区块链技术视角下的企业金融科技数据安全共享方法研究

姚　元
山钢资本控股（深圳）有限公司　广东　深圳　518000

摘　要：金融科技蓬勃发展的驱动下，企业对数据安全共享的需求日益增长，而区块链技术的出现为数据安全共享提供了一种全新的解决方案。区块链技术作为一种具有去中心化、不可篡改、可追溯等优势的分布式账本技术，日益受到业界关注。在此背景下，如何确保企业在运用区块链技术进行数据共享时，同时确保数据安全成为亟待解决的问题。本文从区块链技术视角，提出了一个融合区块链技术与密码学、大数据分析等技术的综合解决方案。该方案通过构建一个去中心化的安全共享平台，实现数据的加密传输、授权访问和可追溯性，从而确保数据在共享过程中的安全性。

关键词：区块链技术；企业金融科技；共享方法；数据安全

前言

在21世纪信息化快速发展的背景下，金融科技成为推动全球金融行业创新与重构的核心动力。随着金融业务的线上化、智能化，大数据分析、云计算、人工智能等技术的广泛应用，涌现了对数据安全性与可信共享的迫切需求。数据，作为金融科技生态中不容忽视的资产，其透明性、准确性与防篡改特性对于银行、保险、证券等领域日益重要。在此背景下，区块链技术应运而生，其不仅能够为金融数据提供去中心化的存储方式，还可以通过加密算法和共识机制保障数据的隐私性与一致性，大幅度提升数据的安全共享能力，有效防止数据篡改与滥用。

1　区块链技术在企业金融科技数据安全共享领域的应用现状

1.1 区块链技术发展概述

区块链技术起源于比特币，而自2008年比特币白皮书发布以来，已经经历了一个多阶段的演进历程。最初，区块链作为比特币的底层技术，由神秘人物中本聪提出，其主要目的是创建一个去中心化的数字货币系统，解决传统货币体系中的双重支付问题[1]。这一阶段的核心在于通过分布式账本技术确保交易数据不可变性和全节点共识。随着时间的推移，区块链技术初步验证了其在数字货币领域的应用价值，逐渐吸引了行业和学术界的广泛关注。

进入第二阶段，以以太坊为代表的区块链2.0时代来临。开发者开始探索除了加密货币以外的应用场景，如智能合约、去中心化应用（DApps）等，这使得区块链的应用领域得到扩展。智能合约的出现，实质上是一种在满足预定条件时自动执行合同条款的程序，极大推动了区块链技术向更复杂的交易和程序自动化领域拓展[2]。当前，区块链技术已经走进3.0时代，这个阶段被定义为将区块链与其他技术（如人工智能、物联网、大数据等）融合的探索时期。目前，各行各业正积极探索区块链技术的潜在应用，包括供应链管理、医疗保健、金融服务、版权保护、身份验证等。

1.2 企业金融科技数据安全共享现状及挑战

随着金融科技的发展，越来越多的企业开始利用数据驱动业务创新。然而，在这个过程中，数据安全问题也日益凸显。根据IDC的报告，2022年全球企业在金融科技领域的支出达到了1080亿美元，同比增长了12.5%。这些投资主要用于开发和部署金融科技应用，以提高效率、降低成本并改善客户体验。然而，随着数据量的增长和应用的复杂性增加，数据安全问题也变得越来越严重。

一方面，由于缺乏有效的安全防护措施，企业的数据容易受到黑客攻击和内部人员的恶意行为的威胁。例如，在2017年，美国信用报告巨头艾科瑞（Equifax）遭受了一次严重的网络攻击，导致约1.43亿用户的敏感信息泄露。另一方面，不同国家和地区对于数据保护有着不同的法律法规要求。企业在进行跨境数据共享时，需要遵守当地的法律法规，否则可能会面临严重的法律后果。例如，在欧洲经济区（EEA），企业需要遵守GDPR（通用数据保护条例）的规定，对涉及欧盟公民的数据进行保护。

1.3 区块链技术在企业金融科技数据安全共享中的优势

区块链技术在企业金融科技数据安全共享中的优势主要体现在增强的数据安全和完整性以及高效的数据一致性和透明度两方面。通过利用区块链技术，企业能够

构建一个透明、可信、互联的金融科技生态系统。

1.3.1 增强的数据安全和完整性

区块链技术提供了一种去中心化的数据管理框架，其内置的加密特性使得金融数据在传输和存储过程中保持高度安全。每笔交易都要通过网络节点的共识机制来验证，并以加密的形式存储在不可篡改的区块中。一旦数据被写入区块链，要改变它几乎是不可能的，因为这需要同时改变网络中大多数节点上的数据[3]。这种安全性质极大地降低了数据泄露和篡改的风险。

例如，分布式账本的不可篡改特性对于确保交易记录的永久性至关重要。通过使用散列函数在每一个区块中存储前一个区块的哈希值，链上每个区块与前后区块之间形成了不可更改的链条。如果试图更改一个区块中的信息，这将破坏整个链上从该点开始的区块的完整性，且这种变动会被网络上的其他节点迅速检测出来，从而保护数据不被未授权篡改。

1.3.2 高效的数据一致性和透明度

在传统金融系统中，信息在不同机构间的共享往往需要复杂和耗时的协调过程，而区块链使这一过程实现自动化和简化。区块链上的共识机制确保所有授权参与者都能看到一个唯一、统一版本的真实记录，从而减少了数据不一致的问题。

例如，智能合约是基于区块链的自动化执行合同的程序，它可以在预设条件达成时自动执行合同条款，无需中介机构。智能合约在金融中的应用，比如自动化的债券支付和保险索赔处理，提升了操作效率和准确性。由于智能合约放在区块链上，其执行是透明的，并且能确保数据的一致性[4]。智能合约还能将合同关系代码化，显著减少了金融交易过程中的失误和不一致性。

2 基于区块链技术的企业金融科技数据安全共享方法

区块链技术以其独特的去中心化、数据不可篡改的特性，为金融科技数据的安全共享提供了新的解决方案。然而，单纯依赖区块链技术仍存在一些局限性，如数据处理、隐私保护等。因此，融合区块链技术与其他相关技术，如密码学和大数据分析，就显得尤为重要。通过多种技术的融合，企业可以在更好地保障金融科技数据安全共享的同时，满足业务需求。

2.1 数据安全共享流程与机制

为了实现基于区块链技术的企业金融科技数据安全共享，一个完善的数据安全共享流程与机制是必不可少的，其应该包括数据生成阶段、共享阶段以及处理阶段。在数据的生成阶段，企业需要对敏感数据进行加密处理，确保数据在传输和存储过程中的安全性。在数据的共享阶段，企业需要通过授权访问控制来限制不同角色的用户对数据的访问权限。而为了实现数据的可追溯性，还需要将每次数据访问操作记录在区块链上，以便后续的审计和监控。在数据的处理阶段，企业可以利用大数据分析技术对接入区块链的金融数据进行实时监控和分析，从而实现数据的实时处理和智能决策。通过这样一个完善的数据安全共享流程与机制，企业可以在保障数据安全的同时，充分利用区块链技术的优势，为企业的金融科技业务提供有力支持。

2.2 去中心化的安全共享平台构建

基于数据安全共享流程与机制，对于企业金融科技数据安全的共享方法，需要构建一个去中心化的安全共享平台。这个平台将采用区块链技术作为底层架构，通过去中心化的方式实现数据的存储、传输和访问控制。

2.2.1 数据加密传输

为了确保数据在传输过程中的安全性，企业相关技术人员可以采用密码学中的加密技术对数据进行加密。具体来说，可以使用对称加密算法（如AES）或非对称加密算法（如RSA）对数据进行加密。在数据传输过程中，发送方使用接收方的公钥对数据进行加密，接收方使用自己的私钥对数据进行解密。这样，即使数据在传输过程中被截获，攻击者也无法获取到原始数据的内容。

而为了提高数据传输的效率，还可以考虑使用零知识证明等密码学技术。零知识证明是一种允许一方证明给另一方自己知道某个信息，不需要透露任何其他信息的技术。通过零知识证明，企业方面可以在不泄露原始数据的情况下，实现数据的验证和共享。

2.2.2 授权访问控制

在区块链网络中，每个参与者都有一个唯一的身份标识，即公钥。通过公钥，即可以确定参与者的身份，并对其进行授权访问控制。具体来说，企业领导可以通过区块链网络权限为每个参与者分配一个角色，如管理员、普通用户等，并为每个角色设置相应的权限。这样，只有具有相应权限的参与者才能访问特定的数据[5]。

而为了实现授权访问控制，则可以采用基于角色的访问控制（RBAC）模型。在RBAC模型中，权限与角色相关联，而不是直接与用户相关联。这样，当用户的角色发生变化时，只需要修改其角色对应的权限即可，而无需重新分配权限。不仅如此，RBAC模型还支持继承和委派等功能，可以实现更灵活的访问控制。

2.2.3 数据可追溯性

在区块链网络中，所有的交易记录都会被记录在区块链上，并形成一个不可篡改的数据链。这意味着，一

旦数据被写入区块链，就无法被修改或删除。因此，可以通过查看区块链上的交易记录，实现对数据的可追溯性。具体来说，平台可以为每个数据访问操作生成一个唯一的交易记录，并将其写入区块链。这样，相关管理人员可以通过查询区块链上的交易记录，找到数据的来源和访问历史[6]。同时，由于区块链上的数据是不可篡改的，这保证了数据的真实性和完整性。

然而，仅仅依靠区块链技术并不能完全满足企业在数据安全共享方面的所有需求。在某些场景下，企业可能需要借助大数据分析技术来实现数据的实时处理和智能决策。例如，通过对交易数据进行实时统计和分析，可以发现潜在的风险和异常行为；通过对客户行为数据进行分析，可以为客户提供更加个性化的服务等；而通过将分析结果反馈到区块链网络中，也可以帮助企业优化业务流程和提升服务质量。

3 区块链技术背景下推动企业金融科技数据安全共享的建议

3.1 建立完善的区块链技术标准和规范

为了推动企业金融科技数据安全共享，首先需要建立一个统一、完善的区块链技术标准。这个标准应该包括区块链技术的基本框架、数据格式、接口规范、安全性要求等方面的内容。通过制定统一的标准，可以使各个企业在开发和使用区块链技术时有一个共同的参考依据，从而提高整体的应用效果。但是，由于区块链技术在金融领域的应用涉及到大量的敏感数据，如个人隐私、交易记录等。因此，需要制定一套完善的区块链技术安全规范，包括数据加密、访问控制、审计跟踪等方面的要求。这些规范应该具有可操作性，能够指导企业在实际工作中进行安全防护。

除此之外，为了确保区块链技术在金融领域的合规应用，还需要建立一个有效的监管机制。这个机制应该包括对区块链技术的研发、应用、运营等各个环节的监管，以及对违反规定的企业和个人进行惩罚的措施。通过建立监管机制，可以有效地防止区块链技术被用于非法目的，保障金融数据的安全。

3.2 加强区块链与企业金融科技的融合创新

区块链技术因其独特的特点，非常适合应用于金融领域。企业应该积极探索将区块链技术应用于金融业务的各个场景，如支付结算、供应链金融、跨境汇款等，以提高金融服务的效率和安全性。

而为了推动企业金融科技数据安全共享，企业应该加大对区块链技术的研究与开发力度。这包括建立专门的技术研发团队，引进优秀的技术人才，以及投入足够的研发资金等。通过加强内部研究与开发，企业可以更好地掌握区块链技术的发展动态，为实际应用提供技术支持。同时，企业还应该积极参与到与其他企业技术研发的合作中，共同研究和解决区块链技术在实际应用中遇到的问题。

结论

综上所述，通过建立去中心化的数据共享平台，利用区块链的不可篡改特性，可以有效保障数据的安全性和真实性。而伴随着区块链技术的不断发展和完善，其将在企业金融科技数据安全共享领域发挥越来越重要的作用。但是在这个过程中，也需要注意区块链技术的实施成本和监管问题，需要不断进行研究和探索，以实现最佳的应用效果。

参考文献

[1]雷莹莹,廖小琴.区块链技术的价值审思与实践路径探究[J/OL].大连理工大学学报(社会科学版),1-7[2023-12-12].

[2]顾晔,陈甜妹,徐天天.基于区块链技术的数据中台安全性提高研究与分析[J].制造业自动化,2023,45(11):26-30.

[3]聂朝冬.基于区块链的科技数据共享平台关键技术研究[J].长江信息通信,2023,36(10):29-31.

[4]施亚东.基于区块链技术的企业金融科技数据安全共享方法[J].产业与科技论坛,2023,22(12):41-43.

[5]周倩霞.区块链技术在供应链金融中的应用研究[D].广州大学,2022.

[6]龚强,班铭媛,张一林.区块链、企业数字化与供应链金融创新[J].管理世界,2021,37(02):22-34+3.