一种基于区块链的票据可信管理方案

陈辛迪[1],沈苏彬[2]
(1. 南京邮电大学 物联网学院,江苏 南京 210003;
2. 南京邮电大学 通信与网络技术国家工程研究中心,江苏 南京 210003)

摘 要:在传统票据市场中,以电子商业汇票系统为核心的集中管理模式导致信息不对称、人工操作失误、监督溯源效率低等问题频发,因此,票据交易的真实性、安全性存疑。针对以上问题,该文利用区块链技术去中心化、不可篡改、可溯源的特性,提出了一种基于区块链的票据交易可信管理方案。通过设计去中心化的数据结构和验证机制,实现了交易合同的去中心化可信存储,确保了交易背景的真实性;并采用去中心化的验证方式建立了票据交易真实性和完整性验证机制,实现了交易数据的可信验证;此外,通过结合区块链技术和可信执行环境,建立节点身份远程验证机制,实现了节点身份信息的去中心化真实性验证,确保了参与方身份真实性。最后,采用 Hyperledger Fabric 区块链平台对方案进行了仿真实现和测试,结果表明,该方案实现了票据交易合同和签发的可信管理。

关键词:区块链;票据交易;可信管理方案;身份验证;Hyperledger Fabric
中图分类号:TP309.2 **文献标识码**:A **文章编号**:1673-629X(2024)11-0065-08
doi:10.20165/j.cnki.ISSN1673-629X.2024.0219

A Bill Trusted Management Scheme Based on Blockchain

CHEN Xin-di[1], SHEN Su-bin[2]
(1. School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. National Engineering Research Center on Communication and Networking, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: The conventional bill market faces challenges like information asymmetry, human errors, and low supervision efficiency due to its centralized management model centered on the electronic commercial bill system. Consequently, doubts arise regarding the authenticity and security of bill transactions. In response, we propose a trustworthy management solution for bill transactions based on blockchain technology. Leveraging the decentralized, tamper-resistant, and traceable nature of blockchain, the scheme designs decentralized data structures and verification mechanisms, which enables decentralized and trustworthy storage of transaction contracts, ensuring the authenticity of transaction backgrounds. Furthermore, a decentralized verification approach establishes a mechanism to verify the authenticity and integrity of bill transactions, facilitating trustworthy validation of transaction data. Additionally, by integrating blockchain technology with trusted execution environments, a remote verification mechanism for node identity is established, ensuring decentralized authentication of participant identities. Simulation implementation and testing of the proposed scheme using the Hyperledger Fabric blockchain platform validate its efficacy in achieving trustworthy management of bill transaction contracts and issuance.

Key words: blockchain; bill transaction; trusted management scheme; identity verification; Hyperledger Fabric

0 引 言

随着数字经济的迅速发展,电子票据业务呈现出持续增长趋势。2023 年票据市场业务总量突破 200 万亿元大关,企业户数和用票金额均创历史新高。然而,传统的票据交易存在一系列不可忽视的问题:

(1)中心化模式易受恶意攻击或单点故障影响,少数中心化机构维护全部交易数据信息,导致交易过程缺乏透明度,数据共享困难[1]。

(2)人工失误或者违规操作可能导致交易数据的丢失或篡改。金融机构为了追求利润放宽审核标准,仅仅进行形式上的审核,票据真实性存疑[2]。例如,某银行因违规审核背景与非法中介合作,造成 13 亿元的

收稿日期:2024-03-25 **修回日期**:2024-07-26
基金项目:国家重大基础研究计划(973)项目子课题(2011CB302903);江苏省产学研联合创新资金项目(BY2013095108)
作者简介:陈辛迪(2000-),女,硕士研究生,通讯作者,研究方向为区块链;沈苏彬(1963-),男,博导,研究员,CCF 高级会员(E200005482S),研究方向为物联网及其应用、未来网络及其应用。

严重金融损失[3]。

(3)缺乏统一的包含票据总体信息的平台,各个机构间独立存储票据信息,导致整个票据交易结构复杂,涉及多个层级[4],交易周期漫长,违规交易往往无法及时发现,监管溯源难,成本高。

区块链技术具有去中心化、不可篡改、公开透明、可溯源等特点,能有效解决票据交易管理中存在的信任和安全问题。目前,该技术已被广泛应用于国际贸易结算、保险服务、数字资产等领域[5],区块链技术在金融领域的实施将减少对第三方的依赖,降低交易成本,提升交易平台的安全性和透明度[6]。

针对以上问题,该文利用区块链技术的去中心化、不可篡改、公开透明、可追溯等特点,提出了一种基于区块链的票据可信交易管理方案,主要优势包括:(1)使用公用账本实现交易信息透明和跨企业信任;(2)利用智能合约自动化交易审查,降低中介风险和成本;(3)通过哈希链结构确保数据不可篡改性和可追溯性。该方案首先确保票据交易合同在区块链上的真实性和完整性,避免交易数据的篡改。其次,针对交易过程提出了真实性和完整性验证机制,保证了交易数据的可靠性。此外,提出了一种去中心化的节点身份真实性验证方法,结合可信执行环境(Trusted Execution Environment,TEE)实现节点的身份信息存储与验证,防止了恶意节点的冒充,保证了节点身份信息的真实性。最后,在 Hyperledger Fabric 平台进行仿真实验,验证了方案的基本可行性。

1 相关工作和问题分析

近年来,区块链技术在票据交易领域受到了广泛关注和研究。学术研究方面,文献[7]通过运用区块链技术解决了第三方中介参与票据交易带来的风险问题,实现了货权单据的去中心化所有权。文献[8]提出企业可以通过区块链票据平台将转让交易相关的合同及贸易背景信息进行上链存证,关键在于统一存证信息的标准。文献[9]分析并论述了区块链技术与医疗电子票据结合的优势,从区块链医疗电子票据支撑系统、业务系统和展示服务系统三个方面分析其技术架构,实现了医疗电子票据的可信流转。文献[10]通过构建财务共享服务平台与内部和外部联盟链网络的耦合架构,有效解决了票据管理的数据安全风险问题,并实现了采购业务的区块链票据可信管理。Wang 等人[11]对智能合约进行编码,实现了基于区块链的电子票据交易服务模型,包括票据发行、转让、贴现等功能。文献[12]采用多方安全计算技术对区块链票据交易平台的参与节点进行身份验证,以增强参与方的安全性。Chen 等[13]提出了区块链票据应用数据管理机制,包括数据注册、验证、存储流程,并通过证书管理确保了数据访问权限的合法性。黄玉清等人[14]通过数字身份管理加强了医疗电子票据的身份验证。

金融实践方面,赣州银行的区块链票据平台提供了高效便捷的融资功能,利用区块链的不可篡改性和时间戳,确保了融资账本的真实性[15]。美的集团通过公钥基础设施实现了参与者的身份认证和资产证明,同时保障了票据交易记录的不可篡改性[16]。央行于 2018 年推出的区块链票据交易实验性平台,采用了同态加密和零知识证明技术,引入非交互式密钥来生成交易签名和身份证明[17],进一步提升了参与方身份真实性。农行利用区块链技术重构票据承兑、流转和托收业务流程,实现了去中心化的出票,使用不可篡改的时间戳记录数据,提供了信息追溯的有效途径,增强了数据的可信度[18]。

综合上述分析,考虑到票据交易场景涉及节点的数据访问和交易操作的权限控制,公有链虽强调去中心化和匿名性,但可能无法满足票据交易中的数据隐私和交易保密性要求。因此,不适合照搬适用于比特币交易系统的公有链方案。此外,票据数据的可信存储和验证不仅包括交易背景数据源的真实性和可信性,还需考虑交易过程的真实性和完整性。现有方案尚未提供可靠的票据交易背景真实性验证方法,无法保证数据源的真实性和可靠性。为此,该文借鉴了现有的许可链票据交易平台[19]研究,提出了一种基于超级账本的票据交易方案,提供了一种可靠的票据交易背景真实性验证方法,增强了数据源的真实性和可靠性。

交易过程真实性指票据交易各个环节,包括交易申请、验证、确认等步骤,需要确保每一步的操作和记录都是真实可信的。交易过程完整性确保票据信息、交易金额和交易时间等关键信息未被篡改或损坏,维护数据的完整性。引入第三方平台[20]作为区块链票据的生产者,负责维护票据数据的真实性和有效性。然而,第三方平台可能面临安全威胁,其安全性若未经验证可能影响整个系统的可信度。

在传统票据交易中,身份验证依赖于中心化机构,通过查验身份证明文件来确保参与方的真实性。但在去中心化环境下,这种方法可能存在身份隐私数据泄露的风险,因此不再适用。在区块链去中心化环境中,身份验证面临限制,复杂的加密算法可能需要大量的计算资源,增加验证过程的复杂度和开销。引入复杂的密钥交互过程是常见的身份验证方法,但直接对交易进行加密可能导致其他节点无法验证交易的正确性,从而使交易作废。

经总结,现有研究和应用存在以下问题:(1)尚未

明确提出将区块链技术应用于票据交易背景信息的上链存证和真实性验证的方案,无法有效确保数据源的真实性和完整性;(2)虽然区块链技术能确保交易记录的不可篡改性,但忽略了交易合同等关键信息的完整性验证,现有方案并不完善;(3)传统的身份信息验证方案在去中心化环境下效果有限,部分方案依赖于复杂的密钥和算法,影响身份信息保密性且增加了节点的计算负担。综上,该文提出了一种基于区块链的票据可信管理方案,拟解决以下的技术问题:

交易合同的可信存储和验证。交易合同包含交易方、交易金额、交易时间等相关信息的数据集合,其真实性指交易合同信息反映了交易双方之间的真实意图和行为,是建立交易方之间信任的基础。同时,完整性即交易合同中数据未被篡改。该文考虑通过建立可信的交易合同上链数据结构,将交易合同的哈希值作为唯一标号上传至区块链,通过提取哈希值比对实现对交易合同的可信验证,确保其来源的真实性。

交易过程的真实性和完整性验证。真实性要求票据交易各个环节,如交易申请、验证、确认等步骤,都是真实可信的。完整性则确保票据信息、交易金额、交易时间等关键数据未被篡改或损坏,该文考虑建立多重验证机制,通过多个独立的验证步骤,如用户身份验证、交易合法性验证和交易有效性验证等,通过建立票据交易可信管理的区块结构、区块链结构,并基于智能合约验证算法,实现交易的真实性和完整性验证,确保交易方的身份和操作的真实性和完整性。

参与方身份真实性验证。Fabric 平台通过成员管理服务(Membership Service Provider,MSP)管理和验证节点身份与权限,MSP 使用由证书颁发机构(Certificate Authority,CA)颁发的数字证书来验证和识别区块链网络中的节点身份。结合可信执行环境的远程认证机制,该文提出一种新的远程身份真实性验证方法,以实现节点身份的去中心化真实性验证,确保节点身份真实性,有效防止恶意节点的冒充。

2　方案设计

本节构建了区块链票据交易系统模型,该系统的主要目的是实现票据交易合同的可信存储、交易过程的真实性和完整性验证功能。接着描述了交易操作的可信表示、交易合同上链存储结构、交易真实性和完整性验证机制以及区块创建及验证流程。

2.1　系统模型

本模型基于 Fabric 许可链平台进行构建,区块链票据可信交易管理模型如图 1 所示,包括三类节点:客户端(Client)、对等节点(Peer)和排序服务节点(Ordering Service Node)。客户端代表参与交易的企业用户,通过连接对等节点提交交易提案,并与排序服务通信请求广播。对等节点包括银行等金融机构,作为验证节点,负责验证交易提案的有效性。智能合约定义一组验证条件,这些条件决定了一个交易何时被视为有效。作为记账节点,对等节点根据验证条件确保验证阶段的一致性,并更新账本。排序服务节点接收来自客户端的交易提案及响应,按照共识算法对交易进行排序,并生成区块,广播至其他排序节点。节点间通过 gossip 协议同步账本状态。

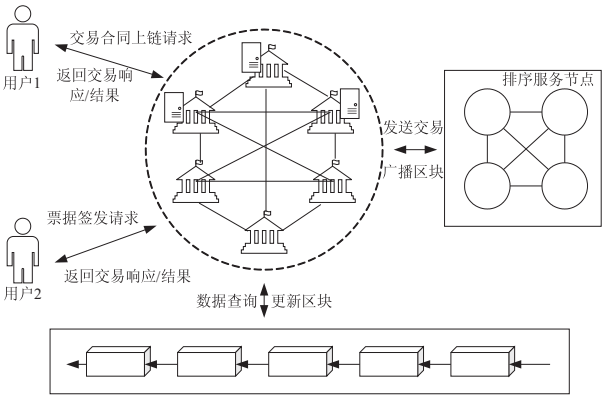

图 1　系统总体模型

区块链采用公私钥机制作为用户识别方式,每个用户都拥有一对公私钥。私钥用于对消息进行签名,以确保消息来源和不可篡改性,公钥用于验证签名和加密通信。超级账本网络依赖于成员服务提供者(MSP)管理身份,每个组织都拥有独立的根证书和唯一的 MSP ID 作为标识。例如,企业和银行分别属于两个不同组织。Fabric 使用证书颁发机构(CA)颁发的数字证书建立信任,该证书包含公钥、申请人信息和数字签名,用于证明用户的身份和权限。节点首次访问区块链票据平台需注册,系统审核成功后通知用户注册成功,并为其颁发数字证书和私钥文件。用户通过用户名和密码登录,服务器使用 MSP 进行验证,确保用户信息有效并来自合法组织,并通过 CA 的公钥验证用户数字证书的有效性。

在本模型中,各个节点均为经过注册并完成身份认证的实体。用户提交交易提案申请后,验证节点执行智能合约验证交易有效性,并生成交易合同信息哈希值作为唯一编号,同时生成读写集合响应,但并不更新账本。客户端收到足够数量的验证响应后确认交易的有效性。然后,客户端连接到对等节点将交易广播至排序服务节点。排序节点按照共识机制排序并生成区块。最终,该区块被广播至记账节点,记账节点对区块进行验证后,将其写入账本。

2.2　系统实施流程

2.2.1　交易的可信表示

在票据交易中,每笔交易包含交易发起方、接收

方、交易金额等关键信息。这些信息构成了交易的核心内容,对于确保交易的合法性和有效性至关重要。交易状态信息反映了当前票据的交易状态,包括交易是否已完成、是否被撤销等。交易数据结构如图 2 所示。为了实现票据交易的可信操作,定义了交易提案的典型数据格式如下:

$$tx = < client\_ID, contract\_ID, txPayload, timestamp, clientSig > \quad (1)$$

其中,client_ID 为客户端 ID,contract_ID 是验证节点将要调用的智能合约 ID,txPayload 即交易信息载体,分为操作(operation)和元数据(metadata)两部分。其中,operation 指定了智能合约调用的函数和输入参数信息,metadata 表示与此次调用关联的其他元数据部分,timestamp 即时间戳,clientSig 即客户端签名。交易操作类型指定了交易执行的具体动作,如票据签发、转让或贴现等。智能合约会根据操作类型执行相应的业务逻辑。票据信息包括票据号码、票据金额和日期等基本属性。交易参与者信息包括交易的各方,如交易发起方、接收方等。

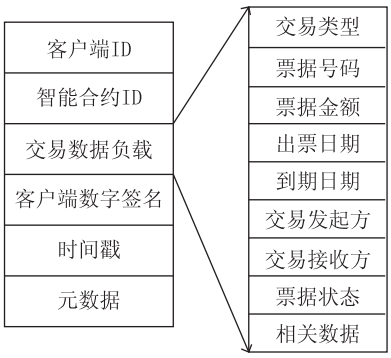

图 2 交易数据结构

2.2.2 交易合同信息链上存证

在区块链票据交易平台中,授权企业用户首先发起交易合同信息上链存储请求。然后验证节点提取票据交易合同信息,进行交易合法性验证,确保其票据金额不超过合同金额,并确保交易日期有效性,随后,对交易合同数据信息进行哈希处理,并上链存储,实现区块链上交易合同编号与其数据的轻量化的存储映射。交易合同上链信息如表 1 所示。

表 1 交易合同上链信息

参数名称	类型	说明
Initiator	string	出票人
Receiver	string	收票人
ContractAmount	float64	合同金额
BillAmount	float64	票据金额
TransactionDate time	Time	交易日期
ProductInfo	string	商品信息
OtherTerms	string	其他条款

为确保合同的真实性和不可篡改性,交易双方进行电子签名,只有具备交易双方的电子签名合同才可生效。完整的交易合同上链过程如图 3 所示。

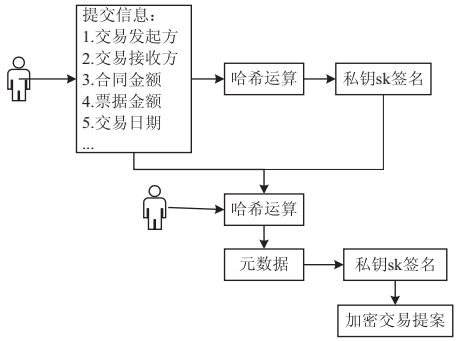

图 3 交易合同上链过程

步骤 1:出票人对交易合同 BoE(Bill of Exchange)进行哈希运算,得到 H(BoE),以增强交易合同的完整性。

步骤 2:出票人利用私钥 sk 进行数字签名,生成 $sig_{sk}(H(BoE))$,以保证交易合同的真实性。

步骤 3:生成 operation $\{sig_{sk}(H(sp-Contract)), BoE\}$。

步骤 4:为确保交易数据的完整性,生成 $H_m() = Hash(operation, client\ ID)$,即 metadata 部分。

步骤 5:对等节点使用私钥对交易负载 tx Payload 进行签名:$sig(tx\ Payload) = sig_{sk}(txPayload)$,并将其发送至验证节点。

在上述步骤中,节点的数字签名保证了交易合同文件的完整性和签署者身份的合法性。任何对文件的篡改都会导致数字签名验证失败。数 metadata 元数据部分存储交易的关键信息,如客户端的签名和参与方身份,通过对 operation 和 client_ID 进行哈希运算,可以验证数据的完整性,同时记录参与方信息以防止数据篡改,也方便追踪和审计交易,确保交易的合法性和透明度。

2.2.3 交易可信验证

在票据交易数据完整性验证机制中,研究内容主要集中在以下 3 个方面:(1)票据交易合同可信验证;(2)票据签发交易可信验证;(3)票据所有权转让交易可信验证。

为了确保交易的真实性和完整性,验证合约包含用户身份与权限审核、交易合同验证、交易合法性验证以及生成读写集验证响应。验证节点首先需要校验用户证书的合法性,检查其 MSP ID 是否在已知列表中,验证其根证书签名,最后,检查 CRL(证书吊销列表)以确保证书的有效性。通过身份验证后,交易验证流程包括如下步骤:

步骤 1:通过出票人的证书生成其公钥 pk,并使用

该公钥解密得到 H（BoE),接着,对交易合同进行哈希得到 H ＊(BoE),如果计算出的交易合同哈希值与解密后的 H（BoE)一致,那么就证明交易合同未被篡改,且来源于此公钥代表的出票人。

步骤 2:当交易合同完整性验证结束后,对交易合同基本信息进行合法性和有效性验证,确保票据金额不大于交易合同金额,并验证交易日期的合法性。

步骤 3:生成读写集响应,将合同基本信息进行哈希,作为合同在全网的唯一编号 ID,与已经登记过的票据交易合同 ID 进行逐一对比,若无记录,则生成票据交易合同成功上链存储信息的读写集,并将票据状态登记为未签发,返回成功上链存储信息至客户端,如有记录,则验证节点返回出错信息。

完成节点身份验证后,票据签发交易具体步骤如下:

步骤 1:验证节点首先根据票据基本信息计算票据对象的哈希值作为票据唯一编号 ID,并检查票据是否已经存在,获取交易合同基本信息并对其哈希,与出票人提交的哈希值进行对比,若一致,则证明该出票交易来源于签发交易合同的申请人。

步骤 2:生成读写集响应,将票据基本信息进行哈希,作为票据在全网的唯一编号 ID,并更新票据状态为已签发。

步骤 3:返回响应结果至客户端。

票据所有权转让交易可信验证旨在确保用户身份与权限合法有效的前提下,保证票据历史转让交易记录的真实性、有效性、连续性。票据在成功登记为已签发后,可以进行后续的票据所有权转让和贴现操作。完成节点身份验证后,如图 4 所示,执行票据转让交易的可信验证流程。

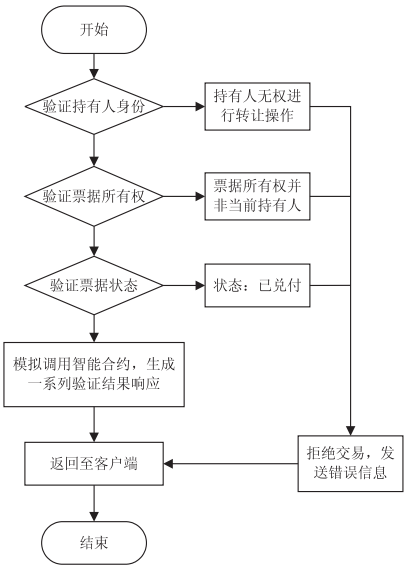

图 4　票据转让交易验证流程

2.2.4　票据可信交易管理的区块及区块链

客户端节点收到验证节点的响应后,需确认是否已获得足够数量的验证节点同意,否则交易不通过。随后,客户端将交易提案及足够数量的响应发送至排序服务节点。排序服务节点负责对交易进行排序,并打包成区块。经过共识算法确认后,该区块会被广播给所有提交节点进行最终验证。提交节点对接收到的区块进行 3 个验证步骤:(1)确认是否获得足够的有效性验证;(2)检查交易的读写集冲突;(3)将区块附加到本地存储账本,并更新区块链状态。

为确保票据管理中的票据可信操作,构建了票据管理的区块和区块链结构,如图 5 所示。区块结构对确保交易的可信性和完整性至关重要,它规定了交易数据的存储和管理方式,实现了数据的去中心化可信存储和共享,防止数据篡改和丢失。

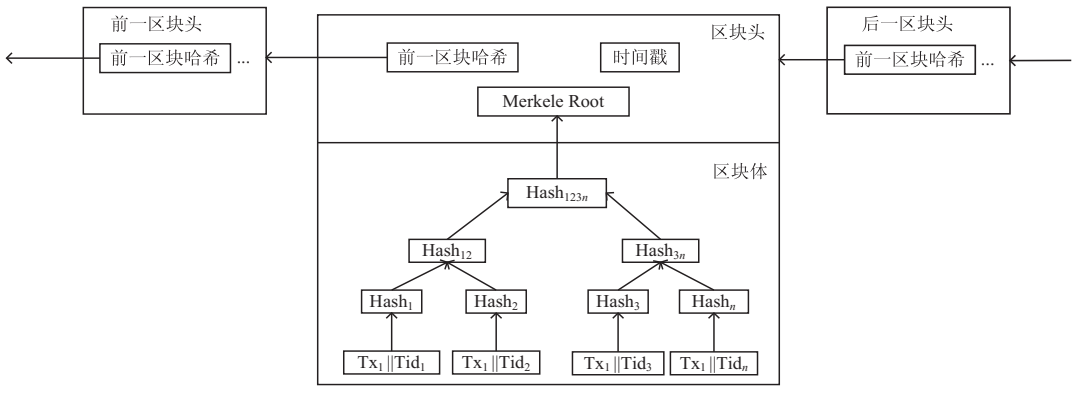

图 5　区块和区块链结构

与比特币相似,票据交易的区块由区块头和区块体两部分构成。区块头包含前一个区块的哈希值、默克尔根和时间戳。前一个区块的哈希值将当前区块与前一区块连接,确保了区块链的连贯性。默克尔根通过对区块中的交易进行哈希计算得到的根哈希值,用于验证区块中的交易数据的完整性。时间戳记录了区块的创建时间,有助于确定交易发生的时间顺序,并验证了区块的合法性和一致性。区块体包含了交易提案(TX_i)及其标识(Tid_n)。交易提案包括了票据交易的详细信息,如交易发起方、接收方、交易金额等。而交

易提案的标识则用于唯一标识每笔交易,以便进行交易的追溯和验证。

受比特币的区块链设计的启发,其中,当前区块的区块头中存储了前一区块的哈希值,确保各个区块按照时间戳递增的顺序进行链接,有效防止了交易历史的篡改和数据伪造,为票据管理提供了可靠的数据保护。此外,通过共识机制来保证所有节点账本数据的一致性。在去中心化的模式下,新生成的区块必须通过共识机制的验证才能被添加到区块链中,确保交易数据的可信性和安全性。与比特币公有链不同,本方案采用了 Raft 共识机制,通过管理日志一致性确保节点状态的一致性,Raft 共识机制提供了优于 Proof-of-Work 的事务延迟和吞吐量,同时减少了资源消耗。

2.3 参与方身份真实性验证过程

Intel 的软件保护扩展(Software Guard Extensions,SGX)作为一种可信执行环境的实现,提供了硬件级别的安全保障,它通过创建受保护的执行环境,确保节点的身份验证过程在受信任环境中进行,防止身份信息篡改或攻击。SGX 采用可验证的远程认证机制,使用内部增强型密钥 EPID 生成一个为 QUOTE 的结构体,允许其他节点通过使用 IAS 服务器来验证和证明 SGX 的身份真实性[21]。

在 SGX enclave 初始化时,会生成用于保护内部数据和通信的加密密钥对(pk,sk),为后续数据加密、签名和验证等操作提供基础,确保数据的真实性与不可篡改性。Fabric CA 为可信计算节点生成和签署专用的 CA 证书,以确保其信任级别。在智能合约注册阶段,SGX 需要在初始化阶段将智能合约的地址和相关信息注册到自身内部,验证节点生成智能合约内容地址 Adr = Hash(c) 。其中 c 表示智能合约,将向 REE 发送注册请求(pk,Adr),TEE 保存注册请求并返回成功消息{pk_{sgx},key length},智能合约保存 pk_{sgx}。

在基于 Fabric CA 的基础上,可信节点身份验证过程包括如图 6 所示的 7 个步骤:

步骤 1:银行节点向 SGX 发送远程认证请求,SGX 执行 EREPORT 命令生成报告结构,然后向银行节点发送 CA 证书等待验证。

步骤 2:银行节点检查证书的签名是否有效,证书是否过期,以及证书是否在 CA 的信任链中。

步骤 3:证书验证通过后,向 SGX 节点返回验证通过消息,SGX 利用 EPID 签名生成 QUOTE 发送至区块链节点,以等待服务器验证。

步骤 4:银行节点通过 IAS 服务器完成节点身份验证,并返回成功消息。

步骤 5:验证完成后,双方使用 Diffie-Hellman 密钥方案建立安全的会话密钥 sek,加密数据传输。

步骤 6:银行节点通过解密获得会话密钥 sek 后,使用该密钥向 SGX 发送加密后的随机数,防止了中间人攻击,进一步保证数据传输的机密性。

步骤 7:SGX 节点解密获得随机数,返回成功建立安全连接的消息。

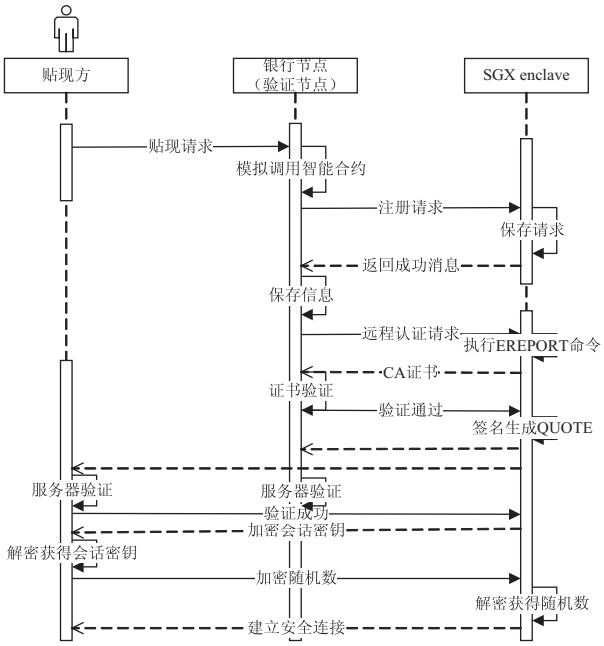

图 6 身份真实性验证时序

在一笔票据贴现交易中,涉及到多个参与方,根据上述真实性验证过程,构造以下命题以及验证过程。符号定义如下:银行节点 $B(x)$,SGX 节点 $S(x)$,$V(x)$ 表示节点 x 经过验证是合法的。根据命题可以确立如下事实,存在一对公私钥,其中公钥用于加密信息,私钥用于解密信息。如果任意的私钥都可以成功解密使用某个公钥加密的信息,则这对公私钥是有效的非对称加密。验证过程公式如下:

$$\exists x \exists y D(Y, E(x,m)) \tag{2}$$

$$\forall x \forall y (D(y, E(x,m)) \rightarrow K(x,y)) \tag{3}$$

$$B(x) \rightarrow V(x) \tag{4}$$

$$B(x) \rightarrow \text{ValidateCertificate}(x) \tag{5}$$

$$\exists x \exists y (B(x) \wedge S(y) \wedge \text{DH}(x,y) \rightarrow \text{sek}) \tag{6}$$

$$\exists x \exists y (B(x) \wedge S(y) \wedge D(S(y), E(r, \text{sek}))) \tag{7}$$

$$\exists x \exists y (B(x) \wedge S(y) \wedge D(B(x), D(r, \text{sek}))) \tag{8}$$

其中,公式 2、3 是命题前提,其中 $E(x,m)$ 表示用公钥 x 对消息 m 进行加密,$D(y,E)$ 表示用公钥对密文 E 进行解密,DH(x,y)表示银行节点 x 和 SGX 节点 y 之间进行 Diffie-Hellman 密钥交换协议,r 表示随机数,sek 表示会话密钥。公式 4 表示任意银行节点可以向 SGX 发送远程认证请求都可以通过验证。公式 5 表示银行节点使用公钥验证证书的有效性,验证通过后,

公式 6 表示节点双方成功交换了会话密钥。那么,公式 7、8 代表通过对随机数的加密和解密过程,交易双方成功建立了安全的通信连接。通过身份认证,可以确保通信的两个参与方是其声称的实体,并且具有执行所需操作的权限。

3　仿真实现与测试

根据第 2 节描述的基于区块链的票据可信管理方案,本节基于超级账本平台进行仿真实现与测试。对票据交易进行用例测试,并对操作进行性能分析。

3.1　实验环境搭建

Hyperledger Fabric 作为区块链票据平台的核心技术,用于构建可信交易网络。该文在 Intel Core i5 - 8250 CPU @ 1. 60 GHz 1. 80 GHz,系统为 CentOS Linux release 7. 9. 2009 上搭建 Hyperledger Fabric V2. 1 区块链网络,智能合约选择由 go 语言编写的链码,并在 Docker 环境下运行。在 CentOS 操作系统上配置 Docker17. 12. 1 运行环境,并安装了 Docker compose 工具以管理各种节点容器。在 Hyperledger Fabric 网络中,对等节点加入通道后需安装并实例化智能合约以在网络上执行。

以票据签发为例,票据签发验证的智能合约函数关键代码见算法。

算法:IssueBill
输入:args [ ]string:参数数组,包含票据各项信息
输出:peer. Response:返回的响应对象

```
1:function IssueBill(args):
2:    if args.length ! = 7:
3:        return Error( " Incorrect number of arguments. Expecting 7" )
4:    bill := createBill(args)
5:    if existsBill(bill):
6:        return Error( " Bill already exists" )
7:    if not validateContractIntegrity(bill. contract):
8:        return Error( " Failed to verify transaction contract)
9:    putBillOnBlockchain(bill)
10:    return Success(bill)
```

3.2　测试与结果分析

客户端节点作为系统用户,可以通过调用智能合约发起交易合同上链、票据签发、票据转让等操作。在完成了智能合约安装和实例化后,进行用例测试,对票据交易合同上链存证、签发进行功能测试。图 7 表示票据交易合同上链功能页面,输入合同信息后提交,交易合同信息登记至区块链。该用例测试通过。

对票据签发交易进行功能测试,在输入票据信息后提交,票据签发交易存储至区块链。票据详细信息包括当前交易的哈希值、验证节点信息、交易类型以及时间戳。且票据的状态被修改为“已签发”,该用例通过测试。

图 7　交易合同上链页面

为了评估系统的写入数据功能,本系统采用 Caliper 工具对区块链进行压力测试,测试指标包括事务处理吞吐量(TPS)、事务延迟及 CPU、内存和网络 IO 的资源消耗情况等。吞吐量表示在规定时限内完成被节点认可的交易的速率,平均延迟指网络节点完成验证交易所需要的平均时间,单位为 s。

表 2 展示了写入操作压测结果。在测试期间,共进行了 100 次操作,全部成功完成。发送速率为每秒 2. 4 次操作,最大延迟为 2. 75 s,最小延迟为 0. 56 s,平均延迟为 2. 04 s。系统的吞吐量为 2. 3 TPS。在写入操作的压力测试中,系统表现稳定,虽然发送速率相对较低,但整体性能仍然可以接受。

表 2　写操作压测结果

名称	成功	失败	发送速率/TPS)	最大延迟/s	最小延迟/s	平均延迟/s	吞吐量/TPS
写集合	100	0	2. 4	2. 75	0. 56	2. 04	2. 3

为了验证基于 SGX 的区块链票据交易身份真实性方案的性能,在 Intel® Core™ i5 - 8250U CPU 和 8 GB 内存上进行仿真实验,利用 Fabric 提供的 private - chaincode SDK,将对等节点与 SGX 集成,将智能合约部署到独立的 encalve 中。对在 SGX 和非 SGX 环境[11]下的 ECDSA 非对称加密算法,以及 SGX 下环签名[22]算法下执行身份验证流程,获得了它们在不同环境下执行所需的平均时间。结果如图 8 所示。结果表明,本方案的身份认证时间比文献[11]增加了约 50 ms。与文献[22]相比,本方案执行时间节省了约 200 ms。这些额外时间主要用于 enclave 初始化和调用,但在实际应用中,ms 的开销可以忽略不计,此外,本方案不仅有效保护了节点的隐私信息,而且在时间开销上占据一定优势。

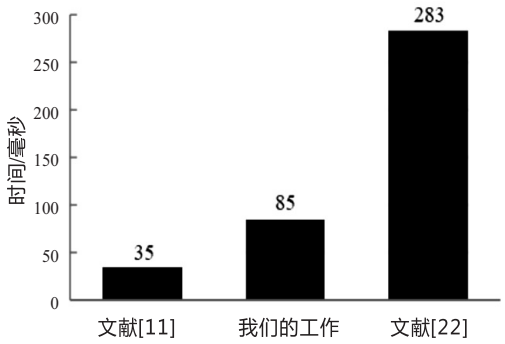

图 8 不同环境下执行身份认证所需平均时间

4 结束语

针对传统票据交易管理中存在的安全隐患,以及当前区块链票据交易可信方案中的交易真实性、完整性和身份信息真实性等技术挑战,该文提出了一种基于区块链的票据可信管理方案,通过描述可信交易参与方、交易管理数据结构和交易真实性、完整性机制,实现了票据交易的可信管理。该方案将区块链技术与安全硬件执行环境相结合,实现了去中心化环境下节点的身份真实性验证。在 Fabric 平台上进行仿真实验,并对系统进行性能测试,测试结果明确展示了该方案的可行性、正确性以及在实际应用中的优势。未来研究将考虑引入更多的隐私保护机制,探索参与方交易隐私保护方案。

参考文献:

[1] 朱佳金. 票据中介视角下的票据业务操作风险管控研究[J]. 上海立信会计金融学院学报,2017,29(4):63-72.

[2] 肖 凰. 票据业务的区块链应用[D]. 广州:广东财经大学,2021.

[3] 罗思佳. 商业银行电子票据业务风险防范研究[D]. 南昌:江西财经大学,2020.

[4] 马云龙. 区块链票据融资平台应用研究[D]. 上海:上海财经大学,2021.

[5] LIU N, ZHANG Y, LI H, et al. Secure transaction mechanism of blockchain digital assets based on distributed identity[C]//Proceedings of the 2023 4th international conference on computing, networks and internet of things (CNIOT). Xiamen: ACM, 2023: 948-956.

[6] 徐 响,田 宁,赵科杰,等. 区块链技术赋能药品供应链:应用与挑战[J]. 计算机应用研究,2023,40(9):2573-2581.

[7] LIU H. Blockchain and bills of lading: legal issues in perspective[J]. Maritime Law in Motion, 2020, 8: 413-435.

[8] 沈 伟. 用区块链技术重构票据业务流程[J]. 中国金融,2020,11:70-71.

[9] 林永民,张鸿飞,崔雨彤. 区块链技术下医疗电子票据可信流转模式创新研究[J]. 中国卫生经济,2023,42(3):87-90.

[10] 张蔚虹,李春钰,王禹心. 区块链赋能企业财务共享服务平台:票据管理[J]. 西安电子科技大学学报:社会科学版,2022,32(3):1-8.

[11] WANG X, GUO J, LI D, et al. A transaction model of bill service based on blockchain[C]//2021 artificial intelligence and security: 7th international conference (ICAIS). Dublin: Springer, 2021: 279-288.

[12] 余 辉,程 波,马文学. 区块链在银行承兑汇票中的应用[J]. 现代经济信息,2020,6:149-151.

[13] CHEN J, LIU X, HAN W, et al. A model design of blockchain-based data storage for e-government application[C]//2021 advances in artificial intelligence and security: 7th international conference (ICAIS). Dublin: Springer, 2021: 666-676.

[14] 黄玉清,熊尚华,葛邦彪. 基于区块链的医疗电子票据应用模型研究[J]. 医学信息学杂志,2022,43(8):67-70.

[15] 张群辉. 区块链技术在票据市场的应用,风险与规制[J]. 北方金融,2019,6:18-22.

[16] 李 昂. 区块链技术在承兑汇票领域的应用研究[D]. 北京:北京邮电大学,2019.

[17] 金筠杰. A 公司数字票据平台运行机制研究[D]. 南昌:江西财经大学,2019.

[18] 朱佩君. 基于区块链技术的商业银行票据管理优化问题研究[D]. 上海:上海国家会计学院,2017.

[19] MAHINDRE S, GUPTA S, RAMBHAD V, et al. Secure splitting of bills and managing expenditure using blockchain[C]//2023 IEEE 3rd international conference on technology, engineering, management for societal impact using marketing, entrepreneurship and talent (TEMSMET). Mysuru: IEEE, 2023: 1-7.

[20] JAMIL F, HANG L, KIM K H, et al. A novel medical blockchain model for drug supply chain integrity management in a smart hospital[J]. Electronics, 2019, 8(5): 505-536.

[21] 董春涛,沈晴霓,罗 武,等. SGX 应用支持技术研究进展[J]. 软件学报,2020,32(1):137-166.

[22] BAO L W, LU G H, FU L Y. Trusted blockchain of ring signature in TEE environment[C]//2022 3rd Asia service sciences and software engineering conference (ASSE). Macau, China: ACM, 2022: 8-13.