 DOI: https://doi.org/10.12349/iser.v4i4.1679

Design and Research on Secure Data Transmission Scheme Based on Blockchain Technology

Daoli Qiu

School of Information and Control Engineering, China University of Mining and Technology, Xuzhou, Jiangsu, 221000, China

Abstract

The new paradigm of blockchain technology provides new possibilities for data transmission and information exchange, but with it comes potential threats and risks. Therefore, a comprehensive system architecture has been proposed that integrates blockchain technology and smart contracts to ensure the security and credibility of data transmission. We also emphasized the key importance of security measures such as identity verification and authorization, data tampering prevention, and dual payment prevention, and discussed the necessity of risk management strategies to reduce system vulnerability.

Keywords

blockchain technology; security data; transmission

基于区块链技术的安全数据传输方案设计研究

仇道理

中国矿业大学信息与控制工程学院，中国 · 江苏 徐州 221000

摘　要

区块链技术的崭新范式为数据传输和信息交换提供了新的可能性，然而，随之而来的是潜在的威胁和风险。因此，提出了一个完善的系统架构，融合了区块链技术和智能合约，以确保数据传输的安全性和可信度。我们还强调了身份验证和授权、防止数据篡改、防止双重支付等安全性对策的关键性，并讨论了风险管理策略的必要性，以降低系统的脆弱性。

关键词

区块链技术；安全数据；传输

1 引言

在当今数字时代，数据的安全传输成为企业、政府和个人的首要关注点。随着信息技术的快速发展，传统的数据传输方法面临着日益复杂的威胁和挑战，如数据泄漏、篡改、双重支付等问题。因此，为了确保数据的机密性、完整性和可用性，需要寻求新的、更加安全的数据传输解决方案。

2 区块链技术基本理论

区块链技术的核心本质在于它是一种去中心化的分布式账本系统。它的基本构建单元是区块，每个区块包含了一定时间内的交易数据以及前一个区块的哈希值，从而形成了一个线性的链式结构。这种链式结构具有高度的透明性和不可篡改性，因为一旦一个区块被添加到链上，它几乎不可能被修改。区块链的去中心化性质意味着没有中央权威机构来控制整个系统，而是由网络中的多个节点共同维护和验证交易的有效性，从而确保了系统的安全性和可信度 [1]。

区块链的分布式共识机制是其关键特征之一。这种机制用于确保所有参与节点对交易的顺序和有效性达成一致意见，从而避免了双重支付等问题。最著名的共识机制是工作量证明（ProofofWork，PoW）和权益证明（ProofofStake，PoS）。在 PoW 中，节点通过解决复杂的数学问题来争夺区块的生成权，而在 PoS 中，区块生成权取决于节点持有的加密货币数量。这些共识机制确保了网络的安全性和稳定性，并防止了恶意行为。

区块链技术不仅用于加密货币交易，还可以支持去中心化应用（DApps）和智能合约。去中心化应用是构建在区块链上的应用程序，它们不依赖于单一的中央服务器，而是由智能合约控制其逻辑和运行。智能合约是自动执行的合同，其中的规则和条件被编码为代码，并在区块链上执行。这使得无需中介机构，便可以实现各种自动化的交易和合同执行，从而降低了成本并提高了可信度。

【作者简介】仇道理（2002–），男，中国山东聊城人，在读本科生，从事电子信息与通信工程研究。

3 基于区块链技术的安全数据传输方案设计

3.1 硬件设计

基于区块链技术的安全数据传输硬件结构如图 1 所示。

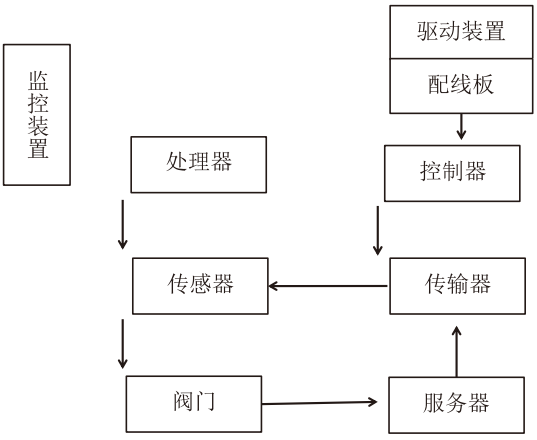

图 1 基于区块链技术的安全数据传输硬件结构示意图

硬件设计的核心之一是集成安全硬件模块，以加强数据传输的保密性和完整性。这些安全硬件模块可以包括硬件加密引擎、安全存储模块、随机数生成器等。硬件加密引擎用于对传输的数据进行加密和解密操作，确保数据在传输过程中不被窃取或篡改。安全存储模块用于存储敏感信息，如密钥和证书，以免受到未经授权的访问。随机数生成器可用于生成随机数，以增强加密操作的随机性，从而提高系统的安全性。

数据传输方案的硬件设计还需要考虑性能因素，以确保高效的数据传输。这包括选择适当的处理器、内存、网络接口和存储设备，以满足实际传输需求。高性能硬件可以提高数据传输的速度和响应时间，从而降低了延迟和数据包丢失的风险。此外，硬件设计还应考虑可扩展性，以便在需要时能够轻松扩展系统的容量和性能 [2]。

硬件设计不仅仅关乎性能和功能，还需要考虑物理安全性。这包括选择安全的硬件存放位置、采用硬件封装和外壳，以及实施物理访问控制措施，以防止未经授权的物理访问和潜在的硬件攻击。物理安全措施对于保护硬件中存储的敏感信息以及确保硬件的可靠性和稳定性至关重要。

3.2 软件设计

3.2.1 架构设计

在软件设计的初期阶段，需要制定合适的架构，这是软件系统的骨架和基础。架构设计包括选择适当的软件模式和架构风格，以及确定组件之间的交互方式。一种常见的方法是采用分层架构，将系统划分为不同的层次，如用户界面层、业务逻辑层和数据访问层。此外，架构设计还应考虑性能、安全性、可扩展性和可维护性等因素，以确保系统能够满足其预期的功能和性能要求。

3.2.2 模块化设计

模块化设计是将系统划分为独立的模块或组件，每个模块负责执行特定的任务或功能。这种设计方法有助于简化开发过程，提高代码的可读性和可维护性，并促进团队协作。模块应该具有清晰的接口和功能，以便于测试和重用。在模块化设计中，模块之间的依赖关系需要明确定义，以确保模块的相互协作是有效和可靠的。模块化设计还使得系统更容易进行单元测试和集成测试，从而提高软件质量。

3.2.3 数据设计和算法选择

软件设计还包括数据设计和算法选择，这涉及如何存储、管理和处理数据以满足应用程序的需求。在这一阶段，需要选择适当的数据结构和数据库系统，以确保数据的有效性和一致性 [3]。此外，需要选择合适的算法来执行各种操作，如搜索、排序、过滤和计算。算法的选择和优化对于软件的性能至关重要，因此需要仔细权衡不同算法的复杂性和效率。数据设计和算法选择应与架构设计和模块化设计协同工作，以确保整个系统的一致性和协调性。

3.3 数据传输过程

3.3.1 数据加密和解密

数据传输过程中的数据加密和解密是确保数据隐私和安全的关键环节。在数据发送端，原始数据将通过加密算法转化为密文，以确保只有授权的接收端可以解密和读取数据。加密过程通常涉及使用加密密钥，这个密钥只有发送和接收双方共享，并且应该被严格保护。接收端使用相同的密钥来解密接收到的数据，以还原原始信息。流行的加密算法包括对称加密算法（如 AES）和非对称加密算法（如 RSA）。正确实施数据加密和解密确保数据在传输过程中免受窃取或篡改的风险。

3.3.2 数据验证和确认

数据验证和确认是确保数据传输的完整性和准确性的重要步骤。在接收端，接收到的数据需要经过验证，以确保其在传输过程中未被篡改。这可以通过使用散列函数来生成数据的摘要，并将摘要与传输过程中接收到的数据进行比较来实现。如果摘要匹配，就表明数据完整且未被篡改。此外，还可以使用数字签名来验证数据的真实性，数字签名使用发送端的私钥进行签名，接收端使用发送端的公钥来验证签名的有效性。数据验证和确认确保数据在传输过程中的可靠性，防止数据损坏或篡改引发的问题。

3.3.3 交易管理

交易管理是数据传输过程中的关键组成部分，特别是在基于区块链技术的系统中。在这一阶段，发送方和接收方之间的数据交换被记录在分布式账本中，以确保交易的可追溯性和可证明性。每个交易都包含了必要的信息，如发送方、接收方、交易金额和时间戳等。交易需要遵循智能合约规则，这些规则事先编写并嵌入区块链网络中。交易管理还包括网络中节点的共识过程，确保只有有效的交易被添加到区块链上，从而维护系统的安全性和可信度。区块链技术的不可篡改性保证了交易的历史记录不会被篡改或删除，这有助于建立可信的交易历史和数据传输的安全性。

3.4 安全性和可信度机制

在基于区块链的安全数据传输方案中，确保安全性和可信度是至关重要的。这涉及多个机制和措施来保护数据和交易的完整性，防止未经授权的访问，以及确保数据传输的可信度。安全性和可信度机制通常包括数据加密、身份验证、数字签名、共识算法等，这些机制共同确保了数据传输的安全和可靠性，同时降低了潜在的风险。

3.4.1 身份验证和授权

身份验证和授权机制用于确保参与数据传输的各方都是合法和授权的。通常，这包括使用公钥基础设施（PKI）来验证参与者的身份。每个参与者都拥有自己的公钥和私钥，公钥用于验证身份，私钥用于数字签名和授权。只有通过身份验证的参与者才能参与数据传输和交易，并且只有在获得授权的情况下才能执行特定操作。这种身份验证和授权机制确保了系统的合法性和可信度。

3.4.2 防止数据篡改

数据传输过程中，防止数据篡改是至关重要的。一种常见的方法是使用哈希函数来生成数据的摘要，并将摘要附加到数据中。接收端可以再次计算数据的摘要，并与发送端发送的摘要进行比较，以确保数据在传输过程中未被篡改。此外，数字签名也用于验证数据的真实性，发送方使用其私钥对数据进行签名，接收方使用发送方的公钥验证签名的有效性。这些机制协同工作，确保数据在传输过程中的完整性。

3.4.3 防止双重支付

在基于区块链的系统中，防止双重支付是一个重要的安全性机制。这种机制确保同一笔交易不会被发送方多次执行，以防止欺诈行为。通常，区块链系统使用共识算法来确保只有一笔交易被确认和添加到区块链上。一旦一笔交易被确认，系统会阻止任何尝试重复执行相同交易的尝试，从而防止双重支付问题的发生。这种机制提高了数据传输的可信度，特别是在金融和支付应用中。

4 安全性分析和风险管理

4.1 攻击威胁分析

当设计基于区块链技术的安全数据传输方案时，首先需要进行攻击威胁分析，以确保系统的健壮性和安全性。以下是关于攻击威胁的分析：

①双重花费攻击：区块链上最常见的攻击之一是双重花费攻击，其中攻击者试图使用相同的数字资产进行多次交易。设计方案时需要引入足够的确认机制和智能合约以防范此类攻击，并确保交易历史的透明性。②共识算法攻击：攻击者可能试图攻击区块链的共识算法，以篡改交易历史或分散式账本。这需要采用强大的共识机制，如 Proof of Work（PoW）或 Proof of Stake（PoS），并不断监控网络以侦测任何异常活动。③网络层攻击：区块链网络可能受到分布式拒绝服务（DDoS）攻击，干扰数据传输和共识过程。防范这种攻击需要网络层的安全防护和备份节点以确保系统的连续性。在设计基于区块链的安全数据传输方案时，必须综合考虑这些攻击威胁，并采取相应的安全措施，以确保数据传输的保密性、完整性和可用性。此外，还应考虑身份验证和访问控制措施，以限制未经授权的访问和数据泄露 [4]。

4.2 安全性对策

在设计基于区块链技术的安全数据传输方案时，以下是一些关键的安全性对策，需要详细分析：①加密和隐私保护：使用强加密算法，如 AES 或 RSA，来保护数据的机密性。确保数据在传输和存储过程中都受到加密保护。考虑使用零知识证明或同态加密等隐私保护技术，以在不暴露数据内容的情况下进行验证和计算。②智能合约审计：对智能合约进行全面的安全审计，以识别潜在的漏洞和风险。可以借助安全审计工具和专业审计团队来进行审查。实施合约升级机制，以允许在发现漏洞或需要改进时安全地更新智能合约。③身份验证与授权：实施强制身份验证，确保只有经过授权的用户或节点可以参与数据传输和共识过程。

4.3 风险管理策略

首先，需要建立一个全面的风险识别和评估流程，以识别潜在的风险因素。这包括对攻击威胁、数据泄露、合规性问题等进行评估。一旦风险被识别，就可以根据其严重性和概率来优先考虑，以确定应该采取什么样的措施。

基于识别的风险，需要制定风险应对和缓解策略。这包括制定计划来应对潜在的攻击，保护数据的完整性和可用性，确保合规性。这些策略可能包括定期的安全审计、应急响应计划、备份和恢复机制的建立，以及定期更新的安全培训和意识提高活动，以确保团队和用户能够妥善处理风险情况。

5 结语

总之，基于区块链技术的安全数据传输方案的研究不仅对于数据安全和隐私保护具有重要意义，还为未来的数据传输和信息交换提供了新的范式。然而，我们也必须认识到区块链技术的不断发展和演进，以及不同应用场景的独特性，需要不断调整和优化方案。我们希望本研究可以为进一步的研究和实际应用提供有益的参考，并为构建更加安全、可信的数据传输生态系统做出贡献。

参考文献

[1] 刘文娟.基于区块链技术的档案信息化与数据安全管理[J].兰台内外,2023(24):14-15+21.

[2] 薛中伟.基于区块链技术的工控数据安全传输系统设计[J].计算机测量与控制,2022,30(4):161-164.

[3] 张伟,丁朝晖,杨国玉,等.基于区块链和数字签名技术的智慧电厂数据安全传输系统研究与设计[J].电力信息与通信技术,2021,19(7):33-39.

[4] 陈志涛,金波,杨小东.基于区块链技术的数据安全传输方案研究[J].电子测试,2020(4):79-80+65.