《电信和互联网行业数据安全标准体系建设指南》，明确了区块链和数据安全相结合的标准制定方向，数据安全标准体系包括基础共性、关键技术、安全管理、重点领域四大类标准，其中在重点领域标准中，基于区块链方向，指南明确了区块链隐私数据保护和区块链数字资产存储与交互防护两大方向。

在地方标准层面，2019 年 12 月 31 日，贵州省市场监督管理局发布《基于区块链的数据资产交易实施指南》，规定了基于区块链的数据资产交易实施的术语、定义和缩略语、基本要求、数据资产交易规范等要求，旨在为数据资产交易平台的实施提供正确的指引。2020 年 4 月 3 日，山东省市场监督管理局发布《基于区块链技术的疫情防控信息服务平台建设指南》，规定了基于区块链技术的疫情防控信息服务平台建设的基本原则、平台用户、建设要求、架构、功能要求、性能要求、管理要求等内容，并根据实际疫情防控工作需要，按照不同数据内容定义上链客体数据格式规则。

在团体标准方面，2018 年 12 月，中国电子工业标准化技术协会发布《区块链隐私保护规范》标准，规定了区块链隐私保护规范，包括隐私保护的原则、关注点、管理要求、监管和审计要求。2019 年 4 月 4 日，中国商业联合会发布《区块链应用指南 商品及其流通信息可追溯性要求》，规定了

区块链技术在商品流通信息可追溯体系中的应用要求，包括应遵循的原则、应用框架、数据要求、应用支持等内容。该标准既适用于经营者的商品信息追溯体系建设，也适用于监管部门的商品流通信息追溯。2020 年 4 月，中国防伪行业正式发布首个区块链标准《区块链防伪追溯数据格式通用要求》，规定了区块链防伪追溯信息系统的物品流通追溯信息、防伪码信息等数据上链和查询的数据格式。2020 年 5 月 11 日，浙江省电子商务促进会发布《电子商务商品交易信息区块链存取证平台服务规范》，规定了电子商务商品交易信息区块链存取证平台服务的建设原则、平台架构、功能框架以及基本功能要求，指导区块链服务供应商结合电子商务商品存取证业务，设计和开发基于区块链的存取证平台，为需要存取证服务的用户提供选择依据和参考。截至 2020 年 7 月，区块链与数据安全方向另有三个标准即将出台，分别是《基于区块链的物联网设备可信接入与数据共享技术研究（征求意见稿）》《金融交易中的区块链智能合约与分布式账本安全技术研究（征求意见稿）》《区块链开发平台网络与数据安全技术要求（报批稿）》。

2. 国际技术标准

在国际标准方面，ITU-T 国际电联 SG17 安全标准工作组的研究项目《基于分布式账本技术的数据访问和共享管理系统的安全框架》《身份管理中使用区块链数据的安全考虑》

已经启动。2020 年 4 月，德国标准化学会（DIN）发布《区块链的隐私设计：使用区块链技术处理个人数据的标准化模型》，建立了在区块链生态系统中处理个人数据的一般原则和方法，指定了数据保护的技术和组织措施，考虑了“设计隐私”的原则以及受法律框架（例如 GDPR）启发的规范，帮助识别数据类型（例如加密或未加密）以及导致正面或负面归类为“个人数据”的数据处理方法。

三、行业应用

（一）数据安全治理行业推进情况

随着数字经济时代浪潮全面来临，以“数字新基建、数据新要素、在线新经济”为核心的新一轮数字经济正在蓬勃发展。在此背景下，数据安全问题逐渐成为各行业突破关键转型期必须解决的重要制约瓶颈。数据价值的凸显与数据安全的风险将数据安全治理问题呈现在大众视野中。

目前，政务、金融、能源、电信、医疗等关键信息基础设施所在行业和领域普遍在加快推进数据安全治理相关工作。随着相关企业数据总量及流动性的高速发展，以及各类场景化方案的逐步落地，中国数据安全市场呈现出高速增长的态势。据相关研究，2018 年中国数据安全市场达到 29.7 亿元，增速 29.6%，而 2019 年增速进一步提升至 32.7%，规模达到 39.4 亿元。预计 2023 年数据安全市场规模将达到 97.5

亿元水平。

我国最早意识到数据安全治理重要性的行业是金融行业。由于对数据的强依赖，金融业非常重视数据平台的建设。几代数据平台的验证表明，数据安全治理问题是限制平台建设发展的主要因素。目前，金融行业面临着诸多问题，例如跨境支付周期长、费用高、结算环节效率低等，而区块链自身具备的数据可追溯、不可篡改、智能合约自动执行等技术特点，使其在金融领域方面有天然的结合能力，并在支付交易、资产管理、供应链金融等业务领域形成了较为丰富的区块链应用场景。

从国内数据安全治理市场来看，可以将其分为传统市场和新兴市场。传统市场以数据库审计、数据防泄漏、数据加密、数据脱敏等产品为代表，“以系统为中心”的传统安全思路保护静态数据。新兴市场由数据治理、隐私保护和相关政策法规驱动，旨在解决数据流动中使用与共享的问题。目前，数据安全治理关键技术（如数据发现、数据分类、隐私增强计算）仍处于发展早期。据 Gartner《2020 年数据安全技术成熟度曲线》预测，数据安全治理仍处于创新萌芽期，属于新兴技术，市场渗透率约为 1%至 5%，全球在数据安全治理方面的技术和产品还不太成熟。

（二）区块链解决数据治理问题的现有路径

当下，区块链技术在政务、电力、医疗、金融、交通、

征信、教育、医药、工业等数据场景都有广泛的应用。区块链可以在不同行业和领域的数据安全治理工作中重点发挥安全存储、安全共享、数据确权、数据存证、真实可靠、开放透明、生态构建等作用。

1. 安全存储路径

当下，数据安全存储需求日益迫切。利用区块链技术可以保证个人敏感信息在存储环节不被泄露、篡改、盗用。以医疗数据为例，针对患者在不同医疗机构就诊产生的医疗记录的隐私安全问题，利用区块链的特性和改进的加密算法，行业提出了一种基于区块链的医疗数据存储与共享模型。在该模型中，采用区块链技术维护和控制医疗数据访问策略，使用云服务对加密的医疗记录进行分布式存储，从而有效地实现医疗数据安全存储并保证其可用性。

2. 安全共享路径

区块链技术是实现数据安全共享的重要手段。随着大数据技术的不断提升，数据的服务对象、服务内容、服务过程等都更趋多样化、复杂化，安全问题也愈加突出。目前，数据湖是大数据应用最常用的数据共享形式。区块链技术可以弥补数据湖设计中的缺失，有效解决数据共享带来的隐私问题，特别对于一些数据保密性要求较高的行业。以电力数据为例，利用基于区块链的数据访问与控制模型优化区块链中的智能合约模块，即在区块链中存储数据的哈希值并使用可

信执行环境将加密后的原始数据存储在数据湖中，不仅实现了数据访问控制和安全共享，也确保了敏感数据的安全性和隐私性。

3. 数据确权路径

区块链可以提供可追溯路径，能有效破解数据确权难题。在数据流通领域中，数据透明度低、伪造篡改、非法倒卖等问题一直存在，利用区块链技术可以解决数据交易触及法律时的举证和追责难问题。以数据交易为例，使用区块链技术开发的数据交易溯源平台，可以把每一笔交易信息都放入区块链中存储起来，并为数据购买者提供一个交易凭证。这个交易凭证记录了该笔交易的数字证书以及该笔交易信息在区块链中的存储地址。用户需要进行数据确权时，可以进入溯源平台，输入交易凭证中的相关信息，查询到存储在区块链中的该笔交易信息，从而完成交易数据确权。

4. 数据存证路径

现行法律体系已经实现了对区块链技术可靠性及其产生的电子证据效力的一般性司法确认。2018 年 9 月，最高人民法院发布《关于互联网法院审理案件若干问题的规定》明确了当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认。2018 年 6 月，杭州互联网法院通过司法

判决对采用区块链技术存证的电子数据的法律效力予以确认，并明确了区块链电子存证的审查判断方法。通过区块链技术，可以对作品进行鉴权，利用电子数据存证证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。作品的电子数据在区块链上被确权后，后续交易都会进行实时记录，实现数字版权全生命周期管理，也可作为司法取证中的技术性保障。

5. 真实可靠路径

区块链技术可以解决许多行业面临的信息不对称困境，保证信息的真实性。以物流数据为例，区块链技术可以很好地解决“大物流”模式下的信任问题。在物流商品上链后，包装、运输、交接以及送达等每一环物流信息都被清晰地记录在区块链上，保障了物流数据的真实可靠，进而在流程优化、物流追踪、物流金融、物流征信等方向上发挥作用。

6. 开放透明路径

区块链可以解决社会普遍关注的数字服务和算法决策的开放透明性问题。以政务为例，目前数字政务推进工作仍面临数据孤岛、监管缺失、效率低下、成本高昂等问题。区块链的分布式技术可以让政府部门集中到一个链上，所有办事流程交付智能合约，办事人只要在一个部门通过身份认证，智能合约就可以自动处理并流转，顺序完成后续所有审批和签章。利用区块链技术不仅可以促进跨部门的数据交换

和共享，更可以大力推进政府数据的开放透明，实现政府治理透明化、城市管理精细化、公共服务多元化。

7. 生态构建路径

利用区块链技术能够实现特定行业数据生态系统的建设。以再保险数据为例，区块链技术解决了保险公司与再保险公司线下交互、分别录入的低效操作方式。运用区块链技术搭建的试验验证平台，可保证各场景、全流程地完成磋商签约、分保、账单交换、理赔处理等各交易环节，形成统一的多链交易生态系统。

CIC 工信安全

第三章 区块链与数据安全治理综合分析

一、数据安全问题的痛难点

在互联网经济时代，数据正朝着生产要素形态演进。早在 2017 年，习近平总书记就提出“数据是新的生产要素，是基础性资源和战略资源，也是重要生产力 ”。2020 年 4 月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，再次将数据列入重要生产要素。在全球数字化发展的大背景下，数据展现出了巨大的潜在价值，在深刻改变人们生活方式的同时，也成为了国家社会治理和企业生产的重要抓手。研究发现，当前数据在全生命周期的各个阶段都面临较多安全风险。同时，随着大数据行业的快速发展，数据安全问题越发凸显，呈现出以下三种趋势。

（一）数据安全事件的影响范围不断扩大

随着信息化、网络化高速发展，数据尤其是高价值的数据不断向大数据节点汇集，这给数据治理带来了严重的安全隐患。不断出现海量敏感数据泄露事件，影响范围从最初的企业和个人逐步向整个行业及全社会蔓延。2018 年 3 月，Facebook 超过 8700 万用户数据泄露，剑桥分析公司通过分析这些数据预测用户的政治倾向，在总统大选期间开展定向政治宣传，影响美国总统选举。2020 年 5 月 19 日，美国电

信巨头 Verizon 公司发布《2020 年数据泄露调查报告 DBIR》。报告显示在 81 个参与调研的国家中，58%的数据泄露事件涉及个人隐私泄露；72%的受害者为大型企业；企业内部攻击占 30%，外部攻击占 70%；55%的泄露事件和有组织犯罪有关。

（二）数据安全风险危害程度日趋严重

随着全球信息化和智能化程度的不断加深，大国战略博弈和科技与市场竞争态势的不断加剧，国家经济、金融、能源、交通运营所依赖的关键信息基础设施数量和重要性逐渐上升，数据安全的内涵不再单单是个人信息安全，针对国家数据基础设施的网络攻击呈现出“高发、高危、扩散、伴生、难防”的趋势。以获利为目的的数据泄漏事件占所有泄漏事件的 80%以上，2020 年勒索攻击和数据泄漏事件占所有数据安全事件的 15%，成为常态化的数据安全事件。2020 年 7 月，IBM 发布《2020 年数据泄露成本报告》指出，数据泄露事件给企业造成的平均总成本已达到 386 万美元。其中，虽然由国家资助的攻击造成的数据泄露事件在恶意事件中仅占 13%，但是由于这类攻击具有高度战术性、长期性和隐蔽性等特点，而且针对的都是高价值数据，通常会导致受害者受到更大的破坏，平均数据泄露成本增加至 443 万美元。

（三）数据安全治理难度持续升级

随着海量数据的快速积累，数据作为资产被频繁使用和

交易，使得数据在采集、传输、存储、处理、交换、销毁的整个生命周期的各个环节都面临着威胁和挑战。复杂数据的分级分类，多层级、多系统、多角色使用、提取，海量数据的流动和分布，敏感数据的外泄，数据外包加工中的泄露，加之大数据、人工智能技术催生出很多新型的高级网络攻击手段，都进一步增加了数据泄露的方式和途径以及不可预测性，使得数据安全治理难度持续升级。

二、区块链与数据安全治理的关联性

数据安全治理体系中的目标是建设以数据为核心的安全合规、安全保护、安全管理三方面能力。基于此，数据安全治理的实践过程一般可划分为三个阶段：第一阶段是帮助数据安全治理主体了解其已有数据资产的分布、访问和使用现状，然后结合业务需求、安全风险容忍度评估和预算计划等，设计和制定数据安全管理与流程规范；第二阶段是数据安全治理主体对数据客体在其全生命周期中实现全过程的安全管控，并定期对数据生命周期中的各种访问和操作行为进行审计与核查；第三阶段是当发生数据安全事件时，利用审计日志等历史记录对事件的原因、经过和责任人等进行追查和取证。

区块链的根本能力和核心优势在于为一个非信任的网络环境提供一个可以保证数据信息完整和不可篡改的基础

服务。因此，区块链与数据安全治理的关联性主要体现在两种场景下的应用：一种场景是在数据安全治理实践中的第二阶段，利用区块链技术对数据的流转轨迹进行可信可证的存证；第二种场景是在数据安全治理实践中的第三阶段，利用存储在区块链中的数据流转轨迹记录信息，对数据安全事件进行调查、分析和举证，客观准确地还原事件经过，公平公正地判定各相关实体的具体责任。

由此可见，区块链技术为数据安全治理提供了新的思路和方案。

（一）区块链用于保证数据一致性

当前，数据来源千差万别、错综复杂，在感知、采集、汇聚各类数据时，数据的一致性往往是数据安全治理需要面临的核心问题，一般需要通过复杂的数据安全治理工程来解决。区块链技术分布式强一致性的特点，则可以在数据采集、存储、使用和共享等各环节保证数据的一致性。

（二）区块链用于数据安全存储

数据存储安全是数据安全治理的基础。数据存储在中心化的数据库或机构的其他存储中，一旦被窃取和破坏，会造成巨大损失。区块链技术天然的去中心化的存储模式，可有效解决数据应用过程中，在中心化模式存储下面临的安全问题。首先，基于杂凑算法的块链式存储结构，利用杂凑算法的单向性和耐碰撞性保障数据的存储安全，有效防止数据被

恶意篡改。其次，由于区块链底层平台可支持多节点间的数据同步，利用多节点分布式存储方式防止单点故障，强化数据安全存储。最后，为了确保密钥等重要数据的安全性，区块链可通过与安全中间件，USBKey 强认证体系和密码机硬件平台相结合，对存储和传输中的重要信息进行加密保护。

（三）区块链促进数据流通共享

数据价值能够在流通和共享中得以飞跃式提升保值增值。目前在实际应用中，大量数据呈现分散、多样的特征，组织间形成“数据孤岛”。如何实现数据安全的流通共享也是数据安全治理需要解决的关键问题。

区块链技术在实现跨平台数据共享、数据鉴真方面具有优势。数据作为一种资产，可以通过杂凑算法处理生成唯一标识符，在区块链网络中流通。区块链上的交易记录是全网认可的、透明的、可追溯的，可以明确数据资产来源、所有权、使用权和流通路径，对数据的共享和流通具巨大价值。一方面，去中心化的系统结构剔除了传统数据流转过程中中介复制数据的风险，保障数据拥有者的合法权益。另一方面，区块链可支持对数据的分类分级管理，根据不同安全级别设置不同的安全策略和访问控制策略，通过智能合约实现自动验证，利用分布式共识机制实现对数据指纹的跨平台共享，既为跨主体数据鉴真提供有效依据，也保障了数据拥有者的数据隐私。

（四）区块链助力数据安全审计

数据安全审计是数据安全治理生命周期中的重要一环，可有效保障数据安全治理的策略和规范被执行和落实，确保快速发现潜在的风险和行为。但数据安全审计在涉及跨组织、大流量、人为干预的业务面前，也面临着很大挑战。

区块链技术在实现事后追溯方面有着天然的技术优势。区块链通过网络中多个参与节点共同完成数据或交易的验证、计算和记录，互相验证其信息的有效性，并通过共识机制实现数据同步，既可以进行信息防伪，又提供了可追溯路径。通常，区块链在基于杂凑算法的块链式结构基础上，采用 Merkle 树结构存储数据交易日志、权限变更、访问记录等信息，并加盖可信时间戳，这不仅为实现数据安全审计提供了不可篡改的数据支撑，还能有效破解数据确权、事后追溯等难题。

（五）区块链保障个人信息安全

在区块链技术中，各通信节点通过匿名方式通信，用户身份信息只是由一串数字表示，不记录真实身份信息，仅通过业务数据无法获知用户身份。而且，相关数据在存储时可通过密码学手段进一步进行加密，最大限度地保证数据安全。

用户在业务开展过程中会获得自己的个人密钥，每次启动应用后可使用加密技术对产生的数据加密存储。若无用户

授权则无法使用该数据，从而保证用户个人信息安全。

（六）区块链防止数据遭篡改

在区块链技术中，即便某个数据中心节点被攻击者控制甚至篡改部分数据，但通过区块链本身的共识机制，这些被篡改的数据也会被其他数据中心节点在验证哈希值时发现不匹配，从而起到防篡改的作用，保证数据的合法性与真实性。

三、区块链与数据安全治理结合的可行性

对国家而言，大数据是国家基础性战略资源，大量数据日益频繁地在全球范围跨境流动引发的安全风险对国家安全将造成巨大威胁，加强数据安全治理已经成为维护国家安全的战略需要。对企业而言，大数据是重要的商业资源和生产要素，数据安全治理能力已成为企业的重要竞争力之一。对个人而言，大数据收集处理技术和开放共享的要求，进一步弱化了用户对个人信息的自决权力，多源数据汇聚降低了用户隐私被恶意滥用的门槛。

区块链技术有着分布式网络、点对点传输、透明、可追溯、不可篡改、保证数据安全等特点，是数据安全治理的天然工具。具体体现在以下三个方面：

（一）可追溯的分布式数据系统提高数据质量

区块链在不同利益主体间构建一个点对点、分布式的数

据系统，各主体通过访问数据系统，将关键业务数据上链并确认交易，使得业务数据事件、信息能在大范围、短时间内实现快速的全网广播、匹配、核查和认定。任何治理活动的信息与数据只有通过全网广播获得其他主体的核实与认可后，才能被完整地写入区块链。如果数据不实或不被认可，系统将自动拒绝写入，这有助于提高数据质量。

（二）非对称加密技术与哈希算法保障数据安全

数据的保密性和完整性是数据安全的重要内容。区块链运用非对称加密技术、零知识证明算法以及哈希算法等技术可以实现数据安全和隐私保护。其中，非对称加密算法能验证数据来源，保护数据安全；哈希算法等匿名算法能保护数据隐私，防止泄露；时间戳能记录读取数据的时间，当任何一方发现不合理时，可以随时随地通过区块数据和时间戳来追溯历史数据。此外，区块链的数据存储在分布式的链式结构中，确保了数据的多重备份，提高数据库的容错性和安全性。这些技术加大了试图篡改、删除数据或者恶意攻击数据库等行为的难度和成本，从而保证链上数据的真实性、完整性、隐私性和安全性。

（三）对等网络技术与智能合约实现数据共享

作为一种“去中心化”的分布式账本系统，区块链中的每个参与主体都能单独地写入、读取和存储数据，并在全网迅速广播和及时查证。经全体成员确认核实后，数据作为某

一事件的唯一、真实的信息在区块链全网实现共享。区块链的智能合约技术打破各自为政的数据统计标准和方法，取代传统的数据协议，通过在智能合约中写入指定、统一的代码，实现对合约自动化执行，从而扩大数据共享的范围、响应速度和影响程度，提高数据共享的及时性和标准化程度。

CIC 工信安全

第四章 区块链在数据安全治理领域的应用方案

当前，基于区块链的数据安全治理方案主要包括数据防护方案、数据共享方案、数据存储方案等，主要涉及政务、电力、医疗、金融、汽车、个人征信、教育、中医药、数据交易、工业互联网、供应链、计量等多个领域。目前，在各个领域的数据安全治理过程中依然存在产业应用规模小、应用同质化、实现路径单一等问题。

一、电力大数据安全方案

在电力行业内，电网公司依托数据中心建设，对电力数据（包括营销数据、综合数据、ERP 数据、生产数据等）进行归集与整理，在内部单位之间实现数据共享。电力行业对于信息安全的要求高，数据仅允许在行业内部单位之间流通，不对外开放。虽然能够提高信息安全水平，然而这种壁垒也导致海量电力数据难以有效发挥其应有作用。

整个电网系统包含了许多子系统以及种类繁多的电气设备和电网交互系统，产生大量数据信息，这些数据信息来源广泛，而且信息储存的类型较为丰富，信息收集和传输的途径呈现出多样性特征。如何实现这些数据的安全共享以及利用数据进行合理的输配电决策，是能源电力领域需要解决的重点问题。

区块链技术具有数据不可篡改、隐私安全、全流程数据可溯源的特点，可以实现共享数据的确权、隐私保护、共享溯源等功能，可保证数据所有方源数据的安全性，防止数据滥用及数据泄露。基于区块链的电网数据可信共享技术有利于推动电网数据对外共享，打造输配电均衡的能源网络，打破行业内信息壁垒、遏制数据信息“孤岛”、促进数据资源利用率，推动电网企业向共享型企业转型，促使电网企业能更好地履行服务社会的责任。

二、政务大数据安全共享方案

近年来，随着政务数据不断扩大开放共享，其安全问题也越来越受到重视。一旦数据共享不当造成政务信息泄露，将使得各部门难于相互信任，业务协同困难，引起民众恐慌。区块链技术利用共同记录的共享账本，可以实时追踪和管理数据在多方之间的流动，保护数据在共享过程中的安全。

政务大数据的安全共享是跨部门和跨层级相对固定并且时常发生的交互过程，需要采用安全有效的技术措施，实现多部门多层级的数据安全共享。当政务数据在各部门共享时无法清楚地知道数据的来源，利用区块链技术的可追溯性可以在数据被共享时追溯数据的原始信息。另外，有些部门敏感数据在共享时存在泄露风险，应用区块链的加密技术可以有效防止数据在共享过程中出现泄露。

目前，基于区块链的政务大数据安全共享方案还处于研究过程中，需要研究确定数据采集系统、传输系统以及数据分析系统等系统的构成与建设方案，要求所有的建设系统都具备极高的完善度。

三、医疗数据安全存储方案

随着“互联网+”、5G、大数据等技术的高速发展，医疗行业掀起了挖掘数据价值的浪潮，同时也滋生出大量数据安全问题。而区块链技术具备去中心、不可篡改、可追溯等特性，能够保证医疗大数据的存储和共享过程的安全。

共享医疗健康大数据是提高医疗服务质量的重要保障。个人健康数据一般存放在医疗机构的信息系统中，各医疗机构间数据存储碎片化、共享困难，医疗数据的校验、保存和同步一直是一个难点。病人、医生以及研究人员在访问和共享医疗数据时存在严格的限制，需要在权限审查和数据校验上花费大量的资源和时间。因此，如何安全可信地共享医疗数据已成为该领域的挑战。

基于区块链打造的医疗信息共享平台，可提供对患者数字医疗信息的确权、存证、共享、溯源等数据治理服务，其不可篡改的特性可对医疗数据流转过程中的记录进行追踪，验证其真实性与完整性。

四、金融数据安全采集方案

由于金融行业业务价值突出，使其对于数据安全较为重视，率先发布多个数据安全领域的行业标准及相关规范，要求金融行业做好数据安全相关工作。金融行业在业务发展过程中会采集大量的数据，这些采集的数据中可能存在非法、违规获取的与金融业务没有直接关系的数据信息。应用区块链技术可以保证采集数据不能被篡改和可追溯。

目前，基于区块链的金融数据安全采集方案还处于完善过程中，将进一步在数据采集的监管方式和合规性等方面制定合理技术方案。

五、汽车数据共享方案

汽车数据共享方案基于汽车生态联盟链底层区块链平台，提供对于汽车生态数据的数据共享及业务协同服务。通过建设汽车生态区块链联盟开展开源联盟链研发，形成支撑联盟内相关机构业务发展的数据共享底层区块链技术平台。该平台支持业务数据流上链存储，企业数据共享，支持以OpenAPI 等技术实现链上交互，支持链上自动业务触发。在API 交互的基础上，可以调取生态内企业共享的数据，构建链上链下的汽车生态数据共享和协同体系，形成跨企业协同数据业务。

汽车数据共享方案提供底层联盟链之上的数据连接能

力开发和适配工具，降低应用研发门槛。通过提供数据上链和业务协同合约的在线编辑功能，实现汽车生态业务协同的工作流链上处理。在上述协同工具的基础上，建设联盟内汽车生态数据流和协同业务流的链上交换服务，实现基于区块链的汽车生态开源服务。

六、个人征信惩戒方案

区块链具有可溯源、不可篡改的技术特点，是失信人员数据公开透明的理想载体。将失信人员名单上链后，由于区块链信息保密且不存放明文信息的特性，即使数据被完整获得，也无需担心身份信息泄露问题。当失信人员前往某服务机构要求提供某项高消费时，服务机构通过区块链平台验明个体身份，并向失信人名单区块链进行密文查询。查到则通知服务机构限制服务；若查不到，则不影响个体消费。

利用区块链互信机制，多方可基于可信数字身份区块链，建立跨部门、跨区域的信用联动机制，在最大保障公民基本权利的基础上，构建联合惩戒体系，推动社会信用机制建设。

七、教育领域应用方案

当前，学习型社会和终身教育体系的构建对教育数据的产生、存储、使用、共享和数据安全治理提出新的挑战。区

块链技术具有去中心化、加密安全、自信任、准匿名、防篡改、可追溯等特性，利用区块链技术进行重要数据的存储、使用、共享和验证具有显著优势。

为学习者建立可信可追溯的终身学习档案。记录学习者在学习过程中取得的标志性学习成果，包括学历证书、学位证书、职业资格证书等。采用区块链技术将终身学习档案中关键信息上链，确保上链数据真实且不可篡改。终身学习档案支持关键学习信息的存储、查询及验证等，可为学习者、教育机构、用人单位等提供重要信息的可靠查询与认证服务。

为各类教育机构提供学分互认业务。支持学习者在不同教育机构获得的各类学习经历和成果的连续记录，有效认证和等值转换，支持学分互认和转换。利用区块链技术记录可信的教育记录，为信息查询与共享、数据分布式存储、学习过程记录、学习成果认证等问题提供解决方案，显著提升学分互认的效率。

互联网教育资源的数字知识产权保护和溯源。采用区块链技术上链存储数字教育资源的关键信息如资源提供者、资源信息、发布时间等，利用智能合约实现资源或知识成果的交易和使用，能够有效解决知识产权的保护及溯源，促进优质教育资源的共享和利用。

目前，基于区块链的教育领域应用方案还处于研究阶

段。需要明确数据存储方式，区块链数据和已有数据库的关系，解决大数据量的扩展和性能、参与主体的监管、数据隐私保护等问题。

八、中医药领域应用方案

重要药材产业链条较长，涉及环节较多、地点多、主体多，产业高质量发展对上下游之间、各生产主体之间的联动、全过程溯源和信息共享等方面提出了较高的要求。针对行业发展对中药材“安全、有序、优质、优效”等方面要求的提升，区块链技术可以解决中药领域信息不对称的问题、营造良好的市场环境和社会秩序，打通药材生产、流通、营销和消费等各个环节，维护地药材良好声誉，形成产业良性生态和保护机制。

利用区块链建设基于中医诊疗特点的电子病历动态管理平台，向医疗机构、医生、患者提供关键信息查询，数据共享等服务。区块链技术不仅可以保证数据的安全性和透明性，支持中医诊疗信息的长期稳定存储和跨区域追溯，而且其高可靠性可以保护数据的多样性，实现中医电子病历中独特的数据记录。

九、大数据交易应用方案

数据价值在企业升级转型中的作用愈加凸显，企业对于

专业数据的需求越来越强烈。然而，数据流通市场中，数据提供方卖出的数据，面临被无限次盗卖、市场价值不断损减的风险，严重制约了数据市场的规模与发展。因此，需要通过区块链解决数据产品合法化、规范化、可预期的问题。

基于区块链技术能够进行数据资产确权，通过建立基于区块链的数据交易所，记录交易数据，共同验证交易，实现数据资产的可信交易。针对大数据交易面临的数据归属、交易安全、二次售卖等问题，构建基于区块链的可追责数据共享平台，构建分布式安全可信的数据共享环境。

此外，通过共识建立可信任的数据资产交易环境，消除数据被任意复制的隐患，保障数据拥有者的合法权益。首先，构建公共区：由第三方及交易中心建设运营，通过搭建基础通讯架构，实现成员之间的连接和通讯隐藏，成员认证和接入管理，维护公共记录块链，实现对数据的索引记录、交易记录，制定数据规范和交易规则，维持交易秩序，协助交易方完成数据的追溯维权。其次，构建成员区：即参与方数据区，主要保存公共区记录块链的备份，监督公共区的区块链记录的正确性，维护自己可共享的隐私数据，提供对外的查询服务，发起查询，获取外部数据。最后，搭建节点设备：连接公共区和成员区，实现从公共区域中备份记录块链，完成自有数据的块链生成和提交，接收来自公共区域的消息，实现安全通讯。

十、工业互联网数据审计方案

在传统的信息化模式下，对于已经形成的数字化文件信息在各个节点的传递，缺乏完备的数据安全保护措施，会出现数据文件的失窃和篡改的风险。利用区块链多方参与的特性，在区块链网络中接入监管节点，可以在不影响原有生产及操作流程的基础上，快速同步区块链存储数据，支撑监管部门对工业互联网数据进行柔性监管与合规审计，如数据录入的准确性、及时性等进行可信审计，采用基于区块链的全流程审计，通过多方监控确保数据真实性，应用密码学算法进行隐私审计，可全方位保证数据的使用安全，确保数据不泄露。

十一、供应链数据共享方案

现存供应链平台网络中信息孤岛现象普遍存在，难以保证上下游企业间信息沟通的及时性和准确性。仓储、物流、交易、资金等信息分别存放在核心企业、物流公司、交易双方以及银行系统中，存在信息不对称、不透明等问题，供应链金融业务的各个环节形成闭环，信息难以流通共享。

区块链技术的共识信任、信息可追溯、智能合约等特点，能够有效解决信息流共享难题。构建基于区块链的供应链信息共享平台，接入银行、核心企业、物流公司等各参与机构，保证数据公开透明，实现物流、资金流、信息流、商务交易

流“四流”合一。利用区块链技术，能确保互认流转、数据可信，降低履约风险，提高操作效率，降低业务成本，形成互信共赢的物流服务供应链网络。

目前区块链技术还未完全成熟，区块链供应链平台仅能够保证链上数据的真实有效，但信息上链之前还需进行真实性的确认。为实现上链前数据的真实性，需要利用物联网、人工智能、机器学习等新兴技术实现可信数据上链。

十二、计量领域应用方案

传统检定数据及检定证书的存储采用硬拷贝方式。这种方式存在纸质数据易丢失或损坏、中间物流环节耗时长、搬运易造成仪表二次损伤等风险。

现在，计量领域利用物联网技术，实现数据远程检定过程有效监管监控。计量单位对仪表厂的检定装置可以远传管理、授权，对检定过程全程监视，实现出厂检验与首次强检二检合一，有效减少中间物流环节。结合区块链的分布式存储及加密技术，将检定数据上链，通过区块链的加密算法的不可篡改、高可信性，实现检定数据追溯、检定证书存证及查找举证、信息公开公正等功能。

第五章 发展建议与展望

一、遵循由易到难、稳步推进的建设思路

数据安全治理的本质是通过具体的机制和持续的工作，实现对数据可用性、完整性和保密性的整体管理，使数据价值实现最大化。因此，利用区块链技术进行数据安全治理是一项持之以恒的工作，不可能一蹴而就，需要一个循序渐进的过程，需要遵循由易到难、稳步推进的建设思路。

数据安全治理建设初期应以搭建基础框架和小范围试点为落脚点，通过对整体方案和规划进行反复论证，确保其可实施性与可延续性，夯实数据可信存储与共享的基础，在可控范围内验证对数据安全和数据隐私的保护效果；中期应着重维护整体架构，建立健全机制，积极寻找和征求区块链节点运行过程中存在的问题和意见建议，对系统进行持续的优化更新和快速迭代，逐步稳定整体架构，建立健全运作流程与管理机制，确保系统尽可能地满足数据安全治理的需求；后期应实现从数据共享到能力共享的转变，通过全面推进数据安全治理机制，形成业务闭环，为实现穿透式监管奠定基础。同时，应鼓励企业通过统计与分析，深度挖掘数据价值，优化服务流程，提高服务质量。

二、建立健全区块链政策与法律体系，加强数据安全治理能力建设

首先，建立健全区块链与数据安全治理技术研发与应用相关的政策与法律体系，明确区块链与数据安全治理的技术范围与可接受程度。其次，培养区块链与数据安全治理专业人才，把握好技术与人的关系，既要大力发展技术，更要匹配高水准的技术人才。最后，区块链技术应用范围很广，存在与许多行业结合的可能性，应注重强化区块链基础理论研究，提升原始创新能力，努力走在区块链领域的前沿。

此外，应加强人员关于区块链与数据安全意识培训。通过对组织、制度和流程的培训，提高政府和企业对于区块链与数据安全治理的认识水平；加强区块链与数据安全相关法规、标准在政府部门以及企业的落实，可结合实际情况将数据安全治理情况纳入年度考核指标；鼓励在可操作范围内对大型互联网平台数据安全治理相关活动进行安全众测，开展第三方安全监管和审计，督促安全整改。

三、着眼行业应用，打造“区块链+数据安全治理+全场景应用”生态

当下，区块链凭借安全、透明、共享的技术优势深刻影响着社会的各个领域，在金融、政务、司法、供应链领域均有项目落地。作为将区块链应用于数据安全治理领域的机构

或企业，应在明确业务需求，紧密联系业务属性的基础上，建立符合自身业务特点和数据特点的数据安全治理体系，做到在数据安全治理过程中有的放矢、张弛有度。当企业发现新型数据保护及运营的更新需求，或对部分商业活动的习惯性做法有所创新时，应鼓励相关机构及时提供行业意见，不断提升区块链技术对于数据运营的更新服务能力。

当下，以数据为核心的产业创新系统需要更加重视数据的共享和开放，进而提升系统效率，激发创新的活力。与此同时，产业侧更需要重视数据安全治理流程、标准和规范的制定，及时和有效地应用包括区块链在内的新兴技术。区块链企业在为数据运营提供服务的同时，业应注重提升权益意识，密切结合知识产权保护路径，鼓励技术和产品的不断迭代更新，促进区块链的自有价值体系逐步完善，在与服务对象良性互动的同时保障自身权益价值。

四、构建多主体共同监管模式，建立系统的预防监控机制

随着区块链技术的发展，数据生成、采集、共享、使用、流传的主体由人与人、人与机器之间，向机器与机器之间转变，给数据安全治理带来了新的挑战。同时，数据隐私保护已不仅是技术问题，还和个人及社会息息相关，需要各方协作完成，共同承担数字化社会下数据安全的治理和监管的责任。

因此，建立政府、企业、社会组织、公众共同参与的，利用区块链技术搭建的分布式数据系统将成为可行的解决方案。各方需要共同维护系统的准确性和有效性，不仅对自己录入的数据负责，同时通过验证和审核其他链上节点上传的数据，对他人负责，共同承担对区块链的监管责任。此外，政府需要加快建立针对区块链的长效管理机制，适时出台区块链技术应用与政府数据安全治理的长期规划，明确监管主体、监管责任和监管工作规则，建立行之有效的奖惩机制，形成全面且系统的数据安全风险预防机制。