可信计算与区块链技术的融合机制、挑战与应用研究

张婷
宁夏职业技术大学，宁夏 银川 750021
DOI: 10.61369/TACS.2026090033

摘　　要： 区块链依靠去中心化、不可篡改、可追溯的特点，成为分布式数据协同、跨主体可信交互的重要的技术底座，在数字经济的各个领域都有所应用。可信计算依靠硬件可信根来创建可信执行环境，可以从底层硬件角度改善区块链存在的安全问题。本文在对私钥交易防护、智能合约可信执行、可信数据溯源存证这三个主要的融合机制进行剖析，归纳出目前技术融合中出现的现实问题，进而给出相应的改进措施。从研究结果可以看出，可信计算和区块链融合起来构成了一种硬件可信执行加分布式账本的双重安全架构，破除了链上和链下的信任障碍，加强了分布式系统的安全性、可靠性和合规性，给各个行业的数字化可信转型赋予了技术支撑。

关 键 词： 可信计算；区块链；可信执行环境；数据安全；分布式信任；隐私保护

Research on Integration Mechanism, Challenges and Applications of Trusted Computing and Blockchain Technology

Zhang Ting
Ningxia Vocational and Technical University, Yinchuan, Ningxia 750021

Abstract: With the characteristics of decentralization, immutability and traceability, blockchain has become an important technical foundation for distributed data collaboration and cross-subject trusted interaction, and has been applied in various fields of the digital economy. Trusted computing builds a trusted execution environment relying on hardware trusted roots, which can solve the security problems of blockchain from the underlying hardware level. This paper analyzes three core integration mechanisms, including private key transaction protection, trusted execution of smart contracts, and trusted data traceability and evidence storage. It summarizes the practical challenges existing in the current technology integration and proposes corresponding improvement measures. The research results show that the integration of trusted computing and blockchain forms a dual security architecture combining hardware trusted execution and distributed ledger. It eliminates trust barriers on and off the chain, improves the security, reliability and compliance of distributed systems, and provides strong technical support for the digital and trusted transformation of various industries.

Keywords: trusted computing; blockchain; trusted execution environment; data security; distributed trust; privacy protection

一、可信计算和区块链技术相结合的机制

可信计算向下扎根于硬件可信根来实现设备环境的可信，区块链向上搭建起分布式账本来达成数据交互的可信，两者之间存在着上下层技术互相补充的关系，依靠四层分层架构来达成耦合，硬件可信层给予 TPM、TCM、TEE 硬件安全底座，系统执行层执行可信启动、完整性动态度量和行为风险监控，区块链网络层执行节点可信报告核验、节点准入剔除和日志上链存证，应用服务层向外输出存证、认证、溯源业务能力，以上架构为三类核心融合实现机制的产生提供了基础[1]。

（一）私钥和交易安全防护机制

传统的区块链把私钥存放在操作系统的软件内存中，很容易受到木马的入侵、黑客的窃取，从而造成身份伪造、资产被盗等安全事件的发生。可信计算介入之后，节点的身份私钥、交易签名私钥全部存放在 TPM 或者 TEE 硬件可信根里，私钥明文一直不会导出到操作系统内存中，所有的交易加密、签名运算都在硬件隔离的环境中完成，上层业务系统只给可信硬件传递交易摘要，不能接触到原始密钥的内容[2]。每一个交易产生的签名中都会包含终端硬件环境的度量凭证，区块链网络可以对签名所对应运行环境的完整性进行核验，如果设备系统被篡改，那么对应的签名凭证就不能通过校验，从根本上防止密钥泄露、伪造交易等安全问题的发生，实现密钥全生命周期硬件隔离防护，提升区块链交易环节底层安全能力。

（二）智能合约可信执行机制

传统的智能合约在公开的操作系统环境下运行，合约代码的漏洞很容易被攻击者利用，合约的计算过程没有隔离保护，执行的结果存在被篡改的风险。基于 TEE 的智能合约可信执行机制把合约部署、运算、输出全过程放在可信隔离环境中，合约代码在

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

部署时先做完整性度量，再做漏洞和后门检测，有安全问题的合约立刻停止部署并显示错误消息，合约被校验之后进入 TEE 隔离执行空间，可信执行环境同普通操作系统、外部网络彼此隔离，外界不能干涉、篡改合约内部业务逻辑，合约完成运算之后，结果经由硬件签名之后提交到区块链网络当中去达成全网共识，并且合约完整的执行日志也被同步上链存证起来，从而达成合约运算过程可以被审计、结果不能被抵赖的目的，而且隔离了交易敏感业务数据，兼顾了合约运行安全和交易隐私保护[3]。

（三）可信数据溯源和存证机制

可信数据溯源和存证机制打通数据采集、传输、处理、存储全过程的业务链路，创建起端到端可信溯源体系。业务终端可信节点在原始数据采集环节完成硬件完整性校验，保证数据源设备本身没有被篡改；数据传输过程中执行加密安全传输，流转到 TEE 环境进行数据处理和完整性校验；设备行为日志、度量记录、业务操作记录实时固化，并把数据摘要和日志信息上传到区块链完成共识存证。当出现业务纠纷、数据争议的时候，可以调取链上固化下来的存证记录，准确找到异常发生的位置、异常的操作行为，从而实现责任认定和司法取证的目的，解决传统业务中数据源造假、流转过程无迹可查、责任无法划分的现实问题，给政务、工业、医疗等各个行业的业务审计提供可信的技术支持。

二、可信计算和区块链技术融合所遇到的难题

（一）安全和性能之间存在矛盾

可信硬件完整性度量、硬件隔离运算都会造成一定的性能开销，节点可信校验、交易硬件签名、合约隔离执行都会使系统处理流程变长，从而直接导致区块链共识处理时延变长[4]。根据目前的实测工程数据可知，采用可信计算后的区块链架构吞吐量比原来的区块链架构低50%到70%，交易延迟提高了2到4倍，在高频交易和大规模节点组网的情况下，多层安全校验互相叠加，很容易导致交易排队、系统吞吐量急剧下降。目前大多数技术方案都把安全能力放在首位，缺少增量度量、分级轻量化校验的设计思路，没有对度量策略进行动态适配，很难在安全防护等级和系统并发性能之间找到平衡点，成为制约技术大规模商业化落地的主要障碍。

（二）技术兼容性不好、缺少标准

目前可信硬件种类繁多，Intel SGX、ARM TrustZone、国产 TCM、TPM2.0等各种硬件接口规范、密码运算逻辑各不相同，公有链、联盟链在共识算法、权限控制、网络模型等各方面存在较大差异，可信计算模块缺乏通用适配接口，对不同的硬件、不同的链平台要进行大量的定制开发工作，大大提高了研发成本。行业层面还没有形成可信计算和区块链融合的统一技术标准、测评评估体系，技术方案碎片化严重，不同的厂商开发出来的系统不能实现跨设备互通、组件复用，从而提高技术对接和迭代升级的成本[5]。

（三）部署成本高、运维难度大

原生区块链系统只需要普通的服务器软件部署就可以完成组网，但是两者融合系统必须使用 TPM、TCM 或者 TEE 专用可信硬件，硬件采购、现有节点改造都会增加硬件成本。整个融合系统包含可信硬件、操作系统、密码学组件、区块链网络等多个技术栈，故障来源涉及面广，系统排错定位困难，对于中小企业来说，由于人力、资金等各方面的限制，很难完成系统的部署和常态化的运维工作，从而导致轻量化业务场景的落地门槛较高。

（四）缺少隐私保护以及合规性的改进

目前大多数融合方案把重心放在节点防篡改、数据存证能力的建立上，但是精细化的隐私保护能力还有欠缺[6]。节点运行日志、设备度量记录里含有大量的用户交易信息、设备敏感数据，如果没有做脱敏处理，就会存在敏感信息泄露的风险。政务、金融、医疗等行业监管要求千差万别，不同行业的数据访问、数据脱敏、数据保留的合规要求也不一样，现有的技术体系并没有将这些不同的行业标准区分开来，而是一成不变的一般化隐私保护策略，无法适配强监管行业的深层次业务。

三、可信计算和区块链技术的融合策略以及应用场景

（一）全方位技术改进措施

根据安全性能失衡、兼容性差、成本高、隐私合规弱这四个问题，从四个方面提出改进方案。从性能角度出发加入增量度量、分级校验轻量化机制，在高风险的组件处实行高频度的完整性校验，低风险的组件降低度量频率，从而优化底层密码算法，减少由于硬件校验造成的性能损耗；在兼容性方面推进统一硬件接入接口协议的研发，让一个组件可以对接多种可信硬件以及主流联盟链、公链平台，提高模块的复用程度；从成本上来说，增添轻量化软件可信方案，部分低安全等级的业务可削减专用硬件的依赖，创建自动化运维平台，达成节点度量状态的自动监测，故障的自动报警，缩减运维人力需求，隐私合规部分利用零知识证明，同态加密这些技术保障原始数据保密，给政务，医疗，金融等各类领域规划不同的隐私政策[7]。

（二）政务数据可信共享场景

政务领域一直存在着跨部门数据孤岛、业务权责不清、审计溯源难等状况，依靠四层融合架构，各个委办局的业务节点都安装了国产 TCM 可信硬件，对整机软硬件进行了完整性度量，业务数据被加密后在跨部门之间流转，所有的操作日志都被上链固化；跨部门联合统计分析业务在 TEE 密态环境中完成，原始政务数据不会离开本地业务节点，从而达到数据可用但不可见的目的[8]。以自然资源部不动产登记长安链平台为代表，各个业务节点部署国产 TCM 模块，不动产权属、交易记录经过硬件签名完成存证，跨省市业务查询不需要线下交换原始档案，纠纷溯源效率得到明显提高，完全符合政务业务监管和审计的要求。

（三）能源和工业物联网可信运维场景

在电力能源方面，电网服务器装有 TCM 可信硬件，智能电表带有轻量级 TEE 芯片，发电量、用电负荷数据经由硬件度量签名后上链，智能合约自动执行电费结算、碳资产确权，异常计量节点依靠动态度量来完成实时隔离。国家电网分布式能源区块链试

Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

点接入了数万个可信电表节点，涉及了多省的光伏项目，实现了大量能源交易的可信执行，碳资产数据全部可以追溯，成功地对接到了全国碳市场监管系统中[9]。工业物联网场景下，工业网关装有 TrustZone 可信执行环境，设备工况、故障数据采集前就进行硬件校验，度量报告一同上传到业务数据上链，维保、融资租赁业务在 TEE 环境下调取设备真实工况，三一重工根云平台工程机械设备节点依靠这一机制有效地降低了融资租赁纠纷，减少了整体维保成本。

（四）医疗和供应链金融溯源场景

医疗健康场景中医院服务器部署国产 Occlum TEE 组件，患者病历、影像原始数据保存在本地，只保存哈希摘要和度量日志上链，跨院数据调取、科研建模需要得到患者的授权，所有的运算都在密态 TEE 环境中完成，原始医疗数据不会流出到外面，同济协和医联体可信平台用 FISCO BCOS+TCM 架构实现检验结果跨院互认，保证了医疗业务的协同以及个人信息的保护[10]。在供应链金融和商品溯源场景里，核心企业的节点装入 TPM2.0 硬件之后，供应商的单据、物流信息会被 TEE 进行签名后上链，应收账款凭证支持拆分转融流动，冷链、消费品终端装备可以利用轻量级 TEE 来获取流通数据，监管机构可以实现整个链条的溯源，华能“能信”供应链平台以及京东智臻链一物一码系统都已经证明了该种模式的效果，减少了中小供应商的融资成本，提高了商品问题召回的速度。

四、结语

区块链分布式信任体系和可信计算硬件级安全防护存在很强的技术互补性，两者融合起来，可以很好地解决传统区块链节点环境不可控、隐私保护不足、私钥安全风险大、智能合约执行不可靠等问题。利用私钥交易防护、智能合约可信执行、可信溯源存证这三个主要的机制来创建起一个硬件可信、执行可控、数据可信、全网可溯的全链路分布式可信系统。但是技术落地过程中还存在着安全性能不能兼顾、标准体系缺乏、部署运维成本高昂、隐私合规性不匹配等问题。经过轻量化度量改造、统一接口标准创建、削减落地门槛、行业差别隐私规划，可以促使技术走向规模化落地。政务、能源、工业物联网、医疗、供应链金融等领域的大量工程实践表明，将可信计算与区块链相结合，可以很好地解决链上链下之间信任的难题，给跨主体数据协同和数字化可信业务提供强有力的支撑，并且要不断推动国产可信硬件的适配、行业标准的制定，充分发挥技术应用的优势。

参考文献

[1] 关志，胡建斌，李悦，陈钟 . 基于可信执行环境的区块链技术与应用综述 [J]. 信息网络安全，2025,25(11):1673-1690.

[2] 周子楠，樊星，任思名，等 . 基于区块链技术的可信域扩展 [J]. 计算机工程与应用，2026,62(17):318-331.

[3] 陈辛迪 . 基于区块链的票据可信交易管理技术研究 [D]. 南京邮电大学，2024.

[4] 费书凡 . 基于区块链的跨域通信安全与隐私保护研究 [D]. 西安电子科技大学，2025.

[5] 廉康，刘力铭，罗伟雄 . 隐私计算与区块链在高校间数据共享的应用路径探索 [J]. 软件，2025,46(1):169-171.

[6] 孙爽，唐华云，贾晨 . 面向区块链数字债券应用的链上链下协同方案研究 [J]. 债券，2024,(10):81-85.

[7] 吴忠辉 . 基于区块链的边缘分布式计算卸载关键技术研究 [D]. 北京邮电大学，2024.

[8] 张守恒 . 基于可信执行环境的区块链隐私保护 [D]. 东南大学，2024.

[9] 杨雅萱 . 面向区块链的边缘计算资源调度与任务卸载研究 [D]. 东南大学，2024.

[10] 陈龙飞 . 区块链可信传感器数据上链及跨链关键技术研究 [D]. 中原工学院，2024.

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License