研究与开发

基于区块链的工业数据资产可信确权与价值流转方案及其轻量化研究

王东初[1,2]，伏玉笋[2,3,4]，于亚[1,2]

（1. 上海交通大学宁波人工智能研究院，浙江 宁波 315012；
2. 上海交通大学自动化与感知学院，上海 200240；
3. 系统控制与信息处理教育部重点实验室，上海 200240；
4. 上海市工业网络系统感知与控制重点实验室，上海 200240）

摘　要：工业互联网的发展极大地提升了工业企业的数字化和智能化水平，工业数据资产已经成为一种越来越重要的战略资源和新型生产要素，如何保证工业数据从创建、授权、共享到收益分配的全生命周期安全可信是当前需要解决的首要问题。为此，基于工业数据资产价值流转系统的设计目标，提出基于区块链的工业数据资产可信确权和价值流转框架，构建适用性和可扩展性较强的一般性框架和具体方案，给出了在数据多方参与、多次共享的工业场景下具体保障工业数据资产在确权、访问、收益全流程可信可控的解决方案和流程。为解决安全和效率的矛盾问题，提出了一种轻量级可信区块链模型。基于节点的行为和状态度量节点的可信度，给出节点的动态初始值计算式和整体信任值度量模型信任管理，并基于节点的可信度优化区块链系统共识协议算法，在降低节点恶意攻击概率的同时提高了系统交易共识效率，实现整体系统的安全和轻量级并行。最后通过仿真实验验证了新方案的优越性。

关键词：工业数据共享；区块链；资产确权；价值分配

中图分类号：TP309.2

文献标志码：A

doi: 10.11959/j.issn.1000−0801.2025102

Research on the blockchain-based trusted ownership confirmation and value transfer system and its light weight of industrial data assets

WANG Dongchu[1,2], FU Yusun[2,3,4], YU Ya[1,2]

1. Ningbo Artificial Intelligence Institute of Shanghai Jiao Tong University, Ningbo 315012, China
2. School of Automation and Intelligent Sensing, Shanghai Jiao Tong University, Shanghai 200240, China
3. Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China

收稿日期：2024−11−29；**修回日期：**2025−01−15

通信作者：伏玉笋，fu_yusun@sina.com

基金项目：国家重点研发计划项目（No.2019YFB1705703）；宁波市重点研发计划项目（No.2024Z111）

Foundation Items: The National Key Research and Development Program of China (No.2019YFB1705703), The Key Research and Development Program of Ningbo (No.2024Z111)

4. Shanghai Key Laboratory of Perception and Control in Industrial Network Systems, Shanghai 200240, China

Abstract: The development of industrial Internet has greatly improved the digital and intelligent level of industrial enterprises. Industrial data assets have become an increasingly important strategic resource and new production factor. How to ensure the security and credibility of industrial data in the whole life cycle from creation, authorization, sharing and income distribution is the primary problem to be solved at present. To this end, based on the design goal of the industrial data asset value transfer system, a blockchain-based framework for trusted ownership confirmation and value transfer of data assets was proposed, a general framework and specific solution with strong applicability and scalability were constructed, and specific solutions and processes were provided to ensure the trustworthiness and controllability of industrial data assets throughout the entire process of ownership confirmation, access, and revenue sharing in an industrial scenario where data was involved from multiple parties and shared multiple times. To solve the contradiction between security and efficiency, a lightweight trusted blockchain model was proposed, which measured the trustworthiness of nodes based on their behavior and status, and provided a dynamic initial value calculation method for nodes and an overall trust value measurement model for trust management. The consensus protocol algorithm of the blockchain system was optimized based on the trustworthiness of nodes, reducing the probability of malicious attacks on nodes while improving the efficiency of system transaction consensus, achieving security and lightweight parallelism of the entire system. Finally, the superiority of this scheme was verified through simulation experiments.

Key words: industrial data sharing, blockchain, asset confirmation, value distribution

0 引言

工业互联网通过全面互联的人、机、物，连接全要素、全产业链和全价值链，成为新兴应用模式、关键基础设施和全新工业生态[1-2]。工业互联网以数字化、网络化和智能化为主要特征，实现了智能化制造、网络化协同、个性化定制、服务化延伸等新模式。基于工业数据基础产生的机理模型、工业应用（application，APP）和工业微服务等已经成为提升制造业生产力、竞争力、创新力的关键要素，有效地促进了制造业在更大范围、更深层次的资源配置中变得更高效和精准[3-4]。

目前数据共享流通多为集中式的双边信息传输模式，主要有两种。一种是通过数据交易平台进行共享流通，各方通过数据包传递达成交易，在政务、消费、金融、证券等行业已取得一定成效。但对具有复杂来源的工业数据而言，难以保护数据所有者利益，易导致涉及企业核心竞争力的信息暴露以及数据被使用方二次利用甚至滥用，适用性不强。另一种是基于明文数据应用程序接口（application program interface，API）进行流通，将加工处理完的单方数据结果以API形式输出，一定程度上保护了用户隐私信息以及降低二次利用可能性，但同时也降低了数据价值融合的可行性，难以释放数据协同共享的应用价值[5-10]。

工业数据共享流通正处于起步阶段，还面临许多挑战和问题：（1）工业数据涉及主体众多，数据主权边界难以界定，同时在数据交易过程中产生的数据权属变更有效性难以保证；（2）工业数据涉及企业生产制造的机密信息，需要在共享过程保证数据机密性和隐私性，同时其整个流程处理记录需要透明可视、可监管；（3）数据来源质量难以追溯，仅依靠第三方保证，缺乏有效技术手段保障真实性；（4）工业数据的存储安全性、授权访问细粒度不足，难以兼顾工业场景的使用需求等。具体问题说明如下。

（1）缺乏完善的工业数据资产价值可信流转框架[11-13]

工业互联网模式下的企业参与主体多，数

据资产范围广且异构化强，价值收益严重依赖可信第三方，流通效率低下，难以有效保护数据提供方和数据使用方的业务安全需求，缺乏一种完善且可持续的工业数据资产价值可信流转框架。

（2）数据资产权属不明确，缺乏认证机制[14-15]

传统的工业数据仅在企业内部流通，不涉及企业间互联互通，无须进行数据身份认证，同时数据资产的全生命周期的权属和价值收益缺乏较为明确的认证机制。

（3）数据资产安全性不足，缺乏数据保护机制[16-17]

工业互联网中引入大量异构化设备来进行企业内部和外部的互联互通，设备本身的硬件限制和软件漏洞导致其产生的数据存在真实性和安全性隐患，面临数据泄露和篡改等形式的恶意威胁，同时数据流通过程中不同节点出于自身的经济收益考虑也有做出危害系统行为的可能。

（4）数据资产机密性、透明度和完整性不足[18-21]

工业数据一般普遍采用明文传输，数据在传输过程中缺乏避免数据泄露和被篡改的方案，同时企业内部采用的企业资源计划（enterprise resource planning，ERP）系统难以覆盖数据应用的全生命周期，部分数据对使用者的透明性不足，难以在出现问题时进行有效定位。同时，对数据生成、传输和访问的一致性和正确性缺乏高效的验证手段。

（5）数据流通的安全和效率难以兼顾[22-23]

工业生产现场的数据生成具有高通量和时序性强的特点，将一般的加解密算法直接应用难以满足工业系统高可用的性能需求，需要在数据资产应用过程中保证系统安全和效率的平衡。

因此学术界和工业界亟须寻找一种适合工业场景的新型数据流通解决方案，在数据价值释放及数据安全需求中取得平衡。针对上述问题，本文提出基于区块链的工业数据资产可信确权和价值流转框架，构建适用性和可扩展性较强的一般性数据流通总体框架和具体方案，在数据多方参与、多次流通的工业场景下给出具体保障工业数据资产在确权、访问、收益全流程可信可控的解决方案和流程；针对该方案的轻量级化，把信任管理与区块链相结合，提出一种轻量级可信区块链模型，基于节点的行为和状态度量节点的可信度并给出节点的初始动态值计算式和整体信任值度量模型信任管理，并基于节点的可信度优化区块链系统共识Raft协议算法，在降低节点恶意攻击概率的同时提高了系统交易共识的效率，实现整体系统的安全和轻量级兼具；最后搭建仿真系统对所提方案进行了实现，验证了本文方案的有效性。

1　工业数据资产可信确权与价值流转方案设计目标

针对前面所述工业数据资产流通过程中存在的安全隐患，本文首先给出基于区块链进行数据资产可信确权和价值流转的一般性解决框架设计理念，并在此基础上聚焦在具有“多方参与、多次交易”特点的工业数据应用场景中实现数据可信流通和价值合理分配的方案设计目标。工业数据资产可信确权与价值流转应用场景示例如图1所示，如何保证数据提供方的同一数据资产需要同时流通给具有不同访问权限的多个数据使用方、同一数据资产（数据）经过多个数据使用方计算、加工生成新的数据资产（模型、微服务）并流通给更多的数据使用方使用过程中的数据资产全生命周期的安全、效率和数据收益可信流转。工业数据资产可信确权与价值流转总体框架如图2所示，需要说明的是，第2.1节在图2的介绍中，结合数据资产流通方向的总体框架，将进一步阐释图1的场景示例，因此在此不再展开细节说明图1中的企业A、B、C、D、E在数据资产可信确权与价值流转中的角色。

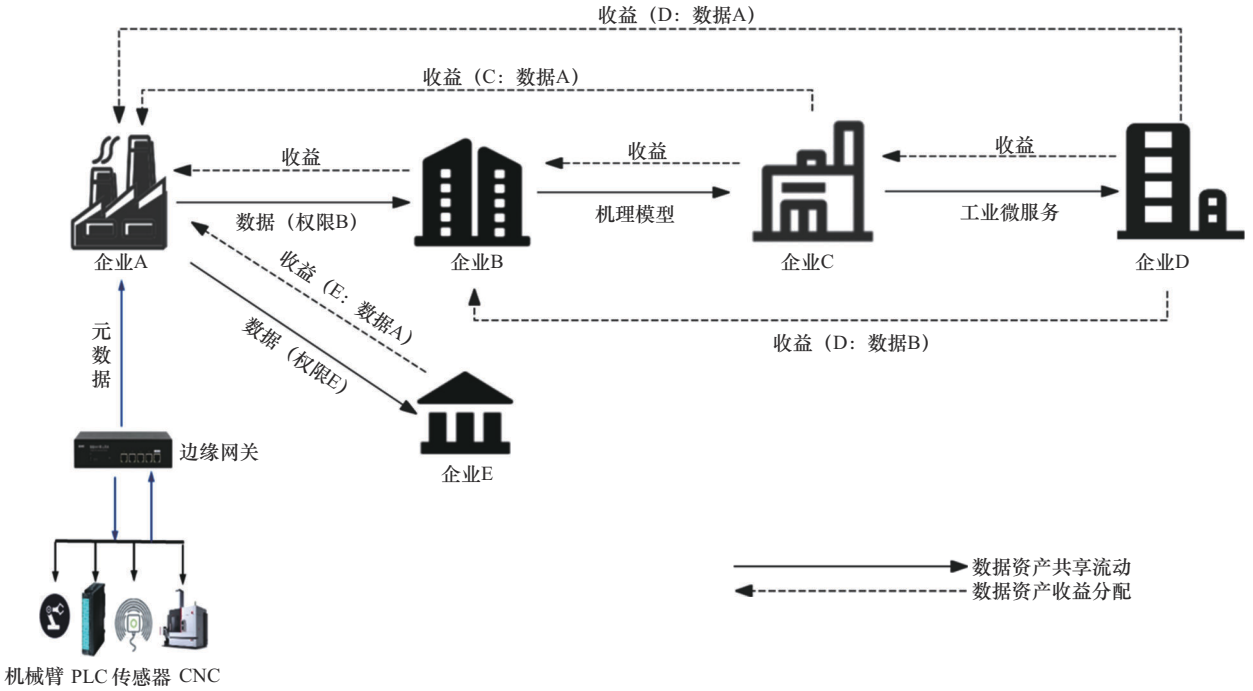

图1　工业数据资产可信确权与价值流转应用场景示例

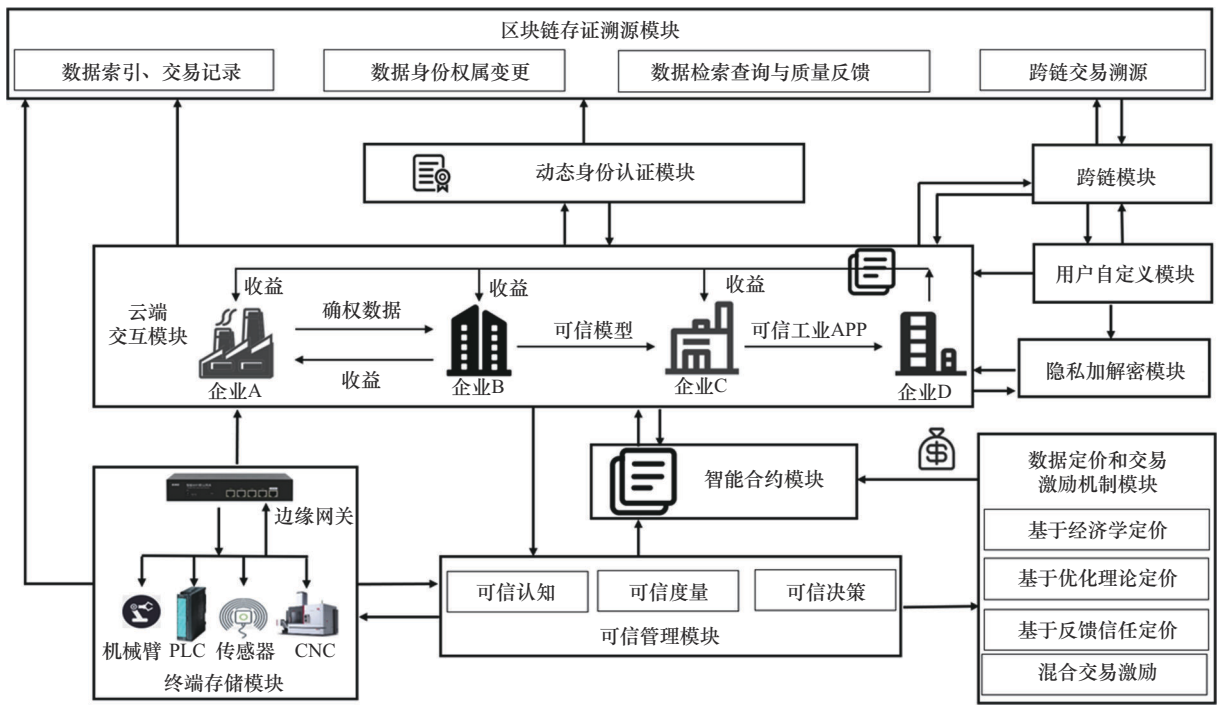

图2　工业数据资产可信确权与价值流转总体框架

本文构建的数据资产流通方案，在满足数据提供方对数据权属的可控和隐私需求、数据资产的价值收益合理分配问题时，也需要满足工业场景下数据交易的效率和安全要求。本文提出的数据资产可信确权与价值流转的一般性框架和解决方案应满足以下设计目标。

（1）权属确定性

数据拥有方和数据使用方对于同一数据资产

具有不同的使用权限，在数据资产使用的多个环节中，需要保障数据拥有方对其提供的数据资产主权不变且被其他参与方承认，同时当数据资产在交易过程中发生变更，那么新的数据资产主权同样需要满足上述需求，且变更记录可审计。

（2）可控可用性

数据资产在共享流转的全生命周期中，数据拥有方能够规定不同需求的数据使用方按照预定的规则访问使用数据资产，实现对数据流通的可控；而符合条件的授权用户可以随时访问和使用数据资产。

（3）抗攻击安全性

参与数据资产流通的用户可能会根据自身的利益需求做出危害当前数据交易的行为，如未授权访问、伪造签名和双重花费攻击等，该类恶意攻击产生的不良影响较大，需要提高系统的抗攻击能力，满足数据交易安全。

（4）价值分配有效性

用户参与数据资产流通的目的是获取数据资产的潜在经济价值，数据价值的合理和可信分配是数据资产流通能否顺利进行的关键。在单次数据资产流通和多次数据资产流通中都需要保证数据提供方能够有效地从数据使用方获取数据资产的价值。

（5）高效性

工业现场级数据具有高通量和时序性较强的特点，进行数据资产交易时系统需要满足低时延和高吞吐量要求。低时延是指较小的数据共享交易延迟，高吞吐量是指系统在有限的时间内完成大量数据资产交易验证，并将交易流程存证固化。

（6）可溯源性

数据资产流通过程中所涉及的重要流程记录、操作属性、价值分配记录等信息都应该上链存证，在出现问题和争端时能够对相关文件进行溯源，查找问题出现的环节。

（7）隐私性

数据拥有方能够对部分敏感数据进行脱敏，同时数据资产流通过程中的部分记录能够对交易以外的参与者不可见，保护流通交易的信息隐私。

2　基于区块链的工业数据资产可信确权与价值流转方案设计

本节从总体框架、具体方案这两个方面分别予以说明。

2.1　基于区块链的工业数据资产可信确权与价值流转总体框架

本文需要构建的工业数据资产可信确权与价值流转方案是一个针对不同行业领域的通用性高、应用性强的框架，实际参与工业数据资产流通的相关方具体如下：工业数据资产的提供方，拥有大量实际生产数据和工业设备的企业方；具有需要了解企业真实运营情况而进行金融业务的银行机构都是工业数据使用方和对企业实际数据有可见可用需求的工业微服务厂商、云服务商、研究机构都是工业数据使用方；同时部分数据资产提供方或者使用方基于企业提供的数据设计并实现工业机理模型或者微服务等模型数据资产，成为新的数据资产拥有方并进行流通；数据流通平台也需要接受相关权威机构的监管和审计。

根据以上各方参与数据资产流通的需求和业务特点，本文提出了一种基于区块链的工业数据资产可信确权与价值流转的一般性框架，说明数据价值安全流通的整体逻辑，并阐述框架中所涉及主要模块的功能作用，其总体框架如图 2 所示。

从数据资产的数据流通方向和资产价值收益模式角度出发说明本文框架的设计原理。从数据流通角度来看，企业 A 的生产元数据从终端设备生成、存储，经过边缘网关上传至企业云端，企业 A

通过动态身份认证模块完成用户身份及其所属数据资产的权属认定，并将对应的数据索引、交易等记录上链存证。完成身份认证后的企业B申请使用企业A的生产数据，通过访问控制和密钥分发等技术手段保证符合授权规则的企业B能够获取企业A的原始数据，并将数据资产的身份权属变更结果存储在区块链溯源模块。企业B在企业A数据的基础上通过机器学习或深度学习等方式训练生成工业机理模型并将模型的权属确权认证存证在链上，在企业C调用模型时提供对应的接口供其可信工业APP等应用调用相关功能，数据从企业A的终端生成并在企业B、C、D之间流通。

从资产价值收益角度来看，企业A根据自身的经济需求发布其所属的数据资产的内容和价格信息，并设置授权访问和使用的规则，将其以智能合约的形式部署到区块链系统中实现自动触发执行。企业B申请访问数据资产并使用其生成工业模型，触发企业A设置的智能合约后，若满足访问使用规则并支付对应的资产价格则获取此数据。在企业C或企业D申请调用企业B产生的工业模型时，若该模型的训练数据来源于企业A，且数据流通时的合约规则保留了企业A的后续收益权属，则企业C或企业D应支付对应的数据价值。数据价值和收益从工业最终服务方逐级向前流动到数据提供方。

本文框架中所涉及的模块围绕如何保证数据资产流动过程中的权属可确认、授权细粒度、价值合理收益、交易安全且高效这些目标构建。（1）终端存储模块存储数据提供方企业的终端生产数据；（2）云端交互模块为用户可视化前端数据交易平台，是用户的直接操作和处理层级，能够实现数据资产的登记、发布、授权设置和价值收益，为整个系统的用户功能交互模块；（3）区块链存证溯源模块主要通过构建联盟链完成数据交易过程的重要流程记录存证，实现交易记录的可溯源、难以篡改，保证数据交易安全；（4）智能合约模块完成资产的登记、发布、安全验证和价值收益等需要自动判定并执行的交易功能，是整个框架自动高效执行的关键；（5）可信管理模块保证整个数据交易过程中的主动安全，即需要发现用户层面基于利益对数据流通产生的恶意攻击行为并降低对数据交易的不良影响；（6）数据定价和交易激励机制模块通过经济学、优化理论或反馈信任等机制设置合理的数据资产价格并对优质和劣质的数据资产建立不同的奖惩机制来提高用户主动参与数据流通并提供优质数据资产的意愿，降低用户作恶概率，提高系统的安全性和用户的数据使用体验；（7）隐私加解密模块通过与密码学相关机制满足部分用户进行交易信息的隐私化处理；（8）跨链模块为处于不同区块链系统的用户进行数据交易提供跨链服务，完成跨链资产交易；（9）用户自定义模块则为用户的个性定制化需求提供一定的改造使用空间。

与现有的数据流通框架相比[3,10]，本文框架给出一般的具有较强通用性和适用性的数据资产流通交易机制，并具有较好的可扩展性和安全性。

2.2 基于区块链的工业数据资产可信确权与价值流转具体方案

结合图1和图2，建立基于区块链的工业数据资产可信确权与价值流转的具体方案架构如图3所示。

本文提出的方案中有4类参与实体：数据拥有方、数据使用方、模型拥有方、模型使用方。

（1）数据拥有方（data owner，DO）：数据拥有方是工业数据资产共享体系中的元数据提供者，在进行身份注册认证后由系统分发身份密钥对，并对后续发布的数据资产进行权属身份签名和加密，同时DO对数据资产的授权使用和价值收益设置合约策略，实现对数据资产的可控授权和可信收益。

（2）数据使用方（data user，DU）：数据使用方首先也需要进行身份认证并获取密钥对。DU根据自身需求申请获取数据资产时需要发送

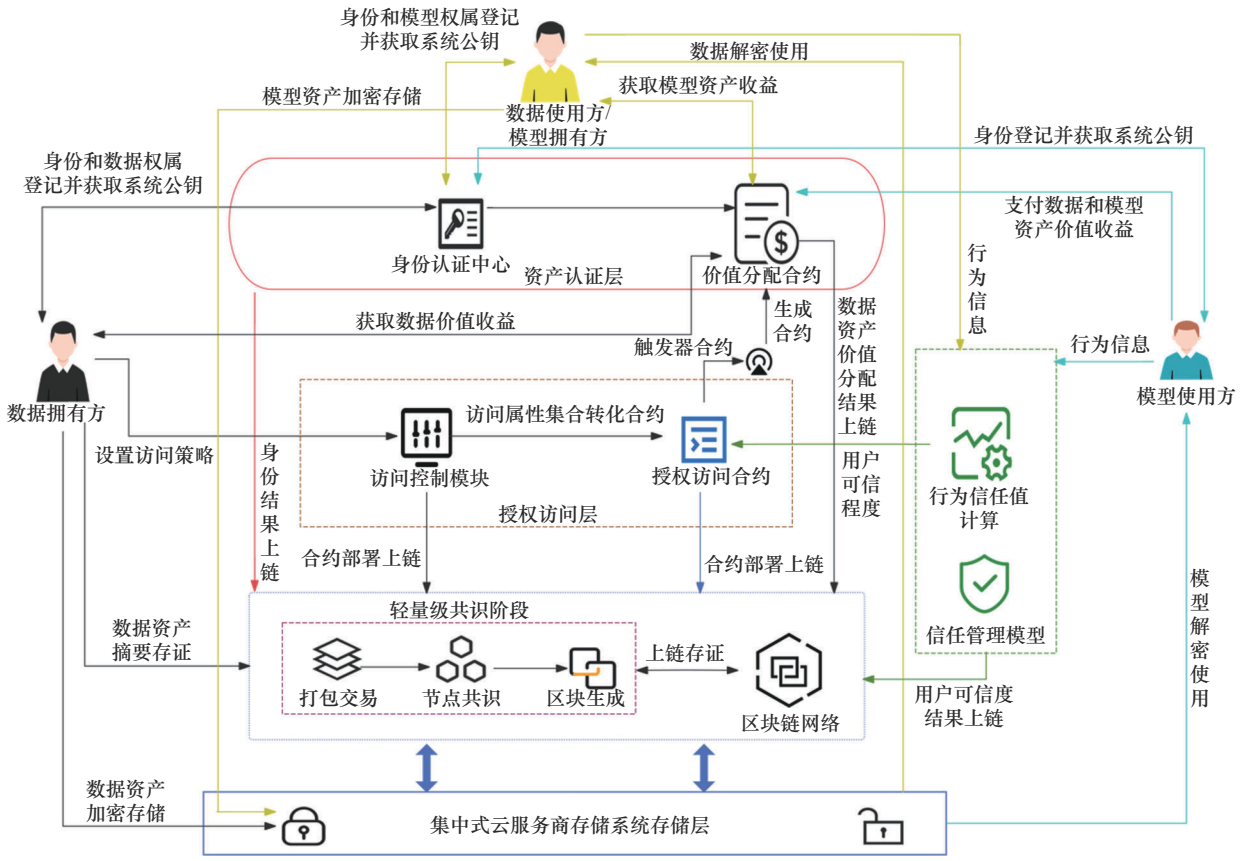

图3　工业数据资产可信确权和价值流转的具体方案架构

自身的属性集合，由访问控制合约验证是否符合访问策略同时需要支付对应的数据价格，取得原始数据后可进行进一步的分析和使用操作。

（3）模型拥有方（model owner，MO）：模型拥有方可根据模型的产生途径分为两种，一种是基于系统中其他DO共享的数据产生的，此时的MO也是对应数据的DU，此时MO已经完成身份认证，只需设置模型的授权策略和价值收益合约；另一种MO基于本身数据产生的模型，两者的主要区别在于模型收益的价值分配方式。

（4）模型使用方（model user，MU）：模型使用方完成身份认证后，发送自身的属性集合获取模型资产，同时根据价值分配合约支付对应的数据和模型资产的价格。

下面从系统层级简要介绍方案各个模块的设计思想和主要作用。

（1）用户层包含以上4种参与实体，主要提供给拥有数据资产和使用参与方实现数据需求的平台，其对数据资产的访问和收益处理过程已在上文进行了简要介绍。

（2）资产认证层包含了用户身份认证和在此基础上数据资产的权属确认，通过将数据资产的不同权属进行分离确权，保证同一数据资产在不同用户、不同使用阶段的可信认证，并在此基础上设置智能合约引擎，实现不同权属的数据价值合理可信的自动化收益执行。

（3）信任管理模型基于系统内生安全需求进行构建，主要用来降低数据资产流通过程中的参与方出于自身利益做出危害数据交易公平公正行为的恶意影响，通过信任度量模型实时检测参与方的行为信息并按照一定的计算规则给出节点的信任度量结果，能够极大提高系统的抗恶意攻击安全性。

（4）授权访问层包含用户申请访问和密钥授权分发过程，基于属性基加密算法设置数据资产的授权访问属性，并设定策略生成智能合约以确保特定用户能够访问使用所需的数据资产，同时需要防止恶意用户访问，保护数据资产完整性和机密性。

（5）区块链网络层主要用于数据交易共识和各种关键流程信息的上链固化，将打包好的交易信息和区块及时进行全网参与方的同步存证，提供数据资产流通的全流程难以篡改和可追溯性，并保证系统的安全性和可用性。

（6）存储层主要为云服务商或共享平台提供存储体系。在本文提出的方案架构中，采用集中式云服务器作为数据资产存储和流通的主要载体，通过可信任的管理节点和全体参与方共同维护一个联盟链网络实现分布式的数据管理，并构建信任管理模型来实时度量参与方的行为状态，同时设计权属可变的身份管理机制，实现数据资产的身份确认，并搭建基于智能合约的授权访问和价值流转收益机制实现数据的可控使用和价值收益。

3　基于信任管理的轻量级区块链设计与实现

需要说明的是，本文提出的基于区块链的工业数据资产可信确权与价值流转方案，其所涉及的关键技术甚多（如基于权属分离的资产可信确权与收益模型设计、属性基加密[24]等），对此不逐一探讨介绍，本文仅聚焦基于信任管理与区块链结合的轻量级实现。

前面介绍了通用的工业数据资产可信确权与价值流转模型和框架以及在本文研究的应用场景下数据资产可信确权和价值流转的具体方案。尽管该方案能够实现可管理、可控、可视和可追踪的去中心化多方数据资产可信交易，但通过区块链技术进行数据资产流通仍存在以下一些挑战。

（1）节点可靠性：由于数据资产交易的一大驱动因素是数据资产的经济价值收益，部分节点出于自身利益因素会产生对自身有利但损害数据资产交易公平的恶意行为，降低系统的交易效率并损害其他参与方的合法权益。

（2）效率与安全之间的权衡：部分工业现场级数据的采集和处理对系统的效率和时效性要求较高，同时工业系统具有高可靠和高可用的需求，现有的区块链系统难以同时满足效率和安全性的标准。

为了解决上述挑战，本文将信任管理方案与区块链系统结合以提高系统的安全性和效率[25-28]。首先，提出基于信任管理模型的轻量级区块链模型的一般架构，并给出系统运行的一般流程。然后，对其中使用的信任管理模型进行了全面描述，以提高整个方案的通用性和安全性。在信任管理模型中设置了节点的动态初始信任值，通过基于参与节点的初始属性信息分配不同初始信任级别，降低了节点在整个信任度量过程中的计算成本并完成系统初始化。最后，基于信任度量计算式得出的节点信任值提出了一种基于信任的Raft共识机制，可以通过改变节点状态和参与共识的节点数量增加可信节点参与共识的概率并据此优化系统共识效率，同时实现系统安全和效率。

轻量级可信区块链模型如图4所示。其中将系统的参与方按照模型节点可分为管理节点、可信验证节点、排序节点、共识节点，各类型节点的定义及功能如下。

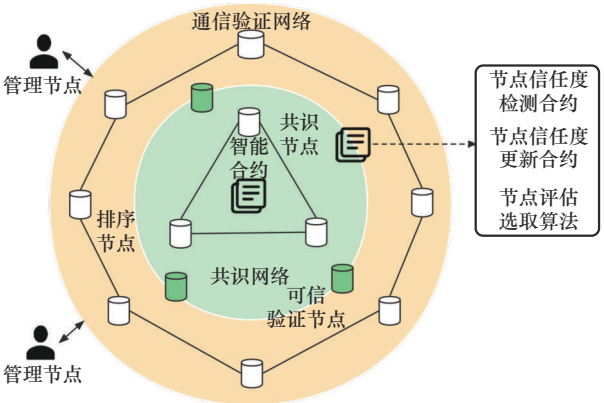

图4　轻量级可信区块链模型

（1）管理节点：作为认证管理中心参与节点，负责管理一组区块链节点的身份验证以及相应智能合约的编写和更新。当节点进入区块链网络时，需要向管理节点发送认证请求，以获取该节点的唯一标识，得到该节点的证书生成时间戳和身份属性信息，以方便对该节点的初始信任赋值，同时该节点部署实现信任管理模型的智能合约上链。

（2）可信验证节点：作为系统管理节点设置的完全可信节点，一般由第三方审计机构担任。可信验证节点不参与区块链系统交易数据的发送和验证，而是作为联盟链中的可信第三方，验证系统中参与节点发送的数据真实性，并将验证结果发送给节点可信度检测合约并生成相应节点的推荐信任值。

（3）排序节点：作为在区块链系统中发送和验证交易的节点，但不参与系统的共识过程。根据系统设置的初始信任阈值，信任值较低的节点在第一轮系统共识中成为排序节点，在行为和状态持续符合信任管理模型的正向行为后，其节点信任值持续上升，高于共识信任阈值的节点在每一轮系统共识之前根据信任计算结果自动转换为共识节点。

（4）共识节点：作为区块链系统中同时发送和验证交易并参与系统数据全网一致性共识的节点。通过设置共识信任阈值将系统中的共识节点数量保持在一定范围内，以最小化网络范围减小数据一致共识的时间来提高系统的共识效率和安全。

（5）智能合约：本文描述的智能合约分为节点可信度检测合约、节点可信度更新合约和节点评估选择算法合约。这些智能合约由管理节点唯一设置管理。

完成系统模型构建后，系统的轻量级可信区块链模型交互流程如图5所示。

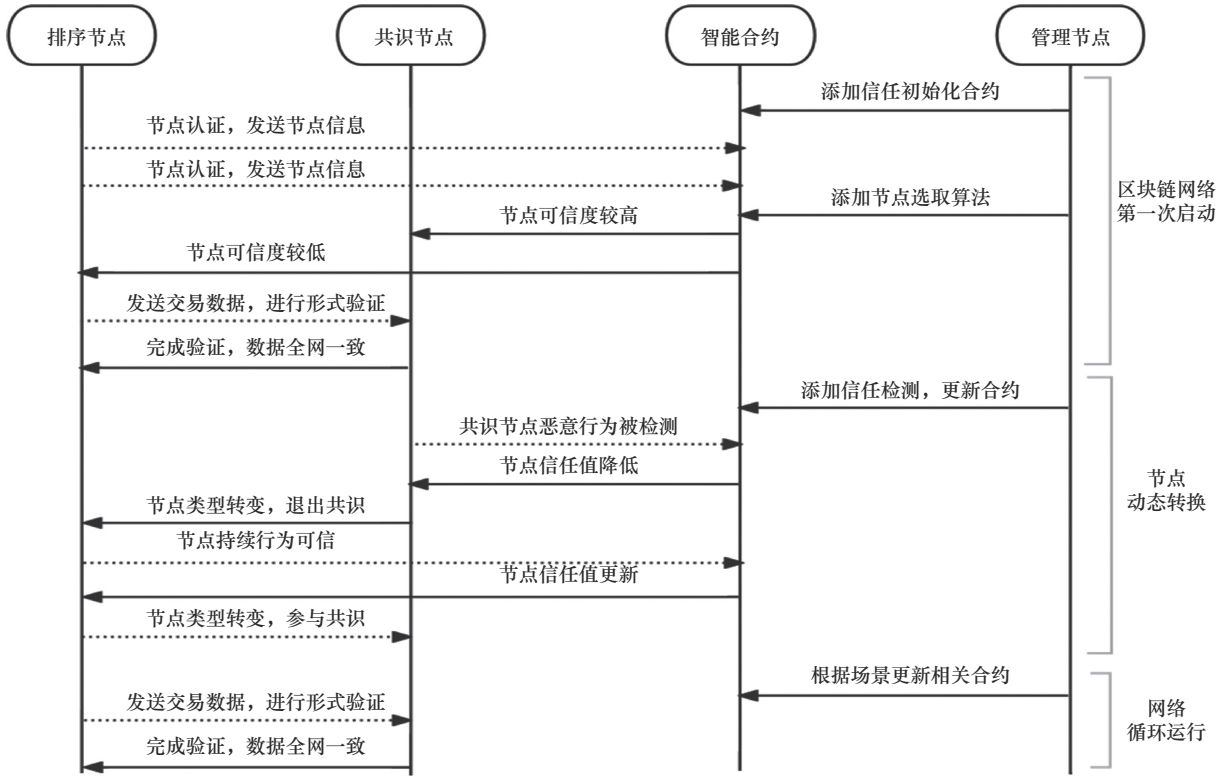

图5　轻量级可信区块链模型交互流程

3.1 用户节点的信任管理模型

本文提出了一个具有通用性的信任管理模型框架，信任管理模型框架和流程如图6所示。该框架适用于不同场景下已提出的众多信任管理模型。框架中由低到高依次为原始层、度量层、决策层、语义层。其中原始层收集信任数据，度量层计算客体的信任度，语义层中存储规则和策略语言，决策层制定可信决策。

信任管理模型包括信息收集、计算处理引擎、可信度量和可信决策。信息收集中采集客体的身份信息、历史行为信息和其他主体的推荐信息，经过预处理（过滤、融合等）后发送至计算处理引擎。随着机器学习、深度学习等技术的发展，各种智能算法也开始应用于信任管理模型中，为了满足算法所需的计算开销，在信任管理模型中部署了计算处理引擎。可信度量是根据得到的信任属性特征，选择聚合算法计算实体的综合信任度。可信决策根据度量模块得到的综合信任度和本地策略库，进行最终的信任决策，并将更新后的信任值发送至信任数据库；本地策略库存储实体间的交互数据信息、系统内实体的历史信任度。

可信度量通常包括以下3个基本步骤。

（1）信任值初始化

信任值初始化是准确计算信任值的先决条件。目前信任值初始化有两种方式：将节点设置为一定的信任值或使用初始化方法计算初始可信度。信任值的选择非常关键，如果赋值较高，节点将具有较高的权限，使系统容易受到新加入节点的攻击。

（2）信任属性的选择与定义

信任属性即信任所具有的特征，表明了需从哪些方面来分析信任关系，其具体特点是什么。信任属性必须具备客观性、关联性、可获得性这3个特征。根据网络的拓扑结构、节点信息和交互数据，将信任属性分为固有属性、交互属性和能力属性3类。①固有属性，由网络自身的结构和参与节点决定，包括位置协同关系、工作协同关系、集群利益和中心性；②交互属性，由网络内节点的交互情况决定，包括节点的交互协作性、频率、时间、声誉、服务质量、交互行为和反馈评价等；③能力属性，由网络内节点的计算和存储资源决定，包括计算能力、可持续服务时间、交互速率、能量维护能力、存储空间大小和传输带宽等。对于模型信任属性的选择和定义，应该基于网络的特点、应用和需求多维度考虑。

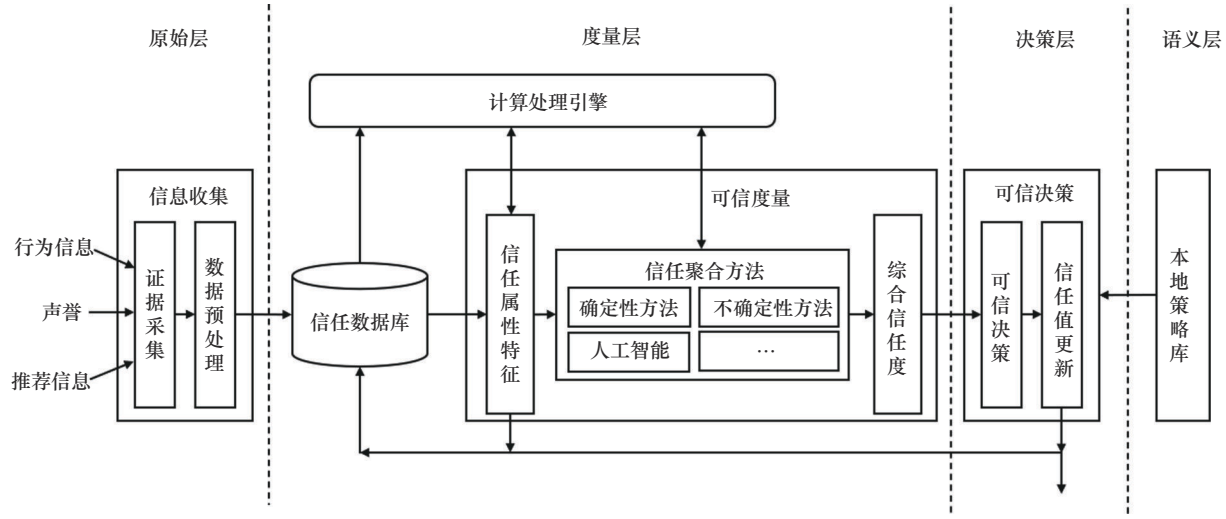

图6 信任管理模型框架和流程

（3）信任属性的融合计算

基于信任属性，采用一定的聚合算法即可得到最终可信度。信任聚合算法有加权和、模糊数学、DS 证据理论、概率统计、机器学习等方法。根据场景安全和性能的不同需求结合使用不同的信任计算方法。

本文按照这个模型流程详细阐述用户节点的信任管理模型设计思路。

（1）数据资产流通场景安全特性分析和信任属性选取

数据资产流通场景的主要安全需求是保障用户资产安全和交易安全，即用户资产注册登记可验证、资产访问权限可控制、资产价值转移安全可确认。节点信任属性的选择是基于待测实体的某种行为或特征的可信度，可以细化为直接或间接检测的相关数据特征。基于有关文献的研究[29]，节点 A 对节点 B 的信用值 C(A, B)是基于直接信任值 D(A, B)和推荐信任值 R(A, B)共同决定。D(A, B)是基于节点 A 和节点 B 的直接交互信任属性，R(A, B)是基于与节点 B 合作的其他节点对节点 B 的评价。借鉴这一思路，针对数据资产流通场景的上述安全目标，选取用户节点属性和行为的信任属性，信任属性分类如图 7 所示。

其中，将用户节点的信任值分为直接信任值和间接信任值，直接信任值包括用户注册金额、合法交易量、合法验证量和用户信息完整度等可以直接从区块链网络中获取的信息；间接信任值主要为可信验证节点通过查询获取特定交易和数据计算用户的推荐信任值，包括可信节点推荐值和数据真实度等属性信息和未授权访问行为、伪造权属行为和多重花费行为等恶意行为信息。属性信息主要用来做节点信任值的静态计算，而行为信息则为了衡量节点的动态信任值。

因此，本文模型选取节点的合法交易发送量 ω、合法交易验证量 μ 作为积极行为信息计算节点的直接信任值，将伪造权属行为 δ_1、未授权访问行为 δ_2 和多重花费行为 δ_3 这 3 种对系统危害较大的恶意行为作为节点被可信验证节点检测计算的间接信任值。节点每次遵守系统的交易规则的积极行为将随着时间的推移逐渐增加该节点的信任值，反之，有异常行为的节点将减少信任值。而属性信息则主要用来计算节点的初始信任值。

（2）节点初始信任值计算

目前关于信任管理与区块链系统结合的较多研究[29-31]不考虑不同节点的属性信息而将所有节点赋予相同的初始信任值，这样做的好处是不同

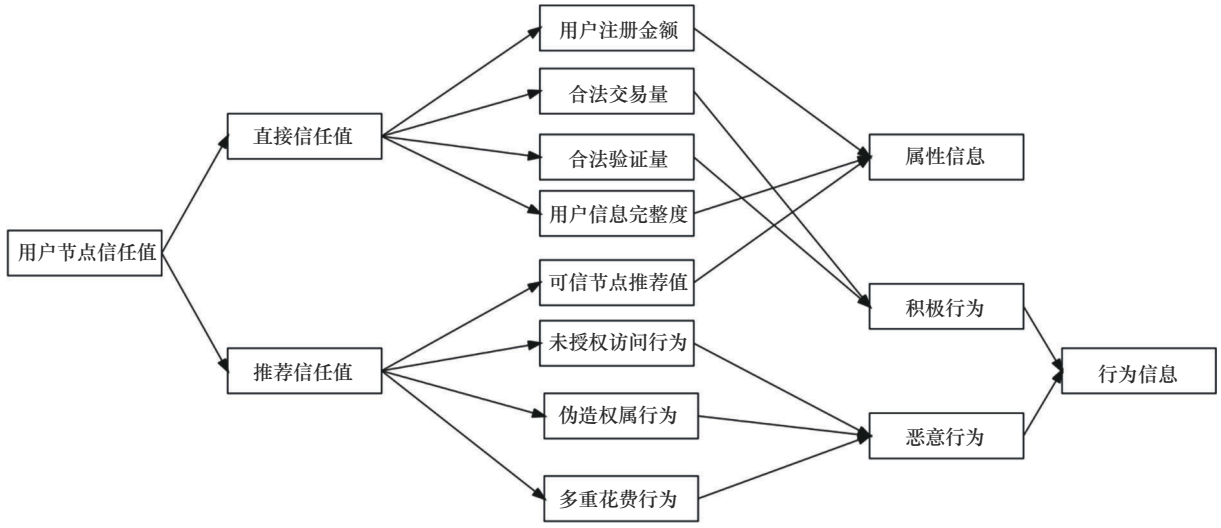

图 7　信任属性分类

节点具有相同的初始信任值，在节点产生不同行为后可以更快反映出信任值的变化，但这也提高了恶意节点攻击的成功率。在实际应用场景中由于不同用户节点具有的属性特征不同，其初始信任值应该是不同的。此外，节点入网就进行一定程度的节点信任值区分，也有利于降低系统的安全开销[32]。本节对不同节点的初始信任值做量化计算，通过身份认证进入区块链系统的节点根据其唯一证书标识查询该节点之前是否在区块链网络中，并以该节点提交的信任属性信息作为度量依据。假设在本文模型中设置时间阈值ΔT，对于首次加入网络或与上次加入网络的时间间隔大于ΔT的节点统一视为新节点。对于一个新节点A，将节点的初始信任值C_{ri}划分为3部分，计算式如下：

$$C_{ri}=\lambda_1\frac{\mathrm{gus}(A)}{\mathrm{tol}(A)}+\lambda_2 C_{rc}+\lambda_3 C_{rr} \tag{1}$$

其中，$\mathrm{tol}(A)$代表A在区块链网络中进行的交易总额，$\mathrm{gus}(A)$代表用户A在登记注册的账户金额，C_{rc}代表可信验证节点对用户A身份数据完整度校验，即提交身份信息属性越多，数值越高；C_{rr}代表可信验证节点推荐信任值，若用户是新节点，则产生一个范围内的随机数值，若用户有交互记录则根据历史记录计算初始信任值。λ_1、λ_2和λ_3分别代表各部分的权重系数。

对于有交互记录的节点考虑信任程度随时间的衰减特性，将该节点的历史信任值与时间衰减因子相乘，得到新的初始信任值，其计算式如下：

$$C_{ri}=C_{rj}\times \mathrm{e}^{-(t_{\mathrm{now}}-t_{\mathrm{last}})} \tag{2}$$

其中，C_{rj}代表总信任值，t_{now}代表当前时间，t_{last}代表该节点最后一次行为的时间。

（3）节点整体信任值计算

计算节点的初始信任值后需要根据节点的行为信息动态衡量节点整体可信度，鉴于区块链系统的计算开销和工业场景的轻量级和高安全的需求，本节采取加权和的方式计算节点的整体信任值，在选择合适的信任属性情况下能对目标场景下所关注的节点可信度进行较好的度量，计算式如下：

$$C_{rj}=C_{ri}+\varepsilon_c-\mathrm{e}^{-(D_r+R_r)t} \tag{3}$$

其中，C_{ri}是节点的信用初始值，ε_c是一个启动常数，用于保证系统初始化正常运行，D_r表示节点的直接信任值，R_r表示来自可信节点的推荐信任值。D_r由节点间的直接交互数据来衡量，如式（4）：

$$D_r=\frac{\sum_{m=1}^{\omega}\alpha_m+\sum_{n=1}^{\mu}\beta_n}{\Delta t} \tag{4}$$

其中，ω是节点合法发送的交易数量，μ是该节点合法验证的交易量，Δt表示一个时间单位，α_m表示对该交易的验证数量，β_n表示该验证的交易价值。

通过建立可信验证节点，减少节点计算推荐信用值的通信开销。可信验证节点主要从网络中检测并获取待度量节点的3种恶意行为记录。信任节点考虑这3种主要的恶意行为，其定义如式（5）：

$$\delta(A)=\begin{cases}-\delta_1, A\text{伪造证书}\\ -\delta_2, A\text{未授权访问}\\ -\delta_3, A\text{多重花费}\end{cases} \tag{5}$$

其中，δ_1表示节点伪造权属行为，即用户生成对应资产的虚假权属来获取资产权属收益的行为，可信验证节点只需将该虚假权属和真实权属做匹配即可证明其伪造性，如果两者比对相同，进一步查询权属授权合约结果或对应权属列表，查询不到则为恶意行为，对应状态标志计数器增加并将时间和对应攻击类型记录。δ_2表示节点未授权访问行为，即用户没有获取资产授权却进行资产访问的行为，可信验证节点只需进行查询链上访问合约结果即可判定是否存在该恶意行为，若存在则同样记录上链。δ_3表示节点多重花费行为，指节点同时申请获取多个数据资产，在满足访问

权限后如果节点账户余额不足以支付多个数据资产的价格，则按照顺序优先支付申请的资产，余额不足时交易会报错并返回回执，用户不能获取对应访问密钥并触发攻击标志记录。

以上 3 种恶意行为的惩罚系数可以根据当前场景对恶意行为的敏感度要求进行调整。在本文研究场景下因为这 3 种恶意行为对系统危害较大，所以选择一个较大的系数值来降低节点发起恶意攻击的概率。推荐信任值 R_r 的计算式如下：

$$R_r = \sum_{l=1}^{v} \delta(A) \times \zeta^{t-t_l} \tag{6}$$

其中，ζ 是一个常数，$0<\zeta<1$；v 在这里为 3，即 3 种恶意行为；t_l 表示节点恶意行为发生的时间，节点恶意行为的影响具有一定的时间衰减性，即最新发生的恶意行为危害更大。通过将信任管理模型的计算式和智能合约相结合，实现信任节点信任值的动态度量。

（4）节点信任程度判定

完成节点信任值度量计算后需要进行信任决策，即判定节点是否可信，本文模型采用二值判定方式，即满足阈值条件的节点是可信的，不满足阈值条件的节点不可信。针对本文信任结果应用类型，分为访问可信阈值 $C_{\text{threshold}}$、参与共识阈值 $C_{\text{consensus}}$ 和黑名单阈值 C_{block}。可信访问阈值 $C_{\text{threshold}}$ 判定用户信任值能否访问数据资产，参与共识阈值 $C_{\text{consensus}}$ 判定节点的类型转换，保证参与系统共识的节点数量保持在给定范围内，黑名单阈值 C_{block} 判定节点能否继续在网络中交易。3 种阈值的设定可由管理节点动态设置或计算得到。通过将上述阈值条件及判定合约通过管理节点部署到区块链系统上，实现系统安全性和抗攻击性的提高。

3.2　基于信任管理模型改进的 Raft 机制

区块链系统是保证数据资产交易可信的关键，而共识算法是确保链上数据一致性的重要机制。文献[33]给出了不同区块链系统共识机制的优缺点及轻量级共识优化的方案对比。现有的公有链系统没有节点管理机制难以适用于对安全性要求较高的工业数据交易场景，而具有节点准入准出控制的联盟链系统中，拜占庭类共识算法如实用拜占庭容错（practical Byzantine fault tolerance，PBFT）算法需要进行较多通信保证节点数据的一致可信，当系统中的节点较多时，系统效率会大幅下降。证明类共识算法如权益授权证明（delegated proof of stake，DPoS）共识中的超级节点投票机制较为复杂，且会出现优势节点持续当选的中心化趋势。而 Raft 共识机制能够快速实现网络中的数据一致性，被广泛应用在分布式系统中，但传统的 Raft 共识机制在本文场景中难以应对节点的拜占庭错误，因此结合上述节点信任管理模型，本节提出一种改进的 Raft 共识算法。

在分布式环境中，Raft 算法通过日志复制解决了节点共识问题[33-34]。每个节点持久性地存储一个一致的日志。日志由日志条目组成，而日志条目由命令、术语和索引组成。状态机的确定性保证了节点在按序执行日志后有一个一致的状态。Raft 算法的节点状态空间包括领导者、跟随者和候选者状态。领导者负责重新响应客户，协调日志复制，并在节点之间达成共识。跟随者对请求进行验证，以确定是否将日志条目追加到日志中，以及是否投票给候选者。如果跟随者在选举超时后没有收到心跳信息，将切换到候选者，并开始新一轮的领导者选举[25]。

本文模型提出的改进 Raft 共识协议主要针对领导者选举阶段，改进 Raft 关键流程如图 8 所示。其中，虚线框图例是原始算法中存在的流程，实线框图例是本文模型添加优化的地方，节点选取算法和选主投票机制在后文有详细阐述。

首先结合信任管理模型计算节点可信度，根据节点信任值选取划分节点为共识节点和排序节点，只有共识节点才能发起投票消息并成为领导

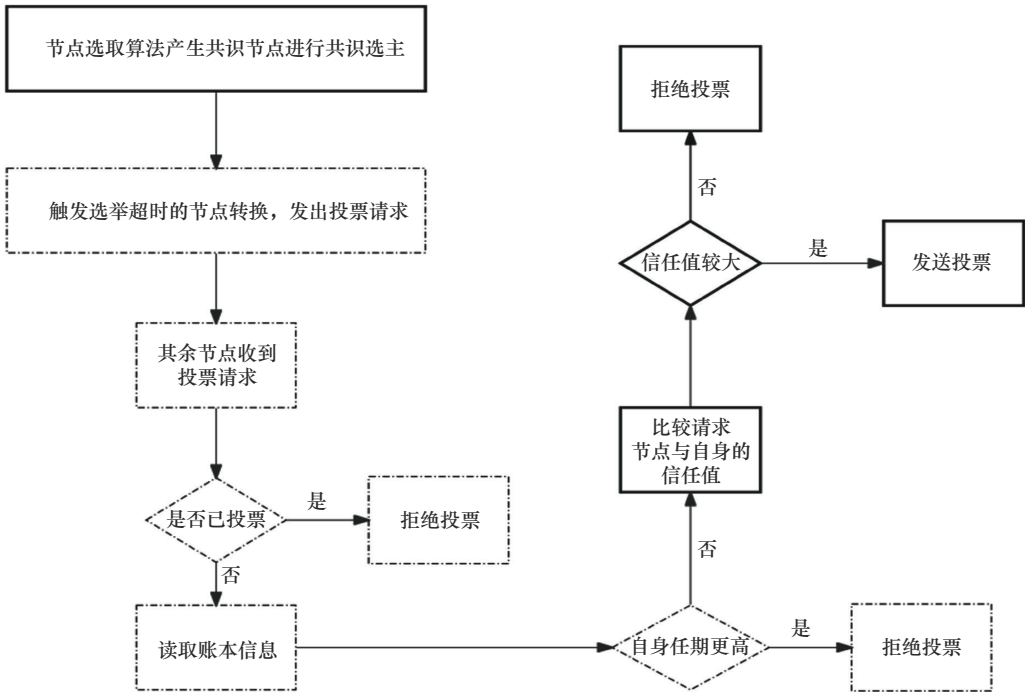

图8　改进Raft关键流程

者。满足参与共识阈值的节点成为共识节点；不满足参与共识阈值，但高于黑名单阈值的节点成为排序节点；低于黑名单阈值的节点则直接被加入黑名单。算法最终输出当前网络群组下的共识节点列表。

通过节点选取算法选出共识节点，只有共识节点才能进行领导者选举过程。当跟随者在共识节点列表中时，该节点才能增加条目成为候选者，并广播投票请求到网络中。其余节点收到投票请求后首先验证该节点标识是否在共识节点列表中，若不在则直接拒绝该投票。满足条件后查询是否自身已投票，如果没有投票则查询自身账本信息和请求消息中的条目，若投票请求的任期小于或等于自己，则拒绝该投票，否则进一步比较节点信任值C_{rj}。只有当请求节点的信任值较大且满足以上条件时才会获得该节点的投票响应。同时，若出现两个节点获得投票数相等则不再重新等待选举超时，直接由信任值较大的节点成为领导者结束选举过程。

3.3　模型分析与对比

本文提出基于行为和状态信息度量节点可信度的信任管理模型并优化共识一致性算法的轻量级可信区块链模型。通过对数据资产流通场景的安全性需求分析，选取参与节点特定的状态和行为数据作为信任值度量依据，基于加权和的计算方式计算节点信任值。在此基础上选取信任值较高的节点参与网络Raft共识协议并根据信任值优化选主流程，实现区块链系统安全和效率的兼具。

将本文轻量级可信区块链模型与目前信任管理和区块链结合的方案从安全性和性能角度进行对比分析。轻量级可信区块链模型对比分析见表1。与现有模型相比，本文模型根据节点的状态信息动态计算节点的初始信任值，在降低系统信任计算开销的同时实现系统初始化，更符合实际场景的设备和用户特征。本文采取的加权聚合计算方法在考虑节点的综合信任值计算选取直接信任和推荐信任，同时定义节点的恶意行为信息作为度量依据。信任计算模型选

取加权和的计算方式主要从信任模型的轻量化角度考虑，降低引入信任计算带来的额外开销。根据节点信任程度优化的区块链共识协议主要根据当前应用场景的特点和区块链类型选取。本节选取的Raft共识协议能够在联盟链场景下以较低的复杂度和较高的易用性实现系统的一致性共识，结合节点的信任值度量结果，选取信任值较高即可信度较大的节点参与系统共识，缩小共识选主范围来提高系统共识效率，并在进行投票选举时添加信任判定来提高可信度更高的节点参与系统共识的概率，在提高效率的同时也保证了系统的安全性。

表1　轻量级可信区块链模型对比分析

功能与安全类型	本文模型	文献[25]	文献[35]	文献[36]	文献[37]
考虑恶意行为	√	√	√	×	√
动态初始信任值	√	×	×	×	×
加权聚合计算	√	×	√	√	√
优化的共识协议	Raft	PoW	DPoS	PBFT	PoW

本文原型基于FISCO BCOS开源联盟链版本进行搭建。硬件设备为Intel CoreTM i5、8核CPU、16 GB内存、1 TB硬盘的台式机中进行实验。底层区块链实现环境为Ubuntu20.04 LTS操作系统，同时安装nodejs、Java、WeBase、MySQL等必需组件。

通过信任度量模型可以实时检测节点信任值，本文创新地提出了节点信任值初始化方案来降低节点的信任计算成本并进行初始化共识。计算节点的初始信任值C_{ri}有3个可调整参数，分别是λ_1、λ_2和λ_3。这里设置λ_1=1.0、λ_2=0.3和λ_3=0.7。设置两个节点以区块链技术开源平台BCOS中游离节点类型加入区块链网络，此时节点不参与区块链交易和共识，其信任值即节点初始信任值，每隔一段时间记录两节点的信任值，不同节点初始信任值变化如图9所示。

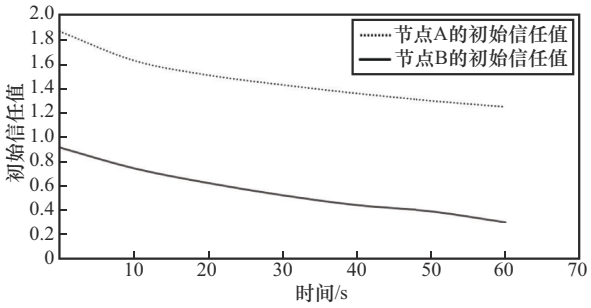

图9　不同节点初始信任值变化

从图9中看出，具有不同属性的节点初始信任值不同，能够实现节点的初始类别划分，但赋予的初始信任值会随着时间衰减，保证系统动态变化，并降低部分信任管理模型的计算开销，即初始信任值较高的节点，做出危害系统行为的概率较低。需要说明的是，节点运行过程中其初始信任值不再改变，仅和节点入网的属性和推荐信任值有关。

为保证总信任值$C_{rj}>0$在$t=0$时成立，本文设置$\varepsilon_c=1$，D_r表示节点的直接信任值，R_r表示节点的推荐信任值，本文考虑3种恶意行为及其权重。设置δ_1= 1、δ_2= 0.5、δ_3=1，表示恶意行为对应的权重参数，根据不同需要，也可以设置为其他值，是可调整参数。本文模拟了3个系统节点的行为，节点信任值变化如图10所示。

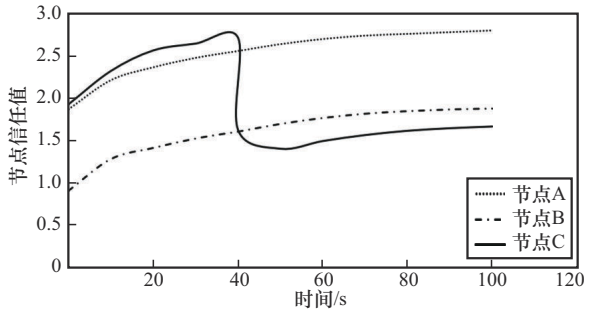

图10　节点信任值变化

从图10得出，不同节点初始信任值不同，但节点正常参与网络交易的发送和验证时，节点信任值逐渐增加，如节点A和节点B的信任值变化趋势。节点C在出现未授权访问行为δ_1、伪造权属行为δ_2和多重花费行为δ_3中的一种恶意行为被

检测出来后，其节点信任值大幅下降，触发阈值条件节点降级或进入黑名单，降低恶意节点参与系统共识的概率，提高系统安全性。

为了验证改进Raft一致性共识算法的效率和安全性，选取了系统交易吞吐量（transaction per second，TPS），也就是单位时间内处理和确认的交易数量作为对比指标。在网络参与节点分别为5、10、15和20个时对传统Raft共识协议的系统和基于信任改进的Raft共识协议系统进行TPS测试，改进Raft共识算法TPS测试结果如图11所示。

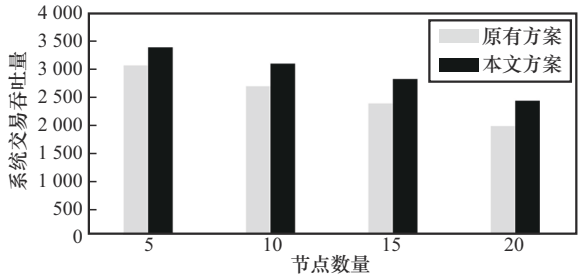

图11　改进Raft共识算法TPS测试结果

从图11看出，在不同节点情况下，本文提出的优化Raft协议表现均优于一般情况下的Raft协议算法，说明本文方案能够起到轻量级共识计算的效果，提高基于Raft协议的区块链在工业场景下的交易效率。由于本文方案同时度量节点信任值，能够实现针对可检测恶意行为的非拜占庭容错，所以在上述实验基础上，设置20%节点会产生3种恶意行为中的一种，重新测试两个方案的TPS，20%恶意节点情况下Raft共识算法TPS测试结果如图12所示。

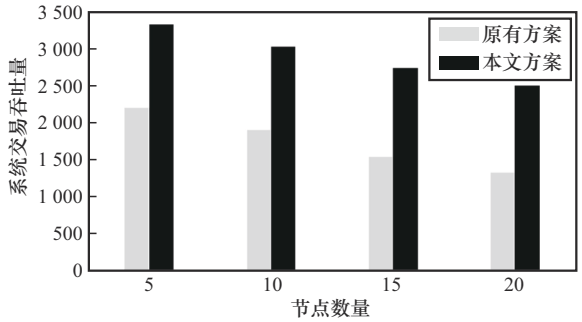

图12　20%恶意节点情况下Raft共识算法TPS测试结果

由上述结果可以观察到，改进后的Raft一致性协议的区块链在效率方面有较好提升，同时对恶意攻击行为具有一定的鲁棒性。虽然传统Raft协议系统的TPS仅部分降低，但是实际上发生恶意行为的节点仍在继续危害系统安全，而本文提出的改进Raft协议算法能够检测并定位恶意节点，显著降低其参与系统共识的概率，在保证安全的同时提高系统吞吐量。

4　结束语

针对工业数据资产的权属身份脆弱性、数据访问自适应不足、数据价值收益执行不足的安全现状，提出了多方参与的数据资产多级交易应用场景的系统设计目标，给出了工业数据资产可信确权及价值流转的整体框架、具体方案和大致工作流程，并根据该应用场景的特点改进区块链底层数据结构保证共享流程的安全可信。基于信任管理模型度量的节点信任值，优化区块链系统共识协议，在降低节点恶意攻击概率的同时提高系统交易共识效率，在一定程度上实现区块链系统的安全和轻量级兼具。

本文提出的工业数据可信确权与价值流转的区块链共享方案在以下几个方面具有一定的扩展和改进空间，也可以作为未来进一步的研究方向。

（1）本文方案能够保证上链数据资产的权属可信、价值分配合理和授权控制，但是对于保障链下数据资产的质量和来源清晰性仍存在不足，如何确保数据在链下生成过程中的安全可信和真实有效仍然是目前需要解决的问题。

（2）本文方案中实现的数据资产价值分配仅考虑了数据价格由数据拥有者设置的恒定价格情况，实际数据资产交易过程中数据价格对多方参与的意愿和数据使用频率都有较大影响，如何设置合理的数据定价和交易激励机制以实现交易系统的效率、安全性并促进数据要素市场的流通发展具有重要意义。目前已有部分学者从博弈论、

拍卖机制等角度取得了一些新的研究进展，具有一定的启发意义。

（3）本文所研究的数据资产流通参与方均在同一个区块链系统中完成数据资产交易全流程，但随着参与者所处的行业领域和业务需求逐渐增多，同一数据资产的提供方和使用方处于不同区块链系统的场景也会出现交易需求，如何保证数据资产的权属和收益跨链执行的安全和效率是未来基于区块链进行数据资产流通方案必须解决的问题。目前关于跨链场景的部分研究能够提供一定的借鉴模式，但仍需在跨链流通方案的通用性和场景适配性等技术上作进一步研究。

参考文献：

[1] 吕金虎, 任磊, 谭少林, 等. 工业互联网层级架构与安全: 复杂网络新视角[J]. 中国科学: 技术科学, 2024, 54(10): 2042-2052.
LYU J H, REN L, TAN S L, et al. Hierarchical architecture and security of industrial internet: a new perspective from complex network[J]. Science China Technological Sciences, 2024, 54 (10): 2042-2052.

[2] 工业互联网产业联盟. 新型工业控制蓝皮书[R]. 2024.
Alliance of Industrial Internet. New industrial control blue book[R]. 2024.

[3] 工业互联网产业联盟, 可信工业数据空间生态链. 可信工业数据流通应用案例集[R]. 2023.
Alliance of Industrial Internet, Trusted industrial data matrix consortium. Case collection of trusted industrial data circulation applications[R]. 2023.

[4] 王健全, 马彰超, 孙雷, 等. 工业网络体系架构的演进、关键技术及未来展望[J]. 工程科学学报, 2023, 45(8): 1376-1389.
WANG J Q, MA Z C, SUN L, et al. Evolution, key technology, prospects, and applications of industrial network architecture[J]. Chinese Journal of Engineering, 2023, 45(8): 1376-1389.

[5] SONG R, XIAO B, SONG Y B, et al. A survey of blockchain-based schemes for data sharing and exchange[J]. IEEE Transactions on Big Data, 2023, 9(6): 1477-1495.

[6] DIXIT A, SINGH A, RAHULAMATHAVAN Y, et al. FAST DATA: a fair, secure, and trusted decentralized IIoT data marketplace enabled by blockchain[J]. IEEE Internet of Things Journal, 2023, 10(4): 2934-2944.

[7] 杨明, 冯宏霖, 王鑫, 等. 数据要素市场研究综述: 价值、定价与交易[J]. 网络与信息安全学报, 2024, 10(3): 1-19.
YANG M, FENG H L, WANG X, et al. Survey of data factor market: value, pricing, and trading[J]. Chinese Journal of Network and Information Security, 2024, 10(3): 1-19.

[8] 文英姿, 江金菁, 杨红, 等. 数据流通安全治理模式及实现: 基于共创共治视角[J]. 大数据, 2024, 10(6): 62-76.
WEN Y Z, JIANG J J, YANG H, et al. Data circulation security governance model and implementation: from the perspective of co-creation and co-governance[J]. Big Data Research, 2024, 10(6): 62-76.

[9] LIU Z M, HUANG B N, LI Y S, et al. Pricing game and blockchain for electricity data trading in low-carbon smart energy systems[J]. IEEE Transactions on Industrial Informatics, 2024, 20(4): 6446-6456.

[10] 可信工业数据空间生态链, 工业互联网产业联盟. 可信工业数据空间系统架构[R]. 2022.
Trusted Industrial Data Matrix Consortium, Alliance of Industrial Internet. Trusted industrial data space system architecture[R]. 2022.

[11] ZHANG X H, LI X H, MIAO Y B, et al. A data trading scheme with efficient data usage control for industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2022, 18(7): 4456-4465.

[12] SHI Z S, DE LAAT C, GROSSO P, et al. Integration of blockchain and auction models: a survey, some applications, and challenges[J]. IEEE Communications Surveys & Tutorials, 2023, 25(1): 497-537.

[13] LI J J, LI J Q, WANG X, et al. Multi-blockchain based data trading markets with novel pricing mechanisms[J]. IEEE/CAA Journal of Automatica Sinica, 2023, 10(12): 2222-2232

[14] 程冠杰, 邓水光, 温盈盈, 等. 基于区块链的物联网认证机制综述[J]. 软件学报, 2023, 34(3): 1470-1490.
CHENG G J, DENG S G, WEN Y Y, et al. Survey on blockchain-based Internet of things authentication mechanisms[J]. Journal of Software, 2023, 34(3): 1470-1490.

[15] COOK M, MARNERIDES A, JOHNSON C, et al. A survey on industrial control system digital forensics: challenges, advances and future directions[J]. IEEE Communications Surveys & Tutorials, 2023, 25(3): 1705-1747.

[16] ALWARAFY A, AL-THELAYA K A, ABDALLAH M, et al. A survey on security and privacy issues in edge-computing-assisted internet of things[J]. IEEE Internet of Things Journal, 2021, 8(6): 4004-4022.

[17] WEI L J, YANG Y H, WU J, et al. Trust management for internet of things: a comprehensive study[J]. IEEE Internet of Things Journal, 2022, 9(10): 7664-7679.

[18] 方栋梁, 刘圃卓, 秦川, 等. 工业控制系统协议安全综述[J]. 计算机研究与发展, 2022, 59(5): 978-993.
FANG D L, LIU P Z, QIN C, et al. Survey of protocol security of industrial control system[J]. Journal of Computer Research and Development, 2022, 59(5): 978-993.

[19] KUMAR R, KUMAR P, TRIPATHI R, et al. Permissioned

blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems[J]. IEEE Transactions on Industrial Informatics, 2022, 18(11): 8065-8073.

[20] 李凤华, 李晖, 牛犇, 等. 数据要素流通与安全的研究范畴与未来发展趋势[J]. 通信学报, 2024, 45(5): 1-11.
LI F H, LI H, NIU B, et al. Research category and future development trend of data elements circulation and security[J]. Journal on Communications, 2024, 45(5): 1-11.

[21] CAO B, WANG Z X, ZHANG L, et al. Blockchain systems, technologies, and applications: a methodology perspective[J]. IEEE Communications Surveys & Tutorials, 2023, 25(1): 353-385.

[22] YANG Z B, ALFAURI H, FARKIANI B, et al. A survey and comparison of post-quantum and quantum blockchains[J]. IEEE Communications Surveys & Tutorials, 2024, 26(2): 967-1002.

[23] HUO R, ZENG S Q, WANG Z H, et al. A comprehensive survey on blockchain in industrial internet of things: motivations, research progresses, and future challenges[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 88-122.

[24] WANG Z H, FU Y S. A unified attribute-based encryption data sharing scheme matching industrial internet framework[J]. IEEE Internet of Things Journal, 2024, 11(5): 9153-9170.

[25] 张乐君, 刘智栋, 谢国, 等. 基于集成信用度评估智能合约的安全数据共享模型[J]. 自动化学报, 2021, 47(3): 594-608.
ZHANG L J, LIU Z D, XIE G, et al. Secure data sharing model based on smart contract with integrated credit evaluation[J]. Acta Automatica Sinica, 2021, 47(3): 594-608.

[26] YU Y, LU Q C, FU Y S. Dynamic trust management for the edge devices in industrial internet[J]. IEEE Internet of Things Journal, 2024, 11(10): 18410-18420.

[27] LIU Y J, WANG J, YAN Z, et al. A survey on blockchain-based trust management for internet of things[J]. IEEE Internet of Things Journal, 2023, 10(7): 5898-5922.

[28] WANG D C, FU Y S. LBDTM: lightweight blockchain with dynamic trust management[C]//Proceedings of the 2022 China Automation Congress (CAC). Piscataway: IEEE Press, 2022: 4059-4064.

[29] KHAN W Z, ARSHAD Q U A, HAKAK S, et al. Trust management in social internet of things: architectures, recent advancements, and future challenges[J]. IEEE Internet of Things Journal, 2021, 8(10): 7768-7788.

[30] YANG Z G, WANG R Y, WU D P, et al. Blockchain-enabled trust management model for the internet of vehicles[J]. IEEE Internet of Things Journal, 2023, 10(14): 12044-12054.

[31] LIU C, GUO S Y, GUO S, et al. LTSM: lightweight and trusted sharing mechanism of IoT data in smart city[J]. IEEE Internet of Things Journal, 2022, 9(7): 5080-5093.

[32] 于亚, 伏玉笋. 工业互联网边缘终端初始接入可信度量方法研究[J]. 物联网学报, 2022, 6(4): 149-157.
YU Y, FU Y S. Research on trust measurement method for initial access of industrial internet edge terminals[J]. Chinese Journal on Internet of Things, 2022, 6(4): 149-157.

[33] 谢晴晴, 董凡. 轻量级区块链技术综述[J]. 软件学报, 2023, 34(1): 33-49.
XIE Q Q, DONG F. Survey on lightweight blockchain technology[J]. Journal of Software, 2023, 34(1): 33-49.

[34] XIAO Y, ZHANG N, LOU W J, et al. A survey of distributed consensus protocols for blockchain networks[J]. IEEE Communications Surveys & Tutorials, 2020, 22(2): 1432-1465.

[35] SU Z, WANG Y T, XU Q C, et al. LVBS: lightweight vehicular blockchain for secure data sharing in disaster rescue[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 19-32.

[36] 蒋伟进, 周文颖, 李恩, 等. 基于区块链技术的云制造服务架构及共识算法研究[J]. 物联网学报, 2023, 7(1): 159-173.
JIANG W J, ZHOU W Y, LI E, et al. Research on cloud manufacturing service architecture and consensus algorithm based on blockchain technology[J]. Chinese Journal on Internet of Things, 2023, 7(1): 159-173.

[37] HUANG J Q, KONG L H, CHEN G H, et al. Towards secure industrial IoT: blockchain system with credit-based consensus mechanism[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3680-3689.

[作者简介]

王东初（1998– ），男，上海交通大学硕士生，主要研究方向为工业互联网与安全可信、区块链应用等。

伏玉笋（1972– ），男，博士，上海交通大学助理研究员，主要研究方向为工业通信与智能信息系统、工业互联网与安全可信等。

于亚（1996– ），男，上海交通大学硕士生，主要研究方向为工业通信系统与安全、可信计算、物联网安全等。