

基于区块链技术的电子轮机日志系统

聂野¹, 毛世红², 张云军², 于书强², 李义华³

(1. 武汉德尔达科技有限公司, 湖北 武汉 430000; 2. 长江航道局, 湖北 武汉 430000;
3. 武汉德尔达科技有限公司, 湖北 武汉 430000)

摘要: 研究了一种基于区块链技术的新型电子轮机日志系统。系统可以定时定点连续性地自动提取船舶轮机日志相关的各项数据, 借助区块链的点对点网络进行自动上传和加密, 利用区块链的不可篡改特性实现了轮机日志的全程留痕、便于追溯的需求。研究协助更加完整和安全的记录轮机日志, 提供更为方便的查询分析方法, 为船舶轮机日常管理和事故追溯提供支撑。

关键词: 轮机日志; 区块链; 数字摘要; 共识机制; 智能合约

中图分类号: U66

文献标识码: A

文章编号: 1006—7973 (2021) 08—0061—03

轮机日志是反映船舶机电设备运行和管理工作的原始记录, 是船舶的法定文件之一, 是海事决策与监管的主要凭借依据, 必须妥善保管。按照规定, 轮机日志应依时间顺序逐页连续记录, 不得间断、遗漏、撕毁和增补, 应使用不褪色的蓝色和黑色笔记录填写, 数字和文字要准确, 字体清楚端正, 计量单位采用国家法定计量单位。

目前船舶上的轮机日志主要是通过人工填写的方式完成记录, 轮机长全面负责审查监督轮机日志的记载及保管, 船舶航行状态信息的记录由船员负责填写, 受船员主观意识影响较大。在船舶发生险情时, 状态信息的记录会面临时间和情形限制, 会导致船舶状态信息记录不完整、不正确的风险。同时, 纸质化手工书写船舶状态数据的记录方式不便于计算机识别、提取、处理, 记录的数据也不便于高效地查询和分析。

在本研究中提出了一种基于区块链技术的电子轮机日志系统, 系统将纸质的轮机日志转化为可靠存储的电子轮机日志, 为用户安全方便的记录、查询、管理轮机日志提供帮助。

1 系统结构

轮机日志包含的内容多且复杂, 而且随着科技发展需要记录的内容和类别会不断变化, 因此本研究没有将轮机日志完全记入区块链, 而是采用数据库存储日志完整内容, 将日志的存储路径和数字摘要部分记入区块链。根据以上思路, 电子轮机日志系统包括日志服务模块、区块链平台和数据库, 如图 1 所示:

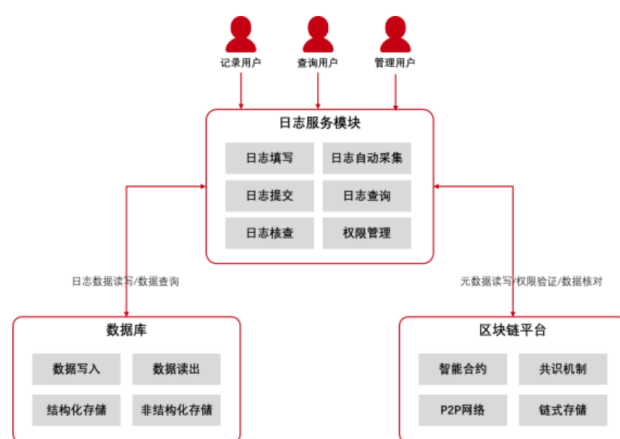


图 1 电子轮机日志系统总体结构

用户按照不同的业务需求分为记录人员、查询人员和管理人员, 用户访问日志服务模块完成轮机日志的记录、查询和核验等业务功能。日志服务模块包括日志填写、日志自动采集、日志保存、日志查询、日志核查等业务功能模块, 通过数据库相关接口完成日志数据的存储工作, 依据约定算法将日志存储路径和日志的数字摘要计算得到元数据, 调用区块链平台的智能合约实现元数据读写、系统权限验证、系统数据核验等功能。

区块链平台采用以太坊技术构建, 以太坊是一种基于智能合约的开放式区块链平台, 开发者可以编写智能合约并将合约部署到以太坊中创建去中心化应用, 实现了在没有可信第三方的情况下进行可追踪、不可逆转的交易。本研究的智能合约主要针对元数据和用户权限构建, 针对轮机日志主要为内部使用的特点优化了系统的共识机制。

数据库部分系统可以采用关系型数据库, 也可以采用非关系型数据库, 只需要具备日志属性等结构化数据

和情况描述等非结构化数据的存储功能即可。从日志数据的安全性考虑,建议采用分布式数据库。

2 系统功能

电子轮机日志系统的功能主要通过日志服务模块体现,包括日志填写、日志自动采集、日志提交、日志查询和日志核查等。在系统功能实现过程中,需要区块链平台和数据库提供支撑。

2.1 日志填写

日志填写功能主要用于记录船舶轮机相关的各类事件及台账,这部分内容多为非结构化数据,系统无法自动获取,需要记录用户按照实际情况填写。填写内容具体包括:船长、轮机长的命令,值班驾驶员的通知;船舶的重要活动;检修工作记录;燃油、润滑油加装、调驳的时间、地点、品种及数量;船舶防污染设备的使用情况,污水的排放时间、地点;机电设备发生故障的原因及其处理经过;船舶应急设备的检查、试验情况;船舶固定消防系统的检查、试验情况;船舶重要设备的检修及进行明火作业的部位、审批情况;船舶重要设备的更换情况及主要技术数据;船舶交通事故、机损事故发生的时间、地点、主要经过及其处理情况;轮机部人员的重大人事变动等。系统将以上内容按照轮机日志的格式要求,分门别类列出供记录人员填写。

2.2 日志自动采集

日志自动采集功能用于采集船舶航行和机舱设备运行情况的结构化数据,本功能无需用户操作。系统可以通过部署于船舶端的各类感知设备中获取数据,完成该部分日志数据的自动采集。可以自动采集的数据包括:主机启动、主机停止的时间,主机正常运行时的转速;船舶靠离码头、进出港区、航行于危险航区及进行编解队作业的时间、地点和车钟令;柴油发电机组、辅助锅炉及机电设备的启用时间和停止时间;驳油量、驳水量,燃油舱转换量及轻重燃油转换的时间;机电设备发生故障及恢复正常的时间;燃油、润滑油消耗量、库存量等。自动采集只需要管理人员针对当前船舶进行系统配置即可,一旦配置完成,系统即可根据约定的采集频率和协议进行连续自动的数据采集,无需用户操作。自动采集的数据类型多样,多数情况下并不能符合轮机日志的格式要求,需要进一步的数据转换和处理。

2.3 日志提交

日志提交功能用于完成日志的数据采集和填写后,定期自动将日志数据提交至后台存储,本功能无需用户操作。轮机日志的提交涉及日志数据的保存和日志元数据的上链,具体过程包括数据处理、日志保存、数字摘要生成和元数据上链等。

(1) 数据处理。自动采集的数据,需要按照轮机日志的格式要求进行处理。在符合轮机日志格式要求后,将自动采集数据和人工填写的数据按照约定的时间段(一般是自然日)组合,形成原始轮机日志数据。根据需要,原始的轮机日志数据可以采用对称加密的方式,生成轮机日志密文存储。

(2) 日志保存。系统调用数据库的相关接口,将原始轮机日志数据上传至数据库进行保存,获取数据的存储路径。

(3) 数字摘要生成。哈希算法是计算机领域中非常基础且重要的算法,它可以将任意长度的二进制数据映射成较短的二进制串(哈希值),且不同的二进制数据映射的结果极大的概率下是不同的。本研究中利用SHA256的算法获取原始轮机日志数据的哈希值,称为轮机日志的数字摘要。利用哈希函数抗碰撞的特点,数字摘要可以用来判断轮机日志内容是否被篡改,对数据完整性进行校验。但是,若数字摘要值被篡改则数据完整性的验证失去了意义。因此,数字摘要需要被保存到区块链中以保证安全性。

(4) 元数据上链。数据的存储路径对应轮机日志的存储内容,数字摘要则可以保证存储的轮机日志未被篡改,本研究将存储路径和数字摘要统称为元数据,下一步就需要将元数据保存在区块链上,这就涉及到区块链平台的机制。系统将采用拜占庭共识机制作为区块链平台的共识机制,元数据产生后当前节点作为输入端启动交易,按照智能合约,交易将被发送给当前视图的主节点,主节点负责分发元数据到在线节点进行运算,当运算结果达到算法要求的一致性时即产生新的区块并加入区块链,完成元数据的上链操作。

2.4 日志查询

日志查询功能用于查询指定条件的轮机日志,并按照指定格式进行展示,本功能主要面向查询用户。轮机日志数据存储在数据库中,数据存储路径作为元数据的一部分存储在区块链中,因此若想访问日志数据,需要

首先进入区块链平台,调用智能合约获取数据存储路径。系统可以设置允许其他哪些节点访问本节点写入的轮机日志,设置完毕后,当某节点发起日志查询交易时,合约函数会对调用者身份进行判断。通过交易的签名可以得到发起者的真实身份,没有私钥的情况下无法伪冒身份。具体的日志查询流程包括:

(1) 查询人员调用日志查询功能,系统根据查询条件构造数据访问交易提交至区块链平台,并使用私钥对交易签名。

(2) 区块链节点先验证交易签名,签名在许可范围内则启动上链机制,将数据访问的时间和以太坊账号打包并广播到全网,在区块链网络对交易达成共识后,形成查询交易区块上链,供数据所有者对访问记录溯源。

(3) 系统获取元数据,根据数据存储路径从数据库中获取对应的轮机日志数据,与元数据中的数字摘要进行核对运算验证数据完整性,最后返回给客户端。

(4) 如果在提交时有对称加密操作,则用户使用对称加密密钥解密获得的密文数据,得到明文。

2.5 日志核查

日志核查功能是定时或在事故发生时对全部或者部分轮机日志进行核查追溯,查看日志数据是否被篡改、日志写入查询等操作记录等,主要面向机务主管部门的管理用户。日志核查的范围主要包括:

(1) 元数据有效性核查。定时在元数据区块链上验证指定区块区间的相邻区块 Hash 值是否吻合。即检查当前区块的 pre-hash 字段值是否为上一区块的头的 hash 值,以及当前区块头的 Datahash 是否为本区块所有交易的 hash 值等。

(2) 数据库数据有效性核查。定时追溯区块链中的元数据区块,提取元数据区块中数据存储路径对应的数据库数据,计算每条轮机日志数据的数字摘要,与元数据中存储的数字摘要进行比对,核查数值是否吻合。

(3) 用户访问记录核查。核查全部或者指定的用户访问记录,查看用户的访问时间及账号,检查是否符合相关审核程序与授权许可。

(4) 特定船舶轮机日志核查。对特定船舶提取符合查询条件的电子轮机日志记录,形成该船舶完整的轮机日志报告,作为相关事件处理的电子依据。

3 结论

电子轮机日志系统可以定时定点连续性地自动提取轮机日志的各项状态和数据,并且自动保存并上传。系统采用了基于区块链技术的分布式存储,并且可以通过数据同步机制自动恢复,避免了传统数据存储模式下的单点故障风险,保证了系统的可靠性。系统利用区块链技术实现了管理范围内全部船舶的分布式透明记账功能,采用数字签名的过程保证了信息传输的安全性,防止了对数据传输内容的篡改行为。系统的研究有助于提升船舶轮机日志的完整性和可靠性,对于降低轮机工作强度和提升轮机工作效率具有重要意义。

参考文献:

- [1] Nakamoto S. Bitcoin: A Peer-to-peer Electronic Cash System [EB/OL].<https://bitcoin.org/bitcoin.pdf>, 2008-10-31.
- [2] King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake[EB/OL]. <https://www.kryptographie.com/peer-peer-crypto-currency-proof-stake>, 2012-08-19.
- [3] drdobbs. The Byzantine General's problem[J]. Acm Transactions on Programming Languages & Systems, 1982, 4(3):382-401.
- [4] Castro M, Liskov B. Practical Byzantine fault tolerance[C]//Symposium on Operating Systems Design and Implementation. USENIX Association, 1999:173-186.
- [5] 熊志强,周吴.基于区块链技术的电子病历研究[J].中国数字医学,2019(01).

