 DOI: https://doi.org/10.12349/iser.v6i7.6723

Security design of electronic contract management software based on blockchain technology

Jie Zhang

Tonghao Information Industry Co., Ltd., Beijing, 100070, China

Abstract

With the rapid advancement of the digital era, electronic contracts have become increasingly prevalent in commercial activities. However, traditional electronic contract management faces multiple security challenges such as data tampering, identity authentication risks, and contract loss. Blockchain technology, characterized by decentralization, immutability, and traceability, offers innovative solutions for enhancing the security of electronic contract management software. This paper explores the security design of blockchain-based electronic contract management systems, analyzes their application principles, and summarizes key technologies. The aim is to establish a secure, reliable, efficient, and user-friendly environment for electronic contract management, thereby promoting its widespread adoption and development across various industries.

Keywords

blockchain technology; electronic contract; management software; security design

基于区块链技术的电子合同管理软件安全性设计

张杰

通号信息产业有限公司，中国 · 北京 100070

摘　要

随着数字化时代的快速发展，电子合同在商业活动中的应用日益广泛。然而，传统电子合同管理面临诸多安全挑战，如数据篡改、身份认证风险、合同丢失等。区块链技术以其去中心化、不可篡改、可追溯等特性，为电子合同管理软件的安全性提升提供了新的解决方案。本文深入探讨基于区块链技术的电子合同管理软件安全性设计，分析其应用原理，总结其中的关键技术，旨在构建一个安全可靠、高效便捷的电子合同管理环境，推动电子合同在各行业的深入应用与发展。

关键词

区块链技术；电子合同；管理软件；安全性设计

1 引言

进入信息大发展的时代，企业业务数字化蜕变带动合同管理从常规纸质模式转为电子模式，电子合同凭借其便利、高效、绿色等长处，被数量渐增的企业采用，电子合同在数据的保存、传输以及管理环节面临严峻的安全隐患，诸如数据泄露状况、合同被恶意涂改、签署方身份难以有效审定等，此类问题极大阻碍了电子合同的普遍应用。新兴的分布式账本技术——区块链技术，为化解电子合同安全难题开拓创新办法，凭借其别具一格的技术特质，说不定能强化电子合同管理软件的安全可靠性，本研究意在设计一套依托区块链技术的电子合同管理软件安全架构方案，全面阐述其技术达成路径与安全管控机制，为电子合同管理软件的开发应用提供理论层面支持与实践方面指导。

【作者简介】张杰（1987–），男，中国天津人，本科，工程师，从事计算机软件开发及软件开发管理研究。

2 区块链技术原理与特性

2.1 区块链技术原理

区块链本质上可看作是分布式账本，多个区块依据时间顺序逐个衔接而成，各区块包含某段时间区间里的交易数据以及前一区块哈希值，对区块内容运用特定哈希算法进行计算，得到的唯一数字标识是哈希值，呈现唯一性及不可倒推性，若一个区块内的数据出现任何细微的变化情形，其对应的哈希值会跟着更改。区块链采用共识机制 以此保证各节点上数据一致，诸如工作量证明（PoW）、权益证明（PoS）、实用拜占庭容错算法（PBFT）等，属于常见的共识机制，在区块链的网络架构里，各个节点凭借竞争或别的规则达成共识状态，将新的交易数据聚合成区块再添加到区块链，以此达成数据的分散式存储及共享目的［1］。

2.2 区块链特质及其对电子合同安全的作用

2.2.1 去中心化

区块链网络未配备中心化的管理相关机构，各节点间

地位无差异，各节点对数据进行分散存储，电子合同管理摆脱对单一中心服务器的依赖，降低了中心服务器故障或被攻击后引发数据丢失、被篡改现象的风险，提升电子合同管理系统的平稳性与可靠水平。

2.2.2 不可篡改

既然每个区块都包含着前一个区块的哈希值，搭建起一条链式的格局，要是某一区块的数据出现篡改情况，后续各个区块的哈希值皆会产生变化，此变化会被区块链网络中的其余节点发觉，进而保障电子合同数据完整与真实，防止合同遭恶意篡改现象出现。

2.2.3 可追溯性

区块链上每一笔交易皆被全面记录，涵盖交易时间、相关参与方及交易内容等详情，经由区块链浏览界面，用户可便利地查看电子合同的签署历史和流转情形，完成电子合同全生命周期回溯，为处理合同纠纷给出有效凭据。

2.2.4 加密安全性

借助非对称加密技术，区块链对数据进行加密后传输存储，在电子合同签署期间，签署方依靠自己的私钥对合同数据进行签名处理，接收方借助签署方的公钥完成验证，保证签署者身份的真实无误与合同数据的完整无缺，杜绝身份盗用与数据外泄。

3 电子合同管理软件面临的安全风险

3.1 数据隐私问题

电子合同管理软件一般会存储海量关乎企业及个人的敏感资料，像企业商业秘密、个人身份资料、财务账目之类，在数据存储以及传输之际，一旦安全措施实施不力，黑客或许会对这些数据进行窃取、篡改或泄露操作，造成合同签署方巨大经济亏损，引发法律风险问题，传输阶段数据存在被截获风险，若服务器被攻击，会造成数据泄露。

3.2 身份验证问题

在电子合同开展签署的时段，精准核实签署方身份意义重大，老派身份认证的模式，就像用户名跟密码，面临易被破解或窃取的隐患，要是身份验证方面出现漏洞，居心叵测之人说不定会冒充他人签订合约，引发对合同有效与否的质疑，引起合同相关的纠葛。

3.3 电子签名问题

电子合同有个核心要素，那便是电子签名，其安全性直接关乎合同的法律效力，电子签名有被伪造、篡改或被否认的潜在威胁，若电子签名技术成熟度不足，难以有效保证签名的独特单一性和不可抵赖性，事后签署方也许会否认合同已被签署，为合同执行增添阻碍。

3.4 合同审计问题

电子合同管理软件需针对合同从创建到执行等一系列过程做审计，保障合同符合要求以及操作的合法属性，审计记录也许会被窜改或者删掉，以此隐匿违规行径，审计日志保存时长以及完整性也许无法符合法律要求，对合同监管及争议解决形成阻碍。

3.5 第三方风险

电子合同管理软件也许会依赖第三方服务供应主体，若涉及如电子签名业务、云空间存储业务等，要是第三方服务提供商安全举措未做到位，存有安全漏洞情况或被攻击，说不定会让电子合同数据泄露、服务中断现象发生，导致电子合同管理软件运行陷入困境。

4 基于区块链技术的电子合同管理软件安全设计

4.1 身份认证与授权机制

4.1.1 多因素身份认证

采用多方面身份鉴权形式，结合密码、短信动态验证码、指纹特征识别、人脸图像识别等诸多元素，保障签署方身份真实且可靠，用户进入电子合同管理软件登录阶段时，一开始便输入用户名跟密码，然后系统把验证码以短信形式发送到用户绑定手机，用户输入符合要求的验证码后，再之后实施指纹核验与人脸鉴定其一，完成多重验证，才可实现成功登录。

4.1.2 基于区块链的身份验证

依靠区块链具有的不可篡改、可回溯的特性，建设去中心化身份鉴别系统，用户在区块链上实施身份信息注册操作，制作仅有的专属身份标识，还会把身份信息跟私钥进行绑定，在实施电子合同签署之际，用户借助私钥给合同签名，验证方借助区块链查核用户的身份信息与签名记录，核实签署方身份真实合法。

4.1.3 权限管理

按照用户的角色与职责，给其安排不一样的操作权限，合同创建者具备对合同进行编辑、更改及删除的权限，签署方仅被赋予签署合同的权限，审计人员被赋予查看合同审计日志的权限，把权限信息存放于区块链，让权限具有不可篡改以及可追溯的属性。

4.2 电子签名与加密技术

4.2.1 数字证书与电子签名

采用数字证书体系，权威的认证机构（CA）颁发数字证书给签署方，数字证书含有签署方公钥、身份方面的信息以及 CA 的签名，签署方凭借私钥对电子合同加以签名，签名这一过程借助哈希算法核算合同内容，得到合同相关哈希值，之后借助私钥对哈希值进行加密处理，得出电子签名标识，验证方依靠签署方的公钥和 CA 根证书开展电子签名的验证，保证合同的完整以及签署方身份属实［2］。

4.2.2 非对称加密与对称加密结合

处于电子合同数据传输以及存储阶段，采取对称加密和非对称加密相融合方式，在筹备数据传输阶段，发送方借助接收方的公钥来完成对称加密密钥的加密，接着把加密后

的密钥和利用对称加密算法加密的合同数据一同发给接收方，接收方凭借自身私钥解出对称加密密钥，再借助此密钥对合同数据做解密处理，维持数据传输阶段的安全状态，在数据开展存储期间，用对称加密算法把合同数据加密后存储，再进一步提高数据的安全系数。

4.3 合同数据存储与管理

4.3.1 区块链分布式存储

把电子合同数据安置到区块链那里，凭借区块链分布式存储的相关特性，让数据分散储存在多个节点里面，各节点分别保存完整的区块链副本，即便部分节点产生故障，甚至被攻击，合同数据的完整性与可用性也不受影响，有了区块链不可篡改的特性，合同数据的安全与真实能得到保证。

4.3.2 数据加密存储

针对区块链上存储的电子合同数据开展二次加密，采用领先的加密算法体系，做合同内容的加密事宜，仅拥有正确解密密钥的用户才有权限查看合同明文内容，杜绝数据外泄。

4.3.3 版本管理与溯源

把电子合同全部版本信息录入区块链，涉及诞生时间、修改详情、修改人等，借助区块链呈现出的可追溯属性，用户可顺畅地查询合同以往版本，探知合同修改过程与变化动态，达成合同变更流程的透明与可追溯目标［3］。

4.4 合同审计与监管

4.4.1 审计日志上链

把电子合同审计日志存于区块链，囊括合同的创立、修改、签署、查看等操作的相关记录，审计日志存有操作时间、进行操作的人、操作所涉内容等详细资料，鉴于区块链不可篡改这一属性存在，审计日志无法被进行篡改动作，实现审计数据真实与可靠的目标。

4.4.2 智能合约监管

依靠智能合约相关技术，实现电子合同执行程序的自动监查，智能合约作为自动开展执行的合约条文，以代码格式实现在区块链上部署，处于电子合同的范畴，能把智能合约进行嵌入，设定合同执行时的条件与相关流程，倘若合约条件达成，智能合约自动开展相关操作，诸如自动划转资金、自动交付货品等活动，接着把执行结果归档到区块链，实现对合同执行状况的即时监管与跟踪。

4.4.3 多方参与的监管机制

搭建以合同签署者、监管部门、第三方审计机构等多方介入的监督体系，各方借助区块链浏览器可即时把握合同审计日志以及执行状况，对电子合同管理软件运行实施监督，监管机构可凭借审计数据开展电子合同合规性检查，即时识别并处理违规情形。

4.5 安全漏洞检测与应急响应

4.5.1 定期安全漏洞检测

采用面向安全检测的专业工具与技术，周期性对电子合同管理软件实施安全漏洞扫描检测，涉及对区块链节点、应用程序以及网络等层面的检测，及时找出并填补软件存在的安全窟窿，防止黑客借助漏洞开展攻击行动［4］。

4.5.2 应急响应机制

创建全面应急响应机制，筹备应急相关预案，若安全事件降临，像数据外泄、系统遭袭之类，可马上启动应急响应预案，采取相关的处置办法，诸如隔离被攻击的系统、还原数据备份、通告有关用户，把安全事件引发的损失压缩到最小。

4.5.3 安全事件报告与分析

对出现的安全事件进行周全记录及报告，剖析事件出现的缘由、经过及后果，总结安全相关教训与经验，持续优化安全防护手段与应急处理机制，增强电子合同管理软件安全抵御能力。

5 结论

依靠引入区块链技术，能切实提高电子合同管理软件安全度、可靠程度与管理成效，增强电子合同法律上的效力，推进电子合同在各行业普遍推广，伴随区块链技术持续发展与完善，凭借区块链技术而存在的电子合同管理软件在数字经济时代将发挥更关键价值，帮企业与社会实现更大的价值产出，未来研究可进一步把目光投向区块链技术在电子合同管理应用的优化，还可探讨跟其他新兴技术的整合，诸如人工智能、物联网之类，逐步提高电子合同管理智能化及便捷化程度。

参考文献

[1] 刘子煜,张娟,王成章.基于区块链技术的电子合同安全云存储系统[J].自动化技术与应用,2024,43(09):105-108.DOI:10.20033/j.1003-7241.(2024)09-0105-04.

[2] 翟文豪.区块链智能合约的合同属性困境及其化解[C]//《智慧法治》集刊2024年第2卷——“东方法学新锐”研究文集.北京大学法学院;,2024:218-234.DOI:10.26914/c.cnkihy.2024.024789.

[3] 庄语滋.区块链智能合约的CISG适用问题探析[C]//《法律研究》集刊2024年第1卷——贸易强国制度构建研究文集.复旦大学法学院;,2024:123-131.DOI:10.26914/c.cnkihy.2024.002891.

[4] 潘飞.区块链应用背景下供应链采购合同管理研究[J].中国物流与采购,2023,(22):103-104.DOI:10.16079/j.cnki.issn1671-6663.2023.22.029.