DOI 编码：10.13646/j.cnki.42-1395/u.2022.10.021

基于区块链的航运数据安全存储共享方案

高志伟，范洪博，刘锦江

（昆明理工大学信息工程与自动化学院，云南 昆明 650000）

摘　要：随着全球航运业的增长，航运业传统的经营模式如依赖纸质文件等使得贸易通常耗时且昂贵，难以实现各个机构间对于航运数据有效共享。而区块链其不可篡改、去中心化等特点结合智能合约与物联网技术可提供航运过程可靠追踪服务与数据安全存储共享。本文提出一种航运数据安全存储共享方案，在保护数据安全性的同时实现了数据的细粒度共享，并将与星际文件系统融合有效地降低了区块链节点的存储压力。

关键词：区块链；智能合约；航运；IPFS

中图分类号：TP393　　**文献标识码：**A　　**文章编号：**1006—7973（2022）10-0057-02

航运交易涉及大量纸质文件，例如销售合约、租船合同协议、提单、港口文件、信用证以及与船舶和货物有关的其他信息。无论在付款还是运输的各个环节这些文件均需要通过一长串缔约方耗时耗力。此外传统的纸质单证由于处理和审核时间较长，实际交付往往会发生延迟，并且还存在造假的风险。区块链可通过智能合约等对传统航运物流复杂流程极大地简化[1]。航运物流中一个主要挑战是监控产品质量并跟踪其物理运动直至到达最终用户。目前，许多装载射频识别、温湿度传感器、全球定位系统等传感设备的集装箱可以在运输阶段提供实时装运跟踪。但是传感器设备存在遭受网络攻击的风险，如常见的拒绝服务攻击等，这为欺诈行为打开了窗口。区块链与物联网技术在提高安全性和存储从物联网使用中收集的数据方面是互补的。物联网使用传感器监控、收集数据，区块链可以消除对中心化的需求，在分类账上存储不可篡改且可追踪的记录的数据来改进当前供应链中的跟踪系统[2]，从而解决了围绕物联网和数字化使用的一些安全问题，可供所有相关方使用。

1 背景技术

1.1 智能合约

智能合约是一种部署在区块链上可自动执行的协议，允许在没有可信第三方的情况下直接在区块链网络上进行通信，在区块链不可篡改、安全性基础上还具有图灵完备、确定性、可编程等特性，并且一旦满足了触发条件后就会自动执行[3]。并且区块链网络中的节点都会执行，不存在某些节点发生故障影响智能合约的运行。航运中的各种文档或数据，如产品原产地证书和食品植物检疫证书等可以通过智能合约上传到区块链，安全高效地交换信息，从而避免了相关机构跟踪和认证信息的需要，可以最大限度地简化并提高航运交易的效率和透明度。

1.2 物联网技术

物联网（IoT, Internet of things）是一个将互联网与各种信息采集传感设备连接起来的网络。通常将物联网分为感知层、网络层、应用层。感知层由收集信息的传感器等设备组成实现跟踪、监控物体的功能。网络层主要实现网络通信的问题。应用层主要对数据信息进行分析和处理。物联网技术可实时记录航运物流中货物信息，可减少航运业务中多种信息不对称。然而物联网设备数量多且分散以及数据量大，可能出现信息窃取、篡改等安全问题，并且其中心化的管理方式在数据隐私、安全方面存在着隐患。区块链中其不可篡改、去中心化特性与物联网相结合可以为航运提供可靠追踪方案。

1.3 星际文件系统

星际文件系统 (IFPS) 是一个点对点、去中心化的文件系统。综合了分布式哈希表、自认证文件系统、版本控制系统等系统的优点。它将用户数据以 256KB 为大小划分为多个数据块，并分散存储在 IPFS 网络的节点中。每个数据库都是根据其内容生成唯一的内容标识符 (CID)。通过使用路由协议根据其 CID 获取数据。

2 航运数据安全存储共享模型

2.1 模型架构

区块链不是为了存储大量数据而设计的；然而，跟踪供应链上的货物可能会产生大量数据，并需要持续地、长期地处理和存储这些数据。这将需要大量的处理速度和存储空间。此外，在涉及区块链的所有情况下，数据的隐私都是一个潜在问题[4]，因为分类账记录是永久性

的，所有参与者都可以查看和共享可能被视为私人或专有的数据。以及出于保守商业秘密的需求更加需要保护数据，避免数据过度透明等。而且如果将数据明文直接上传至 IPFS，意味着任何人只要能获得 CID 值后，就可以直接访问用户上传的数据，这样无法实现数据的受控访问。

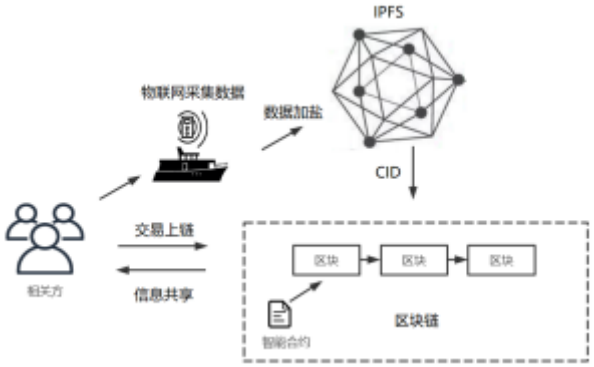

图 1 基于区块链的航运数据安全存储方案

因此提出一种基于区块链的航运数据安全存储方案，如图 1 所示。本文采用电子提单、数字化文档、交易数据等数据通过智能合约上传至区块链中。将跟踪货物产生的数据经过加盐后上传至 IPFS 网络中，得到与其数据内容一一对应的 CID 值，确保数据不可被篡改。IPFS 存储传感器收集到的大量实时货物数据，仅将固定长度、数据量较小的 CID 值存储在区块链中降低区块链节点的存储压力。区块链存储并执行智能合约，将经过共识后的数据写入区块链账本中，同时针对身份不同提供不同的访问权限，以实现信息的安全共享 [5]。

2.2 隐私数据加密和共享

航运数据中可分为包含可能暴露相关方商业机密影响企业利益的信息、利益相关用户在航运过程不愿公开的敏感信息等的隐私数据。以及可在区块链中公开存储所有人可访问的非隐私数据。物联网传感器采集到的数据限于物联网终端设备如传感器等在计算能力、传输带宽等方面资源有限，一些需要一定量数学运算的加密方式可能会降低终端设备采集数据的处理速度。本方案主要包括盐值生成、隐私数据上传、隐私数据共享 3 个部分。

2.2.1 盐值生成

参与航运交易的各相关方包括交易的双方、港口的工作人员、代理人等，每个参与方生成自己的初始值。各相关方共同商讨出一个相关方公共初始值，并对其进行 sha256 运算。

2.2.2 隐私数据上传

（1）每个相关方对自己的初始值进行 sha256 运算得到盐值，并将所要上传的数据与自己的盐值进行一次异或运算，以加密信息。

（2）各相关方对异或自己盐值后的数据再与公共盐值进行一次异或运算，确保除了相关方外的其他人员无法知道数据。

（3）将加密后的数据存入 IPFS 中并获取返回的 CID 值。

（4）调用智能合约将 CID 值上传至区块链，待区块链节点达到共识后将其写入区块链账本中。

2.2.3 隐私数据共享

（1）用户 A 将自己的初始值通过点对点的方式传输给所要共享数据的用户 B。

（2）用户 B 对 A 的初始值进行 sha256 运算得到 A 的盐值。

（3）用户 B 对加密的数据分别用公共盐值与 A 的盐值进行两次异或运算即可得到原文数据。实现了数据在 A 与 B 之间共享。

（4）在上传数据前更改初始值即可结束数据共享。

3 结论

本文利用区块链技术与物联网技术可对航运数据数字化提高航运效率。同时结合 IPFS 构建了一个基于区块链的航运数据安全存储共享模型，可有效降低区块链节点的存储压力，同时区块链其不可篡改、去中心化等特点可解决当前航运数据缺乏数据安全存储以及共享问题，此外还实现了细粒度的访问控制。

参考文献：

[1] 沈庆琼，钟晓燕 . 区块链技术在港口航运领域的应用 [J]. 物流技术 ,2018,37(12):63-66.

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

[3] 欧阳丽炜，王帅，袁勇，倪晓春，王飞跃 . 智能合约：架构及进展 [J]. 自动化学报 ,2019,45(03):445-457.

[4] 刘伟军 . 区块链技术在航运物流业中的运用与法律规制 [J]. 南京社会科学 ,2020,(02):89-94.

[5] 梅颖 . 基于区块链的物联网访问控制简化模型构建 [J]. 中国传媒大学学报 (自然科学版),2017,24(05):7-12.