



## 浅谈区块链新型犯罪的数据分析

魏智煌<sup>1</sup> 胡少华<sup>2</sup> 姜吉国<sup>3</sup> 潘 鹏<sup>4</sup> 冯 源<sup>1</sup>

1. 广东安证计算机司法鉴定所, 深圳;
2. 深圳市公安局南山分局网络警察大队, 深圳;
3. 山东省公安厅网安总队, 济南;
4. 山东省青岛市公安局经济技术开发区分局网警大队, 青岛

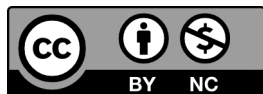
**摘 要** | 本论文旨在探讨区块链技术在新型犯罪领域中的应用, 并重点关注数据分析在司法鉴定中的作用。首先, 介绍了区块链技术的基本原理和特点, 以及新型犯罪在区块链环境下的崛起。然后, 探讨了数据分析在揭示新型犯罪模式、追踪犯罪行为 and 提供证据支持方面的重要性。接着, 介绍了常用的区块链数据分析方法和工具, 并结合实例说明其在新型犯罪领域的应用。最后, 对未来区块链数据分析的发展趋势和挑战进行了展望, 提出了进一步研究的方向。

**关键词** | 区块链; 新型犯罪; 数据分析; 证据支持; 技术应用

Copyright © 2023 by author (s) and SciScan Publishing Limited

This article is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

<https://creativecommons.org/licenses/by-nc/4.0/>



随着区块链技术的快速发展和广泛应用, 我们正处于数字时代的变革之中。区块链作为一种去中心化、不可篡改和透明的分布式账本技术, 引起了各行各业的关注, 并带来了许多新的机遇和挑战。然而, 随着区块链的普及和应用范围的扩大, 也出现了一些新型犯罪行为, 这对司法鉴定工作提出了新的要求和挑战。

### 一、区块链技术概述

#### (一) 区块链基本原理<sup>[1]</sup>

区块链技术是一种分布式账本技术, 其基本原理是将数据按照时间顺序链接形成不可篡改的

数据块, 每个数据块都包含了前一个数据块的哈希值, 从而构成了一个链式结构。以比特币的区块链账本为例, 每个区块基本由上一个区块的散列值、若干条交易、一个调节数等元素构成, 矿工通过工作量证明实现对交易整理为账本区块和区块安全性的维持。一个矿工通过交易广播渠道收集交易项目并打包, 协议约定了区块速度生成速度而产生的难度目标值, 通过不断将调节数和打包的交易数据进行散列运算而算出对应散列值

[1] 维基百科. 区块链 [EB/OL]. [2023-08-30]. <https://zh.wikipedia.org/wiki/%E5%8C%BA%E5%9D%97%E9%93%BE>.

使其满足当时相应的难度目标值，最先计算出调节数的矿工可以将之前获得上一个区块的散列值、交易数据、当前算出对应区块的调节数集成为一个账本区块并广播到账本发布渠道，其他矿工则

可以知道新区块已生成并知道该区块的散列值（作为下一个区块的“上一个区块的散列值”），从而放弃当前待处理的区块数据生成并投入到新一轮的区块生成，如图1所示。

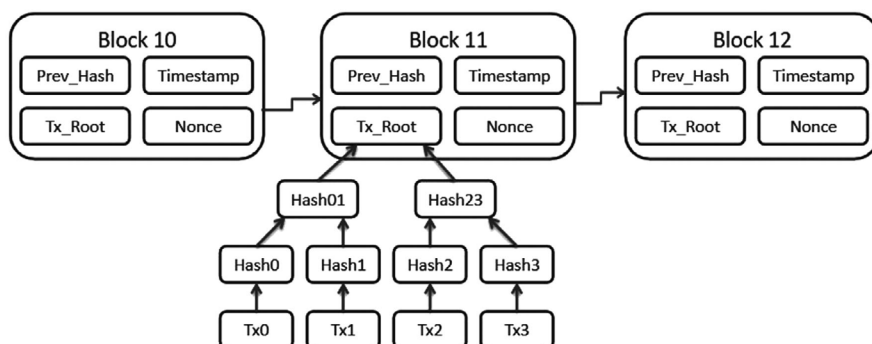


图1 区块链技术图示

区块链的核心是分布式账本，它是由许多节点组成的网络，每个节点都存储了完整的账本副本。这意味着数据不再集中存储在单一的中心化服务器上，而是以分布的方式保存在多个节点上。每个节点都具有相同的账本副本，因此任何数据的更改必须经过网络中的多个节点共识才能被接受和记录。这种分布式账本机制确保了数据的去中心化和冗余性，增强了系统的可靠性和安全性。

为了保证区块链网络中的交易一致性和安全性，节点需要达成共识。共识机制是一种协议或算法，用于决定哪个节点可以添加新的块到区块链中。常见的共识机制包括工作量证明（Proof of Work）、权益证明（Proof of Stake）和股份授权证明（Delegated Proof of Stake）。工作量证明（PoW）是最早应用于区块链的共识机制之一，它基于计算密集型的问题，节点通过解决复杂的数学难题来竞争添加新区块的权利。解决难题需要大量的计算能力，而获得添加新区块的权利的节点被称为矿工。PoW机制的核心思想是通过消耗大量的计算能力来保证网络的安全性，但同时也存在能源消耗高和交易速度慢的问题。权益证明（PoS）是另一种常见的共识机制，它基于节点持有的货币数量或权益来选择出块节点。权益证明机制中，拥有更多货币或权益的节点更有可能被选中来确认交易和添加新区块。PoS机制相对于PoW机制减少了能源消耗，提高了交易速度，但也引入了新的安全性和公平性问题。股份授权证

明（DPoS）是一种改进的共识机制，它通过股东投票系统选择一定数量的节点代表来确认区块和维护区块链的运行。DPoS机制的特点是在区块链中选举出节点代表，由他们来代理全体节点进行验证和记账。股东具有随时罢免和任命代表的权力，实现了实时的民主。DPoS机制通过减少验证节点的数量，实现了快速的共识验证。共识机制的目标是确保网络中的节点就某个事务的状态达成一致，以防止恶意行为和双重支付等问题的发生。它是区块链的关键组成部分，保障了数据的一致性和安全性。

这些共识机制在区块链技术中发挥着重要作用，解决了分布式环境下的数据一致性和安全性问题，并推动了区块链在各个领域的应用和发展。

## （二）区块链特点与优势

区块链作为一种创新性的技术，具备许多独特的特点和优势，使其在各个领域具有广泛的应用前景。

（1）去中心化。区块链的去中心化是其最重要的特点之一。传统的中心化系统依赖于中央机构或第三方中介来验证和管理交易，而区块链通过分布式账本和共识机制实现了去中心化。每个节点都拥有完整的账本副本，并参与到交易验证和共识过程中，消除了单点故障和信任问题。去中心化使得区块链系统具备了更高的可靠性、抗攻击性和防篡改性。

（2）不可篡改性。区块链的数据一旦被写入，

就很难被篡改。每个区块都包含了前一个区块的哈希值,形成了一个链式结构。如果有人试图篡改某个区块中的数据,将会导致其哈希值的变化,从而破坏了区块链的完整性。由于区块链的数据存储在多个节点上,篡改一笔交易或一块数据需要同时控制多个节点,这在实际上是非常困难的。这种不可篡改性确保了数据的可信度和安全性。

(3) 透明性与可验证性。区块链上的交易和操作是公开可查的。区块链的透明性使得任何人都可以查看和审计交易记录,从而增强了信任和可验证性。任何数据的改动都会区块链上留下痕迹,可追溯性强。这对于金融行业、供应链管理、公共部门等领域具有重要意义,可以降低欺诈、不当行为和腐败的风险。

(4) 安全性。区块链采用了密码学和分布式存储等先进技术,保障了数据的安全性。数据在传输和存储过程中使用加密算法进行保护,防止数据泄露和篡改。区块链的去中心化结构使得攻击者难以集中攻击或篡改数据,因为篡改一笔交易或一个区块需要控制网络中的多个节点。区块链的安全性大大增加了数据的保护和信任。

(5) 高效性和成本效益。区块链技术可以简化和加速许多传统的中间商和中介过程,提高交易效率。传统的交易通常需要多个中介和繁琐的步骤,而区块链可以通过智能合约等自动化工具来简化交易流程,减少人为干预。此外,通过去除中间环节和减少人工操作,区块链可以降低交易和管理的成本。这使得区块链在金融、供应链、物联网等领域具有广泛的应用前景。

### (三) 新型犯罪在区块链环境中的崛起<sup>[1]</sup>

随着区块链技术的发展和扩展,新型犯罪也在区块链环境中崭露头角。尽管区块链具有许多优势和安全特性,但其匿名性、不可篡改性和智能合约功能也为犯罪分子提供了新的机会和工具。以下将详细探讨新型犯罪在区块链环境中的崛起。

#### 1. 加密货币相关犯罪

区块链技术的典型应用是加密货币,如比特币和以太坊。加密货币的匿名性和去中心化特点吸引了犯罪分子的目光。他们利用区块链的隐秘性进行洗钱、非法交易、勒索和网络犯罪等活动。由于交易的不可逆性和难以追踪性,加密货币的使用给打

击犯罪带来了巨大的挑战。

#### 2. 智能合约漏洞与欺诈

智能合约是区块链的重要组成部分,它们是以编程方式定义的合约,可以自动执行和实施。然而,智能合约存在漏洞和错误,这为欺诈活动提供了机会。犯罪分子可以利用智能合约中的安全漏洞实施欺诈行为,包括篡改合约规则、窃取资金和操纵交易等。

#### 3. 初始代币发行(ICO)诈骗

初始代币发行(ICO)是一种通过发行代币来融资的方式,而且常常涉及大量的投资者和资金。然而,ICO市场存在许多诈骗行为。犯罪分子可以伪造ICO项目,通过虚假的白皮书、团队成员和承诺吸引投资者,并最终逃离或窃取资金。区块链的去中心化和匿名性增加了追踪和追究犯罪分子责任的困难。

#### 4. 数据泄露和隐私问题<sup>[2]</sup>

尽管区块链技术本身具有较高的安全性,但在区块链应用中,个人和机构的数据仍然可能面临泄露和侵犯隐私的风险。一些新型犯罪分子利用技术漏洞和社交工程手段,窃取用户的私钥和密码,进而获取敏感信息或盗取数字资产。这给个人和组织的安全带来了新的挑战。

#### 5. 虚拟身份和身份盗窃

区块链技术的匿名性使得犯罪分子可以轻松伪造虚拟身份,从而进行欺诈和非法活动。他们可以创建假名或匿名账户,隐藏身份进行交易,从而逃避监管和法律追责。此外,犯罪分子还可能盗取他人的数字身份,冒充其身份进行犯罪活动,给个人和组织造成巨大损失。

## 二、数据分析在司法鉴定中的作用

### (一) 数据分析的重要性和作用

数据分析在司法鉴定中的重要性不可忽视,它

[1] Foroglou G, Tsilidou A L. Further Applications of the Blockchain [C] //Twelveth Student Conference on Managerial Science and Technology. Greece: Athens University of Economics and Business, 2015.

[2] Akins B W, Chapman J L, Gordon J M. A Whole New World: Income Tax Considerations of the Bitcoin Economy [J]. Pittsburgh Tax Review, 2014 (12): 25-33.

不仅可以提供客观的证据支持,还可以揭示隐藏的模式和趋势,帮助鉴定人员更准确地理解案件和犯罪行为。以下是对数据分析重要性和作用的进一步扩充。

#### 1. 证据发现和收集

数据分析在司法鉴定中起着关键的作用,可以帮助鉴定人员发现并收集相关证据。通过对大量数据的筛选、整理和分析,可以确定哪些信息是相关的、可靠的,并从中提取出对案件十分重要的证据。数据分析还可以帮助识别数字证据的真实性和可信度,确保鉴定过程的科学性和可靠性。

#### 2. 识别模式和趋势

数据分析可以揭示案件中的模式和趋势,帮助鉴定人员理解犯罪行为特征和演变。通过对数据的统计分析和模式识别,可以发现犯罪行为中的规律性和重复性,例如特定地区、时间段或特定类型犯罪的集中发生。这些模式和趋势的识别可以为鉴定人员提供重要线索,指导他们进一步的调查和分析。

#### 3. 辅助决策和预测

数据分析可以为司法鉴定人员提供决策的科学依据和预测的支持。通过对数据的深入分析和挖掘,可以发现案件中的关键因素和影响因素,并预测可能的结果和趋势。这些信息可以帮助鉴定人员制定更明智的决策和战略,提高司法鉴定的准确性和效率。

#### 4. 提供专家意见和法庭证词

数据分析的结果和结论可以作为鉴定人员的专家意见和法庭证词的重要依据。通过数据分析得出的结论是基于事实和数据的客观分析,具有较高的可信度和科学性。这些专家意见和证词可以为法庭提供决策的依据,帮助法官和陪审团更好地理解案件并作出公正的判断。

### (二) 数据分析在新型犯罪领域中的应用价值<sup>[1]</sup>

新型犯罪不断涌现,其复杂性和技术性使得传统的司法鉴定方法面临许多挑战。数据分析在新型犯罪领域具有重要的应用价值,主要体现在以下方面。

#### 1. 早期预警与预防

数据分析可以识别新型犯罪的早期迹象和趋

势,提供预警和预防。通过对大量相关数据的分析,可以发现犯罪行为的模式和特征,及时发现犯罪活动的线索,并采取相应的预防措施。数据分析还可以辅助制定预防策略,加强安全措施,防止新型犯罪的发生。

#### 2. 犯罪调查与追踪

数据分析在新型犯罪的调查和追踪中起到关键作用。通过对涉案数据的分析,可以揭示犯罪者之间的关系和网络,帮助鉴定人员构建犯罪链条,确定主要嫌疑人和犯罪组织的身份。数据分析还可以追踪犯罪行为的时间线和地理位置,还原犯罪过程,为司法鉴定提供必要的证据。

#### 3. 情报分析与预测

数据分析可以挖掘犯罪相关数据中的潜在情报和线索,提供更全面和准确的情报支持。通过对大数据的整合和分析,可以发现犯罪行为的模式、趋势和演化规律,为司法鉴定人员提供重要的情报分析和预测能力。这些情报和预测可以帮助鉴定人员更好地了解犯罪背后的动机和目的,并制定相应的对策。

#### 4. 风险评估与安全防范

数据分析可以帮助司法鉴定人员进行风险评估和安全防范措施的制定。通过对相关数据的分析,可以识别和评估潜在的安全风险和漏洞,为安全管理和防范提供科学依据。数据分析还可以帮助制定刑事政策和法律法规,以应对新型犯罪的威胁和挑战。

### (三) 数据分析在揭示犯罪模式、追踪犯罪行为和提供证据支持中的作用<sup>[2]</sup>

数据分析在司法鉴定中的另一个重要作用是揭示犯罪模式、追踪犯罪行为和提供证据支持。

#### 1. 揭示犯罪模式和趋势

通过数据分析,可以识别和分析犯罪行为的模式和趋势。通过对犯罪案件相关数据的整合和分析,

[1] 刘明达,陈左宁,拾以娟,等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1-27.

[2] 刘敖迪,杜学绘,王娜,等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636-2654.



可以发现特定犯罪类型的共同特征和行为模式，例如特定地区、特定时间段、特定受害人或特定手段等。这些模式和趋势的识别可以为鉴定人员提供重要线索，指导他们在调查过程中更有针对性地收集证据，并加深对犯罪行为的理解。

### 2. 追踪犯罪行为和犯罪者

数据分析可以帮助追踪犯罪行为和犯罪者。通过对相关数据的分析，可以还原犯罪行为的时间线、地理位置以及行为轨迹。这些信息可以帮助鉴定人员确定犯罪者的活动范围和行为规律，进而追踪并定位犯罪者的身份和行踪。数据分析还可以通过关联分析和网络分析揭示犯罪者之间的关系和组织结构，为打击犯罪活动提供支持。

### 3. 提供证据支持和分析

数据分析可以提供有力的证据支持和分析。通过对案件相关数据的挖掘和分析，可以发现隐藏在大量数据背后的关联关系和重要信息。这些信息可以用作证据支持，帮助鉴定人员构建案件的逻辑链条和证据链。数据分析还可以进行统计分析、模式识别和行为分析，深入解读犯罪数据中的特征和规律，为鉴定人员提供更深入的案件分析和推理，增强证据的可信度和说服力。

## 三、区块链数据分析方法与工具<sup>[1]</sup>

### （一）区块链数据分析方法概述<sup>[2]</sup>

数据分析在区块链领域扮演着至关重要的角色。通过对区块链数据进行收集、处理和分析，可以揭示其中蕴藏的有价值的信息和模式。本部分提出了一些常用的区块链数据分析方法。

#### 1. 数据收集与清洗

区块链数据分析的首要任务是收集原始的区块链数据，并进行数据清洗和预处理。这涉及从区块链网络中获取区块和交易数据，并对其进行整理和标准化，以便后续的分析应用。

#### 2. 数据挖掘与可视化

区块链数据挖掘是通过应用各种数据挖掘算法和技术，发现区块链数据中隐藏的模式、趋势和关联关系。常用的数据挖掘方法包括聚类分析、关联规则挖掘和时间序列分析等。数据可视化则是将挖掘结果以图表、图形或其他可视化形式呈现，使分析结果更加直观和易于理解。

### 3. 数据分析与建模

区块链数据分析可以应用各种统计分析方法和机器学习算法，对数据进行进一步分析和建模。这包括对交易模式的分析、异常检测、风险评估等。通过构建模型，我们可以预测和识别潜在的新型犯罪行为，并提供有针对性的防范和监控措施。

### （二）常用的区块链数据分析工具介绍

在区块链数据分析领域，有许多工具和平台可供使用，用于收集、处理和分析区块链数据。以下是对一些常用的区块链数据分析工具的介绍。

（1）Blockchain Explorer（区块链浏览器）是一种常见的工具，用于浏览和查询区块链上的交易和区块信息。它提供了实时查看和搜索区块链数据的功能，帮助分析人员获取交易历史、地址余额等基本信息。

（2）CoinMarketCap 是一个广泛使用的加密货币市场数据分析平台，提供各种加密货币的价格、市值、交易量等数据。通过分析加密货币市场数据，我们可以洞察市场趋势、交易模式和投资者行为。

（3）BigQuery 是谷歌云平台提供的一种强大的大数据分析工具，可用于处理和分析大规模的区块链数据集。它提供了高效的查询和分析功能，并支持与其他工具和平台的集成，使得区块链数据分析更加便捷和高效。

### （三）区块链数据分析在新型犯罪领域的实际应用案例

区块链数据分析在新型犯罪领域具有广泛的实际应用价值。以下是一些实际案例的介绍，展示了数据分析在揭示犯罪模式、追踪犯罪行为和提供证据支持方面的作用。

#### 1. 虚拟货币洗钱追踪

通过对区块链数据进行深入分析，可以追踪和识别虚拟货币洗钱行为。通过分析虚拟货币交易的模式、特征和关联关系，可以发现洗钱活动中的关联地址、交易链和转账模式，为执法机构提供重要的线索和证据。

[1] 邵奇峰，金澈清，张召，等. 区块链技术：架构及进展[J]. 计算机学报，2018，41（5）：969-988.

[2] 闫树，卿苏德，魏凯. 区块链在数据流通中的应用[J]. 大数据，2018，4（1）：3-12.

## 2. 众筹欺诈检测

区块链众筹平台的数据分析可以帮助检测欺诈行为。通过分析众筹项目的资金流动、参与者的交易行为和背景信息,可以发现潜在的欺诈行为和非法募资活动。这为保护投资者权益和预防新型犯罪行为提供了有力的支持。

## 3. 数字身份验证

区块链数据分析可以用于数字身份验证,防止身份盗窃和欺诈行为。通过分析个人的区块链交易和历史记录,可以验证其身份的真实性和可信度,提高身份验证的准确性和安全性。这在打击身份欺诈和保护个人隐私方面具有重要意义。

## 4. 知识产权保护

区块链数据分析可以用于保护知识产权。通过分析区块链上的版权、专利和商标信息,可以识别侵权行为和盗版活动,为知识产权保护提供有力的支持和证据。

# 四、未来发展和挑战<sup>[1]</sup>

## (一) 区块链数据分析的未来发展趋势

区块链数据分析领域具有广阔的未来发展前景,以下是一些可能的趋势和发展方向。

### 1. 增强数据分析技术

随着技术的不断进步,数据分析方法和工具将变得更加先进和复杂。机器学习、人工智能和深度学习等技术将被广泛应用于区块链数据分析,以提供更准确、快速和自动化的犯罪模式识别和预测能力。

### 2. 跨链数据分析的需求

随着不同区块链网络的出现和互联互通,跨链数据分析将成为一个重要的研究领域。跨链数据分析涉及收集、整合和分析多个区块链网络的数据,以全面了解犯罪行为和模式的演变。

### 3. 隐私保护与数据安全

随着隐私和数据安全的重要性日益凸显,未来的区块链数据分析将注重保护用户隐私和数据安全。开发更强大的加密和隐私保护技术、设计安全的数据共享和分析机制,将成为研究的重点。

## (二) 面临的挑战和难题

在区块链数据分析领域,仍存在一些挑战和难题。

### 1. 数据质量和可靠性

区块链上的数据由多个参与方共同维护,数据的准确性和一致性可能受到影响。因此,数据分析人员需要解决数据质量和可靠性的问题,采用有效的方法来验证、清洗和纠正数据。

### 2. 法律和伦理问题

区块链数据分析涉及个人隐私和数据保护等法律和伦理问题。数据分析人员需要遵守相关法律法规,确保数据分析过程的合法性和道德性,并采取适当的措施保护个人隐私。

### 3. 技术和人才需求

区块链数据分析需要专业的技术知识和技能。研究人员需要熟悉区块链技术和数据分析方法,以及掌握各种数据分析工具和编程语言。因此,培养和吸引高水平的数据分析人才是一个关键挑战。

## (三) 进一步研究方向和建议

为推动区块链数据分析的发展和应用,本文提出了以下建议。

(1) 强化数据分析方法和模型。进一步研究和开发更高效、准确的数据分析方法和模型,以应对复杂和多变的新型犯罪行为。结合机器学习、人工智能和统计分析等技术,提高犯罪模式识别和预测的能力。

(2) 探索跨链数据分析方法。研究跨链数据分析的方法和工具,以整合不同区块链网络中的数据,实现对全局犯罪行为的全面分析和理解。此外,跨链数据分析也需要解决数据共享和隐私保护的问题。

(3) 强化数据隐私保护和安全性。加强数据隐私保护和安全性研究,开发更强大的加密算法、隐私保护技术和安全机制,确保在数据分析过程中,隐私和安全不受侵犯。

(4) 加强法律法规和伦理准则的制定。制定与区块链数据分析相关的法律法规和伦理准则,明确数据分析的合法性和道德性要求,为数据分析人员提供明确的指导和规范。

(5) 加强合作与交流。促进学术界、产业界、执法机构和司法鉴定机构之间的合作与交流,共同

[1] 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.

推动区块链数据分析在犯罪调查和司法鉴定中的应用。通过合作，共享经验和资源，提升数据分析能力和解决实际问题的能力。

## 五、结语

区块链数据分析在未来将继续发展并发挥重要作用。为了实现这一目标，需要进一步研究和创新，

解决面临的挑战和难题。通过强化数据分析方法、加强跨链数据分析、保护数据隐私和加强合作与交流等措施，我们能够更好地应对新型犯罪挑战，司法鉴定人员也能在取证过程中获得更有效的数据支持和证据分析。

（责任编辑：李 琼）

# Data Analysis of New Types of Blockchain Crimes

Wei Zhihuang<sup>1</sup> Hu Shaohua<sup>2</sup> Jiang Jiguo<sup>3</sup> Pan Peng<sup>4</sup> Feng Yuan<sup>1</sup>

1. Guandong An Zheng Computer Forensics Institute, Shenzhen;

2. Network Police Brigade of Nanshan Branch of Shenzhen Public Security Bureau, Shenzhen;

3. Shandong Provincial Public Security Department Network Security Corps, Jinan;

4. Online Police Brigade of Economic and Technological Development Zone Branch of Qingdao Public Security Bureau, Shandong Province, Qingdao

**Abstract:** This paper aims to explore the application of blockchain technology in the field of novel crimes, and focuses on the role of data analysis in forensic expertise. First, it introduces the basic principles and characteristics of blockchain technology, as well as the rise of new crimes in the blockchain environment. Then, the importance of data analysis in revealing new crime patterns, tracking criminal behavior and providing evidence support is discussed. Then, it introduces the commonly used blockchain data analysis methods and tools, and illustrates its application in the new crime field with examples. Finally, the development trend and challenges of blockchain data analysis in the future are prospected, and the direction of further research is proposed.

**Key words:** Blockchain; New type of crime; Data analysis; Evidence support; Technology application