

中文引用格式:刘正刚,刘晨曦,阮渊鹏. 区块链技术应用中的安全屏障模式研究综述[J]. 中国安全科学学报,2024,34(10):105-115.
英文引用格式:LIU Zhenggang, LIU Chenxi, RUAN Yuanpeng. Review on safety barrier models for blockchain technology applications[J].
China Safety Science Journal, 2024, 34(10): 105-115.

区块链技术应用中的安全屏障模式研究综述*

刘正刚 副教授, 刘晨曦, 阮渊鹏 副教授
(杭州电子科技大学 管理学院, 浙江 杭州 310018)

中图分类号: X913; TP311.5 文献标志码: A DOI: 10.16265/j.cnki.issn1003-3033.2024.10.1891
基金项目: 浙江省哲学社会科学重点规划课题(21NDJC007Z); 教育部人文社会科学研究规划基金资助
(21YJA630064); 教育部人文社会科学研究青年基金资助(23YJC630146)。

【摘要】 为弥补区块链技术应用过程中对预防复杂系统安全问题的安全屏障研究关注不足的缺陷,首先,结合区块链技术在工业领域中的安全应用,介绍区块链自身的安全需求及安全屏障理论的支持;其次,从定性和定量视角总结安全屏障模式主要研究模型,并概述软件系统安全分析模型和安全屏障的绩效评估进展;然后,总结区块链技术安全风险相关安全措施的研究现状;最后,在顺应安全屏障模式研究中注重耦合协调的趋势下,立足研究复杂系统耦合协调及其复杂因果机制的定量方法进展,展望区块链技术应用相关的安全屏障模式研究,构建从安全分析、情景构建、系统建模、机制分析、效应评估至实现路径的安全屏障研究框架体系。结果表明:区块链技术相关安全屏障模式研究应涵盖以蝴蝶结(Bow-Tie)结构模型为核心并衔接工业事故风险评估法(ARAMIS)和耦合视角系统理论事故建模与过程(STAMP)等模型的静态系列图模式;将静态模式转换为贝叶斯网络(BN)并可作动态贝叶斯网络(DBN)分析的动态演化机制研究;以及安全屏障系统的效应评估;而聚焦耦合协调及其非线性因果分析深化该耦合式集成研究体系。

【关键词】 区块链; 安全屏障; 耦合协调; 因果关系; 效应评估; 贝叶斯网络(BN)

Review on safety barrier models for blockchain technology applications

LIU Zhenggang, LIU Chenxi, RUAN Yuanpeng

(School of Management, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China)

Abstract: In the application process of blockchain technology, insufficient attention has been paid to the research on safety barriers that are more suitable for preventing complex system safety problems. To solve this problem, firstly, the safety requirements of blockchain itself and the support of safety barrier theory were introduced, which was combined with the security application of blockchain technology in the industrial field. Then, the main safety barrier models within qualitative and quantitative perspectives were summarized, so were the progress of security analysis model of software system and of performance evaluation of safety barrier. Then, the research status of safety precautions related to security risks of blockchain technology was summarized. Finally, in accordance with the trend of coupling coordination in safety barrier models, a research framework of safety barrier models related to the application of blockchain technology was put forward, which was based on the research progress of quantitative methods studying complex system coupling coordination and complex causal mechanism. It was a framework system including safety analysis, situational construction, system modeling, mechanism analysis, effect assessment and

implementation path. The results show that the research on the safety barrier models related to blockchain technology should cover static series diagram pattern with Bow-Tie model as core and ARAMIS (Accidental Risk Assessment Methodology for Industries System) and coupling perspective STAMP (Systems Theoretic Accident Model and Processes) models as integrators, dynamic evolution mechanism research that includes dynamic Bayesian network analysis by transforming the static models into BN, and the effect assessment of safety barrier system. The study on coupling coordination and nonlinear causal analysis focusing on entropy deepen this coupling integration research system.

Keywords: blockchain; safety barrier; coupling coordination; causal relationship; effect assessment; Bayesian network (BN)

0 引言

近年来,安全领域兴起从整体视角来预防、控制、缓解风险的安全屏障^[1],主要涉及其定义、分类^[2]、功能^[3]、绩效评估^[4]、可靠性分析等^[5]。安全屏障研究源于20世纪70年代高危流程行业,但随着大数据和人工智能技术的发展,化工和过程工业安全格局巨变,表现为:①数字和网络安全问题成为过程安全的新威胁,自动化甚至智能控制系统的安全屏障评估和管理有巨大变化;②数据驱动的智能方法通过各种来源提取和利用大量与安全屏障性能指标相关的数据,有潜力支持安全管理^[6]。然而,当前信息系统尤其是软件相关的安全研究多侧重于安全攻防、危险分析或安全故障^[7],但多数故障是异于传统部件失效的系统事故且人因错误居多^[8],给建模和优化带来很大困难。急需利用人工智能技术和数据驱动的管理来升级安全屏障管理各阶段(即设计、安装、运行和管理)使用的方法,加速实现其监测、检查、维护、性能评估及管理流程的自动化与智能化^[6]。

立足密码学和编程的区块链是一种去中心化分布式共享账本^[9],但作为信任机器的区块链急需加强安全屏障研究。在智能合约支持下,区块链从加密数字货币领域的专有技术拓展为金融、制造、供应链、物联网和公共管理等垂直领域内构建价值互联网信任关系的关键使能技术^[10]。区块链技术可让数据信息得到更高的安全保障,其优良特性便于与大数据结合,与物联网结合^[11]。区块链和物联网驱动产品与社会接入一个庞大的智能网络^[12]。目前,区块链安全问题的研究大多侧重于应对安全风险的一种或几种措施,如应用层、平台层和基础网络层的技术安全措施以及企业安全管理、平台治理及政府监管措施^[13]。仅少数研究关注安全屏障视角,如用故障树分析法评估7个区块链平台的可靠性以识别

薄弱环节^[14]。区块链这种新兴信息系统的安全研究未涉足安全屏障相关的模式、效应评估及实现路径研究,缺乏安全屏障研究。

鉴于此,笔者拟从安全屏障视角研究区块链应用时的安全问题,从发展技术、组织管理、行业治理及政府监管各层面研究和各层松/紧耦合的定量研究方法,构建从安全屏障模式到安全屏障系统效应评估再到区块链安全实现路径的完整安全屏障研究框架,以期对区块链相关安全风险的预防提供新的管治理论和方法。

1 区块链技术的安全应用与需求

1.1 区块链技术在工业领域的重要安全应用

区块链技术的重要安全应用是赋能工业安全。区块链以分布式、共享、安全和许可的交易分类账解决工业界许多难题,建立自动化和高效的供应链流程并提高整个价值链的透明度^[15],而且支持实现工业4.0的智能制造^[16],包括通过提升工业物联网安全性和交易效率^[17],结合自动化业务流程管理的解决方案^[18]。区块链借助多种以人为中心的、面向可持续发展的和增强弹性的3类应用,促进力求以人为本、可持续性和弹性的工业5.0的发展^[19]。

1.2 区块链的安全需求与安全屏障理论支持

区块链有众多安全应用,但自身安全问题限制其大规模应用。对于开放式Web应用程序安全项目的10大安全风险,区块链就面临9个^[20]。表1列出了区块链安全风险类别及常涉应用场景。

区块链技术安全隐患需结合安全屏障研究化解。去中心化的区块链网络能利用安全屏障的多层次防御体系有效提高系统安全性和稳定性^[21]。对网络层与物理层紧密相连的网络物理系统更需安全屏障研究^[22],如扩展了网络层分析的保护层分析(Layers Of Protection Analysis, LOPA)框架^[23]。LO等^[14]利用故障树分析法评估了7个区块链平台的

表 1 全面的区块链安全风险类别
Table 1 Comprehensive blockchain safety risk categories

风险	描述	类型	所涉应用场景
网络攻击	区块链每秒的交易数量有限,此类攻击可能会提交超过区块链能力的交易,导致区块链不可用。用无效的大容量数据淹没节点的人站连接	拒绝服务攻击、边界网关协议劫持、通信流攻击、日蚀攻击、隐秘攻击、域名攻击	设备维护与监控;供应链管理;智能合约的应用(金融服务、版权及知识产权、房地产和租赁、股票及治理)
终端安全	终端可以是异构的也可以是同构的,前者有更多的选择来查找漏洞,后者中的漏洞存在于所有系统中	个人密钥安全、智能合约安全、访问控制、恶意挖矿、51%攻击、女巫攻击	灾害预防和应急响应;身份验证和访问控制;环境监测和数据分析;涉及硬件、软件、网络、数据和操作等多个层面
代码漏洞	由于区块链是分布式网络,漏洞影响广泛,代码一旦部署就无法修改。代码漏洞可能来自任何人都可以编写的智能合约或底层平台代码	交易依赖攻击、时间戳依赖攻击、调用深度攻击、可重入攻击、整数溢出攻击、操作异常攻击、燃料限制、交易延展性攻击、低价操纵、智能合约漏洞、未优化智能合约	智能合约的应用(金融服务、版权及知识产权、房地产和租赁、股票及治理)
数据保护	数据保护依赖于区块链的安全性,而不是数据所有者来提供数据完整性和可用性	中心化问题、后门攻击、单点问题、敏感数据泄露、隐私泄露	信息共享与协作(产品溯源、政府管理、能源管理、医疗卫生、环境保护等);安全审计和合规性;供应链管理
人的因素	日志所有者对其日志的监控、人的监管	日志记录和监控不足、安全配置错误、技术监管缺失	身份验证和访问控制;合规性记录与审计;风险评估和管理

可靠性以识别薄弱环节。除技术挑战外,区块链发展还必须融入复杂的制度、监管、经济和社会等系统^[24]。治理对于成功实施区块链至关重要,区块链虽有自治性,但去中心化系统的监管有很多问题,需要更多共同标准和清晰的法规^[25]。安全屏障理论作为一种治理框架可多维度助力区块链安全。

2 安全屏障模式相关研究

安全屏障概念是基于 LOPA 法和能量障碍事故模型提出的,最初定义为用于预防、控制或缓解意外事件或事故的物理/非物理手段^[2]。当前物理屏障、技术屏障(实现屏障功能的设备和系统)、操作屏障(实现屏障功能须执行活动)和组织屏障(具有规定角色的人员)都是安全屏障^[4]。围绕安全屏障的概念内涵,以安全屏障为相关主题词,结合保护层、安全功能等检索词,在 Web of Science、SpringerLink 等英文数据库及中国知网、万方等中文数据库中检索 2023 年 6 月前的文献,初步得到英文文献 1 042 篇和中文文献 1 168 篇。随后,利用以下标准筛选这些文献:①剔除与文中研究主题不符的文献;②剔除非核心期刊来源文献;③剔除书评、社论、征稿启事等非研究性文献。最终获取符合研究条件的英文 468 篇和中文 485 篇。以 VOSviewer 软件对国外代表性文献作关键词共现分析,结果如图 1 所示。其聚类为 4 类主题:①风险评估与安

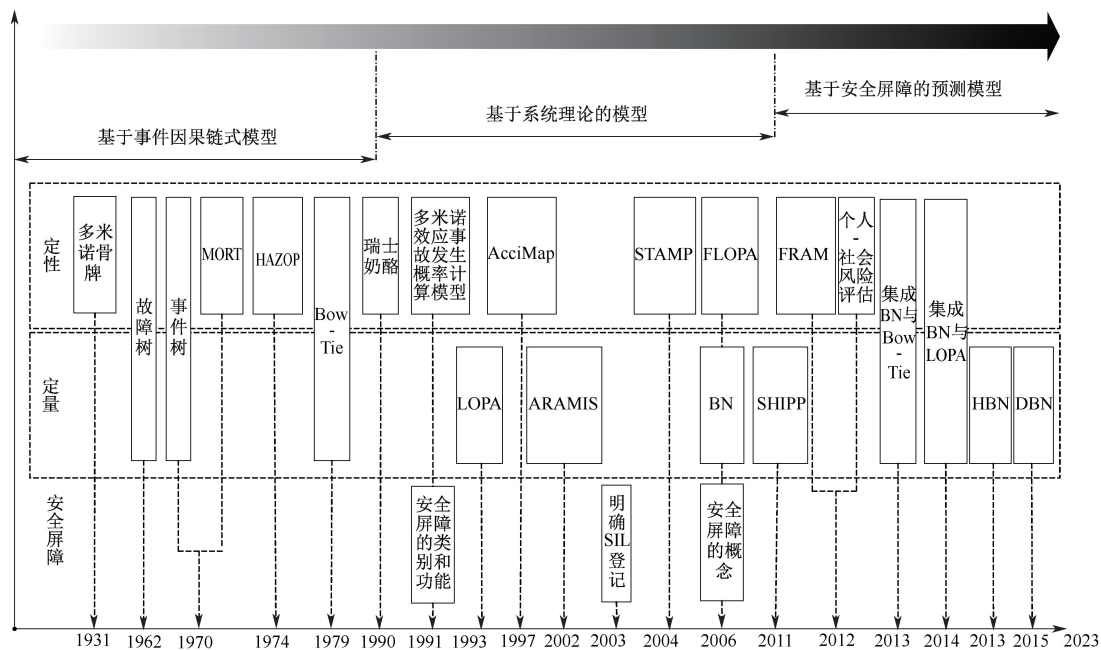
全分析;②风险管理与事故分析;③安全屏障、多米诺效应与定量风险评估;④流程行业、贝叶斯网络(Bayesian Network, BN)与蝴蝶结(Bow-Tie)。分析可知:国内安全屏障研究聚类更多且更分散,较突出主题是多米诺效应、LOPA、事故致因、BN、安全完整性等级、安全屏障、安全管理和安全评价。国内外安全屏障研究主题均凸显与风险评估与管理以及事故分析与安全分析相关的各类定性和定量模型。

2.1 安全屏障分析模型

2.1.1 安全屏障定性分析模型

早期安全屏障模型是基于事件因果链式分析的模型,如多米诺骨牌模型和瑞士奶酪模型。HEINRICH 等^[26]基于事件因果链式分析提出人为差错导致事故的多米诺骨牌模型。鉴于多米诺骨牌简单线性模型不能描述事故发生具体过程且未考虑事故过程的多重因果关系,REASON^[27]提出瑞士奶酪模型,不安全条件依次突破各层屏障系统的薄弱之处则事故发生。结合瑞士奶酪模型,KUJATH 等^[28]发展了结合故障树和事件树来描述事故过程的过程事故模型。姜伟^[29]、傅贵^[30]等基于上述事故致因理论提出行为安全“2-4”模型,将事故发生归结为组织和个人 2 个层面及指导、运行、习惯性、一次性 4 个阶段的行为发展的结果。

针对线性因果机制提出的线性分析模型不能考



注:管理疏忽和危险树 (Management Oversight and Risk Tree, MORT);模糊 LOPA (Fuzzy LOPA, FLOPA);功能共振分析法 (Functional Resonance Analysis Method, FRAM);层次贝叶斯网络 (Hierarchical Bayesian Network, HBN);安全完整性等级 (Safety Integrity Level, SIL)。

图 2 安全屏障事故模型的发展历程

Fig. 2 Evolution of safety barrier accident modeling

表 2 安全屏障相关主要研究模型的分析重点与相互关系

Table 2 Analysis focus of main models related to safety barrier and their interrelationships

模型名称	分析重点	与其他模型的关联
MORT	应用安全分析概念将事故的原因分为管理疏忽漏洞以及假定危险,以便识别安全管理工作的疏忽、失误和管理系统缺陷	在故障树分析逻辑的基础上发展
HAZOP	将分析单元划分为相应的节点,以引导词为主体,结合系统运行操作状态的变动和偏差,以便识别危及系统安全的潜在危险,辨识生产工艺的设计缺陷	—
LOPA	通过分析事故后果的严重性和发生频态参数率,量化评估现有保护措施,以便明确是否需要增加新的措施	一般在定性危害评估(如 HAZOP)后应用
AcciMap	将事故影响因素映射到复杂社会技术系统各层次中,用图形分析各影响因素间的交互关系和安全性的变化过程	—
STAMP*	重点关注整个系统表现,视系统为分层控制结构,每个层级对下一层级施加约束,通过检查每个控制结构层级的失效识别控制缺陷,适用于复杂性和耦合度较高社会技术系统	基于 AcciMap 模型对社会技术系统的分层进行细化和完善
FRAM	将系统分解为不同功能,认为各功能均具备可变量性,而某一要素正常变动与其他要素变化所产生的聚合效应发生耦合时可能导致共振并引发事故。通过分析系统中各功能模块的紧密耦合来解释复杂社会技术系统事故的致因机制	在传统线性模型基础上,突破事故的线性因果性思维建立非线性安全模型
蝴蝶结结构图 Bow-tie	将事故原因和事故导致的后果统一起来,结合故障树与事件树来分析事故的前因后果	集成故障树与事件树
SHIPP	采用故障树表征各安全屏障的因果关系;采用事件树来描述事故从安全状态到灾难性后果的演变过程;基于贝叶斯理论分析现场异常事件数据,以便更新安全屏障失效概率	基于过程事故模型,保留故障树和事件树结合的系统分析方式并增加贝叶斯更新机制
HBA	将层次模型和贝叶斯理论相结合,在数据分组分层构建层次模型后建立相应的基于 BN 的概率模型	—
DBN*	在静态 BN 结构上加入时间属性约束,借助不同时刻节点状态所形成的数据,反映其代表变量的发展变化趋势	—

注:带*的模型表示现已在软件系统中应用。

SFMEA 与 SFTA 能克服 PHA 与 FHA 层次不够清晰和因果关系不够明确的局限;SFMEA 是一种自下向上的归纳方法,而 SFTA 是一种自上向下的演绎方法,两者优势互补^[26,45]。

2.3 安全屏障的绩效评估

在利用安全屏障模型预防事故的过程中,安全屏障的失效概率(Probability of Failure on Demand, PFD)是重要因素。做 LOPA 分析时,识别保护层并估计每个保护层的 PFD 是必备步骤。PFD 可视为安全屏障的可用性^[46]。在评估安全屏障绩效水平时,可参考 ARAMIS 框架常用的有效性、响应时间和置信水平这 3 个指标^[47]。采用贝叶斯方法量化 PFD^[48],或者用多状态 BN 来评估安全屏障的功能性能^[49]。

安全屏障绩效评估指标中的置信水平概念源于 SIL 的定义,并扩大到所有类型安全屏障上^[47]。SIL 确定方法主要有后果法、风险矩阵法、风险图法、改进的 HAZOP 法、LOPA 法及立足故障树和事件树的定量法^[50]。SIL 等级的主要验证方法有故障树法、可靠性框图法和马尔可夫模型^[51]。若各安全屏障间耦合协调不佳则系统总体仍有安全隐患,可借鉴系统成熟度(System Readiness Level, SRL)来协助判断耦合协调的演化进程^[52]。

3 区块链技术安全风险相关措施

在网络攻击方面,多数攻击聚焦于区块链网络安全,包括拒绝服务、劫持边界网关协议、代码漏洞和数据泄露等攻击^[53]。FENG Shaohan 等^[54]提出网络保险和网络风险管理方法来中和或对冲网络攻击。

针对区块链代码漏洞,问题主要集中于智能合约层面。钱鹏等^[55]综述了形式化验证法、符号执行法、模糊测试法、中间表示法、深度学习法 5 类智能合约安全漏洞检测方法。董伟良等^[56]综述了 6 大类智能合约漏洞检测技术:基于符号执行、基于模糊测试、基于污点分析、基于形式化验证、基于机器学习的漏洞检测技术和其他技术。

在数据保护方面,区块链中的网络层、交易层及应用层均面临数据隐私威胁。针对区块链中网络层、交易层和应用层的数据隐私威胁,康海燕等^[57]总结了网络层隐私保护技术、交易层隐私保护技术、应用层隐私保护技术以及隐私保护技术 3 大重点发展方向。梁秀波等^[58]从数据存储安全、数据隐私安全、数据访问安全和数据共享安全

4 个方面概括了区块链系统的各类安全问题及合理解决方案。

此外,人的因素在区块链安全中也扮演着重要角色。尽管区块链有自治性,但去中心化系统的监管问题仍有待解决,需要共同标准和明确的法规^[25]。中国加快推进区块链国家标准的制定和实施,已发布多项国家标准以指导区块链技术在各行业领域的应用和数据交换。区块链网络参与者需记录和监控所属节点和交易的状态以及网络异常事件,以便及时发现和处理安全问题。鉴于区块链网络分布式和去中心化特性,日志记录和监控难度较高,需技术手段(如分布式追踪、智能合约审计、区块链分析)提高记录和监控的效率和效果^[59]。

4 安全屏障相关耦合协调方法

安全屏障部分模型,如 AcciMap、STAMP 和 FRAM,涉耦合问题,区块链安全问题也涉耦合理论,可借鉴研究耦合协调的定量方法。源于物理学的耦合度能显示大系统中各个子系统之间相互作用的强弱,而耦合协调度模型因考虑各致因因素的权重而更能反映系统整体协调情况^[12]。

在大数据时代,立足统计熵的信息论日益重要。基于热力学第二定律的熵概念,SHANNON^[60]提出了信息熵(香农熵)描述信息源不确定程度。基于香农信息熵 $H(X)$ (描述随机变量 X 的总体不确定度),衍生出深入分析协调与耦合关系的多种信息熵,如联合熵 $H(X, Y)$ 描述 X 与 Y 同时发生的不确定度,条件熵 $H(X | Y)$ 描述已知 Y 后 X 的不确定度,互信息 $I(X, Y)$ 描述 X 与 Y 之间相关性,相对熵 $D(p || q)$ 衡量 2 过程 p 和 q 的差异性,直接考察耦合的 Kolmogorov 熵,以及可做因果性耦合分析的多变量转移熵^[61]、分析多尺度数据的联合符号转移熵^[62]。

5 展望

区块链技术应用相关安全屏障研究相关思路如下:首先,构建基于集成故障树与事件树的 Bow-Tie 模型,挖掘安全屏障的动态演化机制以便探索安全屏障模式;然后,基于安全屏障的风险评估、安全绩效、适合性评估、综合效应评估和成熟度评估,发展区块链安全屏障的完整评估体系;最后,借助 Bow-Tie 转换所得 BN 的双向因果和诊断推理机制以及耦合机制,构建区块链安全屏障风险预警及控制平台,相关研究框架体系如图 3 所示。

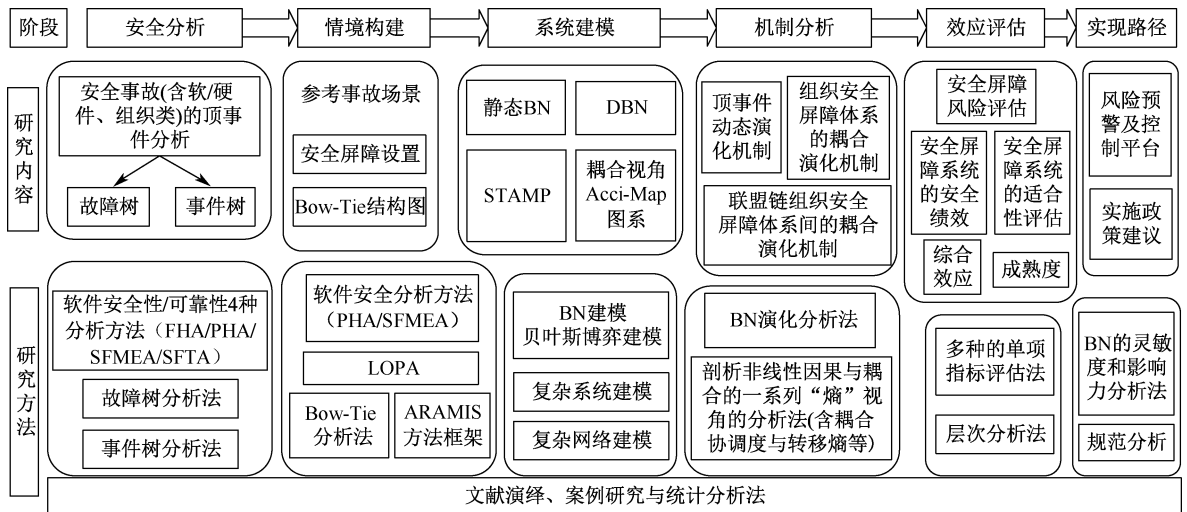


图 3 区块链技术相关安全屏障研究的框架体系

Fig. 3 Framework system for research on safety barriers related to blockchain technology

5.1 区块链应用过程中安全屏障模型

5.1.1 区块链安全屏障静态系列图模式

区块链安全屏障静态系列图模式研究主要是构建集成故障树与事件树的 Bow-Tie 模型。首先,利用软件安全性和可靠性分析方法依次分析区块链的系统级功能、区块链系统危险对应的软件失效模式/原因/影响/改进措施、软件故障树,并提取相应软件安全性需求。其次,在补充硬件或组织类问题所致区块链重大危害事件基础上,运用故障树和事件树从多角度分析重大危害事件顶事件。故障树以安全事故中的关键事件为顶事件,按区块链 6 层技术框架(即数据层、网络层、共识层、激励层、合约层、应用层)作故障树详情分析,再以系统理论为指导分析其社会技术系统中的故障影响因素。事件树构建从各项事件出发,参照满足区块链安全目标(聚焦数据安全、共识安全、隐私保护、智能合约安全、内容安全)的安全模块内容,先构建相关结果事件树,再以系统理论为指导分析社会技术系统中相关事件系列结果。最后,根据区块链开发和运营逻辑为各类安全设置合适的安全屏障。设置分为 4 步:①利用 LOPA 分析初始事件频率、后果严重性和各独立的安全屏障/保护层的失效可能性(失效概率)以便评估分析事故场景风险。②以关键事件为顶事件,基于故障树和事件树构建 Bow-Tie,在 Bow-Tie 中用 ARAMIS 考察安全屏障系统内各安全屏障之间的关系。③在研究区块链相关技术、管理和组织 3 类安全屏障的治理机制、失效模式及其影响因素上,参照 ARAMIS 框架及安全屏障的检测/激活/响应机制,

研究安全屏障设置及相应区块链的参考事故场景,据此完善故障树和事件树并构建完整的 Bow-Tie 模型,再发展立足系统理论的嵌套耦合视角的社会技术系统 STAMP 模型。④在计算各安全屏障的置信水平基础上,考察整体安全功能的置信水平,若仍不足则完善安全屏障设置。

5.1.2 区块链安全屏障模式动态演化机制研究

首先,将 Bow-Tie 模型中事件间的与门/或门关系等转换为条件概率表,将上述模型转换为 BN,做双向的因果推理或诊断推理以及博弈建模与研究涉及安全屏障失效历史的 DBN 的演化,分析区块链相关顶事件的安全屏障动态演化机制。①SFMEA 转化为 BN 进行故障诊断。以条件概率表量化 3 层故障诊断结构(含原因层、模式层和故障层)中各层节点间因果关系,结合条件概率表中依赖关系计算模式层各节点先验概率以及故障发生先验概率;然后,计算各原因节点后验概率,排序后用于因果诊断。②结合 BN 的 LOPA 与 Bow-Tie 分析。对故障树及事件树各层事件之间建立的安全屏障,以其失效为事件利用 BN 计算每个安全屏障的失效概率,应用 LOPA 分析失效概率以完善风险控制措施。将安全屏障失效作为事件实现 Bow-Tie 的 BN 建模外,还将安全屏障(尤其管理类屏障)由 Bow-Tie 中的结点转换为 BN 中的边(考察条件概率),完善立足 BN 的 Bow-Tie 模型。③贝叶斯博弈。网络安全问题本质上是攻防行为的交互问题,在不完全信息条件下基于贝叶斯博弈模型的网络最优防御策略选取合适方法,含静态/动态贝叶斯博弈以及单次/重复博弈等。

④用BN灵敏度分析判断系统薄弱环节以完善屏障,并用BN影响力分析(结合底事件发生概率)计算最可能故障链以便预警与控制。其次,研究组织安全屏障体系耦合演化机制。以区块链相关组织为对象,分析各类安全顶事件之间的耦合互动演化,研究各个相关组织安全屏障体系的发展历程及其耦合演化机制。最后,研究多组织安全屏障体系之间的耦合演化机制。依托区块链技术结构、组织的管理/治理结构以及联盟链等环境治理结构之间的耦合结构,以耦合协调度和分析非线性因果关系的转移熵等方法,分析区块链相关组织安全屏障体系之间的耦合发展历程及其耦合演化机制,总结区块链相关各层次安全屏障的动态演化规律。

5.2 区块链安全屏障系统的效应评估

区块链安全屏障系统的效应评估包括5方面(图4)。①应用BN和LOPA评估区块链相关独立保护层/安全屏障风险;②参照ARAMIS框架对安全屏障的绩效评估方法(含有效性、响应时间和立足PFD的置信水平/可靠性等)和信息安全三元组(保密性、完整性和可用性),即(Confidentiality, Integrity, Availability, CIA),研究相关组织区块链安全屏障系统的安全绩效;③针对相关组织区块链安全屏障系统的完整生命周期做SIL评估,并应用结合初始事件发生概率进行适合性评估;④集成安全绩效、适合性、鲁棒性/弹性和成本等因素,评估相关组织区块链的安全屏障系统综合效应;⑤以耦合协调度和分析非线性因果关系的转移熵等方法,研究区块链“不可能三角”等矛盾体的协同演化,集成安全结构理论模型并且参照软件工程能力成熟模型,构建区块链安全屏障系统的成熟度评估。

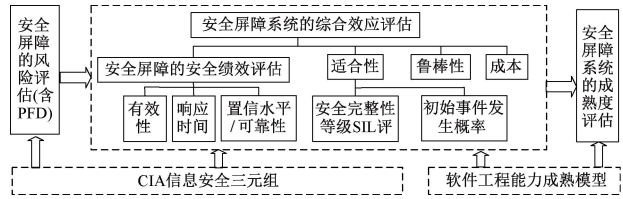


图4 区块链安全屏障系统的效应评估

Fig. 4 Effectiveness assessment of blockchain safety barrier systems

6 结论

1) 区块链技术应用相关安全屏障模式研究的框架体系包括安全分析、情景构建、系统建模、机制分析、效应评估和实现路径6大部分。

2) 区块链技术应用相关安全屏障模式主要的发展方向是注重耦合协调视角研究和复杂因果机制研究,包括借助研究复杂系统耦合协调及其复杂因果机制的熵视角定量方法。

3) 区块链相关安全屏障静态系列图模式研究主要是立足区块链6层技术框架研究集成故障树与事件树的Bow-Tie结构模型,并据此进一步发展衔接ARAMIS和耦合视角STAMP等模型的研究。

4) 区块链相关安全屏障动态演化机制研究主要是将相关静态系列图模式转换为BN并作DBN等演化与博弈分析,研究因果推理/诊断与薄弱环节的预警诊断,尤其注重挖掘其中的耦合演化机制。

5) 区块链技术相关安全屏障系统的效应评估体系包括安全屏障的风险评估,参照ARAMIS框架的安全屏障的安全绩效评估,安全屏障系统的综合效应评估(涵盖安全绩效、适合性、鲁棒性和成本等因素),以及结合区块链“不可能三角”等矛盾体协同演化分析的安全屏障系统成熟度评估。

参考文献

[1] 田水承,景国勋. 安全管理学[M]. 北京:机械工业出版社,2009:114-115.
 [2] SKLET S. Safety barriers: definition, classification, and performance [J]. Journal of Loss Prevention in the Process Industries, 2006, 19(5): 494-506.
 [3] KANG Jian, ZHANG Jixin, GAO Jiancun. Analysis of the safety barrier function: accidents caused by the failure of safety barriers and quantitative evaluation of their performance [J]. Journal of Loss Prevention in the Process Industries, 2016, 43: 361-371.
 [4] LIU Yiliu. Safety barriers: research advances and new thoughts on theory, engineering and management [J]. Journal of Loss Prevention in the Process Industries, 2020, 67: DOI:10.1016/j.jlp.2020.104260.
 [5] DUIJM N J, GOOSSENS L. Quantifying the influence of safety management on the reliability of safety barriers [J]. Journal of Hazardous Materials, 2006, 130(3): 284-292.

- [6] YUAN Shuaiqi, YANG Ming, RENIERS G, et al. Safety barriers in the chemical process industries: a state-of-the-art review on their classification, assessment, and management [J]. *Safety Science*, 2022, 148: DOI:10.1016/j.ssci.2021.105647.
- [7] 张坤,马力,徐亚非. 复杂信息系统安全保障体系的研究[J]. *中国管理科学*, 2000, 8(增1): 336-346.
ZHANG Kun, MA Li, XU Yafei. Research for security safeguard system of complex information system [J]. *Chinese Journal of Management Science*, 2000, 8(S1): 336-346.
- [8] 陈光宇,黄锡滋. 软件可靠性学科发展现状及展望[J]. *电子科技大学学报:社科版*, 2002, 4(3): 99-102.
CHEN Guangyu, HUANG Xizi. Actuality and prospect of development of software reliability subject [J]. *Journal of University of Electronic Science and Technology of China: Social Sciences Edition*, 2002, 4(3): 99-102.
- [9] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. (2008-10-31). <https://bitcoin.org/bitcoin.pdf>.
- [10] 曹雪莲,张建辉,刘波. 区块链安全、隐私与性能问题研究综述[J]. *计算机集成制造系统*, 2021, 27(7): 2078-2094.
CAO Xuelian, ZHANG Jianhui, LIU Bo. Review on security, privacy, and performance issues of blockchain [J]. *Computer Integrated Manufacturing Systems*, 2021, 27(7): 2078-2094.
- [11] ZUBAYDI H D, VARGA P, MOLNÁR S. Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: a systematic literature review [J]. *Sensors*, 2023, 23(2): DOI:10.3390/s23020788.
- [12] 李晓,刘正刚. 基于区块链技术的供应链智能治理机制[J]. *中国流通经济*, 2017, 31(11): 34-44.
LI Xiao, LIU Zhenggang. Study on supply chain intelligent governance mechanism based on blockchain technology [J]. *China Business and Market*, 2017, 31(11): 34-44.
- [13] 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.
- [14] LO S K, XU Xiwei, STAPLES M, et al. Reliability analysis for blockchain oracles [J]. *Computers & Electrical Engineering*, 2020, 83: DOI:10.1016/j.compeleceng.2020.106582.
- [15] AL-JAROODI J, MOHAMED N. Blockchain in Industries: a survey [J]. *IEEE Access*, 2019, 7: 36500-36515.
- [16] LENG Jiewu, YE Shide, ZHOU Man, et al. Blockchain-secured smart manufacturing in industry 4.0: a survey [J]. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020, 51(1): 237-252.
- [17] HUANG Junqin, KONG Linghe, CHEN Guihai, et al. Towards secure industrial IoT: blockchain system with credit-based consensus mechanism [J]. *IEEE Transactions on Industrial Informatics*, 2019, 15(6): 3680-3689.
- [18] VIRIYASITAVAT W, XU Lida, BI Zhuming, et al. Blockchain-based business process management (BPM) framework for service composition in industry 4.0 [J]. *Journal of Intelligent Manufacturing*, 2020, 31(7): 1737-1748.
- [19] FRAGA-LAMAS P, FERNÁNDEZ-CARAMÉS T M, DA CRUZ A M R, et al. An overview of blockchain for industry 5.0: towards human-centric, sustainable and resilient applications [J]. *IEEE Access*, 2024, 12: 116162-116201.
- [20] HOWARD P. Mapping the OWASP top ten to blockchain [J]. *Procedia Computer Science*, 2020, 177: 613-617.
- [21] QIAO Weiliang, HUANG Enze, GUO Hongtongyang, et al. Barriers involved in the safety management systems: a systematic review of literature [J]. *International Journal of Environmental Research and Public Health*, 2022, 19(15): DOI: 10.3390/ijerph19159512.
- [22] BOLBOT V, THEOTOKATOS G, BUJORIANU L M, et al. Vulnerabilities and safety assurance methods in cyber-physical systems: a comprehensive review [J]. *Reliability Engineering & System Safety*, 2019, 182: 179-193.
- [23] TANTAWY A, ABDELWAHED S, ERRADI A. Cyber LOPA: an integrated approach for the design of dependable and secure cyber-physical systems [J]. *IEEE Transactions on Reliability*, 2022, 71(2): 1075-1091.
- [24] LACITY M C. Addressing key challenges to making enterprise blockchain applications a reality [J]. *MIS Quarterly Executive*, 2018, 17(3): 201-222.
- [25] LENG Jiewu, ZHOU Man, ZHAO J L, et al. Blockchain security: a survey of techniques and research directions [J]. *IEEE Transactions on Services Computing*, 2022, 15(4): 2490-2510.
- [26] HEINRICH H W, PETERSEN D, ROOS N. Industrial accident prevention: a safety management approach (5th edition) [M]. New York: McGraw-Hill, 1980: 68-74.

- [27] REASON J. Human error [M]. Cambridge: Cambridge University Press, 1990: 119–124.
- [28] KUJATH M F, AMYOTTE P R, KHAN F I. A conceptual offshore oil and gas process accident model [J]. *Journal of Loss Prevention in the Process Industries*, 2010, 23(2): 323–330.
- [29] 姜伟, 佟瑞鹏, 傅贵. 安全科学与工程导论[M]. 北京: 中国劳动社会保障出版社, 2015: 54–58.
- [30] 傅贵. 安全管理学: 事故预防的行为控制方法[M]. 北京: 科学出版社, 2013: 247–262.
- [31] RASMUSSEN J. Risk management in a dynamic society: a modelling problem [J]. *Safety Science*, 1997, 27(2/3): 183–213.
- [32] LEVESON N. A new accident model for engineering safer systems [J]. *Safety Science*, 2004, 42(4): 237–270.
- [33] 周荣义, 李石林, 刘何清. HAZOP 分析中 LOPA 的应用研究[J]. *中国安全科学学报*, 2010, 20(7): 76–81.
ZHOU Rongyi, LI Shilin, LIU Heqing. Study on application of LOPA in HAZOP [J]. *China Safety Science Journal*, 2010, 20(7): 76–81.
- [34] MARKOWSKI A S, KOTYNIA A. "Bow-tie" model in layer of protection analysis [J]. *Process Safety and Environmental Protection*, 2011, 89(4): 205–213.
- [35] SALVI O, DEBRAY B. A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive [J]. *Journal of Hazardous Materials*, 2006, 130(3): 187–199.
- [36] DE DIANOUS V, FIÉVEZ C. ARAMIS project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance [J]. *Journal of Hazardous Materials*, 2006, 130(3): 220–233.
- [37] RATHNAYAKA S, KHAN F, AMYOTTE P. SHIPP methodology: predictive accident modeling approach. Part II. validation with case study [J]. *Process Safety and Environmental Protection*, 2011, 89(2): 75–88.
- [38] ZHAO Rongyong, LIU Qiong, WANG Yan, et al. Dynamic crowd accident-risk assessment based on internal energy and information entropy for large-scale crowd flow considering COVID-19 epidemic [J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(10): 17 466–17 478.
- [39] JIANG Shengyu, CHEN Guoming, ZHU Yuan, et al. Real-time risk assessment of explosion on offshore platform using Bayesian network and CFD [J]. *Journal of Loss Prevention in the Process Industries*, 2021, 72: DOI: 10.1016/j.jlp.2021.104518.
- [40] 刘书杰, 李相方, 周悦, 等. 基于贝叶斯-LOPA 方法的深水钻井安全屏障可靠性分析[J]. *中国安全生产科学技术*, 2014, 10(9): 187–191.
LIU Shujie, LI Xiangfang, ZHOU Yue, et al. Reliability analysis on safety barriers of deep-water drilling based on Bayesian-LOPA method [J]. *Journal of Safety Science and Technology*, 2014, 10(9): 187–191.
- [41] BADREDDINE A, BEN AMOR N. A Bayesian approach to construct bow tie diagrams for risk evaluation [J]. *Process Safety and Environmental Protection*, 2013, 91(3): 159–171.
- [42] KHAKZAD N, KHAN F, AMYOTTE P. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network [J]. *Process Safety and Environmental Protection*, 2013, 91(1): 46–53.
- [43] ZENG Tao, CHEN Guohua, YANG Yunfeng, et al. Developing an advanced dynamic risk analysis method for fire-related domino effects [J]. *Process Safety and Environmental Protection*, 2020, 134: 149–160.
- [44] RASPOTNIG C H, OPDAHL A. Comparing risk identification techniques for safety and security requirement [J]. *Journal of System Software*, 2013, 86(4): 1 124–1 151.
- [45] VYAS P, MITTAL R K. The application of SFTA and SFMEA approaches during software development process: an analytical review [J]. *International Journal of Critical Computer-Based Systems*, 2015, 6(1): 29–49.
- [46] LANDUCCI G, ARGENTI F, SPADONI G, et al. Domino effect frequency assessment: the role of safety barriers [J]. *Journal of Loss Prevention in the Process Industries*, 2016, 44: 706–717.
- [47] 张新梅, 韩丹丹, 陈晨. 安全屏障绩效评估在装置风险控制中的应用研究[J]. *中国安全科学学报*, 2014, 24(11): 96–101.
ZHANG Xinmei, HAN Dandan, CHEN Chen. Study on application of safety barrier performance evaluation to installation risk control [J]. *China Safety Science Journal*, 2014, 24(11): 96–101.
- [48] KALANTARNIA M, KHAN F, HAWBOLDT K. Dynamic risk assessment using failure assessment and Bayesian theory [J]. *Journal of Loss Prevention in the Process Industries*, 2009, 22(5): 600–606.

- [49] DIMAIO F, SCAPINELLO O, ZIO E, et al. Accounting for safety barriers degradation in the risk assessment of oil and gas systems by multistate Bayesian networks [J]. *Reliability Engineering and System Safety*, 2021, 216(3): DOI: 10.1016/j.res.2021.107943.
- [50] 周荣义, 钟岸, 任竟舟, 等. 安全系统安全完整性等级确定方法比较研究[J]. *中国安全生产科学技术*, 2014, 10(3): 67-73.
ZHOU Rongyi, ZHONG An, REN Jingzhou, et al. Comparative study on determining methods for safety integrity level of safety system [J]. *Journal of Safety Science and Technology*, 2014, 10(3): 67-73.
- [51] SHU Yidan, ZHAO Jinsong. A simplified Markov-based approach for safety integrity level verification [J]. *Journal of Loss Prevention in the Process Industries*, 2014, 29: DOI:10.1016/j.jlp.2014.03.013.
- [52] SAUSER B, VERMA D, RAMIREZ-MARQUEZ J, et al. From TRL to SRL: the concept of systems readiness levels [C]. *Proceeding of Conference on Systems Engineering Research*, 2006: 1-10.
- [53] AHMADJEE S, MERA-GOMEZ C, BAHSOON R, et al. A study on blockchain architecture design decisions and their security attacks and threats [J]. *ACM transaction on Software Engineering and Methodology*, 2022, 31(2): 1-45.
- [54] FENG Shaohan, WANG Wenbo, XIONG Zehui, et al. On cyber risk management of blockchain networks: a game theoretic approach [J]. *IEEE Transactions on Services Computing*, 2021, 14(5): 1492-1504.
- [55] 钱鹏, 刘振广, 何钦铭, 等. 智能合约安全漏洞检测技术研究综述[J]. *软件学报*, 2022, 33(8): 3059-3085.
QIAN Peng, LIU Zhengguang, HE Qinming, et al. Smart contract vulnerability detection technique: a survey [J]. *Journal of Software*, 2022, 33(8): 3059-3085.
- [56] 董伟良, 刘哲, 刘逵, 等. 智能合约漏洞检测技术综述[J]. *软件学报*, 2024, 35(1): 38-62.
DONG Weiliang, LIU Zhe, LIU Kui, et al. Survey on vulnerability detection technology of smart contracts [J]. *Journal of Software*, 2024, 35(1): 38-62.
- [57] 康海燕, 邓婕. 区块链数据隐私保护研究综述[J]. *山东大学学报:理学版*, 2021, 56(5): 92-110.
KANG Haiyan, DENG Jie. Survey on blockchain data privacy protection [J]. *Journal of Shandong University: Natural Science*, 2021, 56(5): 92-110.
- [58] 梁秀波, 吴俊涵, 赵昱, 等. 区块链数据安全管理和隐私保护技术研究综述[J]. *浙江大学学报:工学版*, 2022, 56(1): 1-15.
LIANG Xiubo, WU Junhan, ZHAO Yu, et al. Review of blockchain data security management and privacy protection technology research [J]. *Journal of Zhejiang University: Engineering Science*, 2022, 56(1): 1-15.
- [59] YANG Lu. The blockchain: state-of-the-art and research challenges [J]. *Journal of Industrial Information Integration*, 2019, 15: 80-90.
- [60] SHANNON C E. A mathematical theory of communication [J]. *Bell System Technical Journal*, 1948, 27(4): 379-423.
- [61] RUNGE J, HEITZIG J, MARWAN N, et al. Quantifying causal coupling strength: a lag-specific measure for multivariate time series related to transfer entropy [J]. *Physical Review E Statistical Nonlinear & Soft Matter Physics*, 2012, 86(6): 1-15.
- [62] SINGH A, SAINI B S, SINGH D. Multiscale joint symbolic transfer entropy for quantification of causal interactions between heart rate and blood pressure variability under postural stress [J]. *Fluctuation and Noise Letters*, 2015, 14(3): DOI: 10.1142/S0219477515500315.

作者简介: 刘正刚 (1976—),男,江苏镇江人,副教授,硕士生导师,主要从事运营管理与企业信息化、区块链、供应链治理与安全治理等方面的研究。E-mail: liuzhenggang@hdu.edu.cn。

