基于区块链的矿用产品全生命周期溯源系统

宁振兴，安　迪，杨　博

（中煤科工集团信息技术有限公司，陕西　西安　712200）

摘要：区块链技术的发展在近些年取得了显著成果，作为新一代信息技术，被广泛地应用于智能矿山、交通运输等领域。其中，区块链技术应用于矿用产品安全领域，尤其是在大型设备井下安全问题溯源中的具体应用，可以加强矿用产品的质量安全管理。基于此，本文针对矿用产品质量安全管理监管的薄弱环节，论证区块链技术在煤矿设备安全溯源中的应用的基础上，以区块链为基础构建了矿用产品全生命周期溯源信息平台，研究了区块链技术的创新应用在矿用产品安全溯源上的提升效果，实现了产品质量安全相关问题的有效溯源，有助于建立矿用产品安全可信平台。

关键词：区块链；溯源；矿用产品；全生命周期

中图分类号：F49；TP311.13　　**文献标识码：**A

DOI：10.12230/j.issn.2095-6657.2022.32.025

近年来，由于机械设备故障而造成的重大安全事故不在少数。因此，国家在“十二五”期间，在原国家安全监管总局的明确要求和指导下，建立了煤矿重要设备物证溯源支撑服务系统。这无疑对煤炭行业的设备管理、井下风险规避起到了重要作用。传统溯源有着自身的局限性，例如，数据可以随时通过后台更改，这就导致了数据的不守信，对溯源工作造成了极大的困扰。由于区块链自身具有数据透明、不可篡改、永久运行三大特性，天然地为溯源系统提供了强有力的技术支持。首先，数据受信的问题可以得到技术上的解决，使得溯源链上的数据变得真实可信；其次，由于区块链的数据透明，所有上链数据都可以查询得到，获取信息的难度也较低。因此，采用区块链+溯源技术可以充分完成反应对煤矿重要设备的溯源。

1 区块链技术

从本质上讲，区块链是一个共享型数据库，在其上存储的数据或信息，具有五大特征，分别是“难以伪造”、“过程留痕”、“全链追溯”、“透明公开”、“分布存储”。基于这些特征，区块链天然地拥有了坚实的“信任”基础，为全链创造了可靠的“合作共享”机制，具有广阔的应用前景。区块链通常作为分布式账本、数字签名、溯源存证等核心技术的组合，基于区块链技术创建矿用产品全生命周期溯源信息管理平台，能够强化矿区设备的监测、缩短矿用产品在途时间并使设备维保问题得到有效溯源，对于加强矿用产品质量安全管理、促进矿用产品供应链优化有重要意义。

1.1 区块链架构

数据层是区块链的基础，主要实现了相关数据存储、账户和交易。数据存储主要基于 Merkle 树，通过链式结构实现，以 KV 数据库的方式实现持久化，比如以太坊采用 LevelDB 数据库存储。

（1）网络层是区块链网络节点和通讯，是点对点技术，没有中心服务器、依靠用户群自发地交换信息而构成的互联网体系。与有中心服务器的网络不同，网络里的每个端既是一个节点，也有服务器的功能，这使区块链具有去中心化与健壮性的特点。

（2）共识层实现所有节点的交易和数据的一致性，能够有效地防范拜占庭攻击等共识攻击，其算法称为共识机制。

（3）激励层主要实现区块链代币的发行和分配。智能合约，是由事件驱动的、具有状态和多方承认的，且运行在区块链之上、能够根据相应条件自动处理的程序，智能合约可以利用程序替代仲裁和执行合同[1]。

智能合约具有可编程特性，区块链可以通过 VM 的方式运行。同时，可以通过在智能合约添加可交互的 web 界面，形成 DAPP[2]。

1.2 数据上链

（1）数据上链的意义

数据上链是指用户将自己的数据通过加密上传到 ipfs 的公网侧链，同时在公信链形成相应的数据索引的过程。数据一旦上链，除非本人授权解密外，无论个人或者组织，都无法获取到用户上传的数据，从而保证了数据的绝对安全。

数据上链的意义在于：1）提升数据安全和隐私保护，利用区块链分布式记账技术将数据分割成许多块并存放在网络中的不同节点上时，作为整体，它们是难以被破坏的，这意味着对数据安全性和隐私保护程度的提升，这些文件还使用私钥加密，以确保其他参与节点无法查看用户本人的文件；2）降低社会信任成本，利用区块链技术，经过用户的授权，帮助用户采集自己的数据并加密保存至区块链上，同时将数据私钥 Data-Key 交给用户本

人管理，由用户完全掌握所有权和支配权，用户将数据上传到区块链上，通过私钥掌控自己的数据，通过分享自己的数据产生使用价值，并生成自己的可信数字身份，在与人协作中大大降低了信任成本；3）提高数据的传输速度，传统的云存储系统允许用户将数据上传到云服务器，之后，服务提供者负责在其数据中心保存这些信息，除非特别要求，否则数据中心与用户或用户的客户通常不会在同一个地方，根据地理区域的不同，数据访问可能会出现延迟，因为信息要在不同的服务器之间传输，而区块链使用的是节点网络，利用大量的节点群来存储和管理数据，检索数据时，每个节点从离它最近、最快的节点开始并行搜索，以减少延迟，因此数据传输速度得到了提升。

（2）上链方式

用户可以通过验证哈希存证判断文件内容有无被篡改，例如，把一个原文的哈希值存储上了区块链，当用户再次拿到这个文件时，对其内容进行哈希运算，如果和链上存储的内容一致，则认为内容可信，没有被篡改；如果哈希值不同，则认为内容已经被篡改，不再可信。

本项目采用的是隐私存证，目的是将数据进行加密并存储于区块链上，主要是针对链上的数据公开透明而选取的储存策略。通常对数据加密都采用的是对称加密，所谓对称加密是指加密和解密使用同一个密钥，这样的加密方案比较简单、快速，适合大量数据的加密。

本项目所建设的区块链产品追溯系统应用后，将企业煤机产品及关键零部件有关的大量产品质量检测记录、装配记录等结构化数据和售后用户使用、维护产品的半结构、非结构化数据在与客户方沟通后将数据上链用于质量追溯。同时，通过大数据分析模型建立 FEMA 进行设计、工艺改进，提升产品的质量，也可以基于大数据分析进行关键零部件的使用寿命预警服务，给用户提供更加精准、高效和高价值的服务。

2 区块链溯源

在本文中提出的基于区块链的矿用产品溯源系统建设解决方案中，链上数据虽然是公开的，但是数据在共享时会对矿用产品数据进行加密处理。为保护交易过程中商品售卖方提供的矿用产品溯源文件数据的安全性，一般会通过对称加密的方式来限制矿用产品溯源文件数据的获取。同时，供应链中的原材料供应商以及外协件生产商会将原材料制造过程信息和矿用产品生产过程信息同步至 IPFS 所在的数据库中，为保护矿用产品的数据隐私，还需要将文件进行哈希加密处理，最后将对称加密后的密钥存储于区块链中，使用过程中会通过用户所拥有的权限来控制数据的分享和获取 [3]。

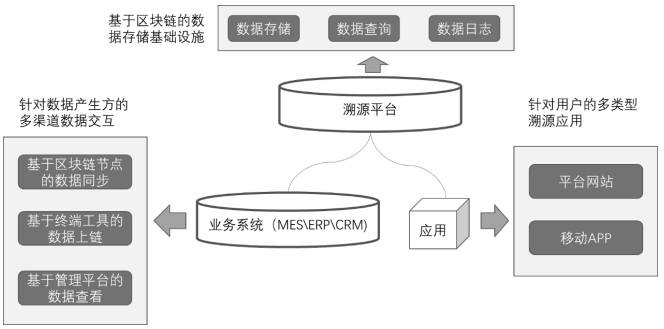

图 1　区块链溯源解决方案

系统将会使用 AES 加密算法对上链的文件进行加密处理，密文传至区块链后再将密钥发送至用户手中。用户通过查询后可以获取文件哈希，然后向上传用户请求解密密钥，并进行数字签名。文件持有者作为生产者，对数据消费者身份确认后，将密钥发送给数据消费者，消费者再使用密钥对数据进行解密，得到文件返回的哈希，利用哈希检索得到源文件。这种通过将文件加密来控制用户访问数据权限的方式，在不改变数据公开透明性的前提下，针对敏感数据做了保密处理，使得用户只能获取与自身消费相关的数据，增强了链上数据的安全性。本方案在实施中通过 Rinkeby Test Network 和 IPFS 系统对方案进行可行性测试。

2.1 系统架构

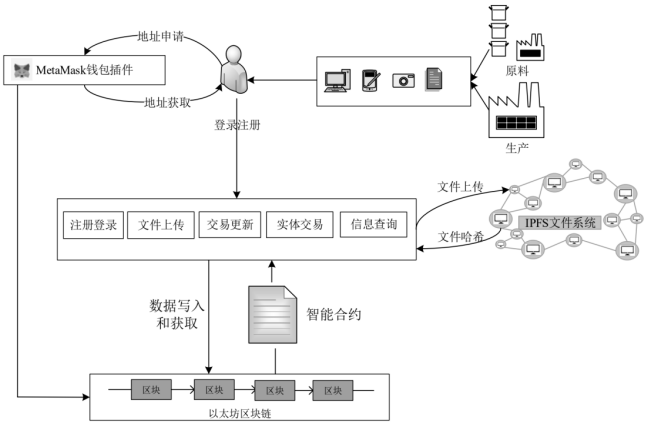

图 2　系统架构设计图

根据对矿用产品全生命周期溯源系统的需求分析和功能描述，本文结合以太坊、MetaMask 和 IPFS 系统搭建了溯源模型架构，如图 2 所示。图 2 详细阐述了区块链溯源模型架构中组件的功能。供应链中可以通过 MetaMask 来获取用户地址，在获得实体属性后，将实体属性分为供应商、生产商、分销商、零售商和监管机构。供应商和生产商在采购和产品生产过程中进行数据采集，通过传感器、射频识别（RFID）、二维码等新一代信息技术，采用非侵入的方式采集矿用产品生产过程的相关数据。由于区块链只能存储一种文本信息，所以引入了 IPFS 系统，可以将图片、文件等数据存入非结构化数据库中，同时将文件哈希回传至区块链。系统使用以太坊作为底层区块链技

术架构平台，便于在区块链中进行数据的写入和读取。本文提出的矿用产品全生命周期溯源系统模型主要涉及区块链中数据的存储、数据共享时的信息写入和读取。

2.2 智能合约实现

本文利用线上编译器进行智能合约 DAPP 的开发。合约在编写完成后通过 JavaScript 进行进一步的开发编译，同时在虚拟机上完成 DAPP 的部署，并测试相关功能。同时加载相对应的 api 作为前端与区块链交互的接口，编译测试完成后，将 DAPP 发布到区块链网络，部署在区块链 EVM 中，生成相对应地址，等待服务器调用 [4]。

2.3 数据存储

矿用产品全生命周期溯源平台方案中，数据的存储主要分为两个部分，第一个是在 IPFS 中的文件，其次是通过 DAPP 将信息写入到区块链中。本次试验首先对 IPFS 的存储性能进行测试。首先进行测试环境的搭建准备工作，安装完成后对 IPFS 进行初始化，在初始化完成后就可以上传本地文件进行读写速度测试；上传后，经过 IPFS 进行分片处理和哈希变化，同时将生成的哈希值返回到用户手中；用户拿到哈希值后便可以对文件进行下载速度测试。在本次测试过程中均采用本地文件 [5]。

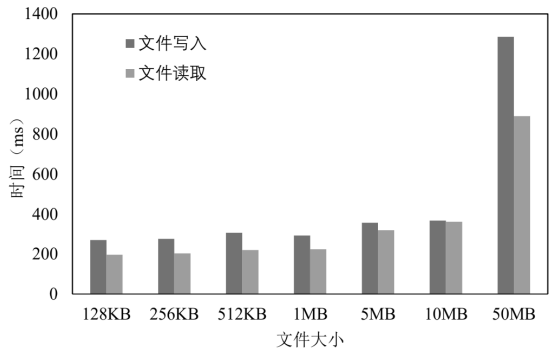

图 3　IPFS 文件读写性能测试

2.4 基于区块链的矿用产品全生命周期溯源系统

通过采集产品的生产信息、产品数据和物流相关数据并将数据同步至区块链，区块链会根据采集到的生产过程数据和相关检测人员等信息，自动生成一个溯源二维码，将二维码对称加密后上传到区块链。溯源二维码与数字签名相绑定，存放在链上，为每台矿用设备生成唯一“身份证”，并附上时间戳。产品的生产过程数据以及出厂合格标准是煤矿企业最关心的问题，产品出厂的信息记录会随着产品出厂、物流使用等的生命周期不断地更新，通过生产设备采集的加工数据，每个环节的安全生产信息、出厂物流信息等，通过更新区块链中的标识，进而更新矿用产品的“身份证”。煤炭企业可以通过手机扫描铭牌包装上的二维码信息并输入加密密钥，就可以获取产品生成、加工、物流运输和销售的全过程信息。

3 讨论

综上所述，本文在系统的数据安全方面，对敏感数据进行了额外加密处理，并根据系统功能设计了 DAPP。区块链技术仍然面临着与身份注册、隐私和法规等相关的问题，并且在系统的实际应用过程中，不能完全保证上链数据的准确性，需要对数据质量进行监督并设立相关的奖惩机制，同时将监管数据上链以保证数据的准确性。

4 结语

本文以区块链技术作为支撑搭建了矿用产品的溯源系统，利用以太网为技术核心对矿用产品的生产、物流和使用等各个环节进行全生命周期溯源，通过对数据跟踪监督，以及分布式存储和执行业务交易数据，消除了煤矿企业担心的追溯性过程中数据的准确性以及可信度问题，实现了矿用产品从生产到使用到报废全生命周期的精准溯源，保证了整个矿用产品的安全性，使得矿用产品的溯源工作简单高效。矿用产品生产过程的可追溯，不仅使得矿用产品质量得到有效保证，同时也保证了下游供应链的可靠稳定，为企业的生产管理和市场开拓提供了方便性和数据支撑，提升了企业在当前形势下的竞争优势。

参考文献：

[1] 贺海武，延安，陈泽华 . 基于区块链的智能合约技术与应用综述 [J]. 计算机研究与发展 .2018，55（11）：2452-2466.

[2] 邵奇峰，金澈清，张召，等 . 区块链技术：架构及进展 [J]. 计算机学报 .2018，41（05）：969-988.

[3] 邢毓华，张瑶 . 工业缝纫中二维码防伪溯源系统的研究与实现 [J]. 计算机测量与控制，2018，26（07）：132-136.

[4] 钱卫宁，邵奇峰，朱燕超，等 . 区块链与可信数据管理：问题与方法简 [J]. 软件学报，2018，29（01）：150-159.

[5] 刘家稷，杨挺，汪文勇 . 使用双区块链的防伪溯源系统 [J]. 信息安全学报，2018，3（03）：17-29.

作者简介：宁振兴（1994–），男，陕西西安人，工程师，从事机械制造业的智能制造转型工作，主要从事新一代信息技术与传统制造行业的交叉学科研究。