基于区块链的加油交易记录防篡改机制设计

杜　剑　索　毅（内蒙古自治区产品质量检验研究院，内蒙古　呼和浩特　010010）

摘　要：为提升加油交易记录的可靠水平和可追溯性，依靠链式存证结构、改进型共识流程和智能合约约束逻辑构建起防篡改机制，把含有内蒙古自治区产品质量检验研究院节点的联盟链架构作为验证环境，探究交易数据上链模型、节点同步策略以及多级校验流程。该机制在多场景篡改测试中可迅速找出异常位置，维系记录结构的长期连贯性，给加油业务的数据治理搭建工程化的方法路径。

关键词：加油交易记录；防篡改机制；区块链存证；共识验证

中图分类号：TP311.13　　**文献标识码：**A　　**文章编号：**1674–5167（2026）009–0034–04

Design of a Tamper-Resistant Mechanism for Blockchain-Based Fuel Transaction Records

Du Jian, Suo Yi (Inner Mongolia Autonomous Region Product Quality Inspection Institute, Hohhot Inner Mongolia 010010, China)

Abstract: To enhance the reliability and traceability of fuel transaction records, a tamper-proof mechanism is constructed using a chained evidence structure, an improved consensus process, and smart contract constraint logic. Utilizing a consortium blockchain architecture incorporating a node from the Inner Mongolia Autonomous Region Product Quality Inspection Institute as the verification environment, this study explores transaction data on-chain models, node synchronization strategies, and multi-level verification processes. This mechanism rapidly identifies anomalous locations during multi-scenario tampering tests, maintains long-term consistency of record structures, and establishes an engineering methodology for data governance in fueling operations.

Keywords: fuel transaction records; tamper-proof mechanism; blockchain evidence storage; consensus verification

加油业务在多源计量设备、站内控制系统及外部结算平台协同工作时，构建起高频的数据交互链路，记录内容在采集、输送和存储阶段，皆可能受未被批准的操作影响，不易满足质量监管与计量追溯的可信性需求[1]。

就该问题而言，构造以链式存证结构、共识过程和智能合约为核心的防篡改手段，规范好交易数据上链格式、节点同步模样和记录校验流程，并在包含内蒙古自治区产品质量检验研究院的监管链路里核实其可追溯能力。

研究试图提出一套可开展工程化部署的可信记录体系，为加油交易全流程的数据一致控制及后续追溯给出技术途径。

1 加油交易记录的可信性需求分析

加油交易记录在采集、传送与存储过程里，都有被截取、替换或者伪造的潜在风险，特别是在计量设备、POS 终端以及结算系统的多源数据汇集时，记录内容往往靠本地程序或人工做校对，缺少统一可靠的核实机制[2]。

不管哪个节点的数据泄漏、缓存被替代或未获准许的修改，都会让交易量、油品类型、单价和时间戳出现差错，进而影响后续账务核算、监管抽检这两项工作的有效性。就“内蒙古自治区产品质量检验研究院”等质量监管机构的抽检流程举例，交易记录完整性对计量准确性判定有直接关系，倘若源端记录跟存档版本不一致，会引起追踪路径的中断，对事故取证以及责任的划分有影响。

伴随站内控制系统与外部结算平台对接频率的提升，跨系统同步出现时间延迟、缓存覆盖写入及本地日志无法验证等问题，进一步拉高了可信的风险水平，交易记录迫切要采用链式结构，做到全阶段可追溯，且能迅速识别篡改举动。

2 区块链防篡改机制的核心原理

2.1 数据结构的不可逆性特征

区块链存储加油交易记录时采用链式哈希结构，借助对区块头部以及业务字段做定长摘要计算，达成不可倒逆的映射[3]。处于上链的流程当中，处理节点先把“交易量、单价、设备编号、时间戳”等相关字段按预设字节序拼接，造就原始数据块 x，随后调用 SHA 256 模块生成当下区块的哈希值。数据结构关系由

$$H_i=SHA256(D_i||H_{i-1})$$

确定，

其中：

H_i 为第 i 个区块哈希；

D_i 为该区块的加油交易数据帧；

H_{i-1} 为前一区块的哈希引用。

在实施生成进程，系统在缓存区采用 32 字节对齐的操作方式，保证摘要计算的输入长度始终固定；当要写入新区块的时候，验证节点借着链式指针对比本地区块副本，借助逐级哈希重算方式对结构一致性进行校验。链路构造完毕后，节点基于增量写入策略只更新最新的区块索引，防止有全链扫描的情况出现，提高上链速度且形成稳固的数据结构依赖链。

2.2 共识过程的可信一致性保障

加油交易链借助改进型 PBFT 共识流程，借助预准备、准备、提交三个阶段，实现交易记录在多节点间的一致落盘 [4]。主节点遇上上链请求以后，按照区块序号、时间戳和摘要值封装交易数据，将其变成提案消息后广播给各验证节点；验证节点在本地进行摘要重算以及签名的核实，验证无误后进入准备阶段，向全网反馈确认讯息。系统采用最小确认阈值判定机制：

$Q=2f+1$

其中：

Q 为完成共识所需最少确认数；

f 为在 n 个节点中允许的最大失效节点数，满足 $n \geqslant 3f+1$。

当收集的准备消息数量达到阈值后，各节点进入提交阶段并写入区块存储区。通信层设置 150–300ms 的消息超时参数，超时节点自动剔除并进入下一轮视图切换。

2.3 智能合约的自动记录约束逻辑

加油交易链上，智能合约凭借事件触发方式执行记录约束逻辑，合约内部依照字段校验、状态迁移以及区块写入三个步骤来固化流水 [5]。业务端提交交易申请之际，采集模块将“油枪编号、加油量、单价、计量时间戳、设备签名”等参数写入输入的结构体，合约入口函数依据预先设定的字段范围与签名验证规则做有效性检查；随后按照状态机顺序实施交易锁定、计量确认与记录封装事宜。状态迁移过程由

$S_{t+1}=F(S_t,e_t)$

描述，

其中：

S_t 为当前交易状态；

e_t 为触发事件（如计量完成、设备上报、校验通过）；

$F(\cdot)$ 为合约内置状态转移函数。

迁移事宜完成之后，合约去调用链上的存储接口，将交易摘要与区块索引写入专属存证区域。合约执行环境给出 10–20ms 的 Gas 限制时段，异常分支进入回退逻辑，杜绝未完成的交易记录进入链上体系，还依靠事件日志向节点传达最终存证结果，达成交易记录在上链前后逻辑边界的一致化管控。

3 加油交易防篡改机制体系设计

3.1 交易数据上链模型构建

交易数据上链模型围绕着加油业务的计量、支付及设备链路展开，创建统一的数据封装格局，保证各字段进入区块前构建出标准化的数据帧 [6]。采集端以计量控制器作为数据起始源，把油枪编码、加油量、单价、时标脉冲与设备签名按固定字节顺序排列，生成字节长度介于 256 到 512 之间的交易报文，且在发送前添加序列号用于链上排序。节点接收到报文的瞬间，依靠预设的字段解析模板对业务参数拆分，将其映射于区块数据区与摘要区的双层框架；原始交易内容由数据区进行记录，摘要区存有哈希值和前一区块引用，造就链式关联。为保障上链顺序具备可验证性，模型在进行写入操作阶段引入局部缓存池，按照序号把多源报文重新排列，杜绝跨设备上报频率的差异造成区块装配混乱。模型设置了按时间戳进行冲突检测的逻辑，若两笔交易在毫秒级时间窗口中出现字段重叠的情形时，系统按照设备签名的优先级挑选有效记录，保证最终写入的区块结构坚实且字段布局相符。

3.2 节点部署与同步架构设计

节点部署架构把加油站本地集控中心作为核心，构筑计量终端、站级服务器与监管侧节点的多层合作结构 [7]。站内节点对加油终端所报交易报文进行预先处理、摘要计算和区块封装操作，在本地维持 2–3 个副本以实现快速校验；区域监管节点（如内蒙古自治区产品质量检验研究院业务链路这般）通过 VPN 隧道加入联盟链，按照周期同步最新区块高度，接着参与共识投票。为降低跨地区网络时延造成的共识阻塞现象，系统在通信层开启以区块高度为基础的轻量同步模式，各节点根据高度的差值请求增量区块，防止整链拉取占用网络带宽。同步窗口按照链负载在 5 至 20 区块范围动态调整，保证高峰期站级节点的写入速率稳定。各节点凭借心跳报文对其对端状态加以监测，若掉线了则触发视图切换流程，保障共识网络在多节点波动的情况下维持持续运转与顺序同步结构。

3.3 记录校验与追溯流程设计

记录校验流程分三步执行：区块索引的定位、哈希值的重算以及交易级证明的生成。查询端把交易序列号输入后，节点借助区块高度映射表找到对应区块，并从数据区拿出原始字段，按照上链时的字节排列顺序去重新拼接数据帧 [8]。系统调用哈希模块再次计算摘要，并同区块头中记录的摘要值开展比对；若摘要达成一致，就进入 Merkle 路径搭建阶段，交易级证明已审核通过

$R=H(H(a||b)||H(c||d))$

计算得到，

其中：

a,b,c,d 为同一区块内与目标交易同层的摘要节点，

$H(\cdot)$ 为哈希函数，

R 为校验所需的 Merkle 根。

追溯过程中，节点按路径顺序验证每级摘要，若任一层不一致则停止流程并返回错误标识。

4 系统实现与效果验证

4.1 数据采集与上链写入实现

数据采集流程在计量控制器、加油终端与站级节点的协同下完成，计量控制器以 50–100ms 的周期去读取流量脉冲、单价参数以及油枪状态，生成带了签名的原始数据帧；终端设备接收数据帧完毕后，添上设备编号和高精度时间戳，按特定格式封装成上链报文。站级节点拿到报文后，先做字段完整性检查以及设备公钥验证，通过相关验证后，把报文放进缓存池且启动摘要计算模块，以 SHA 256 生成 32 字节的哈希数值，依照区块装配规则归入待写入区。装配线程根据给定的区块大小阈值（建议 64–256KB）和时间窗口参数（300–500ms）触发区块生成，达成区块头、区块体与前置哈希的绑定。最终区块依靠共识模块广播给其他节点，监管侧节点（含有内蒙古自治区产品质量检验研究院链路）同步区块高度并保存证的复印件，实现多方可检验的写入体系。

4.2 性能测试与稳定性评估

在开启链式记录结构运行性能验证的时候，把站级节点的并发上报请求由低负载渐渐提升到高负载区间，对写入延时、摘要计算用时与吞吐能力等关键指标开展量化测定，然后结合监管同步节点（包含内蒙古自治区产品质量检验研究院链路）的区块确认情况达成完整评估结果，测试所得结果见表 1。

从表 1 可察觉到，当并发请求数从 50 上升至 500，写入延时呈线性累积走向，共识确认阶段在整体阶段中占比最大，是影响总体响应时间的主要源头；摘要计算耗时的增长幅度呈现相对平稳状态，说明哈希模块在高并发情况中仍可维持可控的负载。吞吐量到 300req/s 之后，增幅呈现减缓态势，主要受区块装配时间的增长以及广播负载增加的共同干扰；高并发阶段节点同步成功率稍有降低，但依旧处在 98% 以上，监管节点的区块高度更新始终维持连贯，契合追溯链搭建需求。

4.3 篡改场景模拟与抗性分析

为验证链式记录结构针对异常输入与恶意构造区块的检测本事，模拟字段伪造、区块替换、节点回滚这三类典型的篡改做法，马上在多节点环境当中记录校验模块、共识模块以及监管节点（含有内蒙古自治区产品质量检验研究院链路）的响应行为反馈，测试的结果于表 2 中可见。

从表 2 可看到，三种单一篡改方式在节点本地

表 1 不同并发条件下写入延时与吞吐性能测试结果

并发请求数（req/s）	平均写入延时（ms）	摘要计算耗时（ms）	区块装配耗时（ms）	共识确认时延（ms）	吞吐量（TPS）	节点同步成功率（%）
50	82	11	24	47	46	100
100	109	14	31	64	87	100
200	153	17	39	92	162	99.8
300	198	20	52	121	215	99.5
400	247	27	66	158	261	98.9
500	302	35	81	203	288	98.1

表 2 典型篡改类型与节点检测响应结果对照表

篡改类型	注入方式描述	节点校验触发点	检测耗时（ms）	共识阶段响应	监管节点同步结果
字段伪造	修改加油量、时间戳等关键字段	摘要比对时发现哈希不符	14–22	拒绝进入准备阶段	记录异常摘要，拒绝入链
区块替换	伪造前置哈希并构造错误区块头	区块引用校验失败	21–33	触发视图切换，丢弃伪造区块	高度偏差报警并阻断同步
节点回滚	强制恢复至旧区块高度并尝试提交新记录	高度比对检测异常	27–41	不满足确认阈值，提交被拒绝	记录回滚事件并重建索引
多字段复合篡改	同时篡改计量字段、设备编号与前置哈希	多级摘要与索引均不匹配	35–58	全网拒绝进入提交阶段	形成完整异常路径记录

校验阶段均被快速拦截，检测花费的时间基本落入 14－41ms 区间，字段伪造的触发起始点最靠前，所以耗时相对较少；区块替换跟节点回滚因为涉及到了链式引用和高度比对，检测时间稍有上扬。在多字段复合篡改这样的场景中，由于多个校验点同时呈现出异常，耗时显著上扬，但全网均不接受提交，而且监管节点同步把完整的异常链路记录了下来，该过程进一步证明了，篡改对照机制在复杂异常情况之下可维持结构化响应能力。

5 结语

加油交易记录的链式存证框架借助数据结构、共识流程跟智能合约约束的协作，架构了可校验、可跟踪的技术体系，达成了从采集链路到监管节点全程的一致性管理。诸多场景模拟表明，借助多级校验，可迅速找到字段伪造、区块替换和节点回滚，夯实了交易链条的结构化安全界限。就后续工作而言，可以把节点部署的区域层级拓展至计量监管与行业质检体系进一步，引入计量设备可信标识及跨链验证手段，以搭建覆盖加油业务全流程的高可信数据基础支撑。

参考文献：

[1] 高志琨，袁亮，马彦，等．智慧运维一体化平台代码防篡改技术研究 [J]. 电子设计工程，2026,34(01):13-16.

[2] 鞠琳．区块链技术在公安档案溯源与防篡改中的应用研究 [J]. 兰台内外，2025(33):6-8.

[3] 代永铨．基于区块链技术的汽车检测数据防篡改机制研究 [J]. 汽车测试报告，2025(07):76-78.

[4] 张西霞，王欢，于浪．基于区块链的嵌入式机器人运行数据防篡改传输控制系统设计 [J]. 计算机测量与控制，2024,32(10):139-145+153.

[5] 吴晗，魏佳，李娟．基于区块链技术的工业互联网数据防篡改共享网络结构模型 [J]. 自动化应用，2023,64(10):220-222.

[6] 王兴泰．信息技术下机械企业防篡改审计系统设计 [J]. 造纸装备及材料，2022,51(02):91-93.

[7] 杨非，曾铮，夏绪彬．区块链在水利行业政府网站防篡改中的应用研究 [J]. 水利信息化，2021(06):34-39.

[8] 周黎．基于区块链技术的防篡改审计系统设计 [J]. 微型电脑应用，2021,37(12):206-208.