•特约综述•　　DOI：10. 13471/j. cnki. acta. snus. 2021A007

区块链交易网络研究综述*

吴嘉婧[1]，刘洁利[1,2]，林丹[1,2]，郑子彬[1,2]

1. 中山大学计算机学院，广东 广州 510006
2. 中山大学软件工程学院，广东 珠海 519082

摘　要：自以比特币为代表的区块链加密货币交易平台诞生以来，基于区块链技术的加密货币获得了广泛的关注并积累了大量的交易数据。这些交易数据包含了丰富的信息和完整的金融活动痕迹，为研究者在这一领域进行知识发现提供了前所未有的机会。网络是描述现实世界中交互系统的通用语言，现有的区块链交易研究中有相当一部分是从网络的角度来进行的。本综述旨在从网络科学的角度分析和总结现有的有关区块链加密货币交易的文献。首先介绍了加密货币交易网络分析的背景信息，然后从交易网络建模、交易网络分析和交易网络上的识别技术3个方面对现有研究进行了综述，希望能为相关领域的研究者提供一个系统的指导。

关键词：区块链；加密货币交易；复杂网络；数据挖掘

中图分类号：TP399　　**文献标志码：**A　　**文章编号：**0529 -6579（2021）05 -0001 -12

Blockchain transaction networks：A survey

WU Jiajing[1]，*LIU Jieli*[1,2]，*LIN Dan*[1,2]，*ZHENG Zibin*[1,2]

1. *School of Computer Science and Engineering，Sun Yat-sen University，Guangzhou 510006，China*
2. *School of Software Engineering，Sun Yat-sen University，Zhuhai 519082，China*

Abstract：Since the debut of Bitcoin，a blockchain platform，blockchain-based cryptocurrencies have received wide attention and accumulated a wealth of transaction data. These transaction data include rich information and complete traces of financial activities，and therefore provide us an unprecedented opportunity for knowledge discovery. Networks are a universal language for describing interacting real systems，and much work on cryptocurrency transactions is conducted from a network perspective. This survey summarizes the existing work on analyzing and understanding blockchain transactions，aiming to provide a systematic guideline in this area. We first introduce the background of blockchain transaction，and then review existing research in three different aspects，i. e. ，transaction network modeling，transaction network analysis，and network-based detection technology，the purpose being to provide a systematic guideline for researchers in this area.

Key words：blockchain；cryptocurrency transactions；complex networks；data mining

* **收稿日期：**2021 -02 -03　　**录用日期：**2021 -04 -20　　**网络首发日期：**2021 -05 -21
基金项目：国家重点研发计划（2020YFB1006005）；国家自然科学基金（61973325，U1811462）
作者简介：吴嘉婧（1989年生），女；**研究方向：**区块链、图挖掘、网络科学；E-mail：wujiajing@mail. sysu. edu. cn
通信作者：郑子彬（1982年生），男；**研究方向：**区块链、服务计算、软件工程；E-mail：zhzibin@mail. sysu. edu. cn

郑子彬，教授、博士生导师，中山大学软件工程学院副院长、国家数字家庭工程技术研究中心副主任、IET Fellow、国家优秀青年科学基金获得者。获得教育部自然科学奖二等奖，青年珠江学者、珠江科技新星。

随着区块链技术的发展，区块链加密货币在近年来也受到了广泛的欢迎和关注。截至2021年1月，区块链加密货币的总市值已超1万亿美元，其中市场占比第一的是比特币，其市值高达7 000亿美元。在区块链加密货币平台上，所有交易记录具备不可篡改的特性，并按照时间顺序链接记录在区块链中。同时，区块链加密货币的交易无需依赖可信第三方，具有去中心化的特点。目前，电子支付和区块链加密货币支付是主要的两种支付方式，现金流通的减少已成为不可扭转的趋势，各国亦在积极探索法定数字货币的发行方案。在此背景下，中国人民银行提出了发布央行数字货币 DCEP（digital currency electronic payment）的计划。央行数字货币的发布将一方面降低纸币发行和流通的成本，提升交易的便利性，另一方面增强国家对交易的监管和对货币的控制力，从而维护国家金融体系的稳定和安全。

由于区块链的开放性和透明性，包含丰富信息和完整金融活动痕迹的加密货币交易数据可以被公开获取，这为金融交易数据挖掘领域提供了前所未有的机会。对区块链交易数据进行分析和挖掘的主要价值有两个：1）通过对区块链交易数据的分析和挖掘，可以广泛探究交易系统中的用户行为、财富分配和交易网络的演化过程，推测加密货币金融市场波动的原因，作为其他金融活动的参考；2）近年来区块链系统中各种类型的网络犯罪现象层出不穷，区块链交易数据分析有助于识别其中的非法交易，为构建更健康的区块链生态提供有效的监管方案，相关技术亦可作为法定数字货币交易监管的参考。总而言之，对区块链加密货币交易数据进行分析不仅可以提升复杂网络、数据挖掘等技术在金融系统中的理论价值和应用价值，而且有利于增强加密货币平台的金融安全和监管。

网络是描述现实世界中交互系统的通用语言，而复杂网络科学被广泛认为是分析网络系统的有效工具。在现有的区块链加密货币交易数据分析文献中，有相当一部分是从网络的角度进行研究，即在分析时先将加密货币系统中的对象（如账户、智能合约等）抽象为节点，将对象之间的关系抽象为连边。不同的加密货币平台可能存在一些不同的交易活动，例如转账、智能合约的创建及调用等，因而我们可以从不同的角度对加密货币的交易活动进行网络构建，然后基于网络性质分析、节点分类、链路预测等网络科学方法完成下游的数据挖掘任务。

作为一个新兴的跨学科的研究领域，区块链加密货币的交易网络分析引起了大量学者的关注。本文旨在全面回顾和总结这一领域的现有文献和最新技术，重点讨论加密货币交易网络的建模、交易网络的分析和交易网络上的识别问题。其中，在进行区块链加密货币的交易网络研究时，我们首先要将交易数据建模为交易网络，通过交易网络分析我们可以了解交易网络上一些特有的性质，最后，我们可以结合交易网络的性质为交易网络上的识别任务设计检测工具。本文内容的顺序安排如下：第1节介绍区块链交易及交易数据来源的预备知识，第2节从交易网络建模、交易网络分析和交易网络上的识别技术对区块链加密货币交易网络的研究现状展开综述，第3节为本文的总结与展望。

1 区块链及其交易

区块链加密货币类型多样，且不同加密货币的数据结构互不相同。具体而言，区块链加密货币的交易主要基于以交易为中心的模型和以账户为中心的模型。本节将对这两种常见的交易模型进行介绍，并且介绍区块链交易数据的收集方式，从而为第2节的交易网络分析打下基础。

1.1 区块链交易模型

区块链交易可被视为加密货币平台上的用户操作。当一个新交易被用户发起时，它将被广播到点对点（P2P，peer-to-peer）网络中的所有节点，经由验证后可被添加到区块链的新区块中。区块链技术最早可追溯于中本聪在2008年发布的比特币白皮书[1]，随后在2009年，第一条区块链伴随着比特币系统的发布和挖矿操作而诞生。自比特币诞生以来，区块链技术得到了广泛的关注，并被应用于智能金融、物联网等多个领域[2-4]。同时，许多被称为altcoins的替代币迅速出现，例如第一个去中心化的域名系统Namecoin[5]；在交易确认速度上得到提升的Litecoin[6]；提出采用股权证明（PoS，proof of stake）作为工作量证明（PoW，proof of work）的替代方案的Peercoin[7]。根据CoinMarketCap.com的统计，到2021年初，市场上已有超过8 000种区块链加密货币，总市值一度超过1万亿美元。其他著名的加密货币包括Monero[8]、Zerocash[9]、EOS[10]和Libra[11]等，其

中，以太坊[11]是最大的具备图灵完备的智能合约的区块链系统，其主要的货币被称为Ether（简称ETH），是仅次于比特币的全球第二大加密货币。在众多区块链加密货币中，它们的交易模型主要可以分为以交易为中心的模型和以账户为中心的模型，其中，比特币和以太坊分别是这两类交易模型的典型代表。

在比特币系统中，作为一种用户标识，比特币地址是由用户公钥经过一系列单向的哈希算法得到的，单个用户可以拥有多个交易地址。比特币系统采用的交易模型是以交易为中心的模型，其中单个交易可以具有多输入和多输出，并且可以与多地址关联。交易的输入由一组未花费的交易输出（UTXO，unspent transaction output）组成，其总金额需不小于交易支付金额。交易输入方的用户可以指定一个新地址来接收找零，用于接收找零的地址又被称为找零地址（change address）。此外，比特币中没有账户余额的概念，可以通过用户钱包中UTXO的金额总和来计算该用户的余额。

以太坊中的交易模型是以账户为中心的模型，它包含两种账户，即外部账户（EOA，externally owned account）和合约账户。其中，EOA类似于银行账户，它具有存款、取款和记录一些动态状态信息（如账户余额）的功能。合约账户关联着一个可执行的字节码，其交易行为由用户编写的智能合约代码所控制，并会对一些状态信息进行维护，如字节码哈希值及合约账户的余额等。与比特币不同，以太坊中的交易是从一个账户到另一个账户的签名数据包，它仅包含一个输入和一个输出。此外，以太坊交易可以完成包括转账、合约创建和合约调用在内的3种主要功能。根据交易发送方，以太坊交易可以分为由EOA发起的外部交易和由合约调用触发的内部交易。图1给出了一个以太坊外部交易和内部交易的典型示例，其中交易1和交易2都是由EOA发起的交易，因此它们是外部交易，而交易3、交易4及交易5是由智能合约触发的交易，因此它们是内部交易。外部交易可能会导致许多内部交易的产生，比如在交易2中，一个EOA调用了一个合约账户，继而触发了后续的3个内部交易。

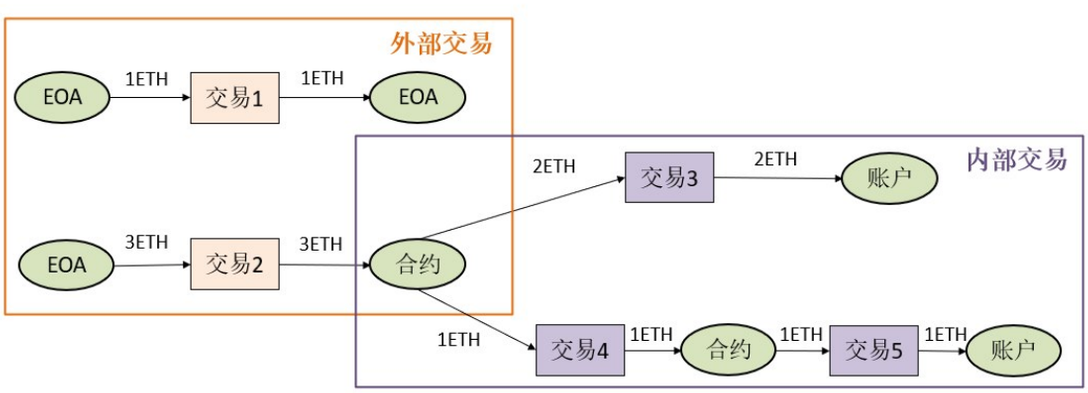

图1　以太坊的外部交易和内部交易

Fig. 1　Examples of the external transactions and internal transactions in Ethereum

1.2　区块链交易的数据源

区块链加密货币交易网络分析的数据源主要包括区块链交易数据和标签数据。最原始的获取区块链交易数据的方法是通过区块链客户端（例如BitcoinCore和Geth）去访问区块链网络并同步区块数据，从而获得区块链的原始数据。但是，对于许多加密货币而言，它们的原始区块链数据以二进制格式存储，需要解析为可读的格式以进一步分析。因此，我们可以根据区块链数据结构构建解析器，从获取的原始数据中提取交易记录。另外，一些区块链客户端为用户提供了JSON-RPC接口以便获取交易数据。然而，对于一些启用智能合约功能的区块链系统，其内部交易记录并未存储在区块链系统中。这些内部交易记录可以通过区块链浏览器检索获取，也可以通过使用自定义客户端重演所有外部交易来获取有关内部交易的详细信息。部分客户端亦提供获取内部交易信息的接口，例如以太坊OpenEthereum客户端的“trace”模块能提供在以太坊虚拟机中生成的详细运行时数据，是访问内部交易记录的便捷工具。

在一些交易网络挖掘任务中，利用标签信息能进一步辅助方法的设计和验证。但是，区块链用户在交易过程中无需暴露真实的身份信息，因此很难找到其对应的标签信息。随着区块链生态的日益成熟，我们可以从一些区块链论坛、区块链浏览器上找到部分人工标记的标签数据。例如，Walletexplorer. com是一个具有地址自动聚类能力，能提供丰富地址标签的智能区块链浏览器；比特币论坛Bitcoin Forum记录了一些跟比特币抢劫、盗窃、诈骗有关的地址①；区块链浏览器Etherscan的标签词云模块②提供了由用户标记的以太坊账户标签；此外，CryptoScamDB. org提供了一个开源数据集，用于跟踪与区块链系统有关的恶意网址及相关加密货币地址。

此外，一些研究者还发布了经过清洗和整理的区块链数据集以供研究。例如XBlock. pro是一个旨在助力区块链良性发展和数据研究的数据集共享平台，它收集了当前主流的区块链加密货币的相关数据，并对数据进行了清洗和归类，是目前学术界数据量最大、覆盖面最广的区块链数据平台之一，可支持科研人员进行区块链链上数据分析、区块链反欺诈、智能合约分析、区块链性能分析等方面的研究。

2 研究现状

现有的区块链加密货币交易网络分析工作具体可以总结为3个紧密相关且逐层递进的部分：交易网络建模、交易网络分析和交易网络上的识别技术。其中，交易网络建模主要涵盖将交易数据以网络形式存储的方法和讨论；交易网络分析从网络科学的角度对交易网络的特有属性进行了讨论；交易网络上的识别技术主要包括账户地址背后的归属识别、交易模式识别和区块链上非法活动的识别。本节将分别对这3个部分的研究现状进行介绍和总结。

2.1 交易网络建模

区块链加密货币交易网络研究的第一步是根据区块链的交易特性将区块链交易数据建模为网络。目前区块链系统的交易模型可大致分为两类，即以交易为中心的模型和以账户为中心的模型。基于这两种不同的交易模型的区块链系统，其交易数据的网络建模亦有很大差别。

比特币是最典型的采用以交易为中心的模型的区块链交易系统，目前已有一系列的对比特币交易数据进行网络建模的工作。文献［12］首先介绍了比特币交易网络建模的概念，并提出将比特币的交易过程建模为将交易作为节点的交易网络和将用户作为节点的用户网络，分别代表交易之间和用户之间的比特币资金流。在比特币交易过程中，由于交易的输入是来自先前交易的UTXO，因此交易网络的构建非常直观及简单，即用节点代表交易，用包含金额和时间戳信息的有向边表示比特币资金流。考虑到用户拥有多个比特币地址的可能，文献［12］首先将属于相同用户的地址以聚类的方式进行聚合，然后构建以用户为节点、用户之间的资金流关系为边的用户网络。这两种比特币交易网络建模方法被广泛应用于后续区块链交易网络分析的研究中[13-14]。此外，文献［15］将比特币交易数据建模为以交易和地址为节点的带权有向超图，可以表示地址和交易之间的输入和输出关系。

以太坊是基于以账户为中心的交易模型的区块链系统的典型代表。在以太坊的相关研究中，文献［16］介绍了3种以太坊交易数据网络建模方式，即资金流网络、智能合约创建网络和智能合约调用网络。在这3个网络中，EOA和合约账户均被抽象为网络的节点，但是3个网络中边的语义有所不同。在资金流网络中，边表示资金流向，而在智能合约创建网络和智能合约调用网络中，边分别表示合约的创建和合约调用。同时，只有合约账户才能作为智能合约创建网络和智能合约调用网络中边的终点。考虑到两个账户之间会发生多个交易，文献［17］提出将以太坊交易记录建模为时序多重网络。其中，账户被表示为节点，每个交易被表示为一条由交易发送方指向交易接收方的有向边，每条边包含了时间和金额信息，具体如图2所示。

作为网络分析的基本步骤，网络建模直接影响上层算法的设计和效果，因此它非常关键。目前的交易网络建模方式有许多种，但是在进行网络构建时，我们会面临区块链交易操作种类繁多、信息多源异构的问题及不同的下游任务。因而如何找到适用于各种区块链数据和不同区块链任务的通用建模方式和建模标准是一个重要的研究方向。

①https://bitcointalk.org/index.php?topic=83794.0

②https://etherscan.io/labelcloud

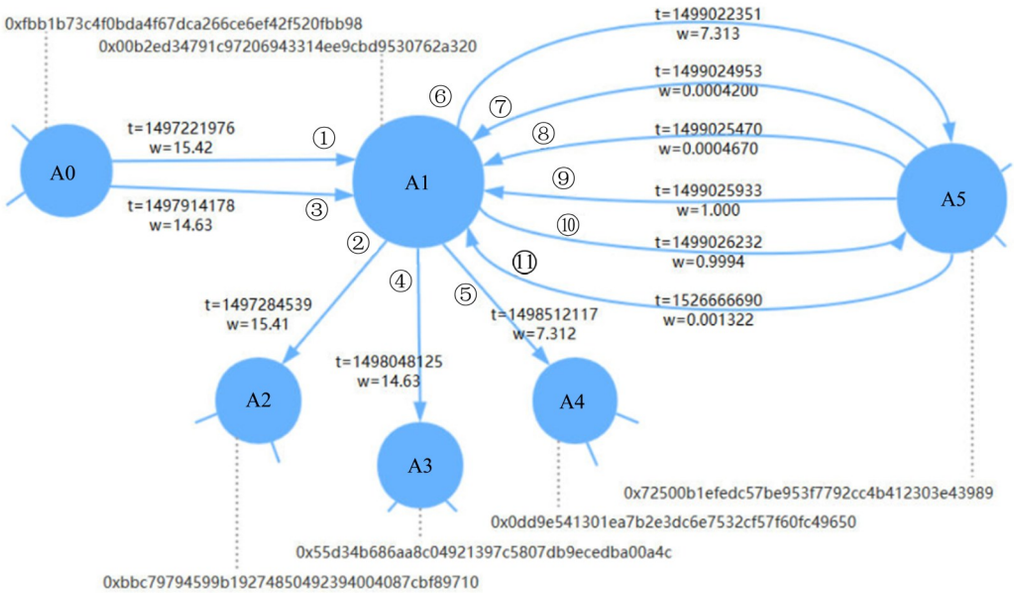

图 2　基于以太坊交易的时序加权多重有向网络 [17]

Fig. 2　Temporal weighted multidigraph in Ethereum[17]

2.2　交易网络分析

复杂网络理论已经被广泛地证明是一种建模和描述各类复杂系统的有效工具。近 20 年来，复杂网络相关的研究者提出了各种各样的研究指标以对网络特征进行描述和度量。本小节将简要介绍一些重要的网络指标以及区块链在这些指标上的表现，以助了解区块链加密货币交易网络的特有性质。

1）节点和边的数量。网络中节点和边的数量是衡量网络规模和密度的常用指标。在对区块链加密货币交易网络进行分析的过程中，Maesa 等 [18] 观察到比特币交易网络的网络规模增长速度比线性增长更快。Alqassem 等 [19] 也注意到了这一现象，并发现比特币交易网络正在变得越来越密集，且其度分布遵循幂律分布。Chen 等 [16] 统计了以太坊的资金流网络、智能合约创建网络和智能合约调用网络中节点和边的数量，发现在以太坊中用户的转账行为比创建智能合约及调用智能合约的行为更频繁。

2）度分布。在无向网络中，节点的度是指节点的边数。而在有向网络中，节点的度分为入度和出度，起始于节点的边的数量称为该节点的出度，终止于节点的边的数量称为该节点的入度。度分布可以表示网络中节点度的概率分布，计算公式如下

$$p(k)=\frac{\text{度为}k\text{的节点数}}{\text{节点总数}}.$$

在复杂网络中，一个有趣的现象是许多从真实系统建模而来的网络的度分布符合幂律分布，即满足

$$p(k)=Ck^{-\alpha},$$

其中 C 和 α 是常数，k 是度的值。Kondor 等 [20] 发现比特币地址网络入度和出度分布都具有高度异构性。Motamed 等 [21] 对 5 种加密货币的交易网络进行了度分布分析，发现这些交易网络的度分布都符合幂律分布，且幂律参数 α 经过一定的波动后会收敛到稳定状态。

3）路径长度。网络中两个节点之间的路径长度定义为连接这两个节点时必须经过的最少的边数，通常可以采用广度优先搜索的方法找到两个节点间的最短路径。网络直径是网络中所有节点对最短路径中值最大的路径长度。Lischke 等 [22] 指出，不同国家比特币用户子网络的平均最短路径在同一范围内。根据交易网络直径随时间的变化，Gaihre 等 [23] 推断出比特币用户对系统匿名性的担忧。Alqassem 等 [19] 分析了比特币交易网络直径增加的 4 个可能原因，即匿名性、窃贼、找零地址和比特币混币服务。此外，许多研究通过计算平均最短路径来评估比特币和以太坊中的“小世界”现象 [4]。

4）聚类系数。聚类系数描述了网络中节点的聚集程度。聚类系数的两种度量方法包括局部聚类系数和整体聚类系数。局部聚类系数量化了共享同一邻居的两个节点本身也是邻居的概率。全

局聚类系数是网络中所有长度为2的路径中闭合路径所占的比例[24]，可通过以下公式计算

$$C_g = \frac{1}{n}\sum_v \frac{t_v}{\frac{k_v(k_v-1)}{2}},$$

其中n是节点数，k_v是无向网络中节点v的度数，t_v是包含节点v的三角形数。Baumann等[13]观察到比特币用户网络具有较高的平均聚类系数和典型的“小世界”特性。在以太坊的资金流网络中也发现了类似的结果[16]。然而，最近的研究表明，Ripple和Namecoin的交易网络的聚类系数相对较小[8]。

5）中心性。网络中计算节点中心性的方法有很多种。其中，最简单的中心性度量是节点度，其他被广泛应用的中心性度量包括特征向量中心性、katz中心性、PageRank算法、介数中心性和接近度中心性。Lischke等[22]使用度中心性识别比特币交易网络中的主要枢纽。Chen等[16]通过PageRank算法获得了资金流网络、智能合约创建网络和智能合约调用网络中最重要的10个节点。他们发现，交易所等金融应用在资金转移、合约创建和合约调用方面发挥着重要作用。

6）同配性系数。同配性系数是用来衡量节点是否趋向于和与之相似的其他节点进行连接的指标。度同配性系数表示网络中的节点是否愿意与具有相似度的其他节点进行连接，其最大值是1，最小值是-1。值为正表示网络是同配性的，值为负说明网络中节点对的度是负相关的，也称为异配，取0代表网络结构不存在相关性。一系列的研究表明，许多区块链系统，如比特币、以太坊、莱特币和达世币，其加密货币交易网络是异配的。

7）连通分量。在无向网络中，定义一个连通分量为一个子图，该子图中每对节点间均有一条路径。而在有向网络中，连通分量的概念包括弱连通分量和强连通分量。弱连通分量的定义类似于无向网络中连通分量的定义。强连通分量是指对于所有节点集，每对节点之间至少存在一条有向路径。在计算弱连通分量时，有向网络的边的方向信息将被忽略。对连通分量进行统计和分析有助于我们了解网络结构，其中在区块链交易网络的分析上，Gaihre等[23]观察到，比特币交易网络中连通分量的数目在2011年之前激增，但后来有所减少。他们分析得到这是因为许多交易所在2010年和2011年前后兴起，促进了比特币的流通。文献［19］提到，大多数比特币地址包含在比特币交易网络的最大连通分量中，这个性质与其他网络类似。Guo等[25]发现，在以太坊中连通分量的大小分布可用幂律分布来近似，并且存在重尾特性。

8）社区。社区是内部节点连接紧密而与外部节点少有连接的网络模块。一个网络可以经过社区检测算法划分为多个社区，不同的社区可以近似反映网络中功能或者结构的划分。Alqassem等[19]研究了比特币中社区结构的性质，发现社区规模的分布可以用指数截断的幂律分布来拟合，且大多数比特币社区都具有树状结构。Moreno-Sanchez等[26]研究了Ripple中社区是如何形成的，他们发现用户社区是动态的，是通过连接到同一地理区域的网关而形成的。

9）网络模体。网络模体是指在复杂网络中出现次数显著高于在随机网络中出现次数的子图模式，它是揭示网络中高阶组织的有效工具，被称为复杂系统中的基础构件。Moreno-Sanchez等[26]从最常见的模体出发，将钱包分为网关、交易所和用户，并分析得出网关是Ripple中的关键角色，这与低聚类系数和异配性的网络特性是一致的。Bai等[27]研究了以太坊资金流网络中13种包含3个节点的模体，并将这些模体分为闭合的和开放的三角形。他们发现虽然闭合的三角形数量有所增加，但其比例呈下降趋势。Paranjape等[28]观察到，比特币中循环三角形模体的比例比StackOverflow等任何其他数据集都要高得多。

除了上述众所周知的网络特性外，一些研究者还从几个新的角度对区块链交易网络进行了研究。例如，不同于以往只关注全局网络性质的研究，Ron等[29]主要研究比特币交易网络上的用户行为，包括用户如何使用比特币，如何在不同账户之间转移比特币，并分析了比特币系统中发生的最大交易。他们发现大部分比特币处于休眠状态，且网络中有许多看起来奇怪的结构，如二叉树结构、长链。Lischke等[22]结合链下数据（包括商业标签、IP地址和地理位置）对比特币系统的用户网络和经济状况进行了分析。他们深入了解了不同国家的业务分布和交易分布，以及不同的业务和不同的国家分别涉及的交易子网络的网络性质。Maesa等[30]分析了比特币用户网络中度分布的异常值，发现了一些异常的交易模式。通过网络分析，Gaihre等[23]回答了比特币用户是否关

心匿名性的问题，他们发现大多数用户对匿名性的关注度很弱，但一个重要的影响因素是用户拥有的比特币的价值。Chen 等[31]通过交易网络分析研究以太坊 ERC20 代币的创建者、持有者和代币交易活动。Liang 等[32]研究了 3 种区块链加密货币的交易网络性质，并从这些性质分析了这 3 种加密货币的竞争力。

尽管目前的研究已经充分涵盖不同时间段主流区块链加密货币交易网络的网络性质分析，但是在网络性质的时序分析及交易网络的生成和演化方面，现有研究讨论非常初步。同时，鲜有研究揭示区块链加密货币交易网络与传统引文网络、社交网络的异同。未来可对区块链加密货币交易网络的网络性质进行更深入的讨论，并结合交易网络的特性辅助下游任务的进行。

2.3　交易网络上的识别技术

由于区块链交易无需真实的用户身份信息，许多区块链加密货币平台已成为各种网络犯罪和非法金融活动的温床。基于区块链交易网络的发展的检测和识别技术，可以帮助我们识别区块链上的异常交易行为。接下来将从实体识别、交易模式识别和非法活动检测展开介绍。其中，实体识别可以帮助找到属于同一用户或组织的账户地址，它通常是后续分析任务的基础，交易模式识别对不同类型用户的交易行为进行区分与识别，为后续的非法活动检测提供依据。

2.3.1　实体识别　大多数区块链加密货币平台创建新的账户或地址的成本很低，且无需验证用户真实的身份信息。因而用户可以很方便地使用多个账户地址来增强区块链交易活动的隐蔽性，这种操作在涉及区块链交易的犯罪案例中很常见。Ron 等[29]第一次提出用“实体”来描述这种多个账户地址的拥有者，其中实体可以是一个用户，也可以是一个组织。为了挖掘区块链账户地址背后真实的身份信息，首先要对属于同一个实体的多个账户地址进行关联，又被称为实体识别。现有的实体识别方法大致分为 3 种类型：基于交易属性的实体识别、基于行为的实体识别和基于链下信息的实体识别。

基于交易属性的实体识别主要利用区块链交易的特有属性来判断账户地址是否属于同一实体。在比特币系统中，交易具有多个输入和多个输出，由于花费一个地址的比特币需要提供该地址的私钥，正常情况下用户不会共享他们拥有的比特币地址的私钥。因此，Reid 等[12]认为比特币交易的多个输入地址处于同一实体控制之下，并通过这种方法对比特币系统的地址进行实体识别，这种方法被称为多输入启发式方法。Harrigan 等[33]进一步调查了这种启发式方法的有效性，并发现多输入启发式方法可能会导致漏检和误判误差。而两种误差可能是由于地址重用、超级集群和持续增长的地址簇等多方面因素造成的。Remy 等[34]结合多输入的启发式方法和社区检测技术提出了一种新的实体识别方法，该方法能以精确度为代价增加召回率，因而在实际应用中可以自行进行调整。比特币系统中利用交易属性进行实体识别的另一种典型方法是找零地址启发式方法，该方法由 Reid 等[12]提出。在比特币交易中，会使用额外的找零地址接收找零，因此我们可以识别交易输出方的找零地址并将其与对应的输入地址进行关联。Klusman 等[35]指出，多输入启发式和找零地址启发式方法并不适用于以太坊等基于以账户为中心的交易模型的区块链系统。为解决这个问题，Victor[36]提出了 3 个在以太坊上的启发式规则：存款账户重复使用，空投多参与以及自我授权。存款账户重复使用规则是以交易所为背景设计的。事实上，交易所通常会为用户生成存款账户，一旦用户将资金转入其存款账户，这笔钱稍后会自动转入属于交易所的热钱包。当存款账户被重复使用，就可以将使用相同存款账户的一系列其他账户识别为同一个实体。空投多参与规则为空投情况而设计，其中，空投是一种通过分发代币来为 ICO 筹集资金的常用营销方式。由于一些用户将注册多个账户参加空投并将代币汇总到一个账户，因此可以将这些账户识别为同一实体。自我授权规则基于以下假设：代币消费者和代币所有者在调用授权函数时可以被识别为同一实体。经过实验分析和验证，Victor[36]认为存款账户规则是实验中最有效的方法。

基于行为的实体识别是利用用户在交易过程中特有的行为偏好来判断多个账户地址是否属于同一实体，因而一些研究者将实体识别问题视为基于交易行为特征的分类或聚类问题。Androulaki 等[37]考虑了一些交易行为特征，包括交易时间、交易方的索引、交易金额等，并通过基于特征的聚类揭示了近 40% 的用户身份。Jourdan 等[38]探索了 5 种类型的特征，包括地址特征、实体特征、时间特征、中心性特征和模体特征，并研究了这些

特征在比特币地址分类任务的效果。Harlev 等[39]将交易行为特征作为监督学习的输入，以实现比特币地址的去匿名。此外，Shao 等[40]通过网络嵌入的方法将比特币地址在交易网络中的交互活动转换为低维特征向量，并结合深度学习方法进行实体识别。

区块链链下数据指未存储在区块链中的相关数据，它可以用来协助去匿名化过程。典型的链下数据包括节点的IP地址、公开的标签等。一些用户会在论坛整理发布带欺诈性的交易地址、混币服务地址等，这为我们创造了一个通过爬虫采集这些信息的机会。同时，如果一位用户暴露了自己的地址信息，可以通过分析用户的交易行为找到其所拥有的其他地址。Reid 等[12]首先在实体识别中应用了这种方法，并利用链下信息识别了一些参与盗窃的实体。根据比特币论坛上提供的链下信息，Fleder 等[41]将比特币地址链接到其对应的真实身份，并发现一些论坛用户参与过暗网交易和赌博活动。Möser 等[42]通过使用混币服务来获取相关的地址信息，并通过分析这些地址信息的交易构建了混币服务识别模型。

2.3.2 *交易模式识别* 在区块链加密货币生态中，不同用户的交易行为大相径庭，例如交易所的交易活动远比普通用户的交易活动活跃。交易模式识别旨在揭示交易网络的特殊结构并进一步分析用户的交易行为，相关方法可总结为：可视化方法、跟踪分析和模体分析。

网络可视化是一种强大的分析方法，可直观了解交易网络及其内部的交易模式。McGinn 等[43]通过可视化某些特定区块中的比特币交易网络，发现了包括洗钱和拒绝服务攻击在内的异常交易模式。Chen 等[44]对异常地址的每日交易网络子图进行可视化，发现了一些与比特币市场价格操纵相关的异常交易模式，如自环、双向、三角形等。McGinn 等[45]将比特币交易的源区块和目标区块视为邻接矩阵进行可视化，并发现这种可视化方法很容易揭示出一些重复交易行为，方便将具有相似行为的交易关联在一起。

在已知特定账户地址身份的情况下，对账户地址的交易进行跟踪分析有利于总结出该类型账户的交易模式。Maesa 等[30]分析了比特币交易网络中度分布的离群点，通过对这些离群点进行分析，他们注意到一种类型刷屏行为的交易。经过进一步分析后，他们总结出这些异常的刷屏交易可能是区块链上的假名攻击、垃圾邮件攻击或者广告行为。Ron 等[29]跟踪了比特币系统中超过50 000 BTC的大额交易，并分析了这些交易在长链和分叉合并模式下背后隐藏的交易意图。

分析加密货币的交易模式的一系列研究是通过对交易网络模体的分析展开的。Ranshous 等[46]使用有向超图对比特币交易网络进行建模，并在有向超图中引入网络模体来揭示交易所的交易模式。Wu 等[47]在时序有向的比特币交易网络中提出了时序异构模体的概念，并将其用于比特币混币服务的地址检测。Zola 等[48]使用网络模体特征设计了一种实体识别方法，同时，他们也研究了不同实体交易模式随着时间推移的相似性，并探索是否有一些交易模式在不同批次的比特币交易中重复进行的问题。Jourdan 等[38]利用网络模体来揭示实体的交易模式信息，并通过实体识别任务说明交易模式可以被看作实体的指纹。

2.3.3 *非法活动检测* 区块链系统的去中心化和交易无需真实身份的特性不仅吸引了大量的投机者，也吸引了许多犯罪分子的注意，因而区块链也成为了诈骗、黑市贸易、洗钱等违法犯罪活动的温床。与传统金融场景不同，区块链系统在进行交易之前不能通过执行“了解你的用户”（KYC，know your customer）流程来验证用户的身份。但是，区块链系统中公开和不可篡改的交易记录为我们提供了非法活动的检测机会。接下来，我们将重点回顾基于交易网络上的识别技术进行的区块链金融诈骗和洗钱的检测工作。

区块链系统上的金融诈骗给加密货币生态的健康发展带来了巨大威胁。在 Vasek 等[49]的研究中，报告了包含庞氏骗局、采矿诈骗、诈骗钱包和欺诈性交易在内的多种比特币诈骗方式，并发现在192起与比特币交易有关的诈骗案中，1.3万名潜在受害者损失了约1 100万美元。此外，其他区块链系统中也发现了丰富的欺诈类型，如ICO诈骗[50]、蜜罐钓鱼合约诈骗[51]等。由于区块链诈骗不仅损害了交易人和投资人的利益，同时也影响了区块链交易的可靠性和人们对区块链的信任，一些研究者展开对区块链诈骗检测的研究。目前的检测方法不仅包含一些基于特征提取的方法[52]，亦包括了一些基于智能特征提取的检测方法。文献［53］提出了一种基于图卷积神经网络的Edge-Prop方法来学习大规模交易网络中节点和边的嵌入。与传统的基于图卷积神经网络的方法不同，

EdgeProp 能学习到多重边的边信息，进而有效地识别以太坊上的非法账户。Wu 等[54-55]提出了两种基于随机游走的嵌入方法，它们在学习节点嵌入时考虑了交易网络的交易量、时间戳和多重边等特性，并在下游钓鱼检测任务中验证了方法的有效性。

在区块链系统中，洗钱也是一个需要得到监管和重视的问题。洗钱通常分为 3 个步骤：首先，将黑钱注入金融体系；其次，将黑钱混入合法的货币中，与非法来源脱钩；最后，这些黑钱被犯罪分子整合和收回，并处于一种看似合法的状态[56]。由于区块链具有去中心化、交易匿名的特性且存在许多可用的隐私保护技术，加密货币已成为洗钱过程中隐藏非法资金流向的选择之一。著名的加密货币情报公司 Elliptic 在关于比特币的洗钱报告中指出，交易所、混币服务和赌博网站是比特币洗钱的主要流向[57]。因此，近年来对加密货币交易网络上的洗钱检测的研究，主要集中在混币业务和交易所的可疑交易模式上。比特币混币服务最初是为了通过混淆交易输入方和接收方的关系来增强交易的匿名性，使资金来源更加不可追踪，但它同时也成为了协助非法洗钱的一大利器。Prado-Romero 等[58]首先强调了混币服务检测的重要性，并将混币服务检测视为一个社区离群点检测问题来解决。因为一旦检测到混币服务，我们就可以进一步分析与这些服务交互的账户地址是否参与了非法活动。然而，这项工作的解决方案缺乏对不同类型混币服务的自动适用能力。Wu 等[47]进一步提出了一种基于网络模体检测方法，从而自动刻画不同混币服务的交易模式。除了混币服务识别以外，Hu 等[59]通过特征分析对比特币洗钱交易模式进行特征刻画，并利用 deepwalk[60]和 node2vec[61]等网络嵌入方法，构建了识别洗钱交易的分类器。Battista 等[62]提出了纯度的概念以理解比特币是何时以及如何混币的，并建立了一个名为 BitConeView 的比特币资金流可视化系统。Ranshous 等[46]指出，交易所提供了匿名身份与真实身份之间的联系，因此研究交易所的交易模式是反洗钱的重要步骤。他们将交易所涉及的可疑洗钱模式用网络模体进行刻画，并利用网络模体作为交易所的识别特征。

除了金融诈骗和洗钱问题，研究者还基于交易网络识别技术提出了其他检测区块链非法活动的方法。Weber 等[57]提供了一个比特币系统上的 Elliptic 数据集，其中包含超过 20 万个交易节点、23.4 万条交易信息以及 166 个节点特征。此数据集中的交易根据真实实体信息被标记为合法类别（如交易所、钱包提供商、矿工和合法服务）、非法类别（如诈骗、恶意软件、恐怖组织和勒索软件）和未标记类别。基于该数据集，研究者使用 EvolveGCN[63]方法对交易进行识别和分类。由于加密货币在勒索软件支付中的广泛应用，Akcora 等[64]提出了一种基于拓扑信息的勒索软件检测框架，用于检测已知勒索软件和新出现的勒索软件的地址。Conti 等[65]从比特币支付的角度研究了最近的勒索软件及其经济影响，并结合共同输入交易和找零地址信息提出了两种聚类启发式算法，以识别与勒索软件相关的地址。在对黑市调查过程中，Foley 等[66]对比特币中的非法交易活动进行了量化，并基于社区检测和分类模型提出两种识别方法。此外，作者通过分析结果指出约有一半的比特币交易与非法活动有关。

总而言之，现有的这些交易网络识别技术不可避免地会受到区块链上隐私保护技术的干扰，这两类技术就像矛与盾的较量和比拼，互相促使各自的技术创新与发展。目前令人棘手的区块链非法活动检测任务也仅仅做到了事后检测，可实际应用的非法活动预警和非法资金追踪与拦截方案较少。因此就未来而言，区块链交易网络上的识别技术仍有非常大的发展空间和应用潜力。

3　总结与展望

由于区块链系统的透明性和开放性，区块链加密货币的大多数交易数据可被公开获取。通过将加密货币系统中不同的对象抽象为节点，并将对象之间的交易关系抽象为连边，区块链加密货币的交易数据可被建模为大规模的复杂网络。在过去的 10 年里，研究者们已从网络的角度进行了大量有关区块链交易分析的研究。本文对区块链交易网络研究的相关工作进行了全面的回顾，并将现有技术和结果归纳为 3 个紧密相关且逐层递进的部分，即区块链加密货币的交易网络建模、交易网络分析和交易网络上的识别技术。从总体来看，目前的区块链加密货币分析领域已有了初步的发现和理论成果，同时也推动了复杂网络理论和图挖掘技术的发展。通过对现有工作的总结与思考，我们提出一些在区块链加密货币交易网络分析领域未来的研究方向：

1）动态信息建模与处理。现有的区块链交易网络分析和挖掘工作通常会忽略时间信息，但是，区块链网络是一个不断增长的网络，新交易的发生伴随着新节点或新连边的出现。这些新节点和新连边可能会改变原有网络的性质，同时也让基于原有交易网络设计的数据挖掘模型的效果受到影响。因而，未来的工作可以进一步探索如何对动态的区块链交易数据进行建模，分析网络的动态特性和演化规律，设计能自适应网络变化的识别技术。

2）交易网络数据扩充。区块链加密货币交易网络的数据扩充将是区块链交易数据分析中值得期待的一大研究方向。一方面，近年来许多用于提升区块链可扩展性的链下交易方案已被提出并得到了初步的应用，比如闪电网络、雷电网络等，而这些方案会使我们无法获取全部的区块链交易数据。另一方面，区块链加密货币的交易数据存在着标签数量少、各类别标签数量不均衡的问题。通过网络数据扩充，可以还原部分缺失的网络结构信息，对交易网络进行有效的信息补全，并且在一定程度上缓解标签获取困难的问题，从而辅助区块链交易数据分析。

3）交易审计与追踪。在区块链交易中，用户无需使用真实的身份信息，且可利用一些服务和工具来增强交易的匿名性。虽然这能为用户更好地实现隐私保护，但也吸引了很多犯罪分子利用区块链交易来逃避监管。现有的交易去匿名和追踪技术非常有限，因此，如何利用交易网络分析在强匿名性、去中心化的区块链上实现交易的可审计、非法交易的可追踪与可拦截是一个重要的研究方向，不仅可以加强区块链交易的合规性，还可以减少用户和潜在投资者的财务风险。

参考文献：

[1] NAKAMOTO S. Bitcoin：A peer-to-peer electronic cash system[EB/OL]. [2021-05-05]. https://bitcoin.org/bitcoin.pdf.

[2] PANARELLO A, TAPAS N, MERLINO G, et al. Blockchain and IoT integration：A systematic survey[J]. Sensors, 2018, 18(8)：2575.

[3] LU Y. Blockchain：A survey on functions, applications and open issues[J]. Journal of Industrial Integration and Management, 2018, 3(4)：1850015.

[4] ABBAS Q E, JANG S B. A survey of blockchain and its applications[C]//2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). IEEE, 2019：1-3.

[5] VINCED. Namecoin：A distributed naming system based on Bitcoin[EB/OL]. [2021-05-05]. https://www.namecoin.org.

[6] LEE C. Litecoin：Open source P2P digital currency[EB/OL]. [2021-05-05]. https://litecoin.org.

[7] KING S, NADAL S. PPCoin：Peer-to-peer crypto-currency with proof-of-stake[EB/OL]. [2021-05-05]. https://www.peercoin.net/.

[8] MONERO. Monero：A secure, private, untraceable cryptocurrency[EB/OL]. [2021-05-05]. https://www.getmonero.org.

[9] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash：Decentralized anonymous payments from bitcoin[C]//2014 IEEE Symposium on Security and Privacy. Berkeley, CA, USA：IEEE, 2014：459-474.

[10] XU B, LUTHRA D, COLE Z, et al. EOS：An architectural, performance, and economic analysis[EB/OL]. [2021-05-05]. https://blog.bitmex.com/wp-content/uploads/2018/11/eos-test-report.pdf.

[11] AMSDEN Z, ARORA R, BANO S, et al. The libra blockchain[EB/OL]. [2021-05-05]. https://developers.libra.org/docs/assets/papers/the-libra-blockchain/2020-04-09.pdf.

[12] REID F, HARRIGAN M. An analysis of anonymity in the bitcoin system[C]//ALTSHULER Y, et al, eds. Security and Privacy in Social Networks. Springer：2013：197-223.

[13] BAUMANN A, FABIAN B, LISCHKE M. Exploring the Bitcoin network[C]//Proceedings of the 10th International Conference on Web Information Systems and Technologies, 2014：369-374.

[14] PHAM T, LEE S. Anomaly detection in the Bitcoin system-A network perspective[J/OL]. arXiv：1611.03942, 2016.

[15] MAESA D D F, MARINO A, RICCI L. Uncovering the bitcoin blockchain：An analysis of the full users graph[C]// International Conference on Data Science and Advanced Analytics. IEEE, 2016：537-546.

[16] CHEN T, ZHU Y X, LI Z, et al. Understanding Ethereum via graph analysis[C]//Proceedings of the Conference on Computer Communications. Honolulu, HI, USA：IEEE, 2018：1484-1492.

[17] LIN D, WU J J, YUAN Q, et al. Modeling and Understanding Ethereum transaction records via a complex network approach[J]. IEEE Transactions on Circuits and Systems II：Express Briefs. IEEE, 2020, 67(11)：2737-2741.

[18] MAESA D D F, MARINO A, RICCI L. Data-driven analysis of Bitcoin properties：exploiting the users graph

[J]. International Journal of Data Science and Analytics, 2018, 6(1): 63-80.

[19] ALQASSEM I, RAHWAN I, SVETINOVIC D. The anti-social system properties: Bitcoin network data analysis[J]//IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2020, 50(1): 21-31.

[20] KONDOR D, PÓSFAI M, CSABAI I, et al. Do the rich get richer? An empirical analysis of the Bitcoin transaction network [J]. PLoS One, 2014, 9(5): e86197.

[21] MOTAMED A P, BAHRAK B. Quantitative analysis of cryptocurrencies transaction graph [J]. Applied Network Science, 2019, 4: 131.

[22] LISCHKE M, FABIAN B. Analyzing the bitcoin network: The first four years[J]. Future Internet, 2016, 8(1): 7.

[23] GAIHRE A, LUO Y, LIU H. Do Bitcoin users really care about anonymity? An analysis of the Bitcoin transaction graph[C]//Proceedings of the IEEE International Conference on Big Data. Seattle, WA, USA: IEEE, 2018: 1198-1207.

[24] NEWMAN M E J. Networks: An introduction [M]. London: Oxford University Press, 2010.

[25] GUO D C, DONG J Q, WANG K. Graph structure and statistical properties of Ethereum transaction relationships[J]. Information Sciences, 2019, 492: 58-71.

[26] MORENO-SANCHEZ P, MODI N, SONGHELA R, et al. Mind your credit: Assessing the health of the Ripple credit network[C]//Proceedings of the World Wide Web Conference. Lyon, France: ACM, 2018: 329-338.

[27] BAI Q L, ZHANG C, XU Y D, et al. Evolution of Ethereum: A temporal graph perspective [J/OL]. arXiv:2001.05251, 2020.

[28] PARANJAPE A, BENSON A R, LESKOVEC J. Motifs in temporal networks[C]//Proceedings of the International Conference on Web Search and Data Mining. Cambridge, United Kingdom: ACM, 2017: 601-610.

[29] RON D, SHAMIR A. Quantitative analysis of the full Bitcoin transaction graph[C]//Proceedings of the International Conference on Financial Cryptography and Data Security. Okinawa, Japan: Springer, 2013: 6-24.

[30] MAESA D D F, MARINO A, RICCI L. An analysis of the bitcoin users graph: inferring unusual behaviours [C]//Proceedings of the International Workshop on Complex Networks and Their Applications. Springer, 2016: 749-760.

[31] CHEN W L, ZHANG T, CHEN Z G, et al. Traveling the token world: A graph analysis of Ethereum ERC20 token ecosystem[C]// Proceedings of the World Wide Web Conference. Taipei, Taiwan: ACM, 2020: 1411-1421.

[32] LIANG J Q, LI L J, ZENG D. Evolutionary dynamics of cryptocurrency transaction networks: An empirical study[J]. PLoS ONE, 2018, 13(8): 1-18.

[33] HARRIGAN M, FRETTER C. The unreasonable effectiveness of address clustering[C]// Proceedings of the IEEE International Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress. Toulouse, France: IEEE, 2016: 368-373.

[34] REMY C, RYM B, MATTHIEU L. Tracking Bitcoin users activity using community detection on a network of weak signals[C]//Proceedings of the 2017 International Conference on Complex Networks and Their Applications. Lyon, France: Springer, 2017: 166-177.

[35] KLUSMAN R, DIJKHUIZEN T. Deanonymisation in ethereum using existing methods for bitcoin [J/OL]. [2021-05-05]. https://homepages. staff. os3. nl/~delaat/rp/2017-2018/p61/report. pdf.

[36] VICTOR F. Address clustering heuristics for Ethereum [C]//Proceedings of the 2020 International Conference on Financial Cryptography and Data Security. Kota Kinabalu, Sabah, Malaysia: Springer, 2020: 617-633.

[37] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating user privacy in Bitcoin[C]//Proceedings of the International Conference on Financial Cryptography and Data Security. Okinawa, Japan: Springer, 2013, 7859: 34-51.

[38] JOURDAN M A, BLANDIN S, WYNTER L, et al. Characterizing entities in the Bitcoin blockchain[C]// Proceedings of the 2018 IEEE International Conference on Data Mining Workshops. Singapore: IEEE, 2018: 55-62.

[39] HARLEV M A, SUN YIN H H, LANGENHELDT K C, et al. Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning[C]//Proceedings of the 51st Hawaii International Conference on System Sciences. Hawaii, USA: 2018.

[40] SHAO W, LI H, CHEN M, et al. Identifying Bitcoin users using deep neural network[C]//Proceedings of the 18th International Conference on Algorithms and Architectures for Parallel Processing. Guangzhou, China: Springer, 2018: 178-192.

[41] FLEDER M, KESTER M S, PILLAI S. Bitcoin transaction graph analysis [J/OL]. arXiv: 1502.01657, 2015.

[42] MÖSER M, BÖHME R, BREUKER D. An inquiry into money laundering tools in the Bitcoin ecosystem[C]// Proceedings of the APWG eCrime Researchers Summit. San Francisco, CA, USA: IEEE, 2013: 1-14.

[43] McGINN D, BIRCH D, AKROYD D, et al. Visualizing dynamic Bitcoin transaction patterns[J]. Big Data, 2016, 4(2): 109-119.

[44] CHEN W L, WU J J, ZHENG Z B, et al. Market manipulation of Bitcoin: Evidence from mining the Mt. Gox transaction network[C]//Proceedings of the IEEE Conference on Computer Communications. Paris, France: IEEE, 2019: 964-972.

[45] McGINN D, McLLWRAITH D, GUO Y. Towards open data blockchain analytics: A Bitcoin perspective [J]. Royal Society Open Science, 2018, 5(8): 180298.

[46] RANSHOUS S, JOSLYN C A, KREYLING S, et al. Exchange pattern mining in the Bitcoin transaction directed hypergraph[C]//Proceedings of the International Conference on Financial Cryptography and Data Security. Malta: Springer, 2017: 248-263.

[47] WU J J, LIU J, CHEN W L, et al. Detecting mixing services via mining Bitcoin transaction network with hybrid motifs [J/OL]. arXiv:2001.05233, 2020.

[48] ZOLA F, BRUSE J L, EGUIMENDIA M, et al. Bitcoin and cybersecurity: Temporal dissection of blockchain data to unveil changes in entity behavioral patterns[J]. Applied Sciences, 2019, 9(23): 5003.

[49] VASEK M, MOORE T. There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams[C]//Proceedings of the International Conference on Financial Cryptography and Data Security. Puerto Rico: Springer, 2015: 44-61.

[50] BIAN S Q, DENG Z P, LI F, et al. IcoRating: A deep-learning system for scam ICO identification [J/OL]. arXiv:1803.03670, 2018.

[51] TORRES C F, SEICHEN M, STATE R. The art of the scam: Demystifying honeypots in Ethereum smart contracts[C]//Proceedings of the 28th USENIX Security Symposium. Santa Clara, CA, USA: USENIX Association, 2019: 1591-1607.

[52] MONAMO P, MARIVATE V N, TWALA B. Unsupervised learning for robust Bitcoin fraud detection[C]// Proceedings of the Information Security for South Africa. Johannesburg, South Africa: IEEE, 2016: 129-134.

[53] HANDASON T D S, LAU W C, HU B, et al. Identifying illicit accounts in large scale e-payment networks - A graph representation learning approach [J/OL]. arXiv:1906.05546, 2019.

[54] WU J J, YUAN Q, LIN D, et al. Who are the phishers? Phishing scam detection on Ethereum via network embedding [J/OL]. IEEE Transactions on Systems, Man, Cybernetics: System, 2020. https://ieeexplore.ieee.org/abstract/document/9184813.

[55] LIN D, WU J J, YUAN Q, et al. T-EDGE: Temporal weighted multidigraph embedding for Ethereum transaction network analysis[J]. Frontiers of Physics, 2020, 8: 204.

[56] BRYANS D. Bitcoin and money laundering: Mining for an effective solution[J]. Indiana Law Journal, 2014, 89: 441-472.

[57] WEBER M, DOMENICONI G, CHEN J, et al. Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics [J/OL]. arXiv:1908.02591, 2019.

[58] PRADO-ROMERO M A, DOERR C, GAGO-ALONSO A. Discovering Bitcoin mixing using anomaly detection[C]//Proceedings of the Iberoamerican Congress on Pattern Recognition. Valparaiso, Chile: Springer, 2017, 10657: 534-541.

[59] HU Y N, SENEVIRATNE S, THILAKARATHNA K, et al. Characterizing and detecting money laundering activities on the Bitcoin network [J/OL]. arXiv: 1912.12060, 2019.

[60] PEROZZI B, Al-RFOU R, SKIENA S. DeepWalk: Online learning of social representations[C]//Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, USA: Association for Computing Machinery, 2014: 701-710.

[61] GROVER A, LESKOVEC J. Node2vec: Scalable feature learning for networks[C]//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. San Francisco, CA, USA: Association for Computing Machinery, 2016: 855-864.

[62] di BATTISTA G, di DONATO V, PATRIGNANI M, et al. Bitconeview: Visualization of flows in the Bitcoin transaction graph[C]//Proceedings of the IEEE Symposium on Visualization for Cyber Security. Chicago, IL, USA: IEEE Computer Society, 2015: 1-8.

[63] PAREJA A, DOMENICONI G, CHEN J, et al. EvolveGCN: Evolving graph convolutional networks for dynamic graphs[J/OL]. arXiv:1902.10191, 2019.

[64] AKCORA C G, LI Y, GEL Y R, et al. BitcoinHeist: Topological data analysis for ransomware detection on the Bitcoin blockchain [J/OL]. arXiv: 1906.07852, 2019.

[65] CONTI M, GANGWAL A, RUJ S. On the economic significance of ransomware campaigns: A Bitcoin transactions perspective[J]. Computers & Security, 2018, 79: 162-189.

[66] FOLEY S, KARLSEN J R, PUTNIŅŠ T J. Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?[J]. The Review of Financial Studies, 2019, 32(5): 1798-1853.

（责任编辑 张 冰）