ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 66

Risk Analysis and Crisis Response under the Background of the Belt and Road (RAC-18)

Research on Dynamic Management Technology of Dangerous Goods Based on Block Chain Technology

Di Li, Jianzhong Sun

Saifeite Engineering Technology Group Co., Ltd. Qingdao,266600, China

基于区块链技术的危险品动态管理技术研究

李迪， 孙建中

赛飞特工程技术集团有限公司，青岛 266600，中国

Abstract

As a decentralized infrastructure and distributed computing technology, block chain has attracted the attention of government departments, financial institutions, and technology companies. Within the characteristics of decentralization, time series data, collective maintenance, security, and trust ability. It is suitable for constructing new currency systems, financial systems, and even social and industrial systems. In this paper, a Blockchain-based infrastructure model for dangerous goods transactions is proposed by deconstructing the core elements of the block chain, the application scenarios and significance are described, which provides reference and reference for future related research.

Keywords: Block chain, Dangerous goods management, Supervision

摘要

区块链作为一种去中心化基础架构与分布式计算，目前已经引起政府部门、金融机构、科技企业的高度重视与广泛关注。区块链技术具有去中心化、时序数据、集体维护和安全可信等特点，适合构建新的货币系统、金融系统乃至社会和行业系统。本文通过解构区块链的核心要素，提出了基于区块链技术的危险品交易区块链基础架构模型，阐述了危险品流动区块链的应用场景及意义，探讨了现有技术存在的一些问题和不足，为未来相关研究提供参考与借鉴。

关键词：区块链，危险品，动态管理，监管

1. 技术背景

目前国民生产存在众多危险品企业，涉及生产、运输、储存等多个环节，任何一个环节出现问题，都有可能造成严重的事故[2,3]，以危险品典型事故“天津 8.12 危险品爆炸事故”为例，该起事故造成 162 人死亡，直接损失超过 60 亿，事故的直接原因就是涉事企业违规超量存放危险品，引发起火爆炸，另外在事故救援过程中因无法明确危险品种类、数量，又导致数十名消防官兵牺牲，企业违规超能力储存、监管空白、数据不明导致灾难性后果非常严重，因而急需加强对危险品动态和过程管理（图 1），目前政府对危险品的管理手段还十分匮乏，尤其是对于危险品的过程管理更是处于盲区，基于区块链技术对于交易数据的可溯源，不可篡改、伪造特性，正可为危险品动态全过程管理提供了解决方向。

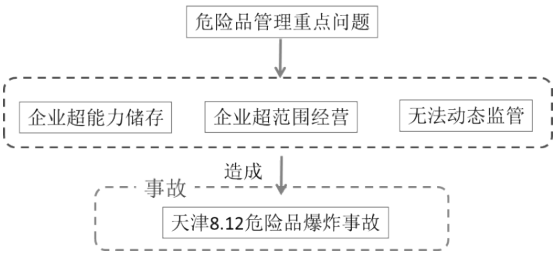

图 1 危险品动态管理典型问题

Fig1 Typical problems of dynamic management of dangerous goods

区块链技术的核心优势是去中心化，能够通过运用数据加密、时间戳、分布式共识和经济激励等手段，在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作，从而为解决数据溯源、数据可信性等问题提供了解决方案。

从数据的角度来看，区块链是一种几乎不可能被更改的分布式数据库。这里的“分布式”不仅体现为数据的分布式存储，也体现为数据的分布式记录（即由系统参与者共同维护）。从技术的角度来看，区块链并不是一种单一的技术，而是多种技术整合的结果。这些技术以新的结构组合在一起，形成了一种新的数据记录、存储和表达的方式。

因此，作为一种存储和记录技术，区块链技术因其可追溯，且不可篡改，去中心化等特性，在危险品交易及动态管理可以解决诸多问题。

2. 区块链实现技术原理

目前区块链技术基础架构模型已较为成熟，典型的基础模型如图 2 所示，一般说来，区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成[4]。其中，数据层封装了底层数据区块以及相关的数据加密和时间戳等技术，网络层则包括分布式组网机制、数据传播机制和数据验证机制等，共识层主要封装网络节点的各类共识算法，激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等，合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础，应用层则封装了区块链的各种应用场景和案例。

该模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点[5,6]。

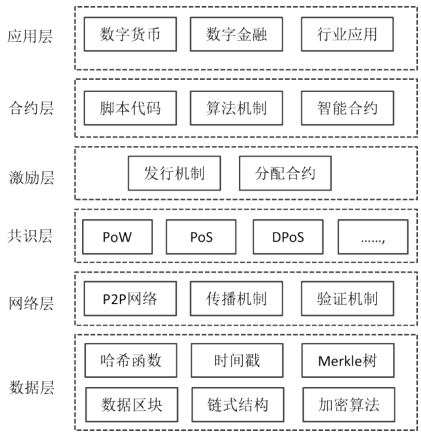

图 2 区块链基础架构模型

Fig.2 A basic framework of blockchain

2.1 数据层

狭义的区块链即是去中心化系统各节点共享的数据账本每个分布式节点都可以通过特定的哈希算法和 Merkle 树数据结构，将一段时间内接收到的交易数据和代码封装到一个带有时间戳的数据区块中，并链接到当前最长的主区块链上，形成最新的区块。该过程涉及区块、链式结构、哈希算法、Merkle 树和时间戳等技术要素。

数据区块：如图 3 所示，每个数据区块一般包含区块头（Header）和区块体

（Body）两部分。区块头封装了当前版本号（Version）、前一区块地址（Prev-block）、当前区块的目标哈希值（Bits）、当前区块 PoW 共识过程的解随机数（Nonce）、Merkle 根（Merkle-root）以及时间戳（Timestamp）等信息 [8]。比特币网络可以动态调整 PoW 共识过程的难度值，最先找到正确的解随机数 Nonce 并经过全体矿工验证的矿工将会获得当前区块的记账权。区块体则包括当前区块的交易数量以及经过验证的、区块创建过程中生成的所有交易记录。这些记录通过 Merkle 树的哈希过程生成唯一的 Merkle 根并记入区块头。

时间戳：区块链技术要求获得记账权的节点必须在当前数据区块头中加盖时间戳，表明区块数据的写入时间。因此，主链上各区块是按照时间顺序依次排列的。时间戳技术本身并不复杂，但其在区块链技术中的应用是具有重要意义的创新。时间戳可以作为区块数据的存在性证明（Proof of existence），有助于形成不可篡改和不可伪造的区块链数据库，从而为区块链应用于公证、知识产权注册等时间敏感的领域奠定了基础[7]。更为重要的是，时间戳为未来基于区块链的互联网和大数据增加了时间维度，使得通过区块数据和时间戳来重现历史成为可能[4]。

哈希函数：区块链通常并不直接保存原始数据或交易记录，而是保存其哈希函数值，即将原始数据编码为特定长度的由数字和字母组成的字符串后记入区块链。哈希函数（也称散列函数）具有诸多优良特点，因而特别适合用于存储区块链数据。例如，通过哈希输出几乎不能反推输入值（单向性），不同长度输入的哈希过程消耗大约相同的时间（定时性）且产生固定长度的输出（定长性），即使输入仅相差一个字节也会产生显著不同的输出值（随机性）等[4]。比特币区块链通常采用双 SHA256 哈希函数，即将任意长度的原始数据经过两次 SHA256 哈希运算后转换为长度为 256 位（32 字节）的二进制数字来统一存储和识别。

Merkle 树：Merkle 树是区块链的重要数据结构，其作用是快速归纳和校验区块数据的存在性和完整性。如图 3 所示，Merkle 树通常包含区块体的底层（交易）数据库，区块头的根哈希值（即 Merkle 根）以及所有沿底层区块数据到根哈希的分支。Merkle 树运算过程一般是将区块体的数据进行分组哈希[4]，并将生成的新哈希值插入到 Merkle 树中，如此递归直到只剩最后一个根哈希值并记为区块头的 Merkle 根。最常见的 Merkle 树是比特币采用的二叉 Merkle 树，其每个哈希节点总是包含两个相邻的数据块或其哈希值 [9]。

2.2 网络层

网络层封装了区块链系统的组网方式、消息传播协议和数据验证机制等要素。结合实际应用需求，通过设计特定的传播协议和数据验证机制，可使得区块链系统中每一个节点都能参与区块数据的校验和记账过程，仅当区块数据通过全网大部分节点验证后，才能记入区块链。

2.3 共识层

如何在分布式系统中高效地达成共识是分布式计算领域的重要研究问题。正如社会系统中“民主”和“集中”的对立关系相似，决策权越分散的系统达成共识的效率越低、但系统稳定性和满意度越高；而决策权越集中的系统更易达成共识，但同时更易出现专制和独裁。

2.4 合约层

合约层封装区块链系统的各类脚本代码、算法以及由此生成的更为复杂的智能合约。如果说数据、网络和共识三个层次作为区块链底层“虚拟机”分别承担数据表示、数据传播和数据验证功能的话，合约层则是建立在区块链虚拟机之上的商业逻辑和算法，是实现区块链系统灵活编程和操作数据的基础。包括比特币在内的数字加密货币大多采用非图灵完备的简单脚本代码来编程控制交易过程，这也是智能合约的雏形；随着技术的发展，目前已经

出现以太坊等图灵完备的可实现更为复杂和灵活的智能合约的脚本语言，使得区块链能够支持宏观金融和社会系统的诸多应用。

3. 危险品动态管理区块链关键技术实现

3.1 整体技术路线

基于区块链技术的分布式账本及数据的不可篡改、伪造特性，将危险品动态交易信息进行区块链技术实现，从而实现危险品交易过程记录，记录危险品的流向分析，通过对交易物流链的分析，判断企业是否存在超能力储存、超范围经营，以及解决以往无法对危险品动态及时管理的问题，危险品动态管理区块链整体技术路线如图 3 所示。

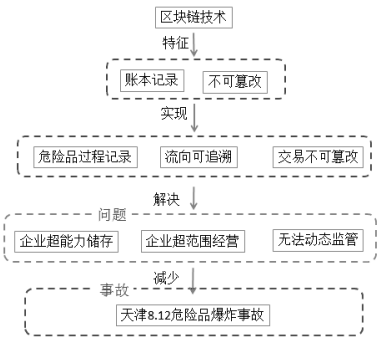

图 3 技术路线图

Fig3 Main technology roadmap

3.2 危险品交易数据结构

实现危险品实施区块链技术的动态管理，构建区块链的数据层极为重要，本节重点对于危险品动态管理区块链数据层进行说明。前面介绍了区块头结构，按照区块链技术构建危险品的区块数据结构，除区块头包括前一区块哈希值、时间戳、随机数、Merkle 根外，对于危险品区块体，应构建相应的交易数据，包括化学品类型、交易量、卖出方、买入方等关键信息，用于记录危险品流通过程，危险品交易区块结构如图 4 所示。

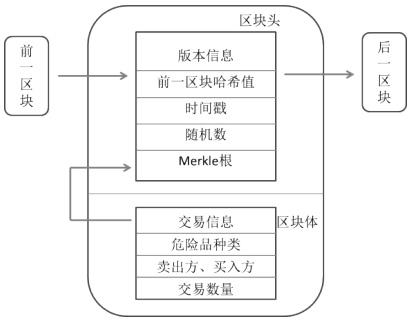

图 4 危险品交易区块结构

Fig 4 The structure of blocks for dangerous goods trading

3.3 构建危险品交易区块链 Merkle 树

前面已经说明了区块头哈希值、区块高度和区块头的结构，对于每次交易还需要构建区块体。区块体存储着交易信息，在区块中以一棵 Merkle 树的数据结构进行存储，而 Merkle 树是一种用来有效地总结区块中所有交易的数据结构。Merkle 树是一棵哈希二叉树，树的每个叶子节点都是一笔交易的哈希值，Merkle 树被用来归纳一个区块中的所有交易，同时生成整个交易集合的数字指纹即 Merkle 树根，也提供了一种校验区块是否存在某交易的高效途径。生成一棵 Merkle 树需要递归地对每两个哈希节点进行哈希得到一个新的哈希值，并将新的哈希值存入 Merkle 树中，直到两两结合最终只有一个哈希值时，这个哈希值就是这一区块所有交易的 Merkle 根，整个危险品交易区块链数据 Merkle 树构建及计算如下图 Merkle 根示意图 5 如下。

整个危险品交易 Merkle 根计算如下：

首先需要使用两次 SHA256 算法对每笔危险品交易数据进行哈希运算得到两笔交易的哈希值，这样可以得到 HA、HB、HC、HD 这 4 个哈希值，也就是这棵 Merkle 树的叶子节点。例如以甲乙企业交易危险品为例：

HA=SHA256(SHA256(交易甲+乙))

随后，对上层两个节点 HA、HB 的哈希值同样使用两次 SHA256 进行组合哈希运算，将会得到新的哈希值 HAB，同样可到另一个

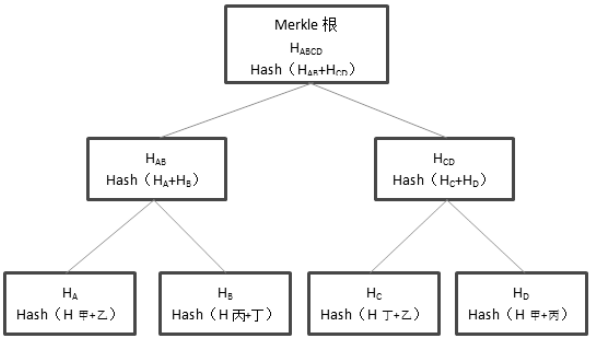

图 5 危险品交易 Merkle 树示意图

Fig5 Merkle tree of dangerous goods trading

哈希值 HCD，即

HAB=SHA(SHA256(HA+HB))

最后对 HAB、HCD 进行组合运算，得到最高层节点哈希值 HABCD，此值即得到危险品交易区块链的 Merkle 值，通过上述说明，可以发现，不管是一笔交易还是十万笔交易，最终归纳成一个 32 字节的哈希值作为 Merkle 树的根节点，同时根节点是根据每笔交易计算得的，因而每个节点数据都会影响最终的 Merkle 根，因此也就决定了数据串联性和难以更改。

另外当需要证明交易列表中某笔交易真实性时，一个节点只需计算 log2N 个哈希值，就可以形成一条 Merkle 树根到特定交易的路径，而不用计算所有的节点哈希值，Merkle 树效率入表 1 所示。

表 1 Merkle 树效率

Table 1 Merkle tree efficiency

交易数量（笔）	区块近似大小	路径大小（哈希数量）	路径大小（字节）
16	4	4	128
512	128	9	288
2048	512	11	352

4. 应用场景分析

根据前文所述，在危险品交易上构建交易区块链，对于整个危险品整个行业来说，可以联合企业构建联盟链，通过构建联盟链将危险品交易过程全记录，从而到起到以下作用。

（1）为监管部门提供危险品的动态信息，包括交易量，交易种类，对于各级监管部门，有效解决职责区域危险品的进出情况，危险品使用及储存情况，查找监管盲区及分析监管重点，避免胡子眉毛一把抓，监管重点不明。

（2）实现重点关注的定向监管

通过对重点关注的危化品进行标识，如剧毒品，进行定向追溯，实现重点控制，对于危险性极大的危险品重点管理，

（3）交易大数据分析

基于海量链上大量数据分析，从整体上掌握危险品的流向，地区分布等，为监管和决策提供参考，结合其他数据，在一定程度上可以为危险品事故预测提供数据支持。

（4）细节监管，如危险品超能力储存监督

现阶段，危险品企业出于各种原因会可能超能力储存经营，危险性极大，运输企业在装卸化学品后均将交易信息加入区块链，形成节点，每当新节点增加，就对节点包含的企业数据进行比对，进而判断是否企业超能力储存，依图 6 节点 3 可判断 A 公司超能力储存。

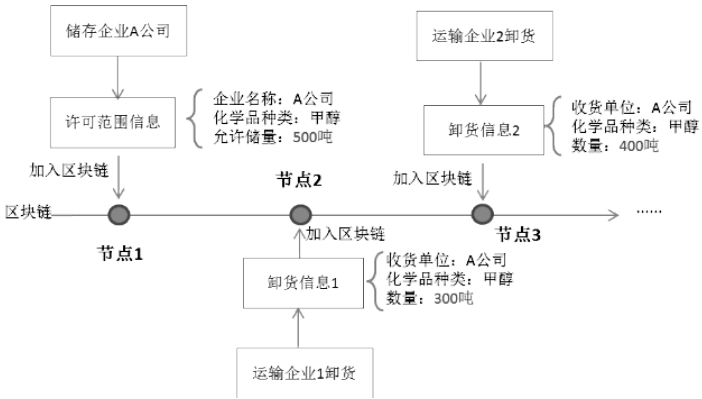

图 6 危险品交易区块链示意图

Fig6 Blockchain of dangerous goods trading

5. 存在的问题

5.1. 效率问题

区块链效率也是制约其应用的重要因素。首先是区块膨胀问题：区块链要求系统内每个节点保存一份数据备份，这对于日益增长的海量数据存储来说是极为困难的。虽然轻量级节点可部分解决此问题，但适用于更大规模的工业级解决方案仍有待研发 [9]。其次是交易效率问题，现有区块链技术每秒能处理的交易还非常有限，这极大地限制了区块链在大多数金融系统高频交易场景中的应用 [1]。

5.2. 技术融合问题

上述效率问题是区块链本身的技术特征决定的，本质上说是该技术本身存在的问题，对于在危险品动态管理应用区块链技术还需要解决与其他数据技术融合的问题，比如如何保证将危险品交易数据加入区块链，如何保证加入的交易数据是有效的等等，区块链技术在危险品动态管理上应用还依赖于相关支撑技术的落地，当然这也是区块链技术在其他行业落地面临的主要问题，这些还需要工程技术进一步发展。

5.3. 算力与能源消耗

区块链技术对于算力和能源消耗也是一个需要考虑的问题，尤其是当交易不断增长，交易数据可能成倍数增长，对于全网的算力以及支撑的电力消耗也会带来巨大的挑战，以目前比特币的电力消耗来说，目前全网的能源消耗已达 25TWh/a，相当于一个西欧国家爱尔兰的年用电量，而且绝对值还在快速增长，未来算力及能源消耗都必须是需解决的问题。

6. 探讨

从实际应用上说，目前区块链技术应用主要是数字货币，如比特币，另外一些金融机构也在构建区块链技术的应用，对于本文所述的危险品交易管理，还尚未有成熟的工业化技术方案，现阶段区块链技术更多的是一种线上技术，若要进一步渗透到各行各业，充分发挥区块链技术的数据的不可更改和可溯源，重构信用体系，还需进一步发展线下数据来源问题，也许当下一步物联网技术到来时，区块链技术就能水到渠成的落到实处，从这个角度来说，现在对于区块链技术的研究也是一种下一代技术的铺垫，本文也作为对新技术应用的思考。

参考文献

[1] Swan M. Blockchain: Blueprint for a New Economy. USA: O'Reilly Media Inc.，2015.

[2] 冷一芳，黄崇福. 社区应急管理风险雷达中预设表单式信息结构化研究初探. 中国灾害防御协会风险分析专业委员会第七届年会论文集(长沙, 2016 年 11 月 4-6 日)，pp. 890-896

[3] Xu X Y， Liu X Y, Guo G, Ji C. A method for assessing risk rating of natural gas pipeline based on accident statistics. Journal of Risk Analysis and Crisis Response, 2012, 2(1): 61-68.

[4] 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报，2016, 42(4): 482-483

[5] 丁未. 基于区块链技术的仪器数据管理创新系统.中国仪器仪表，2015，（10）: 15−17.

[6] Zhao H， Li X F，Zhan L K，Wu Z C. Data integrity protection method for microorganism sampling robots based on blockchain technology. Journal of Huazhong University of Science and Technology （Natural Science Edition），2015，43（Z1）:216−219

[7] Antonopoulos A M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. USA: O'Reilly Media Inc.，2014.

[8] Bitcoin Sourcecode［Online］， available: https://github.com/bitcoin/bitcoin/，January 18，2016

[9] Merkle R C. Protocols for public key cryptosystems. In: Proceedings of the 1980 IEEE Symposium on Security and Privacy. Oakland， CA， USA: IEEE， 1980. 122