

基于智能合约的数据跨境流动多方互信机制构建和应用

蒋荣¹, 侯士平¹, 罗圣美²

1. 南京中孚信息技术有限公司, 江苏 南京 211800;
2. 中孚信息股份有限公司, 山东 济南 250101

摘要

数字经济全球化背景下, 数据跨境流动面临法律差异导致的合规冲突、多方主体信任缺失、监管审计困难等现实挑战。提出一种基于智能合约的数据跨境流动多方互信机制, 从多方互信机制核心要素、关键数据结构、业务流程、系统架构4个方面进行了深入阐述。该机制借助区块链去中心化、极难篡改特性, 构建覆盖身份验证、合规审查、责任追溯的全流程解决方案, 有效解决了传统模式中第三方信任依赖风险与监管滞后问题, 通过技术手段将合规要求转化为自动化执行逻辑, 提升数据流动透明度与安全性。

关键词

区块链; 智能合约; 数据跨境流动; 数据跨境流动监管; 多方互信机制

中图分类号: TP311

文献标志码: A

doi: 10.11959/j.issn.2096-0271.2025047

Construction and application of multi-party trust mechanism for cross border data flow based on smart contracts

JIANG Rong¹, HOU Shiping¹, LUO Shengmei²

1. Nanjing Zhongfu Information Technology Co., Ltd., Nanjing 211800, China
2. Zhongfu Information Co., Ltd., Jinan 250101, China

Abstract

In the context of globalization of the digital economy, cross border data flows face practical challenges such as compliance conflicts caused by legal differences, lack of trust among multiple parties, and difficulties in regulatory audits. This paper proposes a multi-party mutual trust mechanism for cross border data flows based on smart contracts, elaborating from four aspects: core elements of multi-party mutual mechanism, key data structures, business processes, and system architecture. Leveraging the decentralized and tamper proof nature of blockchain, it constructs a full process solution covering identity verification, compliance review, and responsibility tracing. This mechanism effectively addresses the risks of third-party trust dependency and regulatory lag in traditional models. By using technical means to transform compliance requirements into automated execution logic, it enhances the transparency and security of data flows.

Key words

blockchain, smart contract, cross border data flow, regulation of cross border data flow, multi-party trust mechanism

0 引言

随着全球化进程的加速和信息技术的迅猛发展，数据跨境流动已成为当今数字经济不可或缺的一部分，支持政府机构、企业和个人的国际合作、商业活动及技术创新。然而，数据跨境流动的日益频繁也带来了法律合规、监管要求、隐私保护和安全等方面的显著挑战^[1-5]。各国在数据隐私、主权及安全领域的立法差异导致跨境数据流动的复杂性和不确定性日益加剧。国外方面，欧盟的《通用数据保护条例》（GDPR）和美国的《云法案》（CLOUD Act）对跨境数据处理和流动提出了严格要求^[6-9]；国内方面，《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》明确规范了数据跨境流动，中央网络安全和信息化委员会办公室（简称中央网信办）通过《数据出境安全评估办法》《个人信息出境标准合同办法》及《促进和规范数据跨境流动规定》等政策，调整数据出境安全评估、标准合同和认证制度，旨在对数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的施行进行调整，保障数据安全，保护个人信息权益，促进数据依法有序自由流动^[10]。

当前，数据跨境流动面临多重问题：首先，各国法律体系的差异导致合规要求冲突，例如 GDPR 要求数据充分性保护，而我国强调数据本地化和国家安全审查，增加了多方合作的法律风险^[11]；其次，不同参与方（数据提供者、接收者、监管机构）之间缺乏有效的信任机制，透明度不足使得审计和责任界定困难^[12]；最后，地缘政治因素和技术标准的不统一进一步加

剧了信任危机，限制了数据流动的效率与安全性^[13]。

国内外针对数据跨境流动的研究和认证机制取得了一定进展。国外方面，美国通过可信云技术（如 FedRAMP 认证）建立标准和评估机制，确保云服务商满足安全需求；欧盟在 GDPR 框架下推动将“标准合同条款”（SCC）和“约束性公司规则”（BCR）作为认证工具，并结合加密与匿名化技术保护数据隐私^[14]。我国通过数据存储加密技术保护数据库及应用层数据，运用数据脱敏和去标识化技术（如统计技术、密码技术）处理敏感信息，同时依托中央网信办的政策框架建立安全评估和标准合同机制^[15-17]。然而，这些传统方法在复杂多方场景中存在局限：依赖中心化第三方机构的信任背书模式增加了数据泄露和被篡改的风险，且难以适应全球分布式系统的动态需求；此外，现有认证机制多为静态合规检查，缺乏实时性和自动化特性。

为应对上述问题，区块链技术及其核心组件——智能合约，因其去中心化、极难篡改和可追溯特性，逐渐成为研究热点，为构建多方互信机制提供了新路径^[18-21]。本文旨在设计一种基于智能合约的机制，以提升跨境数据流动的信任度、安全性和合规性，确保各方行为可验证、过程透明并符合法规要求。该机制不仅能解决传统信任模型的中心化风险，还能在保障数据隐私和合规性的同时提高流动效率^[22-25]。

本文主要贡献如下：首先，它为跨境数据流动中的信任问题提供创新性解决方案，以克服现有认证机制的局限性；其次，智能合约的自动化合规检查功能可降低法律风险并提升效率；最后，该机制为未来数据跨境流动提供可行路径，促进各国数据交换的健康发展，助力全球数字经济持

续增长。通过总结国内外研究现状并分析问题，本文旨在为后续技术设计奠定理论基础。

1 基于智能合约的数据跨境流动多方互信设计

在跨境数据流动的复杂场景中，多方参与者来自不同国家和地区，面临着不同的法律法规和技术环境。这种背景下，构建一个有效的多方互信机制至关重要。智能合约的去中心化、极难篡改和自动执行特性为解决这一问题提供了可能性。通过智能合约，本文设计建立一个可信的机制，确保跨境数据在不同主体之间的流动安全、透明和合规。

1.1 多方互信机制的核心要素

为了构建一个有效的多方互信机制，首先需要明确该机制的核心要素。这些要素将在跨境数据流动的每个环节中发挥重要作用，确保数据传输过程的透明性和安全性。

(1) 跨境主体识别与授权

在跨境数据流动中，多方参与者之间需要互相识别并确认身份。智能合约可以通过公钥基础设施（public key infrastructure, PKI）或去中心化身份（decentralized identity, DID）技术实现参与方的身份验证，确保数据传输过程中的所有行为都来自可信的主体。此外，智能合约能够根据需要调控参与者的授权权限，确保仅有获得授权许可的实体才有访问和处理数据的权限。

(2) 数据合规与审查

不同国家和地区对数据的处理和流动有不同的法律规定。智能合约可以集成自

动化的合规审查模块，在数据跨境流动之前，智能合约会根据数据的类型和传输目的，自动检查其是否符合目的地国家或地区的法规要求，并据此决定数据是否可以被传输。

(3) 责任追溯与审计

鉴于智能合约能在区块链平台上运行，其执行的每项操作都会被详尽记录且极难篡改，这一特性极大地强化了跨境数据传输中的责任追溯与审计流程的可靠性。因此，相关方可以通过智能合约记录的数据流动日志轻松追溯到数据流动的每一个环节，并确保在数据处理过程中，所有参与方都履行了各自的义务。

(4) 数据流动的实时监控与反馈

智能合约可以结合区块链的实时性，实时监控跨境数据流动的状态。通过区块链网络上的共识机制，各方可以及时获取数据传输的状态反馈，了解数据的流动是否顺利以及是否符合预期的合规标准。一旦出现异常，智能合约可以自动执行回滚操作或暂停数据传输，以防止违规或不当操作的发生。

1.2 关键数据结构设计

基于以上多方互信机制的核心要素，本文提出了关键业务的数据结构（见表1~表3），以满足跨境数据流动过程中的各业务功能。

1.3 业务流程设计

为了实现上述的多方互信机制，基于智能合约的跨境数据流动过程需要精心设计5个关键业务流程。图1所示是典型的智能合约驱动的数据流动过程。

(1) 身份验证与授权配置

在数据流动开始前，各方首先需要通

表1 跨境主体身份结构

序号	字段名称	数据类型	字段描述
1	participantID	Address	跨境主体ID(地址),用于标识身份
2	orgName	String	所属的组织名称
3	CountryCode	String	国家代码
4	isVerified	Bool	是否已通过身份验证

表2 跨境数据传输结构

序号	字段名称	数据类型	字段描述
1	senderAddress	String	跨境主体ID
2	receiverAddress	String	跨境主体ID
3	data Type	Int	数据类型(如个人数据、金融、地理信息数据等)
4	dataHash	String	数据的哈希值,用于在传输后验证数据的完整性
5	timestamp	Date	传输请求时间戳
6	isChecked	Bool	是否通过合规检查
7	status	Int	当前传输状态(传输中、拒绝、完成等)
8	reason	Int	如传输被拒绝或失败,记录失败原因

表3 跨境数据传输审计结构

序号	字段名称	数据类型	字段描述
1	logID	String	日志ID
2	senderID	String	跨境主体ID
3	timestamp	String	审计日志时间
4	data Type	Int	数据类型(同上)
5	dataSize	Int	传输数据量
6	details	String	操作的详细信息(如合规检查结果、加密详情等)

过智能合约完成身份验证和授权配置。智能合约负责自动审核各参与者的身份认证,同时依据跨境数据流通的准则为每位参与者分配相应的数据访问权限及范围。这一流程有效阻止了非授权实体的数据接触,保障了数据的安全边界。

(2) 数据请求与合规性检查

参与方发起数据请求时,智能合约首先会对请求方的身份进行验证,并对其请求的数据进行合规性检查,以确保该数据流转行为符合当地对数据传输的特定要求。如果符合规定,智能合约将授权数据

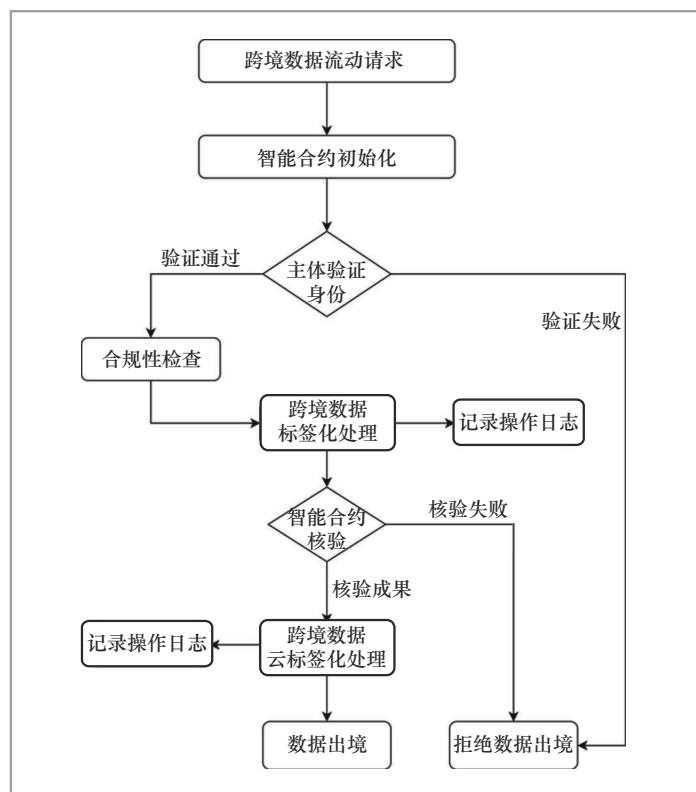


图1 智能合约驱动的数据流程

的正常流通，否则会阻断此次数据传输请求。

(3) 数据传输与标识

一旦数据传输得到授权，智能合约将自动触发数据传输的相关操作。为确保数据传输的安全性，智能合约会对数据进行标签化处理，并选择最优的传输通道。在数据传输过程中，智能合约可以实时监控数据包的流向，确保数据不被第三方截获或篡改。

(4) 跨境数据核验与去标签化

关口侧在完成跨境数据接收后，智能合约会自动生成接收确认信息，并将其写入区块链。这一流程可以确认数据传输的完成情况，并保证数据在传输过程中的完整性和一致性。进一步地，完成跨境数据合法性与有效性核验后，对跨境数据进行去标识化动作。

(5) 执行日志与审计记录

在数据传输的每个步骤，智能合约都会自动记录执行日志，确保所有操作都可以追溯。同时，所有审计记录都会被保存在区块链上，确保不易篡改。这些日志包括数据请求者的身份信息、传输发生的具体时间、传输内容的哈希值、传输状态等关键信息。

1.4 系统架构设计

基于智能合约的数据跨境流动多方互信机制，系统的技术架构设计可以通过以下5个层次开展，如图2所示。

(1) 区块链网络层

区块链网络层包括智能合约存储、智能合约执行、智能合约验证记录等模块，该层为智能合约的运行提供了基础设施，不仅承担了去中心化的账本管理和数据存储功能，还通过共识机制保证了合约执行的安全性和一致性。在跨境数据流动中，分布在不同国家或地区的区块链节点能够共同参与，保障系统的去中心化运行。

(2) 智能合约层

智能合约层包括智能合约定义、执行智能合约、智能合约验证等模块，集成了身份验证、权限控制、合规性校验、数据加密传输、日志记录与审计跟踪等一系列功能，确保了数据传输的高效性、安全性和可追溯性。该层是多方互信机制的核心模块，通过该层的智能合约技术，数据流转的每一步都能自动执行，无须人工干预。

(3) 数据标识层

数据标识层包括标签生成、数据标签封装/解封装、数据标签验证等模块，该模块通过实施严格的访问控制、数据加

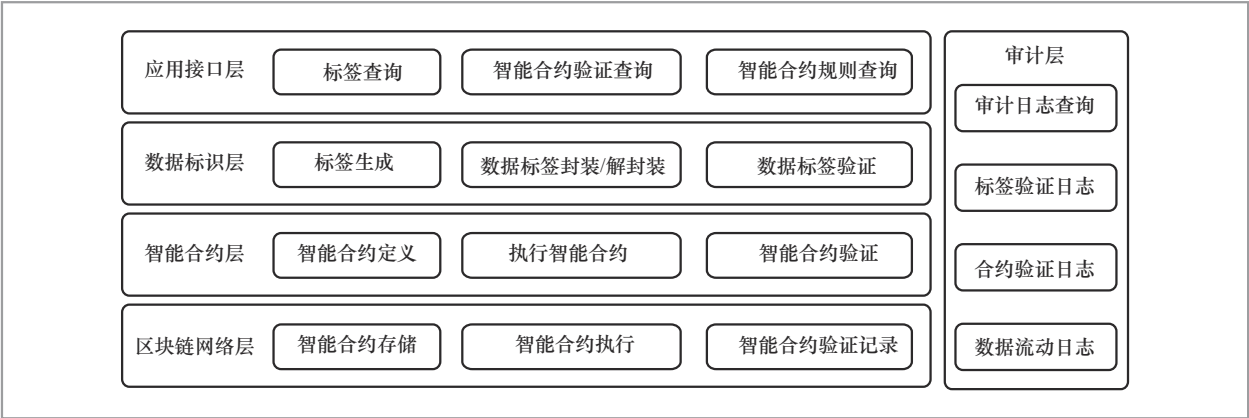


图2 基于智能合约的数据跨境流动多方互信机制架构

密、传输监控以及日志审计等多重安全措施，实时监控数据的动态变化，及时发现并有效应对潜在的安全威胁，从而最大限度地降低数据泄露、非法访问或篡改的风险。它不仅利用智能合约的灵活性与集成性，还借助高级别加密算法库，对数据进行哈希运算与唯一性标识处理，确保数据在传输过程中的完整性和极难篡改性，同时融入了先进的数据生命周期安全管理体系覆盖了从数据生成、存储、传输至销毁的全生命周期。

（4）审计层

审计层包括数据流动日志、合约验证日志、标签验证日志、审计日志查询等模块，通过智能合约预设的规则与逻辑，对数据流动的合法性、合规性进行智能判断与决策，精准把控数据的流向与范围。同时该层详尽记录每一次审查过程与结果，这些记录包含了数据流动的详细信息和审查的时间、执行者、依据的规则以及最终的决定等关键要素，以便未来的监管和审计，确保了数据流动过程的可追溯性与透明度。

（5）应用接口层

应用接口层包括标签查询、智能合约

验证查询、智能合约规则查询等模块，为用户提供了与智能合约互动的途径。通过这些接口，参与方可以发起数据传输请求、查询数据流动状态、访问传输日志记录等。此外，应用层接口具备良好的扩展性与兼容性，能够无缝对接其他系统平台，以促进多方之间数据资源的共享与利用。

2 基于智能合约的数据跨境流动多方互信应用

随着全球化进程的加快，各国政府和公共部门间的跨境数据合作需求日益增加，如气候数据共享、疫情防控数据交流等。然而，政府数据具有敏感性和公共利益属性，数据跨境流动的合规性和安全性尤为重要。智能合约在跨境数据流动中的应用，能够有效应对传统跨境数据流动面临的信任缺失、合规复杂和审计困难等挑战，通过智能合约，可以实现数据流动全流程的自动化管理，确保参与方的信任和合规性。本节将结合政府与公共部门的数据跨境合作的具体应用场景，详细描述基于智能合约的数据跨境流动多方互信的实际应用。

(1) 总体业务应用流程

基于智能合约的数据跨境流动总体流程如图3所示。

企业侧，根据企业的业务需求，对数据类型和敏感性进行分类分级，为每个数据单元生成唯一的标签。这些标签中包含数据的敏感度等级、合法性验证信息以及合规要求等，并通过无感的网络打标技术将标签信息安全地封装到发送的报文中。在此过程中，企业用户通过企业侧专设的标识网关向关口提交数据传输请求，标识网关系统将数据进行标签化处理，并与智能合约中预定义的传输规则进行绑定，数据经过加密处理后，连同标签一同被封装，安全地发往给关口侧。

关口侧，在接收到企业侧传来的封装数据时，会立即启动智能合约的验证检测机制，以确保数据传输的合规性。关口侧的出境网关会对数据标签进行严格的核验，这一过程旨在验证数据的完整性和真实性，确保数据在传输过程中未被非法篡改，并确认其完全符合既定的安全传输和合规要求。只有当数据成功通过智能合约和标签的双重验证后，关口侧才会对其进行解封

装操作，并以安全的方式将其传输至最终的接收方。这一流程不仅确保了数据传输的安全性，还有效地维护了数据流动的合规性。

(2) 智能合约初始化

在跨境数据流转的业务中，智能合约的初始化扮演着重要的角色，是确保数据跨境流动合规性和安全性的第一步。智能合约的初始化过程需要多方参与，本文设计的业务模型中，该初始化操作涉及企业侧网关、区块链网络、关口侧网关等环节。以下通过时序图（图4）的方式展示智能合约初始化过程中具体要做的内容。

如图4所示，智能合约初始化的核心是基于参与方的业务需求、合规要求、数据分类分级标准等，定义和生成一份清晰、可执行的智能合约。合约的初始化过程确保了在实际数据跨境流动过程中，所有操作都可以按照预设的规则执行，且每一步操作都能在区块链技术的支撑下被有效验证与审计，从而全面实现数据流动的安全性、透明度以及合规性的高标准要求。

(3) 跨境数据流动的智能合约

图5描述了针对跨境数据流动场景的

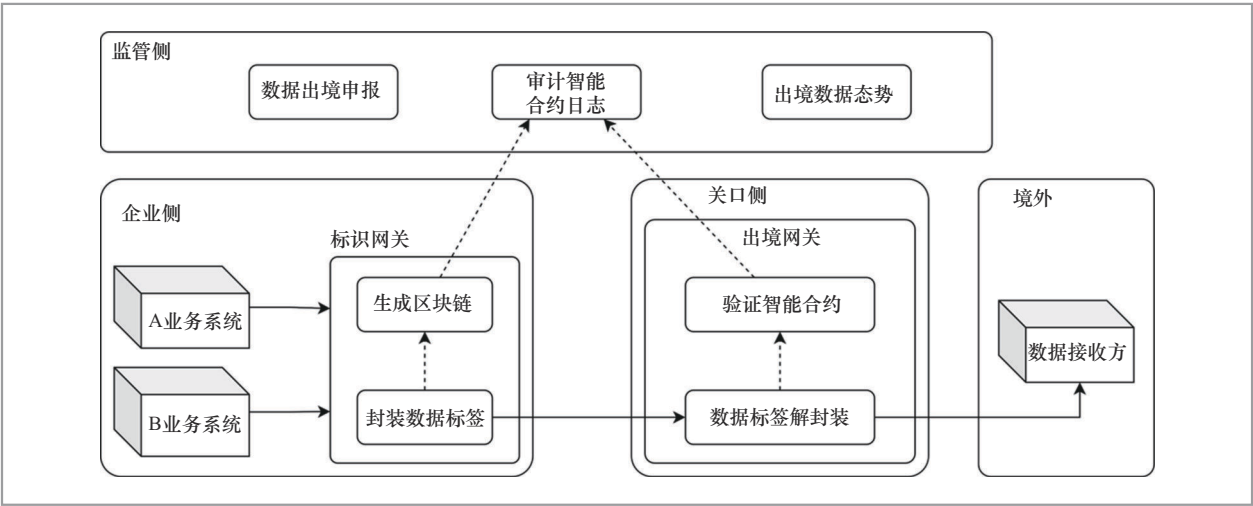


图3 基于智能合约的数据跨境流动总体流程

智能合约的区块链流程。

(a) 创建区块

跨境数据类型：在创建区块时，系统首先定义跨境传输的数据类型，比如文件、数据库、日志数据等。这些数据类型会被打上标签，确保数据在传输过程中可以被识别和验证。

智能合约代码：在区块中初始化智能合约代码，指定数据跨境流动中的规则、合规性要求和各方权利与责任。智能合约以其自动化的执行机制为核心，能够严格依据预定义规则运行，从而有力保障数据传输活动的合法性，并极大提升整个过程的透明度。

(b) 部署区块

区块被添加到区块链网络：在完成区块的创建后，区块会被添加到区块链网络中。每个区块都携带着详细的数据类型描述以及智能合约的具体定义，这些核心要素共同构成了数据流动过程中的每一步都必须严格遵循的运作框架，从而确保数据流转的严谨性、合规性与高效执行。

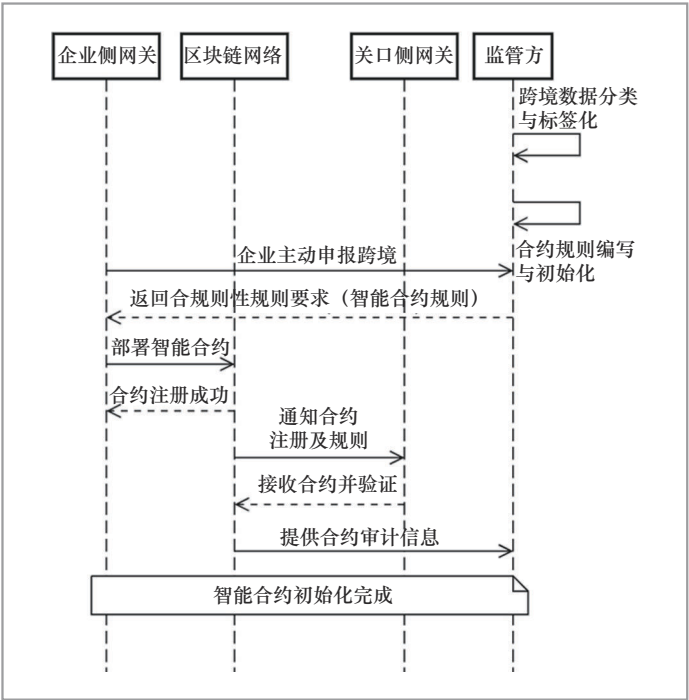


图4 智能合约初始化序列

(c) 执行合约

自动执行合约：一旦数据跨境流动时触发了预定义的条件，智能合约会自动执

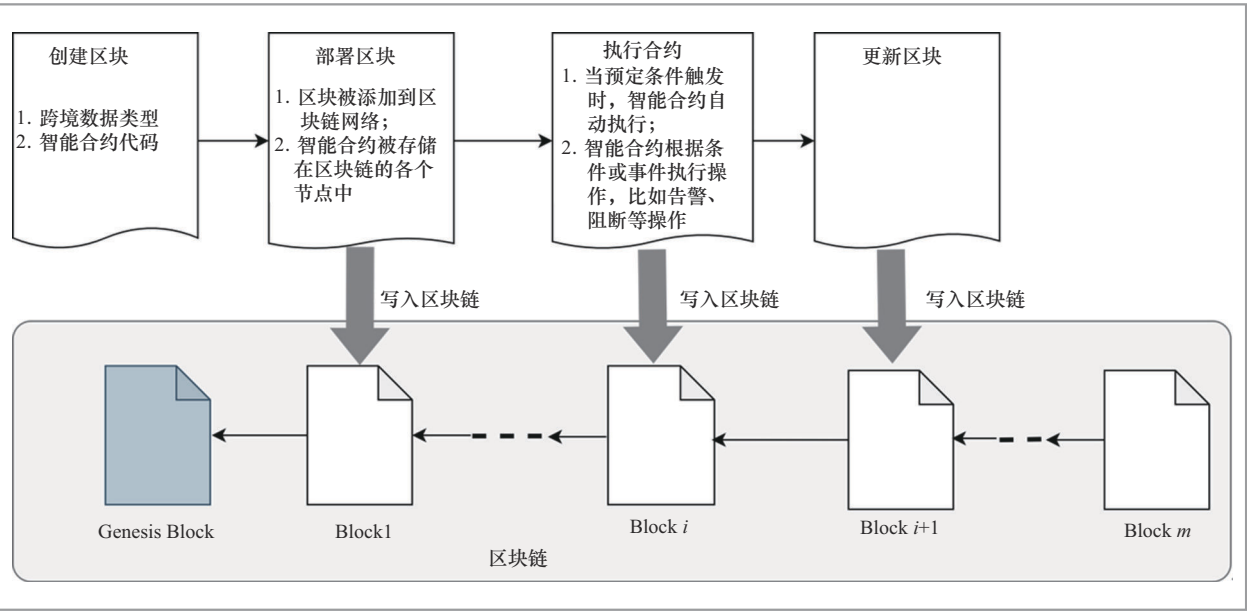


图5 跨境数据流动场景的智能合约的区块链流程

行。这包括检测数据传输的合法性、审计记录的生成、合规性检查等。

事件操作：如果数据流动中出现违反智能合约设定规则的情况，合约会根据条件进行事件操作，比如发出警报或中断数据传输，防止数据非法或不合规的跨境流动。

(d) 更新区块

每当跨境数据流动发生变化或者合约执行完成后，区块链上的区块会进行更新，记录新的数据流动状态或合约执行的结果。这确保了数据跨境流动的全程透明，且数据流动的日志和行为记录极难篡改，便于后续追溯和审计。

(4) 跨境数据流动场景中的应用

合规审查与标签管理：创建区块时，数据会被分配特定的标签，智能合约会根据数据类型、数据源、接收方国家的法律法规等执行相应的合规检查。区块链的极难篡改性确保标签从创建到传输全程不易被更改。

智能化的数据流动控制：合约根据预设条件判断数据是否可以流出，是否需要特定的审批流程等。合约在链上自动执行，减少人工干预，提高效率。

全链路审计和责任追溯：智能合约的执行过程，以及每一次数据的跨境传输，都会被记录在区块链中，生成完整的日志审计信息。如果有不合规行为发生，可以快速追溯到相关责任方。

通过这种机制，智能合约和区块链技术共同为跨境数据流动提供了一个可信、可追溯、自动化的解决方案，有效解决了跨境数据传输中的合规性和安全性问题。

3 结束语

本文探讨了基于智能合约的数据跨境

流动多方互信机制的设计与应用，通过将区块链技术与智能合约相结合，解决了当前跨境数据传输中面临的信任缺失、合规复杂、数据安全等挑战。智能合约的部署不仅能自动执行预定义的合规性规则，还能保证数据传输过程中的透明性和极难篡改性，提升了多方的信任度和监管效率。同时，通过对数据进行标签化处理和合约规则验证，其实现了对数据类型、完整性、合法性的精确控制。

展望未来，随着全球数据流动的日益频繁，跨境数据传输的合规性和安全性将成为各国监管的重要议题。基于智能合约的多方互信机制将进一步拓展其应用场景，不仅限于传统的文件传输，还可以广泛应用于金融、医疗、物联网等领域的数据流动监管。随着技术的进一步发展，智能合约的自动化和智能化程度将持续提升，结合人工智能与大数据分析，未来的跨境数据流动不仅能更好地满足全球各地的合规要求，还能实现更精细的风险评估与动态审计，为国际上的数据流通提供坚实的技术基础，以更好地实现数据价值的全球共享与公平分配。

参考文献：

[1] 方曦, 宋阳. 跨境电商背景下国际贸易的新变化及风险防范机制研究[J]. 商展经济, 2024 (24): 81-84.
FANG H, SONG Y. Research on the new changes and risk prevention mechanisms of international trade under the background of cross border ecommerce[J]. Trade Fair Economy, 2024(24): 81-84.

[2] 郭芳. 产业转型视角下物流产业链与跨境电商融合发展创新研究[J]. 中国商论, 2024, 33 (24): 98-101.

GUO F. Innovative research on integrated development of logistics industry chain and cross-border ecommerce from the perspective of industrial transformation[J]. China Journal of Commerce, 2024, 33(24): 98-101.

[3] 王梓桐. 我国企业数据跨境流动的监管机制研究[D]. 上海: 上海外国语大学, 2023.

WANG Z T. Research on the regulatory mechanism of cross border data flow in Chinese enterprises[D]. Shanghai: Shanghai International Studies University, 2023.

[4] 李兴腾, 任红. 数据要素政策现状及发展趋势[J]. 通信企业管理, 2024(12): 13-15.

LI X T, REN H. Current situation and development trend of data element policies[J]. C-Enterprise Management, 2024 (12): 13-15.

[5] 夏维禹. 法经济学视角下的数据跨境治理观察[J]. 信阳农林学院学报, 2024, 34(4): 11-15.

XIA W Y. Observation on cross-border governance of data from the perspective of law and economics[J]. Journal of Xinyang Agriculture and Forestry University, 2024, 34(4): 11-15.

[6] GENG Q, CHUAI Z A, JIN J. Ensuring consistency in interagency government data exchange: a blockchain-based solution[J]. Proceedings of the Association for Information Science and Technology, 2024, 61(1): 115-126.

[7] GARC A-VALLS M, CHIRIVELLA-CIRUELOS A M. CoTwin: collaborative improvement of digital twins enabled by blockchain[J]. Future Generation Computer Systems, 2024, 157: 408-421.

[8] 张继红, 蔡雨倩. 敏感个人信息跨境流动的国际规制[J]. 广西社会科学, 2023(7): 107-118.

ZHANG J H, CAI Y Q. International regulation of cross-border flow of sensitive personal information[J]. Guangxi Social Sciences, 2023(7): 107-118.

[9] 杨晶, 霍佳鑫. 世界主要国家跨境数据流动的政策法规及其启示[J]. 中国科技资源导刊, 2024, 56(3): 65-71, 93.

YANG J, HUO J X. Policies and regulations of cross border data flow in major counties in the world and its enlightenment[J]. China Science & Technology Resources Review, 2024, 56(3): 65-71, 93.

[10] 朱雅妮. 粤港澳数据跨境规则衔接的指导原则与路径[J]. 法治论坛, 2024(4): 127-140.

ZHU Y N. Guiding principles and pathways for the connection of cross border rules for Guangdong Hong Kong Macao data[J]. Nomocracy Forum, 2024(4): 127-140.

[11] 高松. 数据跨境流通合规治理与技术实践[J]. 中国信息安全, 2023(10): 75-79.

GAO S. Compliance governance and technical practice of cross border data circulation[J]. China Information Security, 2023(10): 75-79.

[12] 曹美荣, 李雅娜. 基于区块链的电子数据存证应用研究[J]. 信息技术与信息化, 2023(12): 177-180.

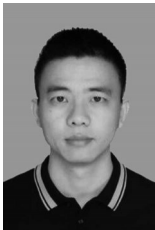
CAO M R, LI Y N. Research on electronic data authentication application based on blockchain[J]. Information Technology & Informatization, 2023(12): 177-180.

[13] 魏际刚, 李苍舒. 建立高效便利的数据跨境流通机制[J]. 中国金融, 2024(22): 46-47.

WEI J G, LI C S. Establish an efficient and convenient cross border data circulation mechanism[J]. China Finance, 2024 (22): 46-47.

[14] MOOSA H, ALI M Z, ALASWAD H, et al. A combined Blockchain and zero-knowledge model for healthcare B2B and B2C data sharing[J]. Arab Journal of

- Basic and Applied Sciences, 2023, 30(1): 179–196.
- [15] 叶华, 曹晓均. 基于区块链技术的医院诚信服务体系应用讨论[J]. 中国数字医学, 2017, 12(28): 88–90.
- YE H, CAO X J. Discussion application of hospital integrity service system based on block chain technology[J]. China Digital Medicine, 2017, 12(28): 88–90.
- [16] 闫青乐, 朱慧君. 基于区块链智能合约的大数据安全[J]. 计算机应用与软件, 2023, 40(12): 332–337.
- YAN Q L, ZHU H J. Big data security based on blockchain smart contract[J]. Computer Applications and Software, 2023, 40(12): 332–337.
- [17] 赵明宇. 基于区块链的安全通信方法研究[J]. 黑龙江科学, 2023, 14(24): 40–44.
- ZHAO M Y. Research on secure communication methods based on blockchain[J]. Heilongjiang Science, 2023, 14(24): 40–44.
- [18] 鲁冰. 区块链技术环境下的征信系统建设研究[J]. 经济动态与评论, 2023(1): 161–173, 196.
- LU B. Research on the construction of credit investigation system under the background of blockchain technology[J]. Economic Dynamics and Commentary, 2023(1): 161–173, 196.
- [19] 武佳. 区块链+地理信息服务探索应用[J]. 测绘与空间地理信息, 2023, 46(11): 66–69.
- WU J. Exploration and application of blockchain+geographic information service[J]. Geomatics & Spatial Information Technology, 2023, 46(11): 66–69.
- [20] 杨叶芬, 何拥军. 基于人工智能和区块链融合的隐私保护技术研究[J]. 信息记录材料, 2023, 24(12): 120–122.
- YANG Y F, HE Y J. Research on privacy protection technology based on artificial intelligence and blockchain fusion[J]. In - formation Recording Materials, 2023, 24(12): 120–122.
- [21] VIDHYA S, SIVA RAJA P M, SUMITHRA R P. Blockchain-enabled decentralized healthcare data exchange: leveraging novel encryption scheme, smart contracts, and ring signatures for enhanced data security and patient privacy[J]. International Journal of Network Management, 2024, 34(5): e2289.
- [22] BOGDANOV A, KHVATOV V, UTESHEV A, et al. Virtual blockchain network: a new way to safe data exchange[J]. Physics of Particles and Nuclei, 2024, 55(3): 394–397.
- [23] ESMAEILZADEH P, MIRZAEI T. Role of incentives in the use of blockchain-based platforms for sharing sensitive health data: experimental study[J]. Journal of medical Internet Research, 2023, 25: e41805.
- [24] 马圆明, 吴东方, 姜心怡. 基于区块链的审计取证研究[J]. 新会计, 2023(12): 12–15.
- MA Y M, WU D F, JIANG X Y. Research on audit evidence based on blockchain[J]. Modern Accounting, 2023(12): 12–15.
- [25] 凡航, 徐葳, 王倩雯, 等. 多方安全计算框架下的智能合约方法研究[J]. 信息安全研究, 2022, 8(10): 956–963.
- FAN H, XU W, WANG Q W, et al. Research on intelligent contract method under the framework of multi-party secure computing[J]. Journal of Information Security Research, 2022, 8(10): 956–963.

作者简介	
	蒋荣（1984-），男，南京中孚信息技术有限公司网络产品研发中心总经理，近年来主要从事网络流量监测、网络安全隔离、数据分类分级、数据安全交换、数据跨境安全监管等技术研究及产业化推广应用工作。
	侯士平（1984-），男，南京中孚信息技术有限公司网络产品研发中心系统部副经理，主要从事网络流量识别与解析、数据安全跨网交换、数据跨境流动监管等技术研究及相关产品建设和推广工作。
	罗圣美（1971-），男，中孚信息股份有限公司高级副总裁，多年从事通信网络、云计算、大数据、数据安全技术研究和产品研发工作，对通信系统和电信业务有深入理解，对数据安全和人工智能有深入研究。
收稿日期: 2025-04-28	