基于人工智能技术的区块链虚拟货币交易检测机制

Detection Mechanism of Blockchain Virtual Currency Transaction Based on Artificial Intelligence Technology

曾　晶，刘大畅，孙石峰（广东南方电信规划咨询设计院有限公司，广东 深圳 518038）
Zeng Jing，Liu Dachang，Sun Shifeng（Guangdong Southern Planning & Designing Institute of Telecom Co.，Ltd.，Shenzhen 518038，China）

摘　要：
针对虚拟货币操作的异常交易检测，提出了一种规则自学习及环境自适应的检测机制，基于Louvain社区算法以及人工智能关联图识别技术实现对区块链异常交易行为的实时识别及检测，并通过试验验证WannaCry事件和Crynlocker病毒的交易监测运作，此检测机制的运用将大力增强我国金融监管与反欺诈的关键技术能力，提升监管效能。

关键词：
区块链；人工智能；关联图；异常交易
doi：10.12045/j.issn.1007-3043.2021.08.014
文章编号：1007-3043（2021）08-0070-04
中图分类号：TN919
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Aiming at the abnormal transaction detection of virtual currency operation, a rule self-learning and environment adaptive detection mechanism is proposed. Based on Louvain community algorithm and artificial intelligence association graph recognition technology, the real-time identification and detection of abnormal transaction behavior of blockchain are realized. The transaction monitoring operation of Wannacry event and Crynlocker virus is verified by experiments. The application of this technology will greatly enhance the ability of China's financial supervision and enhance the work efficiency of the regulatory authorities.

Keywords：
Blockchain；Artificial intelligence；Association graph；Abnormal transaction

引用格式：曾晶，刘大畅，孙石峰. 基于人工智能技术的区块链虚拟货币交易检测机制[J]. 邮电设计技术，2021（8）：70-73.

0 引言

区块链是一种集成分布式数据存储、点对点传输、共识机制、加密算法等多种技术的新型技术。目前联合国、国际货币基金组织、多个国家政府都在积极讨论区块链并持续增加相关投入。我国在区块链技术的探索方面最初仅仅是金融行业的小课题，但从2016年国务院印发的《“十三五”国家信息化规划》中可以看到对区块链技术的支持，规划中强调了要对区块链等技术加强基础研发和前沿布局，构筑新赛场先发主导优势。2020年4月20日，国家发改委首次明确人工智能、云计算、区块链等为代表的新技术基础设施属于新型基础设施范围中的信息基础设施，新型基础设施主要是指基于新一代信息技术演化生成的基础设施。

当前以区块链产品为代表的全球金融科技迅猛发展，对实体经济和金融体系产生深远影响，如何平衡好金融科技的创新和风险，成为金融监管不可忽视的问题。我国基于区块链技术的产品研发进展显著，局部细分市场具备全球领先优势，但同时也暴露了异常交易、欺诈行为、虚假信息诱导和恶意操纵价格等风险。目前以比特币、以太坊、Libra为代表的主流区

收稿日期：2021-06-02

块链平台的国际监管协调难度大，难以适应国内监管框架，研究对异常交易进行跟踪识别的技术迫在眉睫，通过建立非法行为识别信息库，对异常交易进行识别和跟踪，建立有效、快速、准确的异常行为检测机制，将大大增强我国金融监管与反欺诈的关键技术能力，提升监管效能。

1 区块链监管

区块链技术在中国的火热程度不亚于国外，技术实力也在迅猛发展，不断累积。随着区块链技术的突破发展，其衍生品和应用的规范化和合法化问题引起业内、管理部门和监管部门的高度重视。法律法规对区块链的监管应分为以下3个维度。

1.1 区块链技术自身

区块链技术的开发和研究过程会涉及到用户隐私保护、网络安全和智能合约等问题。目前大多数国家的法律、法规及政策对区块链技术本身的态度都是积极肯定的。比如我国广州黄埔区当地政府出台的《广州市黄埔区广州开发区促进区块链产业发展办法》，从适用范围、平台、应用、技术等多个环节对区块链相关企业给予政策上重点扶持。其技术具备安全稳定、高效透明的特点，可以弥补中心化机构及商业模式的缺点。

1.2 虚拟货币

虚拟货币作为区块链的主要衍生品，其在发行、交易、流转等操作过程中，涉及到货币的定性、货币操作过程的行为认定和规范、税收和安全等问题。关于虚拟货币的定性有支付媒介、虚拟商品和证券化凭证3种主流观点。无论哪种定性，其在操作过程中都有违规违法的可能性。

1.3 商业模式

区块链技术会重构商业模式和组织结构，相关法律法规需要监管这方面的问题。区块链发挥去中心化优势将驱动新的商业模式，对现有的商业模式是非常大的冲击，如何平衡好监管与创新的权重，发挥区块链项目的潜力，抑制不良行为，将是一个重要的课题。

本文将对区块链虚拟货币操作过程行为认定方面提出相应的监管技术方法。

2 区块链虚拟货币交易监测技术的最新动态

2020年4月，20国集团金融稳定委员会（FSB）发布了监管咨询报告《解决“全球稳定币”项目所引起的监管、监督挑战》，这里的“稳定币”是指一类特定的加密资产，通过将其价值与其他资产联系在一起，试图解决传统加密资产的高波动性难题，有提高金融服务效率的潜力，但同时也存在一定风险，尤其在大规模应用时会对现有金融监管的全面性和有效性提出很大挑战。该报告阐述了全球稳定币的特征和潜在风险，分析了现有的监管监督方法和当前需要解决的问题，最后提出10项高级别监管建议。2020年10月13日，FSB发布了《“全球稳定币”项目监督管高层级建议》终版报告。此次发表的建议得到各成员国的认可，各国均认为有必要按照“相同业务，相同风险，相同规则”的原则进行监管。

虚拟货币的鼻祖——比特币于2009年诞生，etherscan.io网站的统计数据显示截至2020年3月初，利用以太坊上的ERC20开发的虚拟货币就达到了24万多种。Coinmarketcap网站对5 000多种热门的虚拟货币进行市值排名统计显示，2014年初虚拟货币市场总市值为106亿美元，其中比特币占了88.68%，到2017年底，虚拟货币的总市值为8 003亿美元，其中比特币的比例明显大幅下降，仅有39.99%。虚拟货币本身还存在容量有限等技术缺陷，尚无法成为公众交易媒介，且不能展现普惠金融的优势。另一方面由于存在投机和价格操控现象，其价格波动率是一般风险资产的3~5倍，不具备可信的储藏价值。由于内在价值的不确定性、匿名性和跨国界性，虚拟货币常被各种金融诈骗利用，具有很高的内在风险，诸如异常交易、欺诈行为、虚假信息诱导和恶意操纵价格等。从全球来看，利用虚拟货币进行犯罪和恐怖活动的非法交易数量及规模都非常庞大，急需用监管技术进行监测。

根据中国信通院和中国通信标准化协会发布的《区块链安全白皮书——技术应用篇（2018年）》，目前区块链技术应用架构中关键层次和核心机制已逐渐达成共识，其结构自下而上包含存储层、协议层、扩展层和应用层，每一层都存在相应的安全风险。比如存储层存在基础设施安全风险、网络攻击威胁和数据丢失泄露风险，威胁区块链数据文件的可靠性、数据完整性以及存储数据安全性；协议层存在协议漏洞、流量攻击以及恶意节点的风险；扩展层是实现智能合约的层级，风险主要来自代码的安全漏洞，例如合约开发的漏洞以及合约运行的安全漏洞；应用层则集合了传统安全风险，例如私钥管理安全风险、账户窃取、应

用软件漏洞、环境漏洞和DDoS攻击等。

3 区块链虚拟货币交易检测机制设计

区块链代币交易模式具有动态多样性的特点，且交易模式之间存在差异。本文基于人工智能技术开发一种链上异常交易检测模型，基于特征提取、数据聚类分析、交易关联图等技术，设计一种具有规则自学习、环境自适应的检测模型。

3.1 异常交易检测模型的关键技术

2002年Girvan和Newman 2位学者发现复杂网络中普遍存在着聚类特性，每个类称为一个社团，学术界定义社团结构是复杂网络的普遍特性，整个网络就是由众多社团组成的。随着对复杂网络的不断深入研究，学者们提出了大量发现社团的算法。通常比较流行的社区检测算法有Louvain算法、LPA算法和Infomap算法3种。其中Louvain算法是基于模块度的社团检测算法，整体效率和稳定性较高。LPA算法是比较简单的图传播算法，其经验假设是以节点为中心，进行投票制，十分高效，且容易实现分布式，运行开销较低，但由于随机选择易出现震荡。Informap算法与其他算法思路不同，是从信息论角度出发，清楚地定义各类事件的发生概率，利用信息熵公式，得到路径的最少编码长度，即最小平均比特。

本方案采用的是Louvain聚类算法，其采用高效的社团算法后再结合关联图技术，将用于高效构建用户交易关联关系。具体来讲Louvain聚类算法是一种启发式算法，是基于模块度最优化的社团发现算法。Louvain算法的最终目标就是使整个数据的模块度最大化，模块度的计算公式如式(1)所示。

$$Q = \frac{1}{2m} \times \sum_{ij} \left[A_{ij} - \frac{k_i \times k_j}{2m} \right] \times \delta(C_i, C_j) \qquad (1)$$

式中：

m——边的总数量

k_i——所有指向节点i的连接边的权重之和

A_{ij}——节点i和j之间的连接边权重

C_i——社区C的节点i

Louvain算法的流程是以下2个阶段不断迭代的过程，双层迭代可以弥补聚类算法2个节点合并后无法分开的缺点。第1阶段是外层迭代，采用自下而上的凝聚法，通过反复遍历网络图中的所有节点，比较节点对每个相邻社团所引起的模块度的变化，将节点归属到模块度产生最大增量的社团中。第2阶段是内层迭代，采用凝聚法和交换策略结合的方式，对第1阶段归属后的节点进行处理，将同一社团的顶点进行合并，以社团作为新节点重新构造网络图，重构后2个节点之间边的权重是新社团之间边的权重之和。通过第1、第2阶段的不断迭代，直到模块度稳定不再变化即完成关联关系的匹配过程。

3.2 异常交易检测模型的详细设计

异常交易检测机制分为4个功能模块，分别是交易数据收集模块、规则库模块、关联图模块和特征推理识别模块。

首先数据收集模块是为了将区块链上的交易信息进行收集和整理，通过客户端的可视界面呈现链上的所有交易数据，发挥区块链的优势，该交易数据具有不可篡改的特性，最大限度地保证其真实性。

然后交易数据输入到规则库模块进行匹配检测，利用人工智能匹配检测可以对海量的交易数据进行筛选、匹配、检测，识别出具备异常交易行为特征的交易数据。如果待检测的交易数据符合规则库中已有的交易模型，将直接进行人工智能特征推理，根据关联度、聚类、重要度或结构特征等维度，基于人工智能关联识别算法进行检测，识别出的异常交易模型将用于异常交易检测、交易风险分析、骗局识别或恶意炒作预警等方面。当遇到新的异常交易模型时，监测机制同时也具备自我学习和更新的功能，通过关联图模块，经过预处理、构建和统计3个步骤，可以将新的交易模式反馈更新到规则库中，这样一方面可以保证交易模型的顺利匹配，另一方面大大提高了识别检测的准确度。

实现人工智能匹配的前提是规则库的建立，该规则库是经过机器学习算法将异常交易行为的特征进行学习后存储构成的。

3.3 检测机制的规则自学习及环境自适应两大特性

上文描述的区块链虚拟货币异常交易监测机制具有规律自学习及环境自适应两大特性。

规律自学习是人工智能技术的优势特征之一，也就是说检测机制具备自我演进的能力，该自我演进功能的实现过程如下：检测机制中交易数据收集模块负责采集整理链上交易信息；规则库模块利用机器学习算法对历史规则进行人工智能匹配检测，若检测对象是未知的新交易模型，则由关联图模块构建用户交易关联关系，再通过特征推理识别模块利用人工智能技术进行特征推理识别，对异常交易进行检测。若检测

对象是已知的交易模型，则直接进行特征推理识别。检测的结果将会实时更新到保存到规则库模块中，从而实现模型的自适应演进功能。

本文提出的异常交易检测机制与交易环境的自适应匹配功能的实现过程如图1所示，通过分析区块链链上交易用户间的关联关系及交易类型重叠等特征，建立匹配多种交易模式的用户行为关联图，研究交易关联特征的智能识别机制，并设计检测模型中判定规则的学习更新策略，最终实现检测机制与交易环境的自适应匹配。

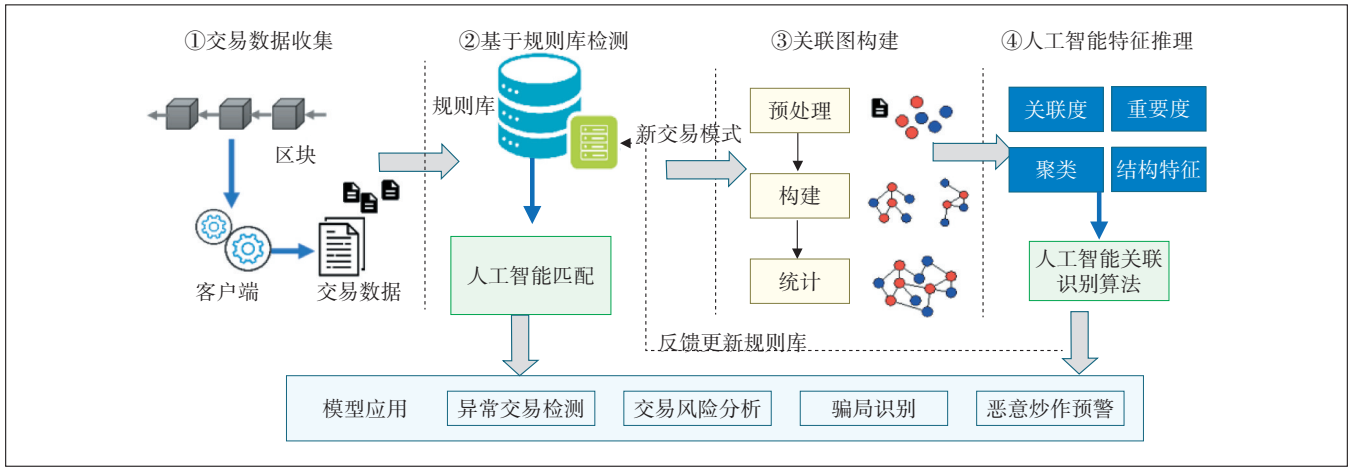

图1　规则自学习及环境自适应的异常交易检测模型原理示意图

3.4 检测机制实验结果

首先以发生在2017年5月的著名的比特币勒索病毒WannaCry事件的行为数据为试验参考数据验证该模型的可行性和效果，此次WannaCry比特币勒索病毒利用MS17-010漏洞攻击了全球超过150个国家，超过15万名用户遭到了勒索病毒攻击，感染的计算机会被植入敲诈者病毒，导致电脑大量文件被加密，遭受攻击的电脑被黑客锁定后，病毒会提示支付价值相当于300美元的比特币才可解锁，因此定性为比特币勒索病毒，该事件持续不到2天，造成的损失超80亿美元。该模型的检测与分析结果显示，此次勒索事件中披露的3个比特币地址仅限于接收来自受害者发送比特币的接收方，通过本文设计的启发式聚类方法分析比特币地址之间的发生率关系，结合Louvain聚类算法进一步获取用户之间的发生率关系，检测结果显示在此后并没有进一步的交易行为。

另外，为了专注于解决跟踪恶意的比特币交易行为，借助于2013年发生的比特币勒索病毒Crynlocker事件，通过监测模型获取交易行为数据并进行验证。黑客编写的“satan_pro”病毒程序将锁定服务器中所有文件，文件的后缀名都变成了“lucky”，被感染的文件和程序均无法正常运行，在C盘根目录下有个自动生成的文本文档，留有黑客的比特币收款地址和邮箱联系方式。通过本文的检测机制分析此交易行为的实施路径，试验数据显示，采用Louvain聚类方法可以明显提高异常交易行为检测的准确性和检测效率。

4 结论

本文通过分析法律法规对区块链监管的3个维度，将监管技术进行细分和定位。针对目前异常交易检测的迫切需求，笔者提出了一种能够实现规则自我学习、环境自适应的检测机制，对区块链异常交易进行实时识别和检测，助力监管部门有效、快速、准确地实施监管。

参考文献：

[1] 周瑞珏. 区块链技术的法律监管探究[J]. 北京邮电大学学报(社会科学版)，2017(3)：39-45.
[2] 叶聪聪，李国强，蔡鸿明，等. 区块链的安全检测模型[J]. 软件学报，2018，29(5)：1348-1359.
[3] 邓建鹏. 区块链监管政策的困境和出路[J]. 民主与科学，2019(4)：54-55.

作者简介：
曾晶，毕业于湖南大学，广东南方电信规划咨询设计院有限公司咨询院院长，高级工程师，硕士，主要从事通信与信息化相关规划、咨询工作；刘大畅，毕业于中国科学院大学，工程师，博士，主要从事电子信息与光通信专业技术工作；孙石峰，毕业于长春邮电学院，教授级高级工程师，学士，主要从事数据通信网络的规划、咨询、设计及技术管理工作。