

doi:10.6041/j.issn.1000-1298.2022.11.043

基于 DEMATEL - ISM 的粮油质量安全区块链优化

许继平^{1,2} 张博洋^{1,2} 张新^{1,2} 王小艺^{1,2} 李飞^{1,2} 赵燕东³

(1. 北京工商大学北京市食品安全大数据技术重点实验室, 北京 100048;

2. 北京工商大学中国轻工业工业互联网与大数据重点实验室, 北京 100048;

3. 北京林业大学工学院, 北京 100083)

摘要: 粮油质量安全直接关系到人民生命健康和国家安全稳定。粮油供应链具有主体复杂、风险多、供应网络跨域、信息链难以打通等特点,以区块链为代表的新一代信息技术为食品质量安全保障和追溯提供了新的解决思路和应用模式,但同时也引入了新的系统性风险,并且存在安全性方面的挑战。在解析粮油质量安全区块链风险和信息技术特征基础上,改进并优化现有完全非可信执行场景中通用型区块链结构,在网络层提出了一种适用于非完全可信执行场景中粮油质量安全专用型区块链网络结构,在共识层提出了一种基于 PBFT 改进拜占庭容错能力的符合粮油质量安全区块链特征的 Kafka 共识优化算法 P - Kafka,分别从正确性、去中心化、安全性、可扩展性、共识效率及一致性 6 个角度与传统共识算法做了性能对比分析。通过分析比较,所提出的网络节点分区与子链划分一定程度上节省了区块链系统运行成本并提高了节点的隐私安全,改进的 P - Kafka 共识算法具有了拜占庭容错能力并继承了 Kafka 分区优化的高吞吐量特性,更加适应粮油质量安全应用场景。

关键词: 粮油质量安全; 共识机制; 风险分析; 区块链; 网络结构; DEMATEL - ISM

中图分类号: TP399 **文献标识码:** A **文章编号:** 1000-1298(2022)11-0412-12

OSID:



Optimization of Grain and Oil Quality and Safety Blockchain Based on DEMATEL - ISM

XU Jiping^{1,2} ZHANG Boyang^{1,2} ZHANG Xin^{1,2} WANG Xiaoyi^{1,2} LI Fei^{1,2} ZHAO Yandong³

(1. Beijing Key Laboratory of Big Data Technology for Food Safety, Beijing Technology and Business University, Beijing 100048, China

2. Key Laboratory of Industrial Internet and Big Data, China National Light Industry, Beijing Technology and Business University, Beijing 100048, China

3. School of Technology, Beijing Forestry University, Beijing 100083, China)

Abstract: The quality and safety of grain and oil is directly related to people's life and health and national security and stability. The grain and oil supply chain is characterized by complex subjects, multiple risks, cross domain supply network, and difficulty in getting through the information chain. New generation information technologies, such as blockchain, providing new solutions and application models for food quality safety assurance and traceability, but also introducing new systematic risks, and there are security challenges. Based on the analysis of the risks and information characteristics of the grain and oil quality and safety blockchain, the general-purpose blockchain structure in the existing completely untrusted execution scenario was improved and optimized. At the network layer, a special blockchain network structure suitable for grain and oil quality and safety in non-completely trusted execution scenarios was proposed, and a Kafka consensus optimization algorithm P - Kafka based on PBFT improved Byzantine fault tolerance and in line with the characteristics of grain and oil quality and safety blockchain was proposed at the consensus layer. The performance of P - Kafka was compared with the traditional consensus algorithm from the perspectives of correctness and decentralization, security, scalability, consensus efficiency and consistency. Through analysis and comparison, the network node

收稿日期: 2021 - 12 - 17 修回日期: 2022 - 01 - 24

基金项目: 国家重点研发计划项目(2019YFC1605306、2017YFC1600605)

作者简介: 许继平(1979—),男,副教授,博士,主要从事区块链、工业互联网和智能信息处理研究,E-mail: xujiping@139.com

通信作者: 张新(1989—),男,副教授,博士,主要从事区块链与 AI 融合应用研究,E-mail: zhangxin@btbu.edu.cn

partition and sub chain partition proposed saved the operation cost of blockchain system and improved the privacy security of nodes to a certain extent. The improved P - Kafka consensus algorithm had Byzantine fault tolerance and inherited the high throughput characteristics of Kafka partition optimization, making it more suitable for grain and oil quality and security application scenarios.

Key words: grain and oil quality and safety; consensus algorithm; risk analysis; blockchain; network structure; DEMATEL - ISM

0 引言

粮油质量安全关系到人民群众的健康和社会的稳定,当前粮油质量安全问题主要集中在真菌毒素污染严重、非法添加有毒有害物、掺假勾兑以及以次充好等^[1]。近年来粮油质量安全事件引起了政府和社会的广泛关注^[2-4]。保障粮油质量安全对国民生命健康、社会和谐发展以及人类营养安全具有重要意义^[5]。

传统粮油质量安全监管体系多为中心化的模式,由供应链中核心企业集中采集全环节数据并存储到中心化的服务器进行管理,但中心化的管理模式易受篡改等攻击^[6],安全性无法保障。区块链作为一种去中心化的分布式账本技术,通过共识机制、加密算法、时间戳等底层技术保证上链的数据不被伪造和篡改^[7],因此适用于多主体业务系统进行数据信息共享管理的场景^[8-10]。区块链的技术特点决定了将其应用于粮油食品质量安全保障领域能够降低交易风险以及监管成本,提高数据可信度以及信息安全性等,为解决粮油质量安全溯源控制问题提供了解决方案^[11]。通过区块链技术建立粮油供应链参与主体间的互信机制,解决信息不透明、不对称等问题,对于快速追踪、精准定位粮油质量安全风险源头有重要意义^[12-14]。

目前粮油领域区块链技术的研究侧重于溯源监管等应用层面,包括基于区块链的信息溯源监管模型的研究以及结合区块链和物联网等技术的溯源监管应用研究等^[15-16]。此类研究虽在一定程度上解决了传统溯源监管技术存在的数据信任等问题,但由于粮油供应链具有主体复杂、风险多、供应网络跨域、信息链难以打通等特点,区块链技术应用于粮油质量安全保障和追溯场景下也引入了新的系统性风险和挑。基于传统公链改进存储、共识等的优化方案未能较好地解决区块链扩展性、性能、安全方面的局限,针对区块链技术的优化改进尤其是针对粮油领域等特定场景区块链技术应用的风险分析及优化改进逐渐兴起^[17-20]。

本文在综合国内外区块链技术应用研究现状及发展趋势的基础上,基于集成决策实验室法(Decision making trial and evaluation laboratory,

DEMATEL)-解释结构模型(Interpretative structural modelling method, ISM)可解释性算法模型解析粮油质量安全区块链风险特征,在此基础上改进并优化现有完全非可信执行场景中通用型区块链结构,包括在网络层研究适用于非完全可信执行场景中粮油质量安全专用型区块链网络结构,在共识层提出一种基于实用拜占庭容错(Practical Byzantine fault tolerance, PBFT)来改进拜占庭容错能力,符合粮油质量安全区块链特征的 Kafka 共识优化算法 P - Kafka(Practical Byzantine fault tolerance - Kafka),使得区块链在风险可辨识和可控的情形下适用于粮油质量安全专用场景。

1 基于 DEMATEL - ISM 的粮油质量安全区块链网络结构优化

粮油质量安全溯源控制场景下,供应链参与主体众多,且从粮油种植到成品售出全供应链中不同参与节点之间存在复杂嵌套、相互交织的关系,采用传统“一条链”式区块链及相应的共识机制容易造成区块链系统网络拥塞、计算成本高以及共识效率低等一系列问题。基于集成 DEMATEL - ISM 可解释性算法构造粮油质量安全区块链风险多级递阶有向图,建立粮油质量安全区块链优化网络结构,并对新型区块链网络中的参与节点进行分层分区以及子链划分,可在一定程度上节省区块链系统运行计算成本,提高节点隐私信息安全性以及全网节点共识效率。

1.1 基于 DEMATEL - ISM 的粮油质量安全区块链多级递阶网络结构

粮油质量安全溯源场景中参与节点众多、风险关联关系复杂且溯源数据量大,容易导致区块链网络负载大、延时较长、广播资源占用严重且耗能高等。粮油质量安全区块链系统中各风险节点关系错杂但处于同一网络系统,符合 DEMATEL 和 ISM 的应用条件,故引入 DEMATEL 和 ISM 两种系统分析方法并进行集成,根据粮油质量安全区块链风险间的关联关系对风险节点进行分层分区处理,以理清粮油质量安全区块链风险因素节点间的关联关系并改进传统粮油质量安全区块链网络的结构。

1.1.1 DEMATEL 和 ISM 结合机理

DEMATEL 是一种通过计算系统各要素的中心度和原因度进而分析该要素的系统重要性以及与其它要素间的相互作用关系的算法^[21]。ISM 是一种研究复杂系统内部各元素间的影响与被影响的关系,且能够清晰反映系统内部结构的结构模型化算法^[22]。

DEMATEL 和 ISM 两种算法各有优缺点,DEMATEL 虽能够通过系统要素的中心度、原因度等识别出复杂系统的关键要素及其影响程度,但其不能明确影响因素间的层次、结构,因此不能有效地对系统进行层次结构的划分,也不能确定系统的基础性要素和每个要素的影响范围。ISM 虽能确定系统各要素间的内在逻辑结构,但却无法知悉各要素的影响度与被影响度,即不能明确要素在系统中的作用。因此,本文综合两种算法的优势,通过 DEMATEL 简化 ISM 中可达矩阵的计算过程,构造集成 DEMATEL-ISM 可解释性算法模型,使得在明确粮油质量安全区块链风险因素影响权重的同时,形成层次性、结构化的多级递阶解释结构模型,具备更强的解释力。集成模型实施流程如图 1 所示。

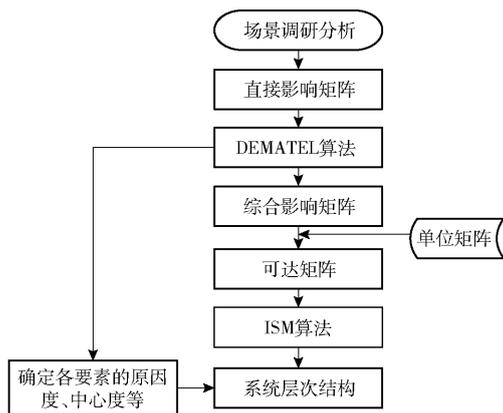


图 1 DEMATEL-ISM 集成模型实施流程

Fig. 1 Implementation process of DEMATEL-ISM integrated model

1.1.2 DEMATEL-ISM 集成模型实施步骤

实施步骤如下:

(1) 确定粮油质量安全区块链风险因素。通过分析已有研究成果并结合业内专家意见进行筛选处理,构建粮油质量安全区块链风险指标体系,如表 1 所示。

(2) 构建直接影响矩阵。基于构建的风险指标体系,通过专家小组问卷调研,对风险因素间影响关系进行量化评价,将风险因素间的影响程度定义为 [0,9] 内 10 个自然数等级,“0”代表影响因素对被影响因素无影响,依次递增,“9”代表影响因素对被

表 1 粮油质量安全区块链风险指标体系

Tab. 1 Risk index system of grain and oil quality and safety blockchain

| 风险分类 | 一级风险标号 | 风险指标 | 二级风险标号 |
|---------|--------|-------------------------------|--------|
| 生产风险 | S1 | 地域气候等环境条件 ^[23-24] | R1 |
| | | 土壤水质情况 ^[23-26] | R2 |
| | | 化肥农药施用量 ^[24-26] | R3 |
| | | 晾晒情况 ^[23,26] | R4 |
| 加工风险 | S2 | 原粮质量 ^[24-25,27-28] | R5 |
| | | 加工设备及工艺 ^[24-25,28] | R6 |
| | | 加工环境卫生情况 ^[25-26] | R7 |
| | | 是否使用非法添加剂 ^[26] | R8 |
| | | 包装材料情况 ^[24,26,28] | R9 |
| 储运风险 | S3 | 仓库运输环境 ^[24-26] | R10 |
| | | 熏蒸施药等措施 ^[24,26] | R11 |
| | | 仓储时间 ^[24-25] | R12 |
| 销售风险 | S4 | 流通销售环境 ^[24-25] | R13 |
| | | 数据存储方式 ^[25,29-30] | R14 |
| 区块链系统风险 | S5 | 数据源头可靠性 ^[25,29,31] | R15 |
| | | 数据匿名风险 ^[25,30-31] | R16 |
| | | 质量检测水平 ^[28] | R17 |
| 监管风险 | S6 | 监管执法力度 ^[27-28] | R18 |
| | | 法律法规惩罚机制 ^[25,27] | R19 |

影响因素影响程度很高,目标风险因素对自身无影响。根据专家打分的平均数得到一个 25×25 的风险因素直接影响关系矩阵 X , 矩阵 X 的行和列元素为二级和一级风险指标,如表 2 所示。

(3) 计算规范化直接影响矩阵。将直接影响矩阵 X 的每一个元素除以 X 中各行元素之和的最大值,得到规范化直接影响矩阵 G , 公式为

$$G = \frac{1}{\max_{1 \leq i \leq n} \sum_{j=1}^n a_{ij}} X \quad (1)$$

式中 n ——矩阵维数

a_{ij} ——矩阵第 i 行第 j 列的元素

(4) 确定综合影响矩阵。将步骤 (3) 得到的规范化直接影响矩阵 G 自乘 n 次,并将此 $n+1$ 个矩阵相加即可得到综合影响矩阵 T , 公式为

$$T = [t_{ij}]_{n \times n} = \lim_{l \rightarrow \infty} (G + G^1 + G^2 + \dots + G^l) = G(I - G)^{-1} \quad (2)$$

式中 I —— n 阶单位阵

t_{ij} ——矩阵中第 i 行第 j 列元素

(5) 确定各要素的中心度与原因度。中心度与原因度是由系统要素的影响度与被影响度决定的。影响度 f_i 、被影响度 e_i 、各风险因素的中心度 M_i 、原因度 N_i 计算公式为

$$\begin{cases} f_i = \sum_{j=1}^n t_{ij} \\ e_i = \sum_{j=1}^n t_{ji} \end{cases} \quad (3)$$

表 2 风险因素间直接影响矩阵

Tab.2 Direct influence matrix between risk factors

| | R1 | R2 | R3 | R4 | R5 | R6 | R7 | R8 | R9 | R10 | R11 | R12 | R13 | R14 | R15 | R16 | R17 | R18 | R19 | S1 | S2 | S3 | S4 | S5 | S6 |
|-----|----|----|----|----|----|----|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|----|----|----|----|----|----|
| R1 | 0 | 8 | 6 | 7 | 7 | 3 | 4 | 3 | 3 | 6 | 4 | 4 | 4 | 0 | 2 | 0 | 2 | 2 | 1 | 5 | 3 | 5 | 2 | 0 | 1 |
| R2 | 5 | 0 | 6 | 4 | 8 | 4 | 2 | 1 | 2 | 1 | 2 | 1 | 1 | 0 | 2 | 0 | 1 | 1 | 1 | 5 | 3 | 2 | 1 | 1 | 1 |
| R3 | 4 | 7 | 0 | 2 | 8 | 3 | 2 | 3 | 1 | 1 | 3 | 3 | 1 | 0 | 2 | 0 | 3 | 3 | 3 | 5 | 4 | 3 | 3 | 0 | 1 |
| R4 | 1 | 1 | 3 | 0 | 7 | 4 | 3 | 3 | 2 | 4 | 5 | 6 | 3 | 0 | 1 | 0 | 1 | 1 | 1 | 4 | 4 | 4 | 3 | 1 | 1 |
| R5 | 0 | 1 | 5 | 5 | 0 | 6 | 4 | 7 | 3 | 4 | 6 | 7 | 3 | 1 | 3 | 1 | 2 | 1 | 2 | 5 | 5 | 3 | 4 | 2 | 1 |
| R6 | 0 | 2 | 2 | 3 | 4 | 0 | 7 | 4 | 3 | 4 | 5 | 5 | 3 | 2 | 2 | 1 | 5 | 2 | 2 | 4 | 7 | 4 | 4 | 1 | 2 |
| R7 | 3 | 3 | 1 | 2 | 3 | 5 | 0 | 6 | 5 | 6 | 5 | 6 | 2 | 0 | 2 | 2 | 3 | 3 | 3 | 3 | 6 | 4 | 4 | 2 | 2 |
| R8 | 3 | 4 | 2 | 4 | 3 | 3 | 4 | 0 | 3 | 4 | 5 | 7 | 4 | 2 | 4 | 4 | 3 | 3 | 4 | 3 | 5 | 5 | 5 | 3 | 3 |
| R9 | 2 | 2 | 0 | 2 | 2 | 3 | 4 | 2 | 0 | 3 | 1 | 5 | 2 | 0 | 0 | 1 | 2 | 2 | 2 | 1 | 2 | 5 | 3 | 1 | 2 |
| R10 | 1 | 0 | 1 | 4 | 5 | 6 | 5 | 2 | 2 | 0 | 3 | 6 | 3 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 4 | 5 | 3 | 1 | 2 |
| R11 | 2 | 2 | 3 | 3 | 6 | 4 | 6 | 4 | 3 | 3 | 0 | 6 | 2 | 1 | 3 | 3 | 2 | 2 | 3 | 5 | 4 | 5 | 3 | 2 | 3 |
| R12 | 2 | 2 | 3 | 4 | 5 | 4 | 3 | 2 | 3 | 4 | 4 | 0 | 3 | 1 | 2 | 1 | 1 | 1 | 1 | 3 | 3 | 6 | 4 | 1 | 2 |
| R13 | 0 | 0 | 1 | 2 | 2 | 4 | 3 | 4 | 4 | 2 | 3 | 1 | 0 | 1 | 3 | 3 | 1 | 2 | 2 | 4 | 2 | 5 | 6 | 2 | 3 |
| R14 | 0 | 1 | 1 | 2 | 2 | 2 | 2 | 3 | 1 | 1 | 1 | 0 | 1 | 0 | 5 | 7 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 5 | 4 |
| R15 | 0 | 0 | 2 | 0 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 3 | 0 | 6 | 2 | 3 | 3 | 4 | 3 | 3 | 5 | 7 | 4 |
| R16 | 0 | 0 | 2 | 1 | 2 | 3 | 2 | 3 | 2 | 2 | 2 | 1 | 2 | 5 | 6 | 0 | 2 | 4 | 3 | 4 | 3 | 4 | 4 | 5 | 3 |
| R17 | 2 | 1 | 4 | 2 | 5 | 6 | 6 | 4 | 3 | 4 | 4 | 2 | 4 | 3 | 5 | 4 | 0 | 6 | 5 | 4 | 5 | 5 | 5 | 3 | 6 |
| R18 | 0 | 2 | 3 | 2 | 6 | 5 | 6 | 6 | 4 | 4 | 5 | 4 | 6 | 4 | 7 | 7 | 6 | 0 | 7 | 7 | 6 | 6 | 7 | 5 | 7 |
| R19 | 1 | 3 | 5 | 3 | 8 | 6 | 7 | 7 | 4 | 6 | 6 | 4 | 5 | 4 | 7 | 6 | 5 | 8 | 0 | 7 | 7 | 6 | 7 | 6 | 7 |
| S1 | 0 | 1 | 2 | 2 | 3 | 4 | 2 | 3 | 2 | 2 | 3 | 3 | 2 | 1 | 2 | 3 | 2 | 3 | 2 | 0 | 6 | 6 | 5 | 5 | 3 |
| S2 | 1 | 1 | 2 | 2 | 2 | 3 | 2 | 3 | 1 | 4 | 3 | 5 | 3 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 0 | 6 | 6 | 4 | 4 |
| S3 | 0 | 0 | 1 | 4 | 4 | 3 | 2 | 4 | 4 | 4 | 4 | 5 | 5 | 3 | 3 | 3 | 3 | 2 | 2 | 2 | 4 | 0 | 6 | 5 | 4 |
| S4 | 0 | 0 | 1 | 1 | 2 | 3 | 2 | 4 | 3 | 2 | 3 | 4 | 3 | 2 | 2 | 3 | 2 | 3 | 3 | 1 | 3 | 3 | 0 | 5 | 5 |
| S5 | 0 | 0 | 3 | 1 | 3 | 3 | 2 | 3 | 2 | 2 | 3 | 2 | 3 | 4 | 4 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 5 | 0 | 4 |
| S6 | 1 | 2 | 3 | 1 | 3 | 3 | 3 | 4 | 3 | 2 | 2 | 3 | 3 | 3 | 5 | 4 | 4 | 7 | 5 | 3 | 3 | 3 | 4 | 4 | 0 |

$$M_i = f_i + e_i \quad (i=1,2,\dots,n) \quad (4)$$

$$N_i = f_i - e_i \quad (i=1,2,\dots,n) \quad (5)$$

(6) 确定风险因素整体影响矩阵。由于 DEMATEL 中默认元素不影响自身,ISM 则相反,因此将综合影响矩阵 T 加上 n 阶单位阵,形成可用于 ISM 计算的整体影响矩阵 H ,即

$$H = T + I \quad (6)$$

(7) 计算标准化可达矩阵。基于整体影响矩阵 H ,采用最大最小算子计算模糊可达矩阵 \tilde{R} ,通过多次实验并结合专家评估意见,阈值 λ 设置为 0.067。利用数值确定原则

$$r_{ij} = \begin{cases} 1 & (\tilde{r}_{ij} \geq \lambda) \\ 0 & (\tilde{r}_{ij} < \lambda) \end{cases} \quad (7)$$

得出标准化可达矩阵 R 。

(8) 确定可达集、先行集。根据标准化可达矩阵 R 对各风险因素的可达集、先行集进行划分。

(9) 元素分层处理。满足

$$R_i = R_i \cap S_i \quad (i=1,2,\dots,N) \quad (8)$$

为第 1 层,然后去除已分层元素并重新筛选第 2 层元素,依次循环至各元素分层完毕。其中, R_i 代表标

号为 i 的风险因素的可达集, S_i 代表标号为 i 的风险因素的先行集, N 代表总的风险因素数,取值为 19。本文风险因素节点层级划分结果如表 3 所示。

表 3 风险因素节点层级划分结果

Tab.3 Hierarchical division results of risk factor nodes

| 层级 | 风险因素节点 |
|----|---------------------|
| 1 | R9,R16 |
| 2 | R13,R14 |
| 3 | R12,R15 |
| 4 | R5,R6,R7,R8,R10,R11 |
| 5 | R2,R3,R4 |
| 6 | R1,R17,R18,R19 |

(10) 多级递阶解释结构绘制及解释。根据风险因素分层结果以及各因素的可达集、前因集,通过缩边、缩点输出最简的风险因素多级递阶有向图结构模型,如图 2 所示。

1.1.3 多级递阶网络结构模型构建

根据图 2 并结合各风险因素间的二元关系绘制粮油质量安全区块链多级递阶解释结构模型图,引入“粮油质量安全区块链风险”作为第 0 级因素,通过缩边、缩点、删除重复强连通关系以及跨层越级关

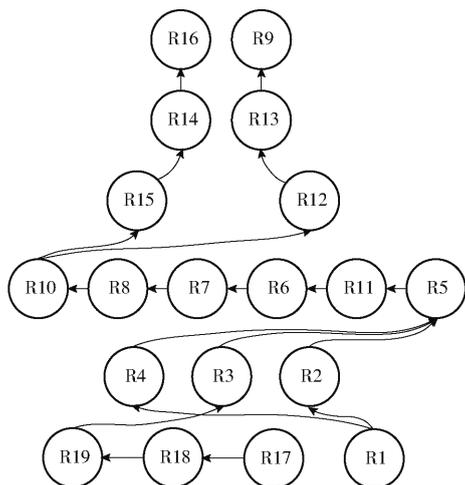


图2 粮油质量安全区块链风险多级递阶有向图
Fig.2 Multi-level hierarchical directed graph of risk factors of grain and oil quality and safety blockchain

系转化等处理简化系统风险传导过程,并以上文中计算得到的各风险因素的可达集、先行集作为参考和检验,最终绘制出粮油质量安全区块链风险多级递阶解释结构模型图,如图3所示。

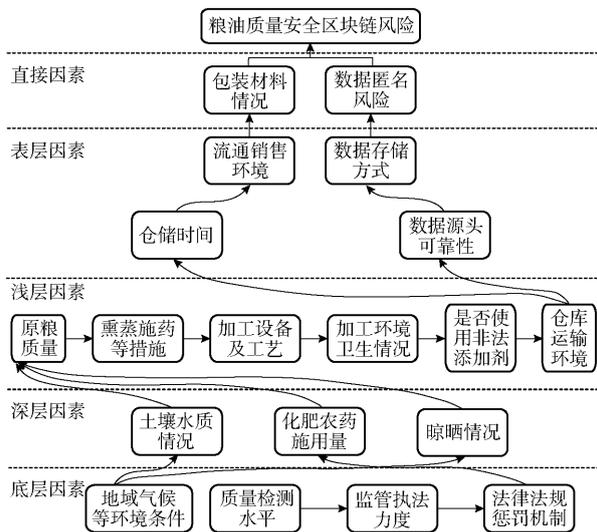


图3 粮油质量安全区块链多级递阶解释结构模型
Fig.3 Multi-level hierarchical interpretation structure model of grain and oil quality safety blockchain

通过分析,把影响粮油质量安全区块链的风险因素归结为直接影响因素、表层影响因素、浅层影响因素、深层影响因素以及底层影响因素5类影响因素(图3)。各层影响因素相互关联,构成了一个复杂的多层递阶结构,反映了各个风险因素对粮油质量安全区块链的影响机理及各节点或风险因素间的传导关系。

1.2 区块链网络节点分区

传统区块链结构中所有参与节点同步共识对区块链网络的性能带来巨大挑战,不仅容易导致共识效率低下,而且还容易造成网络拥塞甚至节点崩溃

的情况发生。因此,基于集成 DEMATEL - ISM 可解释性模型构建的粮油质量安全区块链风险多级递阶解释结构,对粮油质量安全区块链网络中各节点进行分层分区划分处理,实现区块链网络中各参与节点带有交易逻辑关系的分层分区。基于此,建立一种更高效的区块链生成机制,区块链网络中的全部参与节点分层分区共识可有效降低区块链系统运行的计算资源成本、减少网络拥塞情况、提高节点共识效率,进而实现对粮油质量安全区块链结构进行优化。

本文根据各风险节点在区块链网络中的地位重要性以及节点间的交易关联关系对粮油质量安全区块链网络中各风险节点进行分层分区处理。区块链网络中的共识节点的分层是实现节点分区的基础,基于 DEMATEL - ISM 集成模型构建的风险节点多级递阶有向图,根据各个风险节点对整个粮油质量安全区块链系统作用的影响程度和地位对其进行区域划分,建立从底层节点区域、中层节点区域、上层节点区域的“六层三区”区块链网络节点分层分区体系,其中,多级递阶解释结构模型表层影响因素又划分为了层级2和层级3,如图4所示。

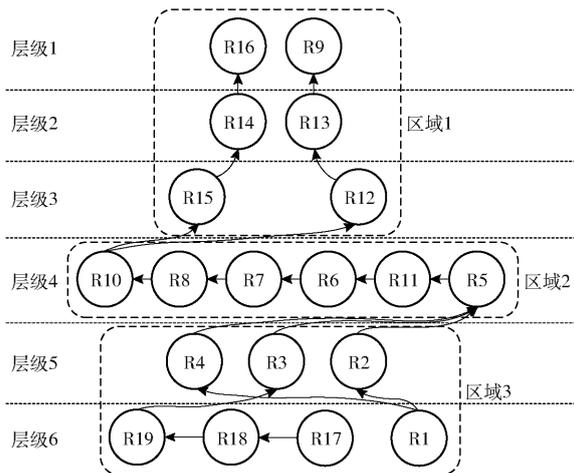


图4 区块链节点分层分区体系
Fig.4 Hierarchical partition system of blockchain nodes

在粮油质量安全区块链共识节点分层分区体系构建过程中,各参与节点在区块链系统中的交易地位与区块链节点分层分区体系的区域层级成反比,由粮油质量安全区块链风险分析结果可知,图4中区域3为底层节点区域,其所覆盖的区块链网络节点主要为对整个粮油质量安全区块链系统影响更为深层和全面的影响因素节点,包括底层因素节点以及深层因素节点,此类节点在区块链网络中节点交易关系中占据的地位也较高。区域2为中层节点区域,其中覆盖的区块链网络节点主要为浅层因素节点,此类风险节点作用机理复杂,

风险节点相互之间也呈集聚的态势, 将其划分为一个单独的区域进行内部共识不仅可显著提高区块链全网共识效率, 还能在一定程度上提升参与节点的隐私信息安全。区域 1 为上层节点区域, 覆盖的区块链网络节点主要为威胁粮油质量安全区块链的直接因素节点以及表层因素节点, 此类节点位于粮油质量安全溯源供应链的末端, 对整个粮油质量安全区块链系统的影响机理相对简单, 作用范围也较小, 因此在区块链全网节点进行交易、共识时的地位也相对较弱。

通过对基于 DEMATEL - ISM 的粮油质量安全区块链网络结构中的共识节点进行分层分区处理, 构建了多个松耦合的区块链共识节点集群区域, 各共识节点区域之间无相互干扰, 可协同并发执行节点共识, 进而提高区块链全网的共识效率、吞吐量等性能。

1.3 区块链网络子链划分

基于集成 DEMATEL - ISM 可解释性算法模型构建的粮油质量安全区块链网络结构, 结合“六层三区”的区块链网络节点分层分区体系以及各风险节点在整个区块链系统中的影响程度, 对分层分区体系内的区块链网络各节点进行进一步的子链划分。在粮油质量安全区块链节点分层体系中, 通过从底层起始节点逐渐向上层节点探寻, 遇分叉节点终止, 将由起始节点至分叉节点之间的所有节点划分为一个共识节点子链, 再以分叉节点作为起始节点重复向上层节点探寻, 直至完成所有子链的划分。并根据划分子链中各节点的中心度, 选举出每一条子链的主节点, 划分后的子链以及每条子链的主节点如图 5 所示, 其中, 6 条子链分别以不同的线型标注以示区分。

图 5 中 6 条不同的线型分别代表划分的 6 条不同子链, 每条子链中中心度最高的节点即为该条子链的主节点, 如图 5 中的加粗节点, 其在子链各节点交易共识中的地位也相对更高。网络内各条子链的主节点之间相互通信, 并通过共识机制保障整个区块链网络的分布式一致性。不同的子链之间能在同一时间段并发执行共识, 打包生成新的区块, 并按照时间的顺序有序地添加到区块子链中, 而不必等待区块链全网所有节点同步完成共识, 这种基于分布式共识的区块链网络子链划分结构从根本上解决了传统“一条链”式区块链无法在短时间全部节点达成共识并完成大量交易的问题, 有效提升了粮油质量安全区块链的共识效率和交易处理能力, 且子链分布共识缩小了参与节点的信息共享范围, 在一定程度上降低了潜在的隐私信息安全风险。

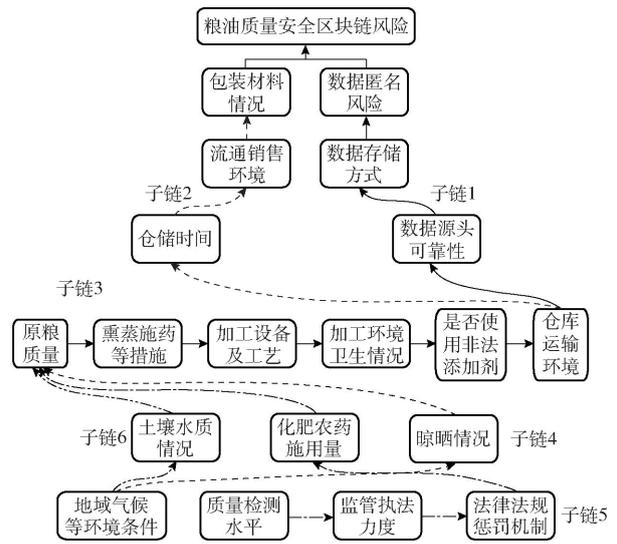


图 5 粮油质量安全区块链网络子链划分示意图

Fig. 5 Schematic of block chain network divided into sub-chains

2 粮油质量安全区块链共识机制优化

粮油质量安全区块链参与节点众多、风险因素复杂且溯源数据量大, 容易导致区块链网络拥塞、延时较长等, 因此对区块链的性能要求较高。Kafka 作为一种高性能、高可扩展性的共识机制, 将其应用于粮油质量安全区块链系统可有效提升区块链网络的扩展性和共识效率, 但对于参与节点众多且关联关系复杂的粮油质量安全区块链应用场景, Kafka 共识仍存在一些不足使得其应用于粮油质量安全区块链优势效果并不突出。一个区块链网络中会有多个 Orderer 节点分布式部署于多个机构, 共同提供排序服务。Kafka 共识过程中, 同一时刻只能对同一个主题中同一个分区的信息进行排序, 不支持跨主题跨分区的排序处理。虽然 Kafka 集群中每个分区都可以拥有相同的副本提升集群的容灾能力, 支持崩溃容错, 但它并不能提供对网络中恶意攻击的保护。因此, 本文针对 Kafka 共识的拜占庭容错能力以及集群分区机制进行优化改进, 以使 Kafka 共识机制在粮油质量安全区块链溯源场景下既能发挥更高的性能优势, 也能对区块链系统的安全性提供较好的保障, 从而使得区块链系统更加适用于粮油质量安全溯源控制专用场景。

2.1 Kafka 共识机制分析

Kafka 共识机制本质是一个性能高、崩溃容错能力强、可扩展性强的分布式消息系统^[32]。Kafka 共识的集群时序消息服务基于 Paxos 算法, 通过 zookeeper 组件进行多通道分区, 无法对抗恶意节点攻击, 但能容忍少于半数的网络节点发生宕机崩溃等故障。Kafka 使用经典的发布-订阅式消息

处理模型,工作原理如图6所示,其中,系统中生产者节点负责交易消息的广播发布,消费者节点通过订阅集群分区中特定的消息主题接收新的交易消息。

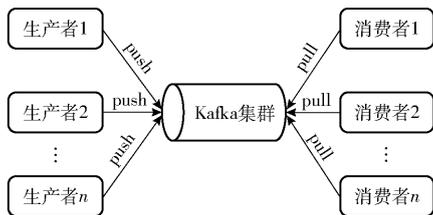


图6 Kafka共识工作原理图

Fig.6 Schematic of working principle of Kafka consensus

Kafka 共识机制下,当网络中数据规模逐渐庞大时,可以将 Kafka 集群拆分为多个分区,Kafka 集群能够在一定时间及规模阈值内保存交易消息且保证各分区内交易消息按顺序排列,但并不读取交易消息,消费者节点根据需求定位查询交易消息,由此形成回溯机制。此外,Kafka 共识下各消费者节点匹配单个或多个消息主题,且属于不同的集群分区,因此使得交易消息进入 Kafka 集群后能够分配给特定的分区并发执行处理进程,且交易消息不会被多次重复读取,有效提高了网络的共识效率。

Kafka 共识通过一种领导-跟随机制在多个排序节点之间进行分区复制以实现崩溃容错。领导节点在网络分区内负责分区的共识以及公共账本的维护,跟随节点则通过复制维护更新分区账本,在分区网络内领导节点发生宕机崩溃等问题时,通过将某一跟随节点转变为新的领导节点继续进行分区内共识,使得网络中的交易数据在当某一节点崩溃失效无法进行共识时也不会丢失。Hyperledger Fabric 中的 Kafka 实际运行逻辑如图7所示。

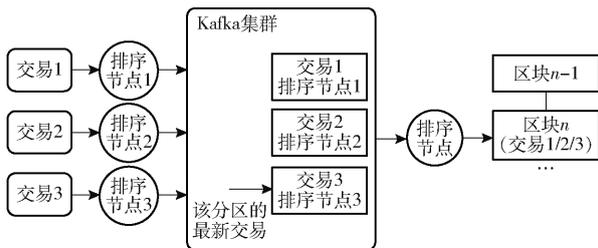


图7 Hyperledger Fabric 中的 Kafka 运行逻辑图

Fig.7 Kafka operation logic diagram in Hyperledger Fabric

2.2 基于 PBFT 改进 Kafka 拜占庭容错能力

传统 Kafka 共识机制下,虽然其能够通过排序节点复制支持崩溃容错,但它并不能抵抗区块链网络中恶意节点进行女巫攻击或验证节点作恶等^[33-34]。针对此类问题,首先,将排序服务节点部署到子链的每一个参与企业节点中,使子链中的每一个节点均参与到交易消息的排序服务中,再通过

引入 PBFT 共识机制的原理,在各排序节点收到交易消息进而将其中继到 Kafka 集群之前先在各排序节点之间进行 PBFT 共识,以此验证交易消息的一致性,防止网络中恶意节点的攻击,实现区块链网络的拜占庭容错能力。本文提出一种基于 PBFT 改进 Kafka 共识机制的拜占庭容错能力的共识算法 P-Kafka,其原理如图8所示,其中,C 代表消息请求客户端,OSN10、OSN12、OSN5 和 OSN19 分别代表粮油质量安全区块链各子链主排序服务节点。

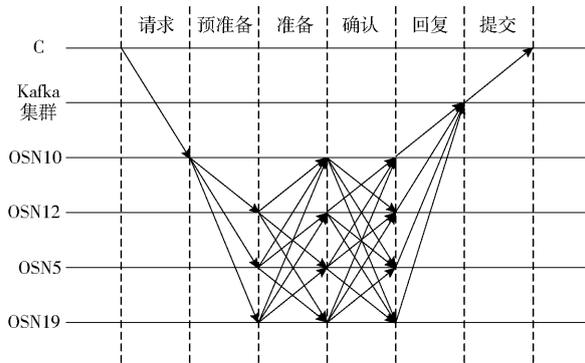


图8 改进 Kafka 共识机制拜占庭容错能力原理图

Fig.8 Schematic of improving Byzantine fault tolerance of Kafka consensus mechanism

改进 Kafka 拜占庭容错能力共识机制的具体执行流程如下:

(1)每次共识执行前,即每次视图开启前,首先计算更新主节点,公式为

$$p = v \bmod n' \tag{9}$$

式中 v 代表当前视图编号, n' 表示每次共识执行中主节点广播消息的唯一递增序号, \bmod 为取余运算。

随着视图 v 不断增长,主节点 p 也相应随之变化,采用这种轮换的方式从各子链产生的排序服务主节点中再次选举产生拜占庭容错共识的主节点,可避免单一节点长期占据主节点位置进而威胁区块链全网数据安全,图8中 OSN10 即代表排序服务主节点。

(2)客户端发送交易消息 m 至排序服务主节点 OSN10,排序服务主节点由此开始执行三阶段协议进行拜占庭容错共识,排序服务主节点若出现崩溃,则通过视图切换更换新的排序服务主节点。

(3)排序服务主节点 OSN10 收到客户端发送来的消息后,构造预准备消息 $\langle \text{pre-prepare}, v, n', dm \rangle$,其中,pre-prepare 代表当前消息所处的共识阶段, d 为交易消息 m 的摘要,并将消息广播至区块链网络中其他排序服务副节点,也即各子链的主排序服务节点,如图8中 OSN12、OSN5、OSN19 节点所示。

(4)排序服务副节点收到主节点的预准备消息后,首先验证交易的合法性,以防止客户端造假或排

序服务主节点进行恶意篡改。若经验证交易消息非法,则该排序服务副节点舍弃该条交易信息并且不参与此次共识过程,若消息验证合法后则进入准备阶段,生成准备消息 $\langle \text{prepare}, v, n', d, i \rangle$, 并将其广播给其他节点。

(5) 排序服务副节点收到准备消息后,同样先验证交易消息的合法性,当排序服务副节点收到包含本节点在内 $2f+1$ 条一致的准备消息后,进入确认阶段,构造确认消息 $\langle \text{commit}, v, n', d(m), i \rangle$ 并且广播至区块链网络中其他排序服务节点,其中 f 代表故障节点数。

(6) 排序服务节点收到包含自身在内 $2f+1$ 条一致性的确认消息后,将交易消息 m 中继至 Kafka 集群,待 Kafka 集群对交易消息处理完毕后,再通过排序服务节点打包生成新的区块添加上链,并将其发送至请求客户端,由此实现 Kafka 的拜占庭容错共识。

2.3 粮油质量安全区块链场景下的 Kafka 分区优化

分区机制是 Kafka 共识实现高吞吐量、高性能的重要手段,但分区的数量并非与分区的效果以及

区块链网络的性能成正比,区块链网络中分区的数量越多,网络消耗的计算资源也就越多,分区数量过多或过少均无法较好地发挥 Kafka 的高伸缩性、负载均衡以及动态调节等能力。尤其当应用于实际场景中时,由于每个业务场景都不同,分区策略的制定,包括分区数目以及分区节点等的设定也需要结合具体业务应用场景。

目前 Kafka 使用随机策略、轮询策略以及按键保存策略 3 种常用的分区策略。随机策略属于最原始的 Kafka 分区策略,通过产生随机数将交易消息随机分配,其分配的均衡性较差,容易给网络造成负担。目前 Kafka 已经默认改为轮询策略,即按交易消息的顺序轮流将每条数据分配到集群分区中。按键保存策略即当区块链网络内的生产者节点发送交易消息时指定一个 key 值,通过计算这个 key 的哈希值,按照哈希值对不同的交易消息进行分区存储。本文考虑粮油质量安全特定应用场景,通过采用按键保存分区策略,结合粮油质量安全区块链优化网络结构以及子链划分情况对 Kafka 集群分区进行优化,分区优化示意图如图 9 所示。

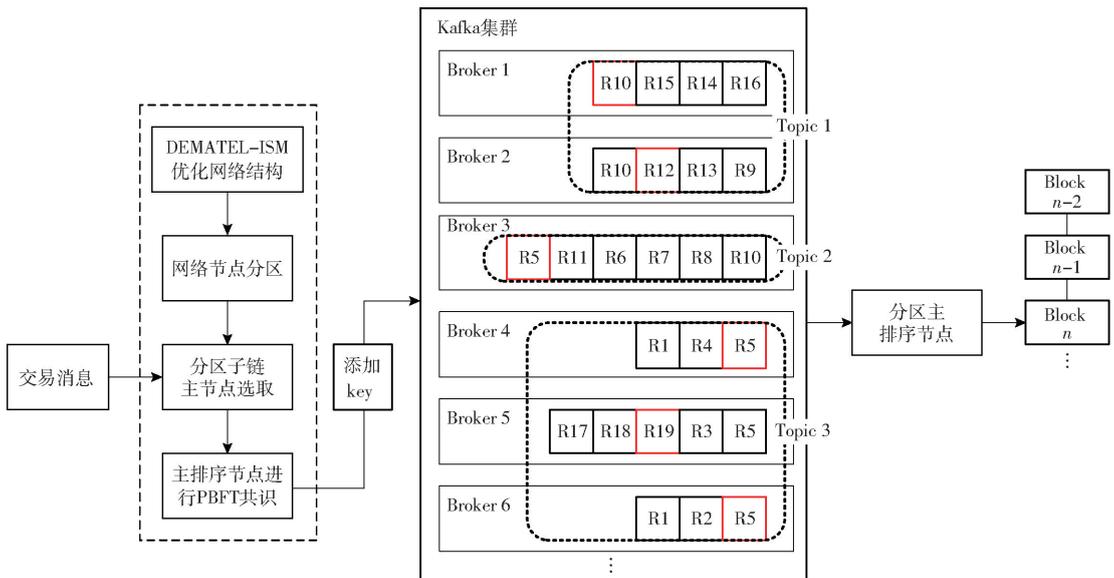


图 9 Kafka 共识分区优化示意图

Fig. 9 Optimization diagram of Kafka consensus partition

Kafka 分区的设置与区块链网络分区体系以及子链划分相匹配,每条子链对应一个 Broker,一个 Kafka 集群可以由多个 Broker 组成,可根据实际业务场景需要进行拓展,如图 9 中一个 Kafka 集群包含 6 条子链对应的 6 个 Broker。此外,根据前文中构建的粮油质量安全区块链网络节点“六层三区”的分层分区体系,分别将底层、中层、上层节点区域设置为 3 个不同的 Topic, Topic 作为 Kafka 集群中交易消息的主题,可对交易消息进行分类。根据粮油质量安全实际业务场景将其分为 3 个主

题,不同区域内节点交易消息相互之间降低干扰,可有效降低区块链网络中交易消息的混乱对系统性能造成的影响,且一个较大的 Topic 可以分布到多个 Broker 上,以提高区块链网络的扩展性,如图 9 中 Topic 1 分布在 Broker 1、Broker 2 上,Topic 3 分布在 Broker 4、Broker 5、Broker 6 上。以子链划分为依据将每个 Topic 内部再划分为若干 Partition,且同一 Topic 内部不同 Partition 分区只处理相关子链节点的交易消息,因此不同 Partition 上的数据是不重复的。通过对每个 Partition 分区设

定不同的参数,节点客户端产生的交易消息在经各子链主排序节点完成 PBFT 共识后,由子链主排序节点添加消息键 key,交易消息进入 Kafka 集群后,由消息键 key 与 Kafka 集群内相应的 Partition 分区进行匹配,Kafka 通过交易消息 key 的哈希值来确定消息需要写入哪个具体的分区,由此确保不同 key 值的数据写入不同的 Partition 分区,不同分区内部各节点再按照交易消息的顺序打包形成交易消息序列并存储,再经由各个子链的主排序服务节点打包生成新的区块,并添加至区块链系统中。通过这种 Kafka 分区优化的方法实现了粮油质量安全区块链各子链分区同步共识,避免重复共识造成的资源浪费,同时也有效提高了交易消息的处理效率和区块链网络的吞吐量。

3 结果分析

本文基于集成 DEMATEL - ISM 可解释性算法模型构建了一种基于多级递阶解释结构的新型粮油质量安全区块链网络结构,在风险节点多级递阶有向无环图的基础上,对区块链网络内部的各个参与节点进行分层分区划分以及子链划分,并对其相应的共识机制进行了优化改进。本文以图 10 所示的架构从正确性、性能等方面对粮油质量安全区块链的优化改进结果进行分析。

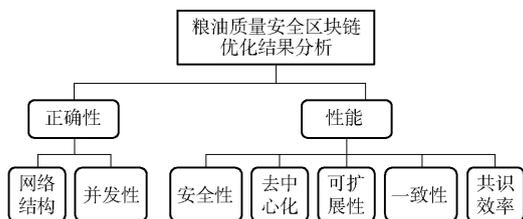


图 10 粮油质量安全区块链优化结果分析架构

Fig. 10 Analysis framework for optimization results of grain and oil quality and safety blockchain

3.1 正确性分析

通过将粮油质量安全区块链的结构设计成基于有向无环图的多层递阶网络结构,使得传统区块链结构形式下对计算资源的大量消耗以及共识效率难以提升的问题得到有效解决。此外,针对粮油质量安全溯源控制场景下传统单链式区块链项目在进行大量验证交易过程中存在的共识效率低等问题,通过对粮油质量安全区块链系统中区块生成共识机制进行优化设计,新的共识机制能够将区块存储结构与 Kafka 集群分区进行有效结合,从而能够有效应对大量验证交易,使得同一时间段内区块链网络内全体用户节点共同进行交易并同时生成区块的目标得以实现,且能够大幅节约区块链系统的计算资源。

区别于传统的公有链、联盟链等形式的区块链,本文提出的基于 DEMATEL - ISM 构建的有向无环图式结构的区块链使得区块链网络内的参与节点可在同一时间内并发执行共识,产生新的区块,不再需要像传统区块链一样等待其他区块生成完毕后才能生成新的区块。“六层三区”的粮油质量安全区块链网络节点分层分区体系使粮油质量安全区块链网络结构更加明晰,对于构建粮油质量安全区块链的共识机制以及底层智能合约提供了一种高效的设计指引。此外,通过划分子链的区块链网络结构使得粮油质量安全区块链网络节点执行共识仅需要同实际业务场景下具有强关联关系的相关子链参与节点之间进行,不需要全网所有节点共同参与共识,极大提高了区块链网络的共识效率、网络吞吐量等性能。

Raft 算法是一种去中心化、高可用的非拜占庭容错分布式一致性算法,设置了 Leader 节点、Follower 节点和 Candidate 节点 3 种角色。Raft 共识中所有操作请求需要先转发到 Leader 节点,再由 Leader 节点发送数据到各 Follower 节点进行同步,Leader 节点选举过程和日志复制过程都会因 Leader 负载不均问题而将直接影响共识效率,例如在 Candidate 节点选举过程中多个节点获得相同票数导致投票分歧。PoS (Proof of stake) 权益证明引入“币龄”概念,持有更多币或更长时间则拥有更多权益,以此将 PoW (Proof of work) 算力竞争转化为权益竞争来节约算力,权益的引入也能够防止节点发起恶意攻击。但是新区块的生成倾向于权益更高的节点,并没有解决中心化程度增强的问题;相比于 PoW 工作量证明效率有所提高,但交易吞吐量小,共识效率仍无法满足需求。PBFT 算法需要预准备、准备及提交三阶段投票达成共识,主节点收到超过 2/3 节点的准备消息就向全网广播一条提交消息,即可提交新区块到本地区块链,达成对最新高度区块的共识,支持 1/3 总节点数量的容错能力。PBFT 通过三阶段投票机制有效降低了恶意节点对共识的影响,但是由于一次共识过程需要经历一次单点全广播与两次全点全广播,通信开销大,并不适用粮油场景下高交易量的需求。

3.2 性能分析

从去中心化、安全性、共识效率、可扩展性以及一致性 5 方面分别对 PoS、PoW、Raft、PBFT 以及 P - Kafka 的性能做了分析比较,如表 4 所示。参与共识的节点数量、主节点的选择方式与共识节点的权重都影响共识的去中心化程度,节点的权利越分散,去中心化程度越高;共识节点数量指参与共识的是部

表 4 共识算法性能比较

Tab. 4 Performance comparison of consensus algorithms

| 性能指标 | PoW | PoS | Raft | PBFT | P - Kafka |
|---------|--------|--------|--------|----------|-----------|
| 去中心化 | | | | | |
| 共识节点数量 | 全网 | 全网 | 全网 | 全网 | 全网 |
| 主节点选择方式 | 竞争 | 竞争 | 选举 | 选举 | 选举 |
| 共识节点权重 | 不等 | 不等 | 相等 | 相等 | 相等 |
| 安全性 | | | | | |
| 容错率 | <50% | <50% | | <1/3 | <1/3 |
| 节点可控性 | 低 | 低 | | 高 | 高 |
| 攻击多样性 | 高 | 高 | 低 | 中 | 中 |
| 攻击成本 | 高 | 高 | 低 | 中 | 中 |
| 安全恢复性 | 高 | 中 | | 高 | 高 |
| 共识效率 | | | | | |
| 延迟 | 高 | 高 | 低 | 中 | 低 |
| 吞吐量 | 低 | 低 | 高 | 中 | 高 |
| 可扩展性 | | | | | |
| 资源消耗 | 高 | 中 | 低 | 低 | 低 |
| 通信复杂度函数 | $O(N)$ | $O(N)$ | $O(N)$ | $O(N^2)$ | $O(N^2)$ |
| 一致性 | | | | | |
| 分叉可能性 | 有 | 有 | 无 | 无 | 无 |
| 最终一致性 | 否 | 否 | 是 | 是 | 是 |

分节点还是全网所有节点;主节点选择方式决定了共识属于竞争类还是选举类;共识节点权重指每一轮共识过程中成为主节点的概率是否相等。安全性主要包括容错率、节点可控性、攻击多样性、攻击成本与安全恢复性等指标;容错率指共识在保证区块链在达成共识的前提下所能接受的拜占庭恶意节点在全网节点的占比;节点可控性指参与共识的节点是否有排除恶意节点参与到共识中的能力;攻击多样性指共识算法所能承受攻击的种类、数量;攻击成本指恶意节点发起攻击所需要的代价;安全恢复性指区块链受到攻击后,使数据恢复到攻击发生前安全状态的能力。共识效率从延迟、交易吞吐量 2 个角度分析;延迟指从一个区块被生成到它的共识过程完成所需要的时间;吞吐量指单位时间内处理交易的数量,吞吐量越高性能越高。可扩展性包含资源消耗与通信复杂度两个因素;资源消耗指共识过程中节点对算力、存储及网络等资源的消耗程度;通信复杂度指节点与节点之间在区块链网络中的通信成本。一致性包含了分叉可能性与最终一致性;分叉可能性指区块链是否存在分叉的情况;最终一致性指各个节点的数据在有限时间内最终是否达成一致。

(1) 去中心化

本文所提算法通过基于 DEMATEL - ISM 集成模型分析粮油质量安全实际场景下网络各节点的中心度,以此作为主排序服务节点选取及进行拜占庭容错共识的依据,子链各节点通过参与 Kafka 共识优化投票过程,具有一致公平性;PBFT 共识中选取 Leader 过程各个节点参与投票,P - Kafka 继承了这一逻辑,各个节点公平竞争,相比于 PoW、PoS 这类

竞争共识拥有更多的资源就可以垄断主节点,去中心化程度更高。

(2) 安全性

基于公链的 PoW、PoS 竞争类共识,对这类共识发动攻击的成本较高、难度较大,并且具有一定的安全恢复性。由于 Raft 共识仅支持故障节点容错,并不支持恶意节点容错,无法抵御拜占庭恶意节点的攻击,不能满足粮油质量安全场景的应用需求。

优化的粮油质量安全区块链网络结构更加关注各个参与节点之间的相互关联关系,将区块链系统的共识以多条子链分布式共识的形式完成,各个参与节点共识的对象和范围大幅减少和缩小,这在一定程度上控制了参与节点信息传播的范围,尤其对于保护粮油供应链中生产加工类企业节点关键生产数据等隐私信息的安全性具有重要意义。改进的共识在 Kafka 排序过程中引入 PBFT 投票机制,提升了共识的拜占庭容错能力,一定程度上提高共识的安全性。

(3) 共识效率

传统的公有链、联盟链式区块链因其结构限制出块效率相对较低,每一笔交易达成共识写入区块链的过程都需要等待区块链全网中所有的节点完成后才能生成新的区块,以比特币区块链为例,其需要每 10 min 才能生成一个新的区块,显然不能满足实际业务场景的应用需求。本文所构建的粮油质量安全区块链网络结构以及优化的 Kafka 共识机制仅在子链主排序服务节点进行拜占庭容错共识时占用一定的计算资源,显著低于传统基于 PoW 等类型的区块链。此外,优化的共识机制基于粮油质量安全溯源场景中授权参与节点建立,其在生成区块后无需像 PoW 等传统公链的共识机制那样需通过连续 6 个区块确认才能添加至区块链,基于场景授权的共识机制能够在新区块打包完成后直接添加至区块链网络。对于节点参与众多、关联关系复杂、数据量日渐庞大的粮油质量安全区块链溯源场景而言,本文所设计的网络结构及共识机制在保证参与节点一致公平性的前提下,一定程度上提高了区块链网络中的交易区块出块效率。

(4) 可扩展性

可扩展性方面,竞争类共识 PoW、PoS 资源消耗大,单个节点性能受限,不适合粮油质量安全这类大规模业务的场景。而本文基于 PBFT 改进的 Kafka 共识 P - Kafka 虽然通信复杂度较高,但是相比于竞争类共识可扩展性得到提升。

(5) 一致性

在区块链网络节点达成共识方面,通过对粮油

质量安全区块链中的 Kafka 共识机制进行优化,在交易消息经区块链网络中各子链排序节点中继到 Kafka 集群之前增加拜占庭容错共识的过程,保障了区块链系统在当网络中存在一定规模的恶意节点攻击时仍能进行分布式一致性共识,维持区块链系统正常运行。

4 结束语

本文通过对粮油质量安全区块链进行系统性的

风险分析研究,通过建立粮油质量安全区块链风险指标体系,并在解析粮油质量安全区块链风险和特征的基础上,改进并优化了现有完全非可信执行场景中通用型区块链结构。包括在网络层提出了一种适用于非完全可信执行场景中粮油质量安全专用型区块链网络结构,在共识层提出一种基于 PBFT 改进拜占庭容错能力的符合粮油质量安全区块链特征的 Kafka 共识优化算法 P-Kafka,使得区块链在风险可辨识和可控的情形下适用于粮油质量安全专用场景。

参 考 文 献

- [1] 许继平,王健,张新,等. 区块链驱动的稻米供应链信息监管模型研究[J]. 农业机械学报,2021,52(5):202-211,101.
XU Jiping, WANG Jian, ZHANG Xin, et al. Information supervision modeling of rice supply chain driven by blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(5):202-211,101. (in Chinese)
- [2] 孙传恒,于华竟,徐大明,等. 农产品供应链区块链追溯技术研究进展与展望[J]. 农业机械学报,2021,52(1):1-13.
SUN Chuanheng, YU Huajing, XU Daming, et al. Review and prospect of agri-products supply chain traceability based on blockchain technology[J]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(1):1-13. (in Chinese)
- [3] 厉曙光,陈莉莉,陈波. 我国 2004—2012 年媒体曝光食品安全事件分析[J]. 中国食品学报, 2014, 14(3): 1-8.
LI Shuguang, CHEN Lili, CHEN Bo. Analysis of food safety incidents exposed by the media in China from 2004 to 2012[J]. Journal of Chinese Institute of Food Science and Technology, 2014, 14(3): 1-8. (in Chinese)
- [4] 于合龙,陈邦越,徐大明,等. 基于区块链的水稻供应链溯源信息保护模型研究[J]. 农业机械学报,2020,51(8):328-335.
YU Helong, CHEN Bangyue, XU Daming, et al. Modeling of rice supply chain traceability information protection based on block chain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(8):328-335. (in Chinese)
- [5] ZHAO G, LIU S, LOPEZ C, et al. Blockchain technology in agri-food value chain management: a synthesis of applications, challenges and future research directions[J]. Computers in Industry, 2019, 109: 83-99.
- [6] OLSEN P, ASCHAN M. Reference method for analyzing material flow, information flow and information loss in food supply chains[J]. Trends in Food Science & Technology, 2010, 21(6): 313-320.
- [7] PECK M E. Blockchains: how they work and why they'll change the world[J]. IEEE Spectrum, 2017, 54(10): 26-35.
- [8] HONG W B, CAI Y F, YU Z R, et al. An agri-product traceability system based on IoT and blockchain technology[C]//1st IEEE International Conference on Hot Information-Centric Networking, 2018: 254-255.
- [9] MALIK S, SINGH A, KUMARI R, et al. Leveraging the potential of agriculture sector and food supply with blockchain technology—a review[J]. Journal of Pharmacognosy and Phytochemistry, 2018, 26(5): 116-119.
- [10] CHEN Yi, DING Shuai, XU Zheng, et al. Blockchain-based medical records secure storage and medical service framework [J]. Journal of Medical Systems, 2018, 43(1):5.
- [11] GALVEZ J F, MEJUTO J C, SIMAL-GANDARA J. Future challenges on the use of blockchain for food traceability analysis [J]. TrAC Trends in Analytical Chemistry, 2018, 107:222-232.
- [12] RAY P, OM H H, DANIEL A, et al. Incorporating blockchain technology in food supply chain[J]. International Journal of Management Studies, 2019, 6(1): 5.
- [13] SAIRAM S D, AMEER A A, AKASH K, et al. Trace and track food supply chain based on block chain and EPCIS[J]. International Journal of New Innovations in Engineering and Technology, 2020, 11(1): 288-295.
- [14] ZHANG Xin, SUN Pengcheng, XU Jiping, et al. Blockchain-based safety management system for the grain supply chain[J]. IEEE Access, 2020, 8: 36398-36410.
- [15] CHEN X, NGUYEN K, SEKIYA H. An experimental study on performance of private blockchain in IoT applications[J]. Peer-to-Peer Networking and Applications, 2021, 14(6): 1-17.
- [16] 许继平,孙鹏程,张新,等. 基于区块链的粮油食品全供应链信息安全管理原型系统[J]. 农业机械学报,2020,51(2): 341-349.
XU Jiping, SUN Pengcheng, ZHANG Xin, et al. Prototype system of information security management of cereal and oil food whole supply chain based on blockchain[J]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(2): 341-349. (in Chinese)
- [17] PRASHAR D, JHA N, JHA S, et al. Blockchain-based traceability and visibility for agricultural products: a decentralized way of ensuring food safety in India[J]. Sustainability, 2020, 12(8):3497.
- [18] 曾友露. 支持高吞吐量区块链的块结构研究[D]. 成都:电子科技大学,2020.
ZENG Youlu. Research on block structure supporting high throughput blockchain[D]. Chengdu: University of Electronic Science and Technology of China, 2020. (in Chinese)

- [19] IFTEKHAR A, CUI X H, YANG Y P. Blockchain technology for trustworthy operations in the management of strategic grain reserves[J]. *Foods*, 2021, 10(10) : 2323.
- [20] 王子岳. 面向供应链溯源的区块链系统研究与优化[D]. 北京:北京交通大学,2019.
WANG Ziyue. Research and optimization of blockchain system for supply chain tracking[D]. Beijing: Beijing Jiaotong University,2019. (in Chinese)
- [21] 孙永河,韩玮,段万春. 复杂系统 DEMATEL 算法研究进展评述[J]. 控制与决策,2017,32(3):385 - 392.
SUN Yonghe, HAN Wei, DUAN Wanchun. Review on research progress of DEMATEL algorithm for complex systems[J]. *Control and Decision*,2017,32(3):385 - 392. (in Chinese)
- [22] 孙慧,周颖,范志清. 基于解释结构模型的公交客流量影响因素分析[J]. 北京理工大学学报(社会科学版),2010,12(1):29 - 32.
SUN Hui, ZHOU Ying, FAN Zhiqing. Analysis of influencing factors of bus passenger flow based on interpretive structural model[J]. *Journal of Beijing Institute of Technology(Social Sciences Edition)*, 2010,12(1):29 - 32. (in Chinese)
- [23] 尹成华. 2007 年河南省原粮卫生状况调查[J]. 食品科技,2008(8):188 - 190.
YIN Chenghua. A survey on the health status of raw grains in Henan Province in 2007[J]. *Food Science and Technology*,2008(8):188 - 190. (in Chinese)
- [24] 周艳华,覃世民,李涛. 粮油质量安全事故防范及应对技术研究[J]. 粮食与油脂,2017,30(8):15 - 17.
ZHOU Yanhua, QIN Shimin, LI Tao. Study of safety accident prevention and response technology of grain and oil quality[J]. *Cereals & Oils*,2017,30(8):15 - 17. (in Chinese)
- [25] 李佳潞. 基于区块链的粮食供应链溯源方案的研究[D]. 北京:北京邮电大学,2019.
LI Jialu. Research on traceability scheme of grain supply chain based on blockchain[D]. Beijing: Beijing University of Posts and Telecommunications,2019. (in Chinese)
- [26] 刘国东. "大数据 + 质量安全"的粮食供应链监测预警机制研究[D]. 大庆:黑龙江八一农垦大学,2020.
LIU Guodong. Research on food supply chain monitoring and early warning mechanism based on big data and quality safety [D]. Daqing: Heilongjiang Bayi Agricultural University,2020. (in Chinese)
- [27] 褚学玉. 粮油行业食品安全源头管控研究[D]. 天津:天津大学,2014.
CHU Xueyu. Research on the sources control for food safety of cereals & oils[D]. Tianjin: Tianjin University,2014. (in Chinese)
- [28] 袁建. 粮油加工环节存在的质量安全问题与对策[J]. 食品科学技术学报,2014,32(5):6 - 9.
YUAN Jian. Quality and safety problems and countermeasures in grain and oil processing[J]. *Journal of Food Science and Technology*,2014,32(5):6 - 9. (in Chinese)
- [29] 韩璇,袁勇,王飞跃. 区块链安全问题:研究现状与展望[J]. 自动化学报,2019,45(1):206 - 225.
HAN Xuan, YUAN Yong, WANG Feiyue. Security problems on blockchain: the state of the art and future trends[J]. *Acta Automatica Sinica*,2019,45(1):206 - 225. (in Chinese)
- [30] KAMBLE S S, GUNASEKARAN A, SHARMA R. Modeling the blockchain enabled traceability in agriculture supply chain [J]. *International Journal of Information Management*, 2020, 52: 101967.
- [31] 欧阳日辉,李林珂. 区块链的风险与防范[J]. 陕西师范大学学报(哲学社会科学版),2021,50(3):165 - 176.
OUYANG Rihui, LI Linke. Blockchain risks and prevention[J]. *Journal of Shaanxi Normal University(Philosophy and Social Sciences Edition)*, 2021,50(3):165 - 176. (in Chinese)
- [32] 吴璨,王小宁,肖海力,等. 分布式消息系统研究综述[J]. 计算机科学,2019,46(增刊1):1 - 5,34.
WU Can, WANG Xiaoning, XIAO Haili, et al. Survey on distributed message system[J]. *Computer Science*, 2019,46 (Supp. 1):1 - 5,34. (in Chinese)
- [33] BANDARA E, LIANG X P, FOYTIK P, et al. Rahasak-scalable blockchain architecture for enterprise applications[J]. *Journal of Systems Architecture*, 2021, 116(6):102061.
- [34] BANDARA E, TOSH D, FOYTIK P, et al. Tikiri-towards a lightweight blockchain for IoT[J]. *Future Generation Computer Systems*, 2021, 119(6):154 - 165.