



中国科学院大学  
University of Chinese Academy of Sciences

# 博士学位论文

## 区块链数字资产治理

作者姓名: 谢雨昊

指导教师: 田英杰 研究员 中国科学院大学

学位类别: 经济学博士

学科专业: 统计学

培养单位: 中国科学院大学经济与管理学院

2023 年 6 月



# **Blockchain Digital Asset Governance**

---

**A dissertation submitted to  
University of Chinese Academy of Sciences  
in partial fulfillment of the requirement  
for the degree of  
Doctor of Economics  
in Statistics  
By  
XIE Yuhao  
Supervisor: Professor TIAN Yingjie**

**School of Economics and Management, University of Chinese  
Academy of Sciences**

**June, 2023**



## **中国科学院大学**

### **学位论文原创性声明**

本人郑重声明：所呈交的学位论文是本人在导师的指导下独立进行研究工作所取得的成果。承诺除文中已经注明引用的内容外，本论文不包含任何其他个人或集体享有著作权的研究成果，未在以往任何学位申请中全部或部分提交。对本论文所涉及的研究工作做出贡献的其他个人或集体，均已在文中以明确方式标明或致谢。本人完全意识到本声明的法律结果由本人承担。

作者签名：

日 期：

## **中国科学院大学**

### **学位论文授权使用声明**

本人完全了解并同意遵守中国科学院大学有关收集、保存和使用学位论文的规定，即中国科学院大学有权按照学术研究公开原则和保护知识产权的原则，保留并向国家指定或中国科学院指定机构送交学位论文的电子版和印刷版文件，且电子版与印刷版内容应完全相同，允许该论文被检索、查阅和借阅，公布本学位论文的全部或部分内容，可以采用扫描、影印、缩印等复制手段以及其他法律许可的方式保存、汇编本学位论文。

涉密及延迟公开的学位论文在解密或延迟期后适用本声明。

作者签名：

导师签名：

日 期：

日 期：



## 摘要

在数字经济时代，区块链技术及其衍生的数字货币正在重塑全球金融格局，带来了前所未有的创新和变革。作为金融科技领域的一个标志性事件，区块链数字货币的发展不仅揭示了巨大的潜在价值，也暴露出一系列的挑战与风险，尤其是在资产安全性、监管遵从性和市场稳定性等方面。随着这一新兴领域的不断演化，对其进行深入的分析和有效的治理显得尤为重要。为此，本文基于机器学习，深度学习和社交媒体传播理论，从多维度对区块链数字货币进行了深刻属性分析、价值确认和风险预警，旨在为数字货币的健康发展和风险控制提供理论依据和实践指南。本文的主要研究内容和贡献包括以下四个方面：

### (1) 金融诈骗检测方法综述

本文首先对传统金融诈骗的类型和特点进行了全面分析，并综述了用于检测这些诈骗的主流学习算法。特别地，文章深入探讨了加密货币诈骗的特点，并将其归类为一种新型的投资诈骗。通过综述 111 篇具有代表性的文献，本文详细分析了生成对抗网络 (GAN)、强化学习、自编码器和图神经网络在加密货币诈骗检测中的应用和效果，为加密货币市场的风险控制提供了重要的技术支持。

### (2) 在大语言模型框架下的加密货币属性判断及投资决策

本文通过对以太坊等主要加密货币与传统商品和科技股票的比较分析，深入探讨了其作为证券或商品的属性。特别地，本研究采用霍威测试发现以太坊具有科技股票的话题属性。使用普通最小二乘法 (OLS) 回归模型分析了 GPT-3.5 对情绪解读与金融资产价值之间的相关性，并通过稳健性检验确认了模型的预测准确性。这一研究不仅揭示了大型语言模型在金融市场分析中的潜在应用，也为加密货币的投资决策提供了新的视角和数据支持。

### (3) 深度学习视角下的 NFT 价值研究

针对当前 NFT 市场的热点——个人社交媒体头像 (Picture for Proof)，本文采用 BSADF 测试、T-SNE 可视化和 VGG-19 特征提取技术，对其市值泡沫、风格相似性和图像相似性进行了细致的分析。研究发现，具有独特知识产权和低图像相似性的 PFP 收藏品在长期内能够带来显著的财务收益，为投资者提供了宝贵的投资决策信息。

### (4) 社交媒体舆情对 IEO 的影响：市场营销与操纵策略的分析

本文通过对首次交易所发行 (Initial Exchange Offering) 项目的社交媒体活动进行深入分析，揭示了市场营销和操纵策略对 IEOs 表现的影响。通过对 54 个 IEO 项目的超过 11,000 条推文的分析，研究发现机器人评分与 IEO 的表现存在显著的相关性，暴露了 IEOs 中存在的市场操纵现象。研究结果为投资者、交易所和监管机构在评估 IEOs 相关风险和设计防范市场操纵措施方面提供了重要的参考。

总体而言，本文为理解和治理区块链数字货币提供了全面的理论分析和实证研究，对推动该领域的健康发展和风险控制具有重要的理论和实践意义。

**关键词：**深度学习，数字货币，非同质化代币，大语言模型，社交媒体分析

## Abstract

In the era of the digital economy, blockchain technology and its derivative digital currencies are reshaping the global financial landscape, bringing about unprecedented innovation and transformation. As a landmark event in financial technology, the development of blockchain digital currencies not only reveals their immense potential value but also exposes a series of challenges and risks, particularly in terms of asset security, regulatory compliance, and market stability. As this emerging field evolves, conducting thorough analyses and implementing effective governance become increasingly crucial. Therefore, this paper, grounded in the theories of machine learning, deep learning, and social media dissemination, offers a profound attribute analysis, value validation, and risk warning of blockchain digital currencies from multiple dimensions, aiming to provide a theoretical basis and practical guidance for the healthy development and risk control of digital currencies. The primary research contents and contributions of this paper include the following four aspects:

### **(1) Overview of Financial Fraud Detection Methods**

This paper initially conducts a comprehensive analysis of the types and characteristics of traditional financial fraud and reviews the mainstream learning algorithms used for their detection. Specifically, this paper delves into the characteristics of cryptocurrency fraud, categorizing it as a novel type of investment scam. By reviewing 111 representative documents, this paper thoroughly analyzes the application and effectiveness of Generative Adversarial Networks (GANs), Reinforcement Learning, Autoencoders, and Graph Neural Networks in the detection of cryptocurrency fraud, providing significant technical support for the risk control of the cryptocurrency market.

### **(2) Assessment of Cryptocurrency Attributes and Investment Decisions under the Framework of Large Language Models**

By comparing major cryptocurrencies such as Ethereum with traditional commodities and technology stocks, this paper deeply explores their attributes as securities or commodities. Notably, this study employs the Howey Test and discovers that Ethereum possesses thematic attributes akin to technology stocks. Using the Ordinary Least Squares (OLS) regression model, the study analyzes the correlation between GPT-3.5's sentiment interpretation and the value of financial assets and confirms the predictive accuracy of the model through robustness testing. This research not only reveals the potential applications of large language models in financial market analysis but also provides new perspectives and data support for investment decisions in cryptocurrencies.

### **(3) Study on the Value of NFTs from a Deep Learning Perspective**

Focusing on the current hot spot of the NFT market—Picture for Proof (PFP), this

paper utilizes the BSADF test, T-SNE visualization, and VGG-19 feature extraction technology to conduct a meticulous analysis of its market value bubbles, stylistic similarities, and image similarities. The research finds that PFP collectibles with unique intellectual property rights and low image similarity can bring significant financial gains in the long term, providing valuable decision-making information for investors.

#### **(4) The Impact of Social Media Sentiment on Initial Exchange Offerings (IEOs): Analysis of Marketing and Manipulation Strategies**

This paper conducts an in-depth analysis of the social media activities of Initial Exchange Offering (IEO) projects, revealing the impact of marketing and manipulation strategies on the performance of IEOs. By analyzing over 11,000 tweets from 54 IEO projects, the research discovers a significant correlation between bot scores and the performance of IEOs, exposing the presence of market manipulation in IEOs. The research results provide important references for investors, exchanges, and regulatory authorities in assessing the risks related to IEOs and designing measures to prevent market manipulation.

Overall, this paper provides a comprehensive theoretical analysis and empirical study for understanding and governing blockchain digital currencies, holding significant theoretical and practical significance for promoting the healthy development and risk control of this field.

**Key Words:** Deep Learning, Cryptocurrency, Non-Fungible Token (NFT), Large Language Model, Social Media Analysis.

## 目 录

<b>第1章 绪论</b>	1
1.1 研究背景与意义	1
1.2 研究内容与技术路线	6
<b>第2章 区块链数字资产治理现状分析</b>	9
2.1 数字货币的共识机制	9
2.2 数字货币的货币属性	11
2.2.1 比特币	11
2.2.2 以太坊	12
2.3 同质化代币发行和平台经济	13
2.4 非同质化代币	16
2.5 社交媒体舆情对资产价格的影响	17
2.6 本章小结	20
<b>第3章 金融诈骗检测方法综述</b>	21
3.1 引言	21
3.2 金融欺诈分类	22
3.2.1 欺诈种类	22
3.2.2 财务报表欺诈	22
3.2.3 信用卡欺诈	23
3.2.4 房贷欺诈	23
3.2.5 电子商务欺诈/评论欺诈	23
3.2.6 保险欺诈	23
3.3 应用算法	24
3.3.1 支持向量机 (Support Vector Machine (SVM))	24
3.3.2 自编码器 (Autoencoder)	25
3.3.3 图神经网络 (Graph Neural Network)	27
3.3.4 生成对抗网络 (Generative Adversarial Network)	28
3.3.5 强化学习 (Reinforcement Learning)	30
3.3.6 决策树/随机森林 (Decision Tree/Random Forest)	31
3.3.7 K 最近邻 (K Nearest Neighbor)	33
3.3.8 隐马尔可夫模型 (Hidden Markov Model)	34
3.3.9 其他检测算法 (Other Fraud Detection Methods)	35

3.4 金融欺诈检测中的挑战与未来发展展望 .....	37
3.4.1 加密货币欺诈 .....	37
3.4.2 加密货币欺诈类别 .....	37
3.5 本章小结：从传统金融欺诈检测（FFD）到加密货币欺诈检测的知识转移 .....	38
<b>第 4 章 在大语言模型框架下的加密货币属性判断以及投资决策 .....</b>	<b>39</b>
4.1 引言 .....	39
4.2 主题建模和预测框架 .....	41
4.2.1 具有普适性的大语言模型（4 比特量化技术） .....	42
4.2.2 Sentence BERT .....	43
4.2.3 Uniform Manifold Approximation and Projection (UMAP) .....	44
4.2.4 HDBSCAN: Hierarchical Density-Based Spatial Clustering of Applications with Noise .....	44
4.2.5 C-TF-IDF: class-based Term Frequency-Inverse Document Frequency	45
4.3 实验数据 .....	46
4.3.1 科技股对比-微软和 Meta .....	46
4.3.2 大宗商品对-黄金和原油 .....	47
4.3.3 加密货币对 - 比特币和以太坊 .....	48
4.3.4 以太坊的属性 .....	49
4.4 模型与结果 .....	51
4.4.1 知识截止日期的稳健性检验 .....	52
4.5 结论 .....	53
4.6 本章小结 .....	54
<b>第 5 章 深度学习视角下的 NFT 价值研究 .....</b>	<b>55</b>
5.1 引言 .....	55
5.1.1 相关研究 .....	55
5.2 NFT 的买卖机制 .....	56
5.2.1 NFT 交易所 .....	57
5.3 研究数据与方法 .....	57
5.4 实证研究 .....	60
5.4.1 PFP 项目的选择 .....	60
5.4.2 风格相似性、知识产权和发布后市场表现 .....	60
5.4.3 图像相似性（独特性）、知识产权和发布后表现 .....	63
5.5 结论 .....	67
5.6 本章小结 .....	67

<b>第 6 章 社交媒体舆情对首次交易所发行 (IEO) 的影响: 市场营销与操纵策略的分析 ······</b>	<b>69</b>
6.1 引言 ······	69
6.2 相关文献 ······	70
6.2.1 初始代币发行 ······	71
6.2.2 哄抬抛售操纵系统 ······	72
6.2.3 社交机器人 ······	73
6.3 研究方法 ······	74
6.3.1 IEO 前期社媒舆情和 IEO 后期表现的时间线 ······	74
6.3.2 数据收集 ······	74
6.3.3 探索性分析-主题建模 ······	75
6.3.4 探索性分析-社交机器人（水军）得分分布 ······	80
6.3.5 探索性分析-卡方检验 ······	80
6.4 研究框架 ······	85
6.4.1 情绪测量 ······	86
6.4.2 测量水军的活跃度 ······	86
6.4.3 IEO 发售后的哄抬抛售 ······	88
6.5 研究结果 ······	89
6.5.1 机器人水军, 情绪以及 IEO 售后市场表现 ······	89
6.5.2 实验结果 ······	92
6.6 结论 ······	93
6.7 本章小结 ······	93
<b>第 7 章 总结与展望 ······</b>	<b>95</b>
7.1 本文总结 ······	95
7.2 研究展望 ······	96
<b>参考文献 ······</b>	<b>99</b>
<b>致谢 ······</b>	<b>111</b>
<b>作者简历及攻读学位期间发表的学术论文与其他相关学术成果 ·</b>	<b>113</b>



## 图目录

图 1-1	比特币交易原理	2
图 1-2	比特币价格走势	2
图 1-3	非同质化代币工作流程	4
图 2-1	工作证明	9
图 2-2	权益证明	10
图 2-3	加密朋克（最早的一批 NFT）	16
图 3-1	金融欺诈分类	22
图 3-2	算法与加密货币欺诈之间的联系	38
图 4-1	主题建模和预测框架	42
图 4-2	左侧：带有思维链和指导性示例的主题建模提示。右侧：带有思维链的预测提示。	42
图 4-3	左侧：与微软相关的话题。右侧：与 Meta 相关的话题。	47
图 4-4	左侧：与黄金相关的话题。右侧：与石油相关的话题。	48
图 4-5	左侧：与比特币相关的话题。右侧：与以太坊相关的话题。	49
图 4-6	以太坊属性分析。	50
图 5-1	NFT 市场中的泡沫期（实线是 1 年 NFT 市场总值的扩散，阴影区域是潜在泡沫，阴影区域是 PSY 统计量超过其 95% 自举临界值的时期）	60
图 5-2	PFP 风格聚类	61
图 5-3	具有相似风格的 PFP 系列间的发布后表现。浅蓝色 = 无知识产权。深蓝色 = 有知识产权。)	62
图 5-4	发布后表现与首日回报之间的关系。具有更高曼哈顿距离的 PFP 系列更为独特。蓝色 = 无知识产权的 PFP 项目。橙色 = 拥有知识产权的 PFP 项目。蓝色线条 = $0.85 \times \exp(0.0016687 \times \text{曼哈顿距离})$ , R 平方 = 0.3704, P 值 = 0.3913 橙色线条 = $4.82 \times \exp(-0.00256 \times \text{曼哈顿距离})$ , R 平方 = 0.2479, P 值 = 0.1726)	64
图 5-5	发布后表现与 30 天回报之间的关系。具有更高曼哈顿距离的 PFP 系列更为独特。蓝色 = 无知识产权的 PFP 项目。橙色 = 拥有知识产权的 PFP 项目。蓝色线条 = $-9.04e-6 \times \text{曼哈顿距离}^2 + 0.01 \times \text{曼哈顿距离}$ , R 平方 = 0.9961, P 值 = 0.0039 橙色线条 = $-6.04e-6 \times \text{曼哈顿距离}^2 + 0.008 \times \text{曼哈顿距离}$ , R 平方 = 0.9056, P 值 = 0.0002 ·	65

图 5-6 发布后表现与一年回报之间的关系。具有更高曼哈顿距离的 PFP 系列更为独特。蓝色 = 无知识产权的 PFP 项目。橙色 = 拥有知识产权的 PFP 项目。蓝色线条 = $0.80 \times \ln(\text{曼哈顿距离}) - 4.68$ , R 平方 = 0.1323, P 值 = 0.6363 橙色线条 = $1.08 \times \ln(\text{曼哈顿距离}) - 3.21$ , R 平方 = 0.0214, P 值 = 0.7070) .....	66
图 6-1 IEO 前期社媒舆情和 IEO 后期表现的时间线) .....	74
图 6-2 每个 IEO 项目下推文集合的前 4 个最常见主题 (AXS 的前 2 个最常见主题) .....	80
图 6-3 每个 IEO 项目的推文的水军得分分布。 .....	84
图 6-4 IEO 前期社媒舆情和 IEO 后期表现的研究框架。最顶端的随机森林, 标记为 $\text{RandomForest}_0 (RF_0)$ , 代表人类检测子系统的基线分类器。每个专门分类器 $\text{RandomForest}_i (RF_i)$ 都是在一个均衡的数据集上训练的。该数据集包括来自机器人类别 ( $BC_i$ ) 和从所有数据集中相同数量的人类账户采样实例。 .....	86

## 目录

表 3-1 金融欺诈与支持向量机 (SVM) 之间的联系 .....	26
表 3-2 金融欺诈与自编码器之间的联系 .....	28
表 3-3 金融欺诈与图神经网络之间的联系 .....	29
表 3-4 金融欺诈与生成对抗网络之间的联系 .....	30
表 3-5 金融欺诈与强化学习之间的联系 .....	31
表 3-6 金融欺诈与决策树/随机森林之间的联系 .....	33
表 3-7 金融欺诈与 K 最近邻的联系 .....	34
表 3-8 金融欺诈与隐马尔可夫模型的联系 .....	36
表 3-9 金融欺诈与其他检测算法的联系 .....	36
表 4-1 实证结果 .....	51
表 4-2 金融资产的稳定性检验 .....	52
表 4-3 金融资产的统计显著性 .....	53
表 6-1 代币分类 .....	76
表 6-2 IEO 项目的卡方检验 .....	85
表 6-3 模型 1 使用常规情绪得分 (E)。模型 2 使用惩罚情绪得分 (S)。模型 3 使用交互项 (R)。括号中为标准误差。N=22 * 在 90% 的水平上显著。** 在 95% 的水平上显著。 .....	89
表 6-4 模型 1 使用常规情绪得分 (E)。模型 2 使用惩罚情绪得分 (S)。模型 3 使用交互项 (R)。括号中为标准误差。N=22 * 在 90% 的水平上显著。** 在 95% 的水平上显著。 .....	90

表 6-5 模型 1 使用常规情绪得分 (E)。模型 2 使用惩罚情绪得分 (S)。模型 3 使用交互项 (R)。括号中为标准误差。N=22 * 在 90% 的水平上显著。** 在 95% 的水平上显著。.....	91
表 6-6 模型 1 使用常规情绪得分 (E)。模型 2 使用惩罚情绪得分 (S)。模型 3 使用交互项 (R)。括号中为标准误差。N=20 * 在 90% 的水平上显著。** 在 95% 的水平上显著。.....	92



## 符号列表

### 字符

Symbol	Description
$s_a$	锚点 (anchor), 参考数据点
$s_p$	代表正例 (positive), 与锚点相似或相关的数据点
$s_n$	代表负例 (negative), 与锚点不相似或不相关的数据点
$u_{x,y}$	模型在图像的像素点处的预测概率
$w_{x,y}$	图像中每个像素点处的权重因子
$E$	普通情感分数
$S$	被感知到的情感分数

### 缩写

PFP	Picture For Proof
NFT	Non-Fungible Token
IEO	Initial Exchange Offering
ICO	Initial Coin Offering



## 第1章 绪论

本文专注于区块链数字资产（加密货币）治理，探讨了区块链技术的应用，分析了加密货币的工作原理。研究的目标是为监管机构、投资者和市场参与者提供有关加密货币市场的深入了解，以帮助促进其健康发展。本章阐述本文的研究背景与意义，并给出论文的组织结构。

### 1.1 研究背景与意义

区块链数字货币，通常被称为加密货币，是一种基于区块链技术的数字或虚拟货币。区块链是一种分布式账本技术，它通过网络上的一系列独立节点来记录和验证所有交易。这种技术的特点包括去中心化、透明性、安全性和不可篡改性。这种全新的货币重塑了我们对货币和交易的理解，因为这是第一种基于信任的货币。区块链网络不依赖于单一的中央权威机构来管理和验证交易，它是由网络上众多计算机（节点）来共同维护的。这种去中心化的特性意味着没有单一实体可以控制整个网络，从而增加用户对系统的信任。如图 1-1 所示，一旦交易记录被添加到区块链上，就不可被更改或者删除，每个区块包含前一个区块的加密哈希值，形成了一个循环的链。这种环环相扣的特性保证了数据的完整性和不可篡改性。虽然区块链上的交易都是匿名的，每笔交易记录都是可以通过公开的网络地址查询。加密货币的工作量证明机制使得网络的参与者（矿工）通过解决复杂的数学难题来证明他们投入了一定的计算工作。每解决一个难题，矿工将有资格将一组待处理的交易打包成一个新的区块，并将其添加到区块链上，并获得一定的区块链奖励。

自 2009 年比特币诞生以来，没有一个加密货币的崩溃是因为区块链内生的技术导致的。作为一个信息系统，区块链毫无疑问是稳健的，但作为一个货币系统来说，区块链货币市场是一片“蛮荒之地”。比特币和区块链的概念由中本聪<sup>[1]</sup>在 2008 年金融危机期间提出，其本意是为了减少人们对中央机构的依赖。但因为缺乏监管，别有用心者会在社交媒体上传播言论使得投资者对某加密货币有过度的自信。第三方服务比如加密货币钱包，加密货币交易所时不时也会因为平台的技术问题和安全漏洞导致资金损失。从本质上来说，只有比特币才是真正的加密货币，这主要是因为比特币运作完全去中心化，没有核心管理团队。与此相反，其他许多加密货币背后都有一个中心化的团队负责管理和发展，这在一定程度上违背了加密货币最初解决信任问题的宗旨。比特币通常被视为加密货币市场的领头羊，其价格的上涨部分反映了其被主流市场接受的程度，如图 1-2 所示。

数字货币的独特性质使得其金融属性难以界定，学术界通常将数字货币与贵金属或股票进行比较，是因为这些资产类别在投资特性和市场行为方面具有

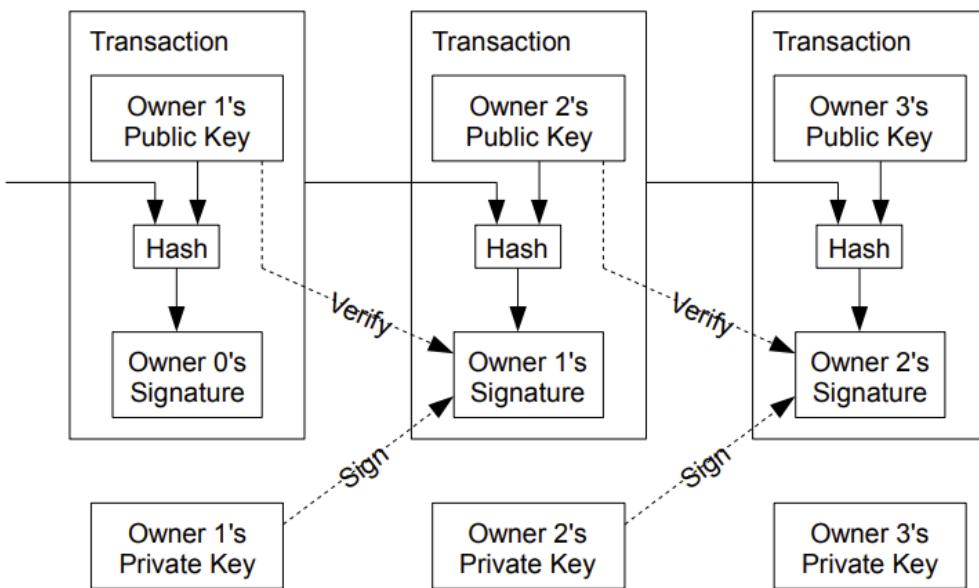


图 1-1 比特币交易原理

Figure 1-1 Bitcoin Transaction Mechanism

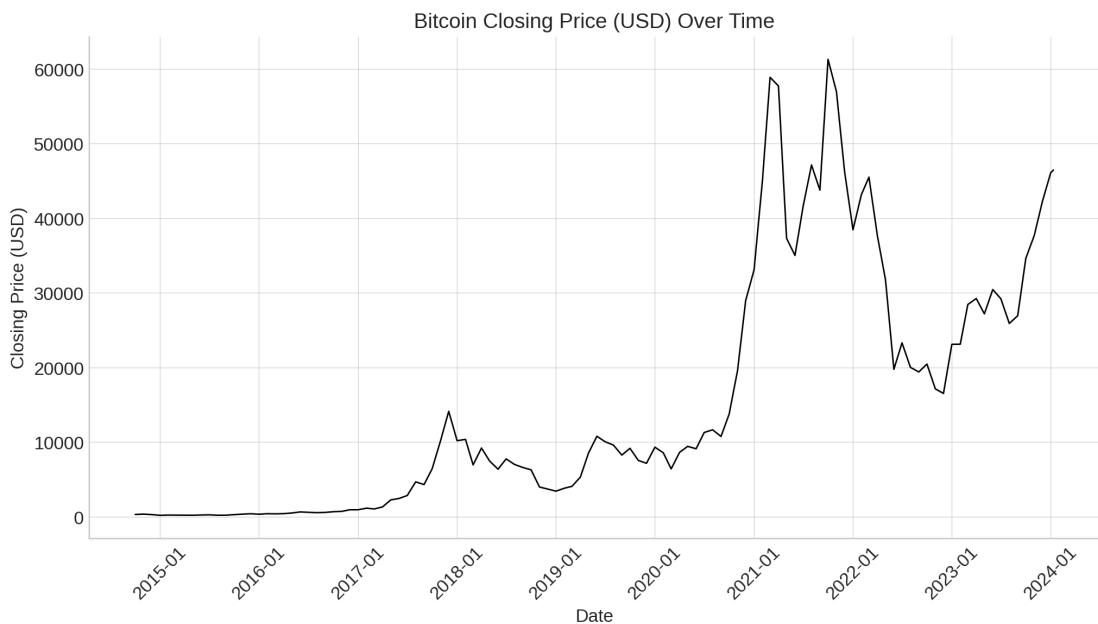


图 1-2 比特币价格走势

Figure 1-2 Bitcoin Price Movement

可比性。贵金属，尤其是黄金，长期以来被视为避险资产和通胀对冲工具，而数字货币，尽管具有一定的避险特性，却更受市场情绪和技术因素的影响。与此同时，股票作为代表公司所有权的资产，通常与企业绩效相关，而数字货币的价值则更多地受到其技术创新和市场接受度的驱动。Liu 和 Tsyvinski<sup>[2]</sup> 的研究中发现，加密货币（如比特币、瑞波币和以太坊）的风险-回报权衡与股票、货币和贵金属有显著不同。Rehman 和 Vo<sup>[3]</sup> 发现在短期内铜为投资者提供了与所有加密货币的最大多样性投资机会，而在中长期投资期间，贵金属在极端正回报分布下与极端负回报的加密货币回报并不相关，这表明贵金属可能为投资者提供一定的多样化投资机会。Kabir 等人<sup>[4]</sup> 通过分析贵金属与加密货币不确定性指数 (UCRY 政策和价格) 之间的时变相关性，发现了一个新的维度。利用动态条件相关性广义自回归条件异方差模型，研究发现，在贵金属中，黄金与 UCRY 政策和价格呈现出一致的正相关性，表明黄金对抗加密货币不确定性具有稳定和可靠的避险属性。一些文献用溢出效应来解释数字货币与其他金融资产的关联。溢出效应是指某一经济变量的变化对其他相关经济变量产生的影响。研究加密货币与其他资产的溢出效应至关重要，因为这有助于了解加密货币市场对其他金融市场的影响。Liu 等人<sup>[5]</sup> 分析了加密货币与其他市场之间的溢出效应，与以往使用 VAR 模型的研究相比，提供了更全面的分析。研究突显了不同资产之间的溢出效应差异，BTC、SP500、WTI 和 COMEX 表现出更强的同期依赖性，而联邦储备资产表则表现出更强的滞后依赖性。Bhanja 等人<sup>[6]</sup> 通过总体、非对称和基于频率的溢出传输框架，评估了不同资产类别（股票、加密货币和贵金属）在 2011 年 4 月至 2021 年 1 月期间的投资组合多元化潜力。结果表明，比特币在与其他资产类别隔离方面具有潜在的分散投资价值。Mensi 等人<sup>[7]</sup> 探讨了五大主要加密货币与黄金、石油、股市不确定性之间的尾部依赖关系。结果显示，加密货币与传统市场波动性指数之间的相互影响在不同市场条件下差异显著，暗示多样化投资策略在正常与极端市场环境下效果不同。此外，发现加密货币在各种市场条件下对波动性指数具有显著影响，这为金融稳定性政策制定和波动性金融工具的运用提供了重要见解。

以上文献探讨的是比特币以及其他同质化代币，NFT（非同质化代币）的概念起源于区块链技术的发展，特别是随着以太坊平台的推出。以太坊作为第一个支持智能合约的区块链平台，为 NFT 的创建提供了基础。最初的 NFT 项目可以追溯到 2014 年，当时被称为“彩色硬币”（Colored Coins）的概念在比特币区块链上被提出。然而，NFT 作为一个独立且广泛认可的概念，真正开始流行是在 2017 年，随着加密猫（CryptoKitties）的推出。加密猫是在以太坊区块链上运行的一个游戏，它允许玩家购买、收集、繁殖和交易虚拟猫，每一只猫都是一个独特的 NFT，这标志着 NFT 作为一种独特的数字资产开始进入主流视野。NFT 代表了对独特、不可替代的项目的拥有权。与传统的、可互换的加密货币（如比特币或以太坊）不同，每个 NFT 都是独一无二的，不能与其他代币等价交换，这正是其名称“非同质化”（non-fungible）的由来。NFT 的创建旨在使数字艺术品和其他独特资产能够在数字空间中被验证其真实性和拥有权，进而实现收藏、买

卖或交易。NFT 的工作流程如图 1-3<sup>[8]</sup>。

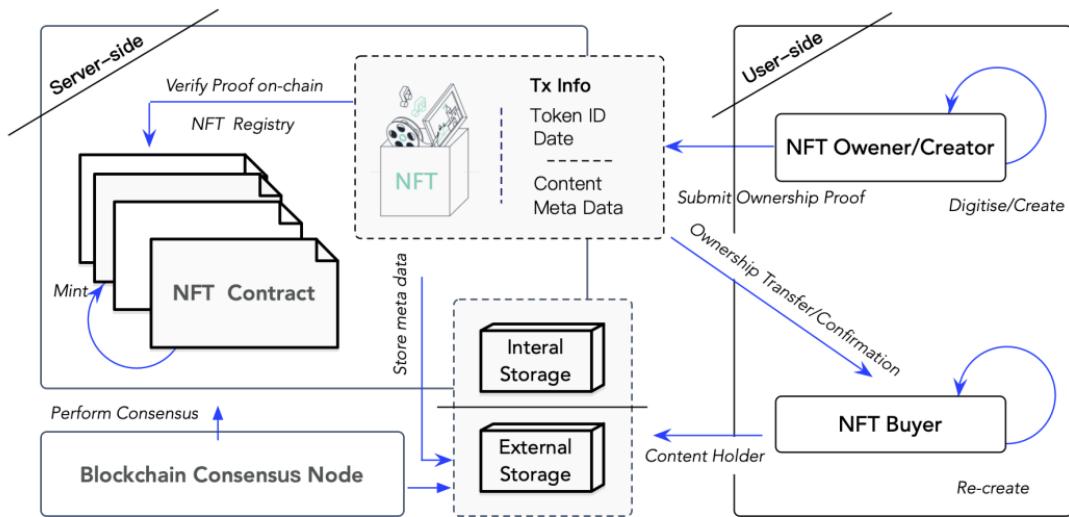


图 1-3 非同质化代币工作流程

Figure 1-3 NFT(Non-Fungible Token) Workflow

NFT（非同质化代币）之所以难以定价，主要是因为它们具有独一无二的属性和极高的个性化特征。与传统的同质化资产（如股票或标准化的商品）不同，每个 NFT 都代表了一个独特的项目或资产，如数字艺术品、收藏品或其他独特物品。这种独特性意味着每个 NFT 的价值在很大程度上取决于个人偏好、稀缺性、艺术价值和市场对该特定项目的需求。Nadini 等人<sup>[9]</sup>通过分析 2017 年 6 月至 2021 年 4 月期间 610 万笔、涉及 470 万 NFT 的交易数据，揭示了 NFT 市场的统计特性、交易网络结构，并发现销售历史和视觉特征是价格的良好预测因素。为了探索人们为何愿意支付高达数百万美元购买 NFT，Yilmaz 等人<sup>[10]</sup>通过分析客户旅程和当前 NFT 空间动态来概念化 NFT 旅程，并评估了基于阶段的关键价值驱动因素，通过三个涉及 NFT 用户的研究，使用基于消费者的价值理论，识别并分类了不同阶段的价值驱动因素。加密货币在 NFT 市场中扮演着重要角色，因为它们可以用于购买 NFT，特别是与相应 NFT 相关联的本地加密货币被称为 NFT 关联代币。通过溢出效应分析，Ho 等人<sup>[11]</sup>发现这两类资产之间的溢出有限，并且在同一 NFT 内及不同 NFT 之间存在多个同类子市场；研究结果显示 NFT 与加密货币及其关联代币有所区别，不同 NFT 之间及同一 NFT 内的子市场之间的溢出也有限，表明通过将 NFT 关联代币和子市场加入非多样化的 NFT 投资组合中，可以实现有效的风险管理。Wang<sup>[12]</sup>基于 LexisNexis 新闻与商业数据库的 5.9 亿条新闻故事，提出了一个衡量公众对 NFT 市场关注度的新直接代理指标——非同质化代币关注度指数（NFTsAI），并运用历史分解法评估 NFTsAI 的历史变化。接着，通过时间变化参数向量自回归（TVP-VAR）波动性溢出关联模型进行实证分析。实证结果显示，NFTsAI 表明 NFT 市场受加密货币、去中心化金融（DeFi）、股票、债券、商品、外汇和黄金市场的主导，且 NFT 市场是波动性溢出的接收者。此外，NFT 资产可以阻碍金融传染，并具有显著的多元化效

益。BenMabrouk 等人<sup>[13]</sup>探讨了 NFT（非同质化代币）的五个主要细分市场（收藏品、艺术、游戏、元宇宙和实用工具）与比特币及美国股市（标普 500 指数）之间的动态溢出效应和对冲效能。使用 TVP-VAR 模型和 DCC-GARCH 模型，研究发现 NFTs 与传统资产和比特币的关联度较低，且将 NFTs 加入标普 500 或比特币投资组合可带来多元化好处，特别是元宇宙在这些资产中表现为有效的对冲工具。

加密货币的去中心化特性意味着它们不受任何中央机构或政府的直接控制，这使得市场情绪和公众舆论，尤其是社交媒体上的言论，对加密货币的价格波动性有着显著影响。社交媒体平台上的信息传播速度快，影响范围广，因此，有关加密货币的新闻、意见、谣言甚至知名人士的评论都可能迅速影响市场情绪，从而导致加密货币价格的短期波动。由于加密货币市场相对较新且参与者多样，从散户投资者到大型投资机构，市场对信息的反应往往更为敏感和迅速。此外，由于加密货币市场的透明度和流动性不如传统金融市场，社交媒体上的信息往往能在没有足够事实验证的情况下产生重大影响，进一步增加了市场的不确定性和波动性。研究发现信息发布增加了价格跳跃的可能性，特别是在事件发生后的 60 分钟内<sup>[14]</sup>。考虑到加密货币市场全天候运作，周末的新闻情绪与价格跳跃关系有所不同，平日与传统金融市场的更紧密互动导致对新闻事件的反应更加活跃；而且，社区驱动型加密货币（如比特币、NEO、莱特币）对信息的敏感性高于公司驱动型加密货币<sup>[14]</sup>。在加密货币市场中，由于对资产基本价值理解不足和高度战略互补性，新闻报道可能成为信号或噪音。Lee 和 Jeong<sup>[15]</sup>通过博弈论模型展示了与基本面相关或无关的新闻报道数量增加了新兴金融市场资产的价格波动。他们使用 2014 至 2017 年间 500 种加密货币的 358,118 次观察和 36,572 次媒体报道的独特数据集进行测试，结果表明无关新闻数量的增加导致主要和次要货币的价格波动性增加，而且次要货币的价格波动随着相关新闻的增加而增加。Agosto 等<sup>[16]</sup>利用大量加密货币新闻和谷歌搜索指数的信息，使用后向优越协变量增强迪基-富勒（BSCADF）测试分析市场情绪，结果显示情绪分析在预测投机泡沫方面具有显著效果，尤其是投资者情绪的两极化版本在预警市场泡沫事件方面起到了更关键的作用。Kulbhaskar 等人<sup>[17]</sup>构建了一个特定于加密货币的新闻情绪指标，通过分析每日加密货币新闻头条将情绪分类为正面和负面，以了解它们对加密货币市场交易活动的不同影响。结果显示，正面新闻能够提升投资者信心，从而增加回报，而负面新闻则引起不确定性。比特币的负面新闻对回报的影响高于正面新闻。甚至埃隆·马斯克的推特活动对加密货币市场确实存在“马斯克效应”，在 47 个与加密货币相关的推特事件后，这些币种明显出现了正向异常回报和交易量增加。Ante 还发现，平均而言，价格效应仅在与狗狗币相关的推特中显著，而比特币方面不是如此。这一发现显示了有影响力的人在社交媒体上的活动对加密货币市场重大影响，突出了道德冲突、市场操纵风险和投资者保护之间的矛盾<sup>[18]</sup>。

本文的核心在于深入理解加密货币的技术特性与市场行为，同时通过机器

学习算法评估这些新型资产对金融市场的影响。尽管加密货币的去中心化特性为交易提供了新的自由度，但也带来了监管上的复杂性。本研究旨在揭示加密货币市场的运作机制，理解其价格波动的原因，并探索其与传统金融资产之间的关系。此外，加密货币的匿名性和全球化特性也给防止洗钱和打击金融犯罪带来了新的挑战。

## 1.2 研究内容与技术路线

本文旨在通过定量分析的方法对加密货币进行评估，并据此向监管机构提供政策建议，以便更好地监管这一新型数字资产。本文主要研究内容分为四个子研究，主要研究及章节安排如下：

第一章，绪论。主要介绍论文的研究背景、研究意义与技术路线。首先，介绍了区块链，数字货币的概念与特性，并指出区块链数字货币治理面临诸多挑战，进一步强调了研究目标是预防并治理区块链数字资产现有的金融诈骗。接着，阐述了本研究的理论和实践意义。最后，概述了本论文的主要研究内容。

第二章，区块链数字资产治理现状分析。本研究介绍的文献以深度学习和机器学习作为主要方法，这是因为传统的金融分析主要关注各个指数的联动效应，并且通常只对价格进行分析。然而，本研究的数据来源更为广泛，包括文本数据和图片数据，这些数据的复杂性和丰富性远远超出了传统金融分析所能覆盖的范围。在这样的数据基础上，本研究深入探讨了货币属性、同质化货币、非同质化货币，以及社交媒体舆情这四个维度，旨在提供一个更全面、更深入的数字资产治理分析框架。

第三章，金融诈骗检测方法综述。考虑到传统金融诈骗检测问题已在很大程度上得到解决，本研究便将重心转向了新技术的应用，特别是机器学习、深度学习和大数据分析在加密货币诈骗检测中的迁移与应用。此外，本研究还致力于对加密货币诈骗的种类进行分类，以明确不同算法与各种诈骗类型之间的关联性。通过这种方法，本研究旨在提供一种新视角，以更有效地识别和应对加密货币领域的诈骗行为，并促进金融科技领域中诈骗检测技术的进一步发展与创新。

第四章，在大语言模型框架下的加密货币属性判断以及投资决策。此研究中将专注于探讨以太坊的特性，并研究了新闻媒体头条新闻对于不同资产对（包括比特币、以太坊、黄金、原油以及脸书和微软的股票）的预测能力。通过深入分析新闻媒体是如何影响这些资产的市场表现的，本研究发现以太坊在其行为和市场反应方面，更类似于证券而非传统的商品。这一点对于制定以太坊的监管框架极具意义，暗示着以太坊或许更适宜接受类似股票的监管方式。此外，本研究还探讨了大型语言模型在解读新闻以及预测资产价格方面的专业性和准确性。研究表明，散户投资者可以利用大型语言模型来做出更加明智的投资决策，这为个人投资者在复杂的市场环境中提供了一种新的决策工具。

第五章，深度学习视角下的 NFT 价值研究。本研究深入探讨了 NFT 市场中的人像头像（PFP）子类别。研究使用了 VGG-19 神经网络模型来提取同一系列

中各个图片的视觉特征，旨在评估系列内图片之间的视觉相似度。通过这种方法，研究能够深入理解并量化每个 PFP 系列的独特美学风格。为了分析不同 PFP 系列间的相似度，研究还采用了 t-SNE 技术。此外，考虑到版权对 NFT 价值的重大影响，研究将每个系列的版权属性与其市场回报相关联。结果显示，具有高度独特性和精良制作的 PFP 系列通常带来更高的市场回报。同时，版权的存在使得 PFP 资产的市场波动性增加。综合来看，这项研究从美学和版权两个关键维度上深入分析了 NFT 作为一种新兴资产的特性，并为 NFT 的创作者和投资者提供了有价值的见解和指导。

第六章，社交媒体舆情对首次交易所发行（IEO）的影响：市场营销与操纵策略的分析。本研究讨论了在首次交易所发行（Initial Exchange Offering, IEO）中普遍存在的“水军啦啦队”现象，旨在分析这种现象是仅仅作为市场营销策略，还是一种更复杂的推高和抛售（pump-and-dump）策略。尽管与首次代币发行（Initial Coin Offering, ICO）相比，IEO 通常被认为更可靠，因为交易所对其进行了严格的尽职调查，但这种现象的存在仍然引起了关注。研究重点分析了 IEO 的市场行为和背后的动机，目的是揭示这些策略的真实意图和潜在影响。此外，研究还关注了社交媒体上自动化消息如何影响公众对 IEO 项目的认知。这包括研究自动化消息——例如机器人生成的推文和评论——是如何塑造或扭曲投资者对 IEO 项目看法的，以及这些认知变化如何转化为实际的市场行为。通过这些发现，研究旨在为投资者和市场监管者提供深刻的见解。

第七章，总结与展望。回顾了主要研究内容及其成果，并对研究中遇到的挑战进行了评估，同时对未来的研究方向提出了预期和展望。



## 第2章 区块链数字资产治理现状分析

本章将深度学习和机器学习的前沿技术应用于区块链数字资产的多维度探索中。本研究以文本和图像数据为基础，从货币属性、同质化货币、非同质化货币，以及社交媒体舆情四个维度出发，利用该框架深入分析并讨论了区块链数字资产治理的现状。通过集合文本挖掘的技术和专家在区块链和金融领域的深厚经验，本章不仅展示了区块链数字资产治理的复杂性和挑战性，而且还总结了在这一新兴领域中深度学习和机器学习面临的核心问题和机遇。

### 2.1 数字货币的共识机制

共识机制在区块链数字货币的运作中发挥着核心作用，直接影响其货币属性，包括安全性、去中心化程度、交易处理速度和能效等。工作证明（Proof of Work, PoW），如图 2-1 所示<sup>[19]</sup> 作为最早的共识机制之一，通过要求参与者解决复杂的计算问题以赢得区块奖励，确保了网络的安全性和去中心化。PoW 机制使得比特币等加密货币在作为价值存储方面建立了信任，但也因其巨大的能源消耗而受到批评。高能耗导致环境问题，同时也增加了挖矿成本，可能会导致网络参与度降低，进而影响交易速度和费用。

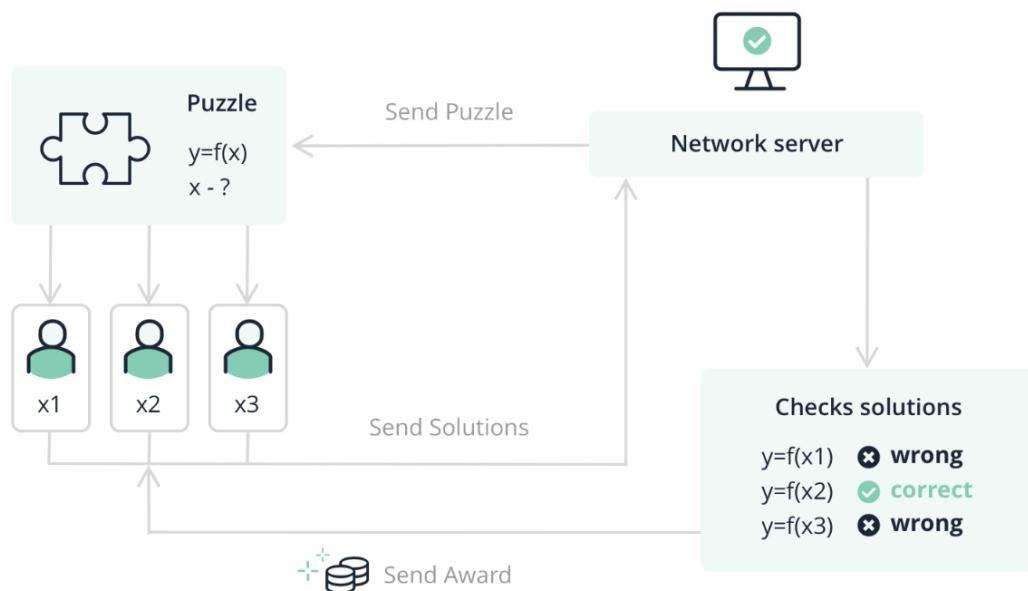


图 2-1 工作证明

Figure 2-1 proof of work

与之相对的是权益证明（Proof of Stake, PoS）机制，如图 2-2<sup>[20]</sup> 所示，它选定区块生产者不是通过计算力竞争，而是基于用户的持币量和持币时间。PoS 降低了能源消耗，提高了交易处理速度，理论上可以增加网络的可扩展性。然而，

PoS 可能会加剧“富者更富”的问题，因为持有更多货币的个体有更大的概率生成新的区块并获得奖励。



图 2-2 权益证明

Figure 2-2 proof of stake

除此之外，还有委托权益证明（Delegated Proof of Stake, DPoS）和拜占庭容错机制（Byzantine Fault Tolerance, BFT）等，它们在提高交易速度、降低能源消耗和保持网络安全性方面各有优势和局限。这些共识机制的设计对于加密货币的货币属性，如其作为交换媒介的效率、作为价值存储的安全性，以及作为计量单位的稳定性，都有着深刻的影响。本论文主要讨论并比较工作证明和权益证明机制带来的货币属性的变化。PoW 机制通过消耗大量能源来维持网络安全和数据一致性，从而使得比特币的价值在某种程度上被能源锚定。这种机制下，能源的投入与比特币产出之间的关系赋予了比特币一种与能源市场相关联的价值基础，因而在某种程度上保证了其价值的稳定性。

相比之下，PoS 机制通过让持币者投入资金来参与网络维护，降低了对物理能源的需求，但同时也带来了新的动态。以太坊等采用 PoS 机制的加密货币更多地依赖于持币者的参与度和对网络的信任。在 PoS 中，持币者的财富不仅体现在他们持有的货币数量上，还体现在他们对网络未来发展的信心上。如果缺乏创新和增长潜力，投资者可能会失去信心，导致资金流出。

因此，PoW 和 PoS 机制不仅在技术执行上有所不同，而且对加密货币的货币属性有着根本的影响。PoW 的能源锚定特性给予比特币一种稳定而可靠的价值印象，而 PoS 的创新依赖特性则为以太坊等货币赋予了更多的创新和增长动力。

## 2.2 数字货币的货币属性

### 2.2.1 比特币

在区块链数字资产治理中深入探讨加密货币的货币属性对于理解其在现代金融体系中的角色及其基本价值至关重要。这不仅有助于确认加密货币是否满足交换媒介、价值存储和计量单位等货币功能，而且对于引导监管政策、保障金融稳定性、促进技术创新和指导投资者决策等方面也具有深远影响。随着加密货币在全球经济中地位日益重要，其货币属性的探讨对于理解和预测其对传统货币政策、金融市场及整体经济体系的影响变得尤为关键。同时，对于加密货币货币属性的深刻理解还能够提高其交易和使用的透明度，促进其在日常交易和商业活动中的广泛应用。因此，加密货币的货币属性讨论不仅有助于明确其作为一种新兴资产类别的本质和功能，还对监管政策制定、投资者决策支持、技术创新推动以及经济模型构建等多个层面产生深远的影响。

Schilling 等人的研究<sup>[21]</sup> 提出了一个由两种内在无价值的竞争货币（美元，比特币）组成的禀赋经济模型。美元由央行发行以实现其通胀目标，而比特币供应量则按确定性规则增长。基本定价方程在最简单的形式下意味着比特币价格形成鞅。“相互不耐烦”暗示着市场参与者不太可能持有资产以期待价格上涨，因此缺乏投机性购买行为。这意味着价格波动，即使存在，也不会影响货币作为交换媒介的基本功能，因为持有者更关注即时的交易而非长期的价值投机。比特币区块奖励并非对比特币持有者的税收：它们是由美元税收来资助的。研究还讨论了货币政策的影响、比特币生产、税收、福利和进入市场的条件，并描述了可能的均衡范围。Yermack<sup>[22]</sup> 认为一个合格的货币应当充当交换媒介、价值储藏和计量单位的角色，但比特币在满足这些条件上未能成功。比特币在消费者交易方面仅取得了微小的体量，对于接受比特币的少数商家来说，其平均交易量远低于每天一笔。比特币的波动性远高于广泛使用的货币，给用户带来了巨大的短期风险。比特币的日交易率与主流货币和黄金几乎没有相关性，这使得比特币在风险管理方面几乎无用，并且为其所有者进行对冲极其困难。比特币价格的消费品需要许多小数位和前导零，这对零售市场的参与者来说是令人不安的。比特币面临每日黑客攻击和盗窃的风险，缺少存款保险的银行系统支持，并且不被用于标记消费信贷或贷款合约。比特币似乎更像是一种投机性投资，而非货币。因为比特币需要电力和算力来维持，还有一些文献从能源角度来考虑比特币的货币属性。区块链的安全性依赖于一种计算密集型的比特币挖掘算法，该算法防止了比特币的双重支付和对已确认交易的篡改。这种“工作证明”算法需耗费大量能源。实际消耗的能源量是有争议的。Vranken 认为<sup>[23]</sup> 目前比特币的能源消耗大约在 100-500 兆瓦之间。文中讨论了比特币挖矿硬件的发展，并简要概述了一些不太耗能的替代方案。最后，研究还考察了其他区块链应用，并指出在这些应用中能源消耗并不是主要关注点。Baur 等人<sup>[24]</sup> 分析了比特币是作为一种交换媒介还是一种资产的问题，更具体地，探讨了比特币当前的使用情况以及鉴于其特性，未来可能占主导地位的使用方式。通过对比特币的统计属性分析，发现在正

常时期和金融动荡时期，比特币与传统资产类别如股票、债券和商品都没有相关性。对比特币账户的交易数据分析表明，比特币主要被用作投机性投资，而非作为一种替代货币或交换媒介。White 等人<sup>[25]</sup>认为确定比特币的属性非常重要。现有法规是否适用于加密货币，取决于加密货币被归类为货币、证券、衍生品还是金融服务（转账）工具。在进行的一系列探索性分析中，尝试对比特币进行分类。通过多种方法比较了比特币的行为与货币、如衍生品的资产类别、基于技术的产品、潜在技术产品（例如以太坊和证券 SPY）以及投机性金融泡沫。分析结果表明，比特币的行为更接近于基于技术的产品、新兴资产类别或泡沫事件，而非货币或证券；因此，正确的判断是现有的货币和证券法律不应适用于加密货币。

## 2.2.2 以太坊

以太坊是一种广泛使用的开源区块链平台，不仅支持其自身的加密货币——以太币（Ether），还能运行智能合约和分布式应用（DApps）。区别于比特币的单一货币功能，以太坊提供了一个更为丰富和灵活的平台，能够支持各种去中心化金融（DeFi）服务和其他区块链应用。以太坊从 2020 年开始逐步升级到权益证明（PoS）。

由于加密货币是由区块链系统生成和使用的，因此区块链特有的信息可以被视为预测加密货币价值的主要组成部分。这种观点已在比特币价格预测的研究中广泛采用。然而，kim 等人研究<sup>[26]</sup>发现，在市场上广受欢迎并处于领先地位的以太坊，其区块链信息与比特币有所不同。因此，本研究探讨了内在的以太坊区块链信息与以太坊价格之间的关系。此外，还研究了市场上其他公开可用货币的区块链信息如何与以太坊价格相关联。主要发现表明，宏观经济因素、以太坊特有的区块链信息以及其他加密货币的区块链信息在预测以太坊价格方面起着重要作用。Nadler 和 Guo<sup>[27]</sup>估算了用户对影响其代币持有量的因素进行定价的定价核心。研究了市场风险等传统风险因素以及区块链特有风险因素是如何被评估和定价的。为此，引入了一种资产定价模型，并修改其属性，使其适用于加密货币市场。将风险因素分为市场相关风险因素以及比特币和以太坊区块链特有风险因素。研究发现区块链特有的风险因素已被纳入定价中。有证据表明，风险因素已从比特币特有的风险因素转向以太坊特有的风险因素，市场因素的重要性日益增加，这为链上和链下交易活动的脱钩提供了证据。Web3 和去中心化金融（DeFi）被广泛宣传为促进更大金融包容性和民主化的创新。Cong 等人<sup>[28]</sup>对最大的 Web3 生态系统进行了初步调查，并使用大规模计算来进行分析。描述了以太坊网络结构、时间趋势以及交易、挖矿和所有权的分布情况。发现挖矿收入和以太币所有权集中在交易所和少数个体节点手中。网络活动从点对点交易演变为用户与 DApps/DeFi 的互动，大型玩家的交易数量显著增加。此外，高交易费用、拥堵引起的 gas 价格波动、次优的储备设置以及代币的大幅回报波动，对小型、贫困、缺乏经验和新节点带来了特别挑战，更不用说高失败率对所有用户都造成伤害。最后，通过提供初步的因果证据表明，基础费用燃烧机

制（例如 EIP-1559）和空投项目（例如 OmiseGo Airdrop）通过代币货币再分配促进了包容性。Chen 等人<sup>[29]</sup>的研究发现在比特币的交易中可能会产生找零，因为如果 UTXO 的大小超过了需要支付的金额，那么在交易中会消耗整个 UTXO，并产生找零。而在以太坊中，账户会发送确切金额的资金到另一个账户，因此不会产生找零。比特币的交易可以有多个输入（即多个 UTXO）和多个输出，因为一个钱包可以聚合同一用户的多个 UTXO 进行支付，并将资金发送给多个接收者。值得注意的是，比特币的一个用户可能拥有多个地址，而以太坊则通常将一个外部拥有账户（EOA）关联到一个地址。Saleh<sup>[30]</sup>提供了权益证明（PoS）的正式经济模型，并确定了 PoS 产生共识的条件。适度的奖励机制不仅暗示了存在一种平衡，在这种平衡中，共识尽可能快地被达成，而且还排除了持续分叉平衡的可能性。后一个结果是由于 PoS 不同于工作证明（PoW），它要求验证者也是股东。

### 2.3 同质化代币发行和平台经济

同质化代币的价格通常由市场供需决定。由于这些代币在功能和价值上是相同的，它们的价格不受个别代币特性的影响，而是受到整体市场情绪、流动性、使用案例以及宏观经济因素的影响。例如，一个同质化代币可以是加密货币市场中的一个标准单位，如比特币或以太坊，它们的价值体现在能够被广泛接受和用作交易。同质化代币的价格还可能受到技术更新、行业新闻、监管变化以及投资者行为的影响。此外，由于同质化代币易于在交易所交易，其价格透明度较高，市场信息较为充分反映在价格变动中。

同质化代币的发行通常通过初始币（代币）发行（ICO）或初始交易所发行（IEO）的形式进行。ICO 和 IEO 都是加密货币项目为筹集资金而销售新创建代币的方法。

ICO 是一种类似于众筹的方式，项目方直接向公众出售新的代币。投资者以现有的加密货币如比特币或以太坊购买新发行的代币，期望代币未来能在加密货币交易所上市交易，并且价格上涨。ICO 允许项目团队绕过传统资本市场和金融中介机构，直接向潜在的投资者募集资金。然而，ICO 也存在风险，因为它们受到的监管较少，且有诈骗和项目失败的可能性。

IEO 是一种新兴的代币销售方式，由加密货币交易所代表项目方进行。在 IEO 中，交易所会筛选并承载代币销售，投资者需要在该交易所注册账户并用加密货币购买新代币。IEO 相较于 ICO 通常被认为更加安全，因为交易所会对项目进行初步审查和尽职调查，从而减少投资者的风险。此外，由于交易所本身的参与，IEO 后的代币上市也更加容易和快捷。

ICO 和 IEO 通常在专门的 ICO 平台（launch pad）或者项目方自己的网站上进行。launch pad 会帮助项目方进行市场推广、投资者关系管理以及资金的募集等。也有许多项目选择在自己的官方网站上直接进行 ICO，这样可以更直接地与潜在的投资者沟通。

一旦 ICO 完成，代币通常需要在交易所上市，以便提供流动性，并允许更广泛的公众购买和交易这些代币。项目方可能会与一个或多个中心化交易所 (CEX) 合作，将他们的代币上市。这通常需要通过交易所的严格审查过程，并可能涉及显著的费用。项目方也可以选择在去中心化交易所 (DEX) 上市。在 DEX 上市通常更加快速和简单，但相对来说，DEX 的流动性可能不如 CEX。因为中心化交易所在功能和操作方式上与传统股票交易所并无过多不同，所以在此以 Uniswap 这个全球最大的去中心化交易所为例，来讲述其中的工作原理。

Uniswap 采用自动化做市商 (AMM, Automated Market Maker) 模型来实现代币之间的交易。在 Uniswap 上，交易不是通过传统的买家和卖家撮合完成的，而是用户与一个流动性池 (Liquidity Pool) 进行交互，流动性池内包含一对代币，例如 ETH/DAI。

Uniswap 的核心是一个简单的数学公式，用于确保交易前后池中两种代币的乘积保持恒定，这被称为“恒定乘积市场做市商”模型 (Constant Product Market Maker Model)，公式如下：

$$x \cdot y = k$$

其中：

$x$  是池中一种代币的数量。 $y$  是池中另一种代币的数量。 $k$  是一个常数，代表池的总价值。

当要用 Uniswap 进行交易时，比如用 ETH 兑换 DAI，实际上是在将 ETH 添加到池中，并从池中取出相应数量的 DAI。这个过程遵循以下步骤：

1. **计算价格**：根据池中 ETH 和 DAI 的现有比例计算价格。2. **执行交易**：向池中添加一定数量的 ETH，并从池中取出相应数量的 DAI。取出的数量基于保持  $k$  值不变的原则。3. **收取手续费**：Uniswap 会收取一定比例的交易手续费（例如 0.3%），并将其添加回池中，作为奖励给流动性提供者。

在执行交易时，假设向池中添加了  $\Delta x$  数量的 ETH，并希望从池中获取  $\Delta y$  数量的 DAI。交易后，池中的 ETH 和 DAI 的数量分别变为  $x + \Delta x$  和  $y - \Delta y$ 。为了保持  $k$  值不变，以下等式必须成立：

$$(x + \Delta x) \cdot (y - \Delta y) = k$$

在考虑手续费的情况下，公式会有所调整，以确保一部分交易额被添加回池中。

通过这种方式，Uniswap 保证了在没有传统买家和卖家的情况下，用户可以随时进行代币交易，并且交易价格是由当前池中的代币比例决定的。同时，为了激励用户提供流动性，向流动性池提供代币的用户可以获得交易手续费的一部分作为回报。

传统的双边平台（如亚马逊、优步）主要依靠佣金合同来产生收入和推动增长，而它们的去中心化对应物（如 Uniswap、Filecoin）通常放弃这些，转而选择保留代币。Gan 等人<sup>[31]</sup>的研究表明，通过适当设计的初始币（代币）发行（ICO），这两种机制都可以独立地缓解初期筹资阶段的市场失败，并激励长期平台建设。然而，它们以不同的方式实现这一目标。虽然佣金合同通常会为创始人带来更高的利润，但代币保留则会导致更高的服务水平，从而惠及用户和服务提供者。本质上，代币保留放弃了一部分收益，以更好地与去中心化治理的原则保持一致。Chod 和 Lyandres<sup>[32]</sup>提出了一种通过加密代币为创业企业融资的理论，这种方式不仅限于基于平台的企业。论文比较了代币融资和传统的股权融资，重点关注了两种融资方法所关联的代理问题和信息不对称摩擦，以及创业者和投资者之间的风险分担。代币融资引入了在股权融资下不存在的代理问题（生产不足），同时减轻了通常与股权融资相关的代理问题（创业者努力不足）。该理论抽象化了代币和股权之间所有的制度性和可能是暂时性的差异，基于代币的一个单一内在特征：它们代表了对企业产出的索赔。研究表明，对于那些边际生产成本低、创业者努力至关重要、和/或收益波动性相对较低的企业来说，代币很可能会胜过股权。此外，在向外部投资者信号企业质量方面，代币也可能有优于股权的优势。Barth 等人<sup>[33]</sup>研究了分析师在首次代币发行（ICO）市场的运作和失败中的作用。自由职业分析师的评估存在偏见，这是由于分析师与 ICO 团队成员之间的相互作用。即使是评级良好的 ICO，在其评级中有较大比例是基于先前评级的回报时，也倾向于在筹集部分资本时失败。在交易所上市 90 天后，相对于最初筹集的资金，有更多相互评级的代币的市场资本化较小。这些发现表明，利益冲突有助于解释 ICO 的失败。Gan 等人<sup>[34]</sup>探讨了在资产代币化背景下如何利用 ICO，其中企业发行由未来资产（例如库存）支持的代币以筹集增长资金。研究建议如何设计这类“资产支持”的 ICO——包括对实用性代币和股权代币（又称安全代币发行）的最佳代币流通和定价，同时考虑到道德风险（资金挪用）、产品特性和客户需求的不确定性；对 ICO 成功/失败进行预测；并讨论其对企业运营策略的影响。研究表明，在非监管环境下，ICO 可能导致重大的代理成本、生产不足以及企业价值损失。然而，这些低效现象随着产品利润率和需求特性（均值/方差）的改善而减弱，并且在发行股权代币（而非实用性代币）时不那么严重。重要的是，股权代币的优势源于其固有的激励对齐能力，因此即使在没有监管的情况下也依然存在。Holden 和 Malani<sup>[35]</sup>对涉及实用性代币和类似结构的 ICO 使用提出了一个基本悖论。为了增加 ICO 筹集的资本，公司可能尝试减少区块链运营成本，从而扩大销售商品的数量。然而，由于矿工补偿机制的原因，这样做会增加在任何时间间隔内发生的实用性代币交易数量（即，增加代币流通速度，从而增加代币的有效供应量）。根据费舍尔方程，这会降低代币的美元价值和投资者愿意为它们支付的金额。研究指出，这个悖论限制了实用性代币 ICO 作为传统融资选项的价值。

## 2.4 非同质化代币

非同质化代币 (NFT, Non-Fungible Token) 是一种独特的数字资产，其代表着对数字或实体物品的独特所有权。与可互换的加密货币（例如比特币）不同，每个 NFT 都是独一无二的，不能被等量替代。NFTs 通常存储在区块链上，这是一个不可篡改的分布式账本，用以确保每个 NFT 的真实性和所有权记录。

NFT 的工作原理涉及几个关键步骤：

1. 创造和铸造：艺术家或创作者生成一个独特的数字项目（图 2-3），如艺术品、音乐、游戏物品或其他形式的创意作品，并使用智能合约将其铸造成 NFT。在铸造过程中，该物品的元数据（包括所有权信息、项目描述等）被记录在区块链上。
2. 验证和所有权：一旦 NFT 被创建，其信息和历史记录就被存储在区块链上。这提供了一个透明和不可篡改的验证过程，确保每个 NFT 的独特性和所有权。
3. 买卖和交易：NFT 可以在各种市场上买卖和交易。流行的市场包括 OpenSea、Rarible、Foundation 等。不同的市场可能专注于不同类型的 NFT，如艺术品、收藏品、游戏道具等。当 NFT 被转移或售出时，所有权和交易记录会在区块链上更新，确保所有权的转移是安全且可验证的。

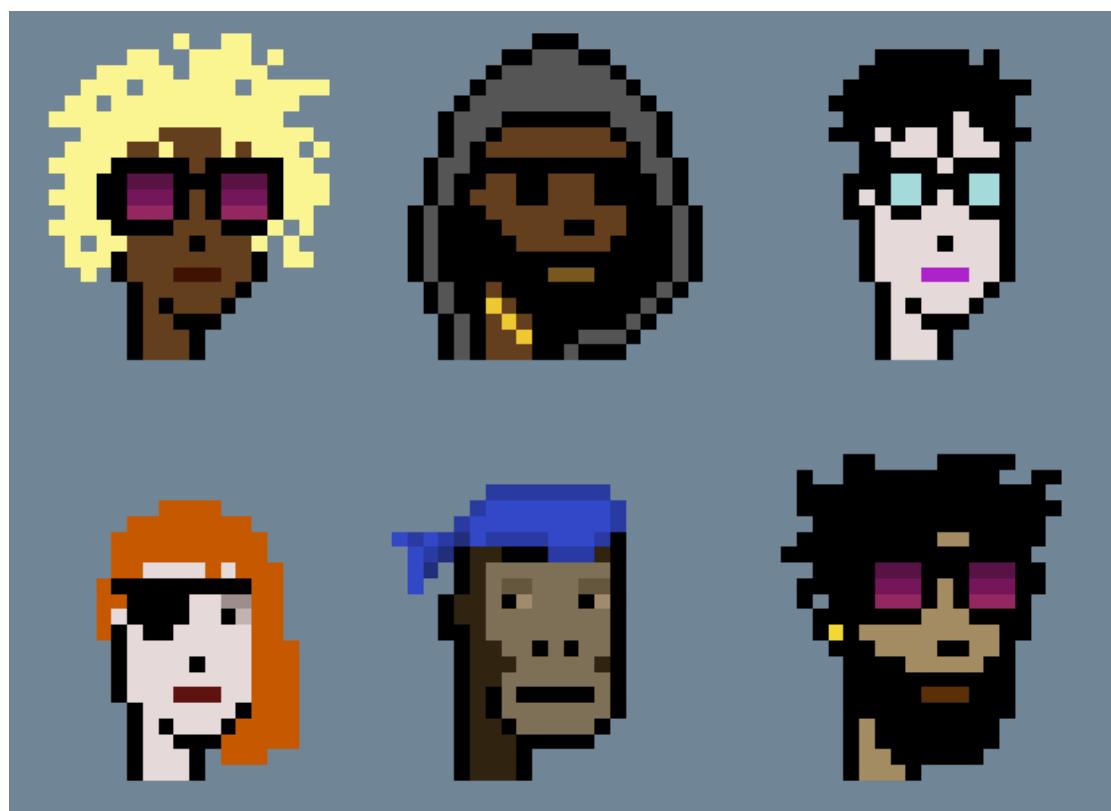


图 2-3 加密朋克（最早的一批 NFT）

Figure 2-3 Cryptopunk

Alsultan 等人<sup>[36]</sup> 通过使用流行的 CryptoPunks NFT 艺术收藏的数据，使用

与文化经济学文献中的情感效果相关的四种审美度量来量化 NFT 的视觉吸引力。利用享乐定价模型，确定了审美作为数字艺术市场价格的驱动因素。研究结果表明，投资者偏好具有更高色彩丰富度和纹理复杂度以及更低饱和度和亮度的 NFT。Bao 等人<sup>[37]</sup>的研究实证检验了新兴非同质化代币（NFT）市场中群体行为的存在和动态，使用了 2017 年 11 月 23 日至 2021 年 4 月 27 日的交易级数据。通过宏观和微观方法探测群体行为，发现了该市场存在群体行为的支持性证据，其动态似乎是由事件驱动的。大量新入市的或经验不足的投资者可能触发群体行为。在 NFT 市场中，当以太坊的回报增加时，群体行为倾向于出现；但随着比特币回报的增加，群体行为则有所减弱。与此同时，与传统资产市场不同，NFT 市场中的群体行为似乎不会跨子市场发生（如 OpenSea、Atomic、Cryptokitties、Godsunchained 和 Decentraland）。活跃投资者在不同收藏品中群体交易 NFT，并在 OpenSea 上列出的 NFT 投资决策中遵循市场共识。Borri 等人<sup>[38]</sup>的研究构建了一个全面的非同质化代币（NFT）交易数据集，创建了 NFT 市场及其组成部分的指数，并分析了它们的特性。NFT 市场的回报显著受到加密货币市场的影响，但大部分回报变化仍然无法解释。NFT 市场回报对其他加密货币因素和传统资产市场的因素暴露度低。在时间序列中，波动性和 NFT 估值比率显著预测 NFT 市场回报。在横截面上，NFT 回报显示出规模效应和回报反转效应。Guadamuz<sup>[39]</sup>从英国视角分析了非同质化代币（NFTs）及其版权问题，包括 NFT 是否能转让版权、作为数字版权管理工具的应用，以及 NFT 的版权侵犯风险。文中考虑了英格兰、威尔士、苏格兰的案例以及欧洲联盟法院的相关判决。由于 NFT 技术较新，文章深入探讨了技术背景及其引发的法律问题，并指出公众对 NFT 的认知存在误解。尽管电子方式转让权利在技术上可行，但 NFT 是否能合法转让版权仍不明确。此外，文章主张未经授权的作品铸造不一定构成版权侵犯，但可能涉及对公众的传播问题。Wilson 等人<sup>[40]</sup>对 NFTs 进行了定义，探讨了它们与区块链和加密货币的关系，以及它们在各行业中的使用情况及带来的机遇和风险。文章的核心贡献是对初步 NFT 生态系统的概念性绘制，提供了关键利益相关者之间的关系映射，包括内容创作者、核心和相关的技术及商业中介、消费者、投资者和投机者。

## 2.5 社交媒体舆情对资产价格的影响

社交媒体舆情在现代金融市场中扮演着日益重要的角色，它能够显著影响资产价格。信息和情绪的迅速传播可以在短时间内形成巨大的市场影响力，从而导致资产价格的剧烈波动。用户的讨论、评论以及分享等互动行为，尤其是在关键事件或数据发布时，可以快速集聚成影响市场情绪的力量。这种舆情动态不仅影响个别股票或加密货币的价格，也可能影响整个行业乃至更广泛市场的走势。因此，对于投资者和市场分析师来说，密切关注并正确解读社交媒体上的舆情变化，已成为捕捉市场动态、做出明智投资决策不可或缺的一环。在一些具体应用场景中，如情感分析和词频计算，会使用一些基础的数学计算来得出最终的分析

结果。

### 1) 情感得分计算:

- **简单计数**: 无特定公式, 仅计算文本中积极词和消极词的数量差。
- **加权计数**: 情感得分可以表示为所有情感词的加权和:

$$Score = \sum_i (weight_i \times orientation_i)$$

其中  $weight_i$  是词  $i$  的权重,  $orientation_i$  表示词的情感倾向 (积极或消极)。

### 2) TF-IDF (Term Frequency-Inverse Document Frequency):

- TF-IDF 用于衡量一个词在文档集合中的重要性, 其计算公式为:

$$TFIDF(t, d, D) = TF(t, d) \times IDF(t, D)$$

其中:

- $TF(t, d)$  是词  $t$  在文档  $d$  中的频率。
- $IDF(t, D)$  是逆文档频率, 计算公式为:

$$IDF(t, D) = \log \left( \frac{|D|}{|\{d \in D : t \in d\}|} \right)$$

$|D|$  是文档集合中文档的总数,  $|\{d \in D : t \in d\}|$  是包含词  $t$  的文档数目。

近年来深度学习在自然语言处理 (NLP) 领域的情感分析中已成为一个热点。深度学习模型能够处理复杂的数据结构, 并从中学习丰富的特征表示, 使其在情感分析任务中表现出色。典型的过程包括:

#### (1) 数据预处理:

- **文本清洗**: 去除无关信息, 如 HTML 标签、特殊符号、停用词等。
- **分词**: 将句子分解成词语或标记 (Token)。
- **向量化**: 使用词袋模型 (Bag of Words)、TF-IDF 或词嵌入 (如 Word2Vec 或 GloVe) 等方法将文本转换为数值型向量。

#### (2) 模型构建:

- **循环神经网络 (RNN)**: 特别是 LSTM (长短期记忆) 和 GRU (门控循环单元) 模型, 能够捕捉文本中的时间序列信息。
- **卷积神经网络 (CNN)**: 虽最初用于图像处理, 但也被用于文本处理, 尤其擅长提取局部区域的特征。
- **Transformer 及其衍生模型** (如 BERT、GPT): 这些模型通过自注意力机制捕捉全局依赖, 对文本情感分析表现出色。

#### (3) 模型训练:

- 使用标注好的数据集训练模型。这一过程包括向模型输入文本向量, 通过模型计算输出, 然后与实际标签比较, 计算损失函数, 最后通过反向传播和梯度下降等优化算法更新模型权重。

#### (4) 评估与优化:

- 使用验证集评估模型性能，监控过拟合或欠拟合现象，并据此调整模型参数或结构。
- 可能采取的优化措施包括调整学习率、增加正则化、改变模型结构、使用 dropout 减少过拟合等。

#### (5) 模型部署与应用：

- 经过训练和评估得到的模型在测试集上进行最终评估。
- 将模型部署到实际应用环境中，对实时数据进行情感分析。

深度学习在情感分析中的应用依赖于大量的数据和计算资源。然而，它能够有效捕捉文本中的复杂特征和依赖关系，为准确理解文本情感提供了强有力的工具。

随着比特币、以太坊等多种加密货币价格的攀升，加密货币市场近年来成为最热门的投资领域。与其他相对稳定的金融衍生品不同，加密货币市场的高波动性要求高频预测模型以进行量化交易。然而，由于预测结果的不稳定性和高误差率，交易数量过多成为一个关键问题。为缓解这一问题，Peng 等人<sup>[41]</sup> 基于对高频数据的观察，采用局部最小值序列替换原始序列，并提出一种更稳定的三重趋势标记方法，通过潜在影响模型训练减少交易数量。此外，提出了一种新的基于注意力机制的 CNN-LSTM 模型（ACLMC），通过利用频率和货币间的相关性来优化模型效果，并通过支持同时多货币预测来平滑与预测错误相关的投资风险。实验表明，使用 ACLMC 的标记方法可以实现比传统基准更好的财务指标和更少的交易数量。Cheng 等人<sup>[42]</sup> 运用了实证分析、金融时间序列和机器学习来预测比特币价格和 Garman-Klass (GK) 波动性，采用了长短期记忆 (LSTM)、季节性自回归综合移动平均 (SARIMA) 和 Facebook Prophet 模型。研究发现，与 SARIMA 和 Facebook Prophet 相比，LSTM 在均方误差 (MSE) 和平均绝对误差 (MAE) 方面有显著改进，但 SARIMA 和 FB-Prophet 在预测比特币价格和波动性方面更可预测。此外，研究确认比特币价值极具季节性波动性和随机性，受加密货币法规、投资或社交媒体谣言等外部因素的影响，尤其在俄乌冲突期间和某些 COVID-19 时期，FB-Prophet 的表现会受到动荡时代的影响。研究为即将到来的加密货币法规、股票市场动态和全球资源分配提供了创新见解。Chakraborty 和 Subramaniam<sup>[43]</sup> 探讨了投资者情绪对加密货币回报的影响。通过使用 Sentix 数据库中的直接调查数据来捕捉比特币投资者的情绪。研究结果发现，投资者对比特币持乐观态度时，比特币价格会升值。比特币情绪在控制相关因素后，对预测比特币价格有显著影响。此外，主导加密货币即比特币的情绪也会影响其他加密货币的价格。研究还进一步调查了股票市场情绪对加密货币回报的影响，发现当股市投资者情绪偏空时，加密货币价格会上涨，表明加密货币可以作为投资的替代途径。在控制可能影响加密货币价格的潜在因素后，这些结果仍然成立。Nguyen 等人<sup>[44]</sup> 运用基于图的方法检验不同市值加密货币之间随时间变化的联系。通过应用随机矩阵理论中的去噪和趋势消除技术及市场组成概念，从历史回报和波动率时间序列中提炼出新见解。分析揭示，基于波动性的网络结构变化能

够识别出影响加密货币市场的重大事件。此外，这些结构反映了投资者情绪，包括恐惧和贪婪等。使用诸如 PageRank 的指标发现，某些小型币种对市场有不成比例的巨大影响，而最大的加密货币如 BTC 和 ETH 影响相对较小。研究结果对投资者具有实际意义：一方面帮助他们规避市场重大中断，保护投资并抓住高回报机会；另一方面，通过了解加密货币的相互联系，优化投资组合。Omar 和 Lasrado<sup>[45]</sup> 通过分析 1724328 条推文，旨在利用社会集合分析（SSA）了解社交媒体用户对加密货币的互动动态。研究结果显示，推特用户对加密货币的态度更为正面，分析还揭示了事件与用户互动之间的关系，加密货币相关事件会改变用户的情感、观点和讨论主题。此研究也证明了社会集合分析框架在分析和可视化大规模社交媒体数据方面的有效性。

## 2.6 本章小结

本章节专注于分析共识机制（工作量证明（PoW）与权益证明（PoS））对货币属性的影响，并以此为基础深入探讨区块链数字货币治理的结构。章节首先探究数字货币的本质属性，讨论其是否应被视为证券或是大宗商品，从而为治理构建理论框架。随后，对同质化代币和非同质化代币进行了细致的价值分析，旨在建立一个合理的价值评估模型。此部分特别关注当前数字资产价格的高波动性及其显著的投资属性，旨在为这一现象提供理论解释和可能的解决路径。进一步地，章节转向分析社交媒体舆论对数字货币价格的影响。由于数字货币的去中心化特性，舆论操纵成为可能，并对价格波动产生重大影响。通过剖析社交媒体舆情与数字货币价格之间的关系，揭示了这一现象的内在逻辑和潜在的经济后果。综合以上内容，本章节确立了论文的结构，并应用机器学习及深度学习技术对各部分内容进行了量化分析。

## 第3章 金融诈骗检测方法综述

加密货币市场高度波动且未受监管，但其赚取巨额回报的潜力吸引了个人投资者。本章首先分析了传统金融欺诈和用于检测传统金融欺诈的流行算法。接着，介绍了现有的加密货币欺诈，并将处理传统金融欺诈的经验转化为一个新颖的加密货币欺诈检测框架。本章识别了四种主要类型的金融欺诈（消费者服务和商品欺诈、投资欺诈、公司欺诈和保险欺诈），并将加密货币欺诈认定为投资欺诈的一种，为以后各章的研究奠定了坚实的基础。

### 3.1 引言

新冠疫情的爆发彻底改变了商业和金融行为的方式。相较于在线购物平台，传统的实体店铺显得不那么灵活，而且亲自前往银行相比于在手机上使用应用程序也更加耗时。据国际贸易管理局 2020 年的数据显示，2019 年全球零售总销售中电子商务的占比从 13.6% 激增至 2020 年的 18%<sup>[46]</sup>。随着数字经济的不断发展，普华永道在 2020 年的报告中指出，尽管自 2018 年以来遇到欺诈行为的组织比例保持稳定，但欺诈者在进行金融欺诈方面的技巧却越来越高超<sup>[47]</sup>。由于缺乏中央监管机构，交易者进行交易时都是自担风险。本章主要聚焦于用于金融欺诈检测的机器学习方法，将介绍传统金融欺诈的定义，然后识别每种算法如何解决伪装、类别不平衡、标签稀缺和高维特征等挑战。

大部分金融诈骗检测综述仅覆盖了用于欺诈检测的数据挖掘方法。Al-Hashedi 和 Magalingam 的研究<sup>[48]</sup> 与本综述尝试的目标最为接近，即寻找金融欺诈检测的机器学习算法解决方案。本综述是首个从传统金融欺诈检测知识角度探索加密货币欺诈检测的研究。总结而言，具有以下三个贡献：

(1) **问题的提出和定义**：技术进步为金融欺诈检测带来新挑战。例如，加密货币虽未受监管，但却在年轻一代中广受欢迎。其高波动性和匿名性成为犯罪分子的滋生地。因此，首先需要概述常见金融欺诈并对其进行定义。本综述采取基于受害者视角的分类新方法，强调当消费者做出购买、投资、职业或保险决策时，他们可能陷入如消费者服务和商品欺诈、投资欺诈、公司欺诈以及保险欺诈。

(2) **算法分类及其新变体**：论文首先介绍原算法，随后探讨其新变体。研究目的不在于列举所有可能的算法，而是探究算法与应用之间的联系。Hilal 等人<sup>[49]</sup> 的研究涵盖了如支持向量机、随机森林、隐马尔可夫模型、多层感知神经网络、自编码器、生成对抗网络 (GAN) 等技术。本综述在选择算法时，不仅考虑高效的机器算法如 SVM 和 K 最近邻，还包括更复杂的深度学习算法如自编码器、强化学习、图神经网络和生成对抗网络 (Generative Adversarial Network)。

(3) **金融欺诈与算法之间的联系**：金融欺诈检测的主要挑战在于研究者需同时掌握算法和金融欺诈领域知识。本综述为他们提供一个快速了解这一领域

的途径。

### 3.2 金融欺诈分类

#### 3.2.1 欺诈种类

Becker 指出当预期收益超过预期成本时，人们就会犯下欺诈行为<sup>[50]</sup>。新冠疫情的爆发加速了金融科技的应用，这意味着人们将主要通过互联网或手机应运来行进行金融或商业活动。在后疫情时代，金融欺诈的可能性更高。Experian plc 在 2022 年的报告中指出，英国金融产品在疫情后欺诈率上升了 33%<sup>[51]</sup>。如图 3-1，本文将传统金融欺诈分类为消费者服务和商品欺诈、投资欺诈、公司欺诈和保险欺诈。鉴于针对加密货币欺诈检测的算法研究较少，本文首先总结传统金融欺诈中的流行解决方案，然后提供关于特定算法如何检测加密货币欺诈的洞见。

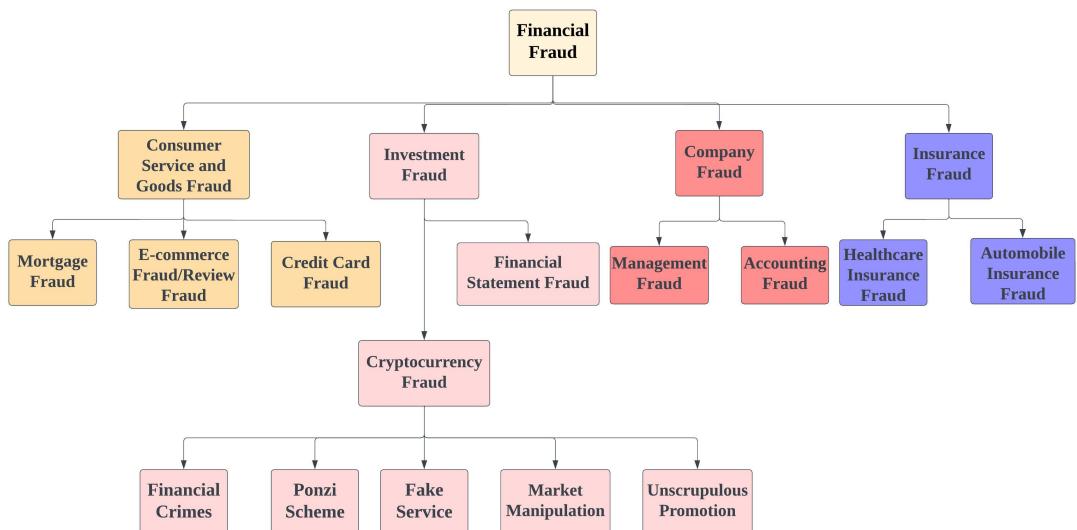


图 3-1 金融欺诈分类

Figure 3-1 Financial Frauds Categorization

#### 3.2.2 财务报表欺诈

财务报表欺诈是指公司故意篡改财务数据，旨在营造公司状况更加稳健的假象<sup>[52]</sup>。这种行为通常是出于达成收入目标、吸引投资者关注和提升公司价值的动机。在应用人工智能方法时，一个主要挑战是如何选择恰当的特征。Hajek 和 Henriques<sup>[53]</sup> 尝试利用诸如盈利能力、经营活动、资产结构、流动性、经营状况、财务杠杆和市值等各种财务指标来全面评估公司的财务状况。此外，Minhas 和 Hussain<sup>[54]</sup> 虽然采用了数值数据，但他们在预测财务报表欺诈时还运用了词袋 (bag of words) 模型和情感分析方法。

### 3.2.3 信用卡欺诈

信用卡的发明使用户能够为自己制定延期付款计划。信用卡记录了个人的身份信息和财务行为。Maniraj 等人<sup>[55]</sup> 将信用卡欺诈分类为简单盗窃、申请欺诈、破产欺诈、内部欺诈和伪造欺诈。学术界和工业界都关注伪造欺诈，因为它更难以检测，且这种欺诈所造成的经济损失最大。信用卡欺诈检测面临四大挑战：数据分布不均衡、用户行为动态变化、高维特征和误报率。不均衡的数据问题是欺诈活动与真实交易的比例远远小于正常交易。用户行为之所以动态，是因为消费行为和交易模式随时间变化其统计特性<sup>[56]</sup>。高维特征问题发生在交易历史特征过多的情况下，必须进行特征选择过程以提高算法效率。在误报率方面，银行需要决定选择哪种敏感度级别，因为顾客不希望被不断的欺诈警报信息打扰。

### 3.2.4 房贷欺诈

房贷欺诈有两种类型：为了财产的欺诈和为了利润的欺诈。为了财产的欺诈是指某人夸大其收入以购买房产。如果这个人没有违约，贷款机构不会实际遭受损失。为了利润的欺诈，欺诈者的目的是让贷款机构发放贷款然后携款潜逃。

### 3.2.5 电子商务欺诈/评论欺诈

电子商务平台的欺诈检测能确保用户和商家的安全公正环境。Zhang 等人<sup>[57]</sup> 指出，电子商务行业现有的欺诈检测系统存在性能衰退问题，无法适应欺诈者采取的对抗性行动。消费者评论在电商平台上对产品销量有直接影响。因此，欺诈者有动机通过发表负面评论来损害竞争对手的声誉。Luca 和 Zervas<sup>[58]</sup> 指出，用于检测虚假评论的深度学习算法简单且成本效益高。然而，这些算法的缺点在于缺乏可解释性。

### 3.2.6 保险欺诈

保险是个人或实体签订的一种合同，旨在补偿因意外造成的任何金钱损失。当个人或实体伪造信息以获得经济利益时，就发生了保险欺诈。保险欺诈存在于多个领域，包括房屋保险、汽车保险、农作物保险和健康保险<sup>[59]</sup>。目前，学术界似乎主要关注汽车保险和健康保险。在汽车保险欺诈中，发生时间和地点起着重要作用，欺诈者可能会策划车祸、计划车辆盗窃，并夸大损坏情况以获得索赔资格<sup>[60]</sup>。Villegas-Ortega 等人<sup>[61]</sup> 将健康保险欺诈定义为基于欺骗或故意误导的行为，以获得与健康保险提供的覆盖范围有关的非法利益。欺诈者会报告或重复虚假的医疗报告以索取保险覆盖。欺诈的其他表现包括为未经培训的人员提供的服务进行编码和收费。作者列出了各种因素（性别、年龄、主要种族等），并建议需要计算方法来识别关键因素。

### 3.3 应用算法

#### 3.3.1 支持向量机 (Support Vector Machine (SVM))

支持向量机 (SVM) 是一种流行的分类和回归算法。经典 SVM 的思想是构建一个超平面或所谓的决策边界，使两组数据点之间的距离达到最大。在金融欺诈检测中的应用是区分真实和欺诈数据。

假设有一个训练数据集  $\{(\mathbf{x}_i, y_i)\}$ ，其中  $\mathbf{x}_i \in \mathbb{R}^n$  是特征向量， $y_i \in \{-1, 1\}$  是类别标签。SVM 的目标是找到一个分割超平面来最大化两个类别之间的边界，这个超平面可以表示为：

$$\mathbf{w} \cdot \mathbf{x} + b = 0$$

其中  $\mathbf{w}$  是法向量， $b$  是偏置项。

SVM 通过以下优化问题来求解  $\mathbf{w}$  和  $b$ :

$$\begin{aligned} & \min_{\mathbf{w}, b} \frac{1}{2} \mathbf{w} \cdot \mathbf{w} \\ \text{s.t. } & y_i (\mathbf{w} \cdot \mathbf{x}_i + b) \geq 1, \quad i = 1, \dots, N \end{aligned}$$

对于非线性可分的情况，SVM 使用核技巧将输入空间映射到更高维的特征空间，在新的特征空间中进行线性分割。核函数  $K(\mathbf{x}_i, \mathbf{x}_j)$  计算输入空间中两个点  $\mathbf{x}_i$  和  $\mathbf{x}_j$  在特征空间的内积。

单类 SVM (One-Class SVM) 是一种用于异常点检测的算法，它试图找到一个最小的超球体来包围所有的数据点。假设数据集是  $\{\mathbf{x}_i\}_{i=1}^n$ ，单类 SVM 的目标是找到一个球体，使得大部分的数据点都在球体内部，同时球体的体积尽可能小<sup>[62]</sup>。以下是单类 SVM 的数学公式表示：

定义球体的中心为  $\mathbf{c}$  和半径为  $R$ ，问题可以表述为：

$$\begin{aligned} & \min_{\mathbf{c}, R, \{\xi_i\}} R^2 + \frac{1}{\nu n} \sum_{i=1}^n \xi_i \\ \text{s.t. } & \|\mathbf{x}_i - \mathbf{c}\|^2 \leq R^2 + \xi_i, \quad i = 1, \dots, n \\ & \xi_i \geq 0, \quad i = 1, \dots, n \end{aligned}$$

其中， $\xi_i$  是松弛变量，用于处理数据点可能不完全位于球体内部的情况， $\nu$  是一个介于 0 和 1 之间的参数，用于控制球体内点的比例以及松弛变量的和的上界。

在高维空间或非线性情况下，单类 SVM 使用核技巧，核函数  $K(\mathbf{x}_i, \mathbf{x}_j)$  被用来计算映射后的特征空间中的内积。

Ruff 等人<sup>[63]</sup> 将深度学习方法引入 SVDD (Support Vector Data Description)。它试图找到包围数据的最小球体，并通过最小化球体半径和处理异常值来实现。以下是 SVDD 的基本数学公式表示：

定义球体的中心为  $\mathbf{c}$  和半径为  $R$ , 对于数据集  $\{\mathbf{x}_i\}_{i=1}^n$ , SVDD 的目标是最小化球体的体积和异常点到球心的距离。问题可以表述为:

$$\begin{aligned} & \min_{\mathbf{c}, R, \{\xi_i\}} R^2 + C \sum_{i=1}^n \xi_i \\ \text{s.t. } & \|\mathbf{x}_i - \mathbf{c}\|^2 \leq R^2 + \xi_i, \quad i = 1, \dots, n \\ & \xi_i \geq 0, \quad i = 1, \dots, n \end{aligned}$$

其中,  $\xi_i$  是松弛变量, 用于处理数据点可能不完全位于球体内部的情况;  $C$  是一个正则化参数, 用于控制错误分类和球体大小之间的权衡。

在高维空间或非线性情况下, SVDD 可以结合核技巧, 通过核函数  $K(\mathbf{x}_i, \mathbf{x}_j)$  将数据映射到高维特征空间, 然后在该空间内寻找最小包围球。

Erfani 等人<sup>[64]</sup> 采用深度 SVDD 来解决欺诈检测数据集中的不平衡问题。提出的方法在效果上优于经典 SVM 和随机森林, 因为它同时具有非欺诈子采样和深度单类分类的优势。Deng<sup>[65]</sup> 将 SVM 应用于财务报表欺诈检测。数据集取自 1999 至 2006 年间中国上市公司。Deng 在实验中选取了 26 个财务比率, 并对样本数据进行了标准化处理, 以避免变量维度的差异。结果显示出相当高的分类准确性。Pai 等人<sup>[66]</sup> 结合了序贯前向选择技术和粒子群优化与 SVM, 以检测高层管理层的欺诈行为。该方法在台湾股市的 75 家上市公司数据上进行评估, 包括 25 家欺诈性财务报表 (FFS) 公司和 50 家非 FFS 公司。结果显示该算法有效且高效。该模型还为审计师提供了易于理解的结果。

Renjith<sup>[67]</sup> 使用 SVM 检测市场中的欺诈性销售尝试。作者与研究新型欺诈策略的欺诈专家合作, 将他们的意见作为检测模块的输入。作者得出结论, SVM 预测新未标记数据集的标签的能力帮助欺诈检测模块覆盖规则引擎不太有效的情景。Rtayli 和 Enneya<sup>[68]</sup> 创建了支持向量机-递归特征消除技术, 用于提取最佳预测特征。此外, 还使用了合成少数类过采样技术, 将不平衡数据集转换为平衡数据集。作者使用了三个真实世界的数据集, 并将每个数据集分成两个子数据集: 70% 用于训练, 30% 用于测试。这种技术使欺诈检测更加高效, 可应用于任何规模的数据。Subudhi 和 Panigrahi<sup>[69]</sup> 测试了 SVM 和四分之一球体 SVM 在检测欺诈电话方面的应用。QS-SVM 是 OC-SVM 的一种表现形式, 它在具有最小半径的超球体内封装特征空间数据点。使用现实挖掘数据集后, 作者得出结论, 该算法不仅成功地检测到欺诈行为, 而且将误报率控制在合理范围内。Qin<sup>[70]</sup> 将支持向量机和逻辑回归模型结合起来, 以识别会计欺诈。SVM 用于提高学习和泛化能力, 而逻辑回归用于解释每个变量。作者试图从资产负债表和损益表中检测财务报表欺诈, 并实现了 94% 的测试准确率。

### 3.3.2 自编码器 (Autoencoder)

自动编码器 (Autoencoder) 是一种无监督的神经网络, 它学习将输入数据  $\mathbf{x}$  编码成一个低维表示, 然后再从这个表示中重构出原始数据<sup>[71]</sup>。以下是自动编

**表 3-1 金融欺诈与支持向量机（SVM）之间的联系**  
**Table 3-1 The Linkage Between Financial Fraud and SVM**

欺诈类型	方法	结果
财务报表欺诈	SVM	分类准确率为 82.19%。
管理层欺诈	SVM	数据集 1 的平均测试准确率为 92%，数据集 2 为 81.33%。
移动欺诈	One-Class SVM	OCSVM 的执行时间小于 SVM。
电子商务欺诈	SVM	SVM 能预测新未标记数据集的标签。
信用卡欺诈	Deep SVDD	平均精度为 90%，ROC-AUC 为 93%。
信用卡欺诈	SVM-递归特征消除	即使在数据不平衡的情况下，也能以高预测率和较低的错误数识别和捕获欺诈交易。
会计欺诈	SVM	测试准确率为 94%。

码器的基本数学公式表示和 LaTeX 代码：

自动编码器由两部分组成：编码器（Encoder）和解码器（Decoder）。

编码器部分将输入数据  $\mathbf{x}$  转换为一个内部表示  $\mathbf{h}$ ，可以表示为：

$$\mathbf{h} = \sigma(\mathbf{W}_e \mathbf{x} + \mathbf{b}_e)$$

解码器部分将内部表示  $\mathbf{h}$  转换回接近原始输入的数据  $\mathbf{x}'$ ，可以表示为：

$$\mathbf{x}' = \sigma(\mathbf{W}_d \mathbf{h} + \mathbf{b}_d)$$

其中， $\mathbf{W}_e$  和  $\mathbf{W}_d$  是编码器和解码器的权重矩阵， $\mathbf{b}_e$  和  $\mathbf{b}_d$  是偏置项， $\sigma$  是非线性激活函数。

自动编码器通过最小化重构误差来训练网络，通常使用如均方误差等损失函数：

$$L(\mathbf{x}, \mathbf{x}') = ||\mathbf{x} - \mathbf{x}'||^2$$

稀疏自编码器通过稀疏激活增加其隐藏节点。但为了施加稀疏性约束，通常会添加曼哈顿距离（L1）和 Kullback-Leibler 散度（KL）散度作为正则化<sup>[72]</sup>。KL 散度是衡量两个分布差异的标准函数<sup>[73]</sup>。总的损失函数  $L$  可以表示为：

$$L(\mathbf{x}, \mathbf{x}', \mathbf{h}) = ||\mathbf{x} - \mathbf{x}'||^2 + \beta \sum_{j=1}^s KL(\rho || \hat{\rho}_j)$$

其中， $\beta$  是稀疏性惩罚项的权重， $KL(\rho || \hat{\rho}_j)$  是隐藏层第  $j$  个神经元激活值  $\hat{\rho}_j$  与期望稀疏度  $\rho$  之间的 KL 散度。

去噪自编码器旨在破坏输入数据，输出将被重构为未损坏的数据<sup>[74]</sup>。鲁棒深度自编码器遵循鲁棒 PCA 的直觉。一个过滤层被添加到自编码器中。过滤层将数据的异常部分和正常部分分离<sup>[75]</sup>。变分自编码器假设潜在表示  $z$  的维度没有简单的解释，并可以从简单分布中抽取  $z$  的样本<sup>[76]</sup>。

当前研究的主流是将自编码器与其他机器学习算法（如决策树和支持向量机）结合起来。Dong 等人<sup>[77]</sup>提出了一个端到端可训练的统一模型，以自编码器和随机森林组成。作者在亚马逊上的假评论上测试了这种方法，结果表明它以 96% 的准确率超越了一系列最先进的算法。Pumsirirat 和 Liu<sup>[78]</sup>比较了自编码器和受限玻尔兹曼机（RBM）在德国、澳大利亚和欧洲数据集上用于信用卡欺诈检测的性能。作者得出结论，自编码器适合实时响应系统。Misra 等人<sup>[79]</sup>提出使用自编码器结合多层感知器、k-最近邻和逻辑回归来检测信用卡欺诈。数据集包含 2013 年欧洲持卡人进行的信用卡交易。自编码器的架构是一个 2 层编码网络和一个 2 层解码网络。实验表明，提出的方法在检测欺诈时在精度和召回率之间保持了良好的平衡。Wong 等人<sup>[80]</sup>提出了一种解决商业领域类别不平衡问题的方法，该方法使用成本敏感的堆叠去噪自编码器集成。堆叠去噪自编码器假设误分类多数类和少数类示例的成本是相等的。通常情况并非如此。因此，作者在原始算法中添加了一个成本向量，并在实际应用的数据集上进行了实施：欺诈检测、直接营销、客户流失预测和信用卡违约支付。提出的方法在三个评估指标上优于其他方法：真阳性率（TPR）、真阴性率（TNR）和曲线下面积（AUC）。该方法还实现了非常低的平均泛化差距，不太可能出现过拟合问题。Zamini 和 Montazer<sup>[81]</sup>使用深度自编码器和 k 均值聚类来捕获最大量的欺诈交易，并降低误报率（FNR）。所实验的数据集高度不平衡，因为欺诈交易与非欺诈交易的比例为 0.17%。该方法在召回率方面优于其他算法。Anh 等人<sup>[82]</sup>分析了使用变分自编码器（Variational Autoencoder）和倾斜随机森林（Oblique Random Forest）进行信用卡和电子商务交易级别的欺诈检测。ORF 作为二元分类器，采用特征的线性组合在每个节点生成倾斜超平面。该模型在亚马逊评论数据集和信用卡数据集上达到了超过 97% 的准确率，并在精度、召回率和 F1 分数方面取得了类似的结果。

### 3.3.3 图神经网络（Graph Neural Network）

图神经网络（GNN）利用图结构数据来预测图级（整个图的属性）、节点级（图中每个节点的身份或角色）和边级（边的预测）任务。节点、边和图的全局上下文可以转换为矩阵。GNN 使用图作为输入（节点、边和全局上下文），并且每个组件通过多层感知器更新，以产生新的图<sup>[83]</sup>。

在 GNN 中，每个节点  $v$  的特征向量表示为  $\mathbf{x}_v$ ，节点状态在每次迭代  $k$  中更新，可以表示为：

$$\mathbf{h}_v^{(k+1)} = f \left( \mathbf{h}_v^{(k)}, \bigoplus_{u \in \mathcal{N}(v)} g(\mathbf{h}_u^{(k)}, \mathbf{e}_{uv}) \right)$$

其中， $\mathbf{h}_v^{(k)}$  是节点  $v$  在第  $k$  次迭代的状态向量， $\mathcal{N}(v)$  表示节点  $v$  的邻居节点集合， $\mathbf{e}_{uv}$  是节点  $u$  和  $v$  之间的边的特征向量， $f$  和  $g$  是可学习的函数，通常通过神经网络实现， $\bigoplus$  表示聚合操作，比如求和、求平均或者求最大值。

图生成对抗网络（GraphGAN）在学习过程中有两个模型：生成器和鉴别器。

表 3-2 金融欺诈与自编码器之间的联系

Table 3-2 The Linkage Between Financial Fraud and Autoencoder

欺诈类型	方法	结果
信用卡欺诈	自编码器和 K 均值	TPR 为 81%，准确率为 98.9%。
信用卡欺诈	自编码器和受限玻尔兹曼机	自编码器适用于实时的欺诈检测。
信用卡欺诈	自编码器和 K 最近邻、多层感知器、逻辑回归	自编码器与 KNN 分类器在检测欺诈方面在精度和召回率之间保持良好平衡。
电商评论欺诈	自编码器和决策森林	超越了一系列最先进的方法，准确率达到 96%。
信用卡欺诈	堆叠去噪自编码器	堆叠自编码器在 TPR、TNR 和 AUC 方面表现优于其他方法。
信用卡欺诈和电子商务欺诈	变分自编码器 (Variational Autoencoder) 和倾斜随机森林 (Oblique Random Forest)	提出的算法准确率超过 97%，在精度和召回率方面也取得了类似的结果。

生成器试图产生鉴别器无法区分的顶点。在这个过程中，真实的连接分布将从这过程中学习到。该算法在社交关系数据集上执行，GraphGAN 超越了所有基准模型，并实现了 0.232 的准确率。尽管数据集并不专门用于欺诈检测，但关系的表示对检测电子商务欺诈有用<sup>[84]</sup>。

Liu 等人<sup>[85]</sup> 在欺诈检测中识别出三个不一致性：上下文（欺诈者伪装成常规实体）、特征（垃圾评论）和关系（多个账户）。作者设计了一个新的 GNN 框架来解决这些不一致性，并且该算法在 80% 和 60% 的训练数据下的 F1 和 AUC 分数上优于其他模型。Cheng 等人<sup>[86]</sup> 利用 GNN 学习位置和时间信息，因为手动生成特征需要领域知识。该算法可以每秒预测约 10,000 笔在线交易，并满足银行的效率要求。Wang 等人<sup>[87]</sup> 提出了 SemiGNN 来解决金融欺诈检测中未标记数据的问题。注意力机制为模型增加了可解释性。该模型在支付宝数据集上表现最佳，无论是在 AUC 分数还是 Kolmogorov-Smirnov 图表（正负分布之间的分离程度）方面均是如此。Zhang 等人<sup>[57]</sup> 指出，传统算法没有考虑欺诈者的对抗行为，因此模型性能随时间衰退。作者使用 competitive graph neural networks (CGNN) 来检测电子商务欺诈。CGNN 由一个图编码器和两个图解码器组成。这两个解码器将竞争以获得更小的重构误差。该模型在与经典自编码器相比获得了最佳的 AUC 分数。

### 3.3.4 生成对抗网络 (Generative Adversarial Network)

生成对抗网络 (GAN) 主要用于非结构化数据，如视频和图像，由两个子网络组成：生成器 (Generator) 和判别器 (Discriminator)。生成器试图生成与真实数据尽可能相似的数据，而判别器试图区分真实数据和生成器生成的假数据。

生成器  $G$  接收一个随机噪声向量  $\mathbf{z}$  作为输入，并生成数据  $\mathbf{x}' = G(\mathbf{z})$ 。

表 3-3 金融欺诈与图神经网络之间的联系

Table 3-3 The Linkage Between Financial Fraud and GNN

欺诈类型	方法	结果
电子商务欺诈	GraphGAN	GraphGAN 超越所有基准模型，准确率达到 0.232
电子商务欺诈	GNN	该算法在 80% 和 60% 的训练数据下的 F1 和 AUC 分数上优于其他模型
电子商务欺诈	带有注意力机制的 GNN	该算法可以每秒预测大约 10,000 笔在线交易，满足银行的效率要求。
电子商务欺诈	Semi-GNN	该模型在支付宝数据集上的 AUC 分数和 Kolmogorov-Smirnov 图表上表现最佳。
电子商务欺诈	CGNN	与经典自编码器相比，该模型获得了最佳的 AUC 分数。

判别器  $D$  接收一个数据样本（可以是真实数据  $\mathbf{x}$  或生成数据  $\mathbf{x}'$ ）作为输入，并输出该样本为真实数据的概率  $D(\mathbf{x})$ 。

GAN 的训练目标是使生成器能生成尽可能接近真实数据的数据，同时使判别器能准确区分真实数据和生成数据。这可以通过以下的最小最大游戏来表示：

$$\min_G \max_D V(D, G) = \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [\log D(\mathbf{x})] + \mathbb{E}_{\mathbf{z} \sim p_{\mathbf{z}}(\mathbf{z})} [\log(1 - D(G(\mathbf{z})))]$$

GAN 主要有两种用途：一种是将 GAN 作为基础模型，因为异常情况与正常实例的分布不同。另一种方法是将 GAN 作为解决欺诈检测中数据不平衡问题的工具，因为异常情况在整个数据集中所占比例较小。GAN 提供了一种增加异常数据集的方法，使分类器更好地检测欺诈。

Zheng 等人<sup>[88]</sup> 采用单类对抗网络进行欺诈检测。LSTM-自编码器能够通过潜在空间捕获用户活动的信息。生成器旨在低密度区域生成正常用户的补充样本，鉴别器旨在区分真实和补充的正常用户。该方法在维基百科欺诈数据集上进行了测试，能够检测到位于正常用户区域之外的恶意用户。Chen 等人<sup>[89]</sup> 提出了稀疏自编码器和 GAN 的组合算法。SAE 产生正常交易的稀疏特征表示，并将其作为输入提供给 GAN。GAN 的生成器学习欺骗鉴别器。结果优于 SVDD 和 One-Class Gaussian Process(GP)。Ba<sup>[90]</sup> 在一组欺诈交易上训练了一系列 GAN，然后生成假欺诈交易以平衡数据。作者还关注分类预测能力，因为错误分类正常交易可能会威胁到商户或金融机构与客户的关系。Wasserstein-GAN 在训练中更稳定，并产生比其他 GAN 更真实的欺诈交易。Charitou 等<sup>[91]</sup> 声称他们的半监督 GAN 不需要过采样技术就能产生良好的分类结果。算法架构包含稀疏自编码器和 GAN。它应用于在线赌博中的洗钱问题。实验表明，与逻辑回归、随机森林和多层感知器相比，F1 分数提高了 3.64%。Charitou 等人<sup>[92]</sup> 专注于通过生成新的高质量实例来解决结构化数据中的类别不平衡问题。为了改进 GAN 训练，Synthetic Data Generation (SDG-GAN) 采用了特征匹配损失而非常规损失。该模

型在信用卡欺诈数据集上实现了最高的 F1 分数，为 91.31%。在现实世界的赌博数据集上，与基于规则的系统相比，SDG-GAN 将识别率（F1 分数）提高了 5%。Pandey 等人<sup>[93]</sup> 在 WGAN-Gradient Policy (GP) 模型之上分别使用三重网络和连体网络作为辅助损失，以学习更具辨别力的欺诈样本。此外，还使用基于神经网络的分类器与 WGAN-GP 一起处理边界扭曲问题。作者得出结论，该算法在信用卡数据集上的召回率提高了高达 6%，精度提高了 3%。

**表 3-4 金融欺诈与生成对抗网络之间的联系**

**Table 3-4 The Linkage Between Financial Fraud and GAN**

欺诈类型	方法	结果
信用卡欺诈	稀疏自编码器和 GAN	精度和 F1 分数在其他算法中最高。
电商评论欺诈	单类对抗网络	鉴别器能区分正常用户和欺诈用户。
信用卡欺诈	Wasserstein GAN	训练中更稳定，生成的欺诈交易比其他 GAN 更真实。
信用卡欺诈	稀疏自编码器和 GAN	F1 分数为 89.85%，比当前检测系统提高了 3.64%。
信用卡欺诈	Wasserstein GAN	在召回率上提高了最多 6%，在精度上提高了 3%。
信用卡欺诈	GAN	与基于规则的系统相比，F1 分数提高了 5%。

### 3.3.5 强化学习 (Reinforcement Learning)

Mnih 等人<sup>[94]</sup> 通过将强化学习 (RL) 应用于玩雅达利游戏。他们的算法在测试的七款游戏中的六款上取得了最先进的结果，且无需调整架构或超参数。

在强化学习中，智能体在每个时间步  $t$  做出动作  $a_t$ ，接收状态  $s_t$  和奖励  $r_t$ ，目标是学习一个策略  $\pi$ ，使得累积奖励  $R_t = \sum_{k=0}^{\infty} \gamma^k r_{t+k+1}$  最大化，其中  $\gamma$  是折扣因子。

价值函数  $V^\pi(s)$  表示从状态  $s$  开始，遵循策略  $\pi$  能获得的预期回报：

$$V^\pi(s) = \mathbb{E}_\pi [R_t | s_t = s]$$

动作价值函数  $Q^\pi(s, a)$  表示在状态  $s$  采取动作  $a$ ，然后遵循策略  $\pi$  能获得的预期回报：

$$Q^\pi(s, a) = \mathbb{E}_\pi [R_t | s_t = s, a_t = a]$$

Shen 和 Kurshan<sup>[95]</sup> 提出使用基于深度 Q 学习的方法来防止欺诈损失，同时保持在日常警报处理能力限制之内。作者们确定，由于个人行为可能随时间改变，静态阈值并不现实。因此，他们使用一个智能体每小时选择一个阈值。在 3 个月的时间里，与每月最佳静态阈值相比，它提供了 9.6% 的改进。Zhao 等人<sup>[96]</sup> 旨在使用强化学习和行动规范惩罚来识别电子商务欺诈，特别是当欺诈性卖家购买自己的产品以伪造大量交易时。作者将平台的决策问题定义为马尔可夫决策过程 (MDP)，其行动是确定排名系统的参数。结果显示，它在可扩展性和解决方案质量方面优于普通的深度确定性策略梯度 (DDPG) 和启发式方法。

Zhinin-Vera 等人<sup>[97]</sup>设计了 Q-信用卡欺诈检测器 (Q-CCFD)，包括一个自编码器、一个中介网络和一个强化学习环境。自编码器将其学习到的特征表示传递给中介网络，以确定交易是欺诈性的还是真实的。RL 扮演人类专家的角色，决定中介网络的分类是否正确。结果显示，Q-CCFD 在使用不平衡数据集时更适应真实世界的问题。Mead 等人<sup>[98]</sup>决定使用强化学习来检测信用卡欺诈，因为欺诈者不断调整其策略以击败欺诈检测模型。在 RL 设置中，智能体试图确定最佳的交易集合，以从银行的欺诈分类器（环境）中窃取资金。作者认为，频繁且规律的变化会导致欺诈智能体学习最大化成功欺诈交易的能力下降。Dou 等人<sup>[99]</sup>使用纳什强化学习研究电子商务网站上的虚假评论。这种算法利用迷你最大博弈的纳什均衡，并在常规 RL 中添加了三个新颖之处：

- (1) 成本敏感损失函数更注重收益而非准确度。
- (2) 垃圾邮件策略依赖于未标记的数据且无需训练参数，使其更能抵抗检测器。
- (3) 发送垃圾邮件者将变化其混合策略以最大化效果，而检测器将重新配置其检测策略以最小化效果。

El-Awady<sup>[100]</sup>提出了一种具有自适应应力测试的欺诈检测系统，以应对信用卡欺诈。RL 中的奖励函数旨在作为主要目标找到失败事件，并作为次要目标最大化路径可能性。这种设计的假设是，欺诈者会尽快执行欺诈活动，并且意识到被盗卡的年龄。作者使用 RL 展示了欺诈者为了最大化利润可能采取的最有可能的路径。该算法实现了 96.8% 的准确率、3.85% 的误报率和 0.1% 的未捕获欺诈率。

**表 3-5 金融欺诈与强化学习之间的联系**  
**Table 3-5 The Linkage Between Financial Fraud and RL**

欺诈类型	方法	结果
信用卡欺诈	强化学习 (RL)	该技术的有效性有限，过于频繁地更换分类器并不有助于改善结果。
电子商务欺诈	深度强化学习	具有更大的可扩展性和解决方案质量。
信用卡欺诈	基于 Q 网络的强化学习	相比每月最佳静态阈值，提供了 9.6% 的改进。
信用卡欺诈	强化学习 (RL)	在准确识别欺诈方面表现出色。
电商评论欺诈	强化学习 (RL)	该算法更擅长识别虚假的长篇评论。
信用卡欺诈	强化学习 (RL)	该算法擅长在大量交易中检测欺诈行为。

### 3.3.6 决策树/随机森林 (Decision Tree/Random Forest)

决策树是一种非参数的监督学习算法。它适用于欺诈检测，因为它具有分类能力、数据准备简单和易于解释的特点。与上文提到的其他深度学习方法不同，决策树可以可视化，甚至让业余人士也能参与算法的制定。随机森林本质上是一系列决策树的集合，它根据多数投票做出最终决策。

给定训练数据集  $D = \{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$ , 其中  $x_i$  是特征向量,  $y_i$  是对应的标签。决策树的构建过程包括:

在每个节点, 选择最佳的特征  $f$  和划分阈值  $\theta$  来最大化信息增益 (或其他度量标准) :

$$IG(D_p, f) = I(D_p) - \left( \frac{N_{\text{left}}}{N_p} \right) I(D_{\text{left}}) - \left( \frac{N_{\text{right}}}{N_p} \right) I(D_{\text{right}})$$

其中:

- $IG$  是信息增益
- $D_p, D_{\text{left}}, D_{\text{right}}$  分别是父节点、左子节点、右子节点的数据集
- $N_p, N_{\text{left}}, N_{\text{right}}$  是对应节点的样本数量
- $I$  是不纯度度量标准 (如基尼不纯度或熵)

对于分类问题, 熵作为不纯度度量, 定义为:

$$I_H(D) = - \sum_{i=1}^m p_i \log_2(p_i)$$

其中  $p_i$  是第  $i$  个类的比例。

对于一个有  $B$  棵树的随机森林, 模型的预测可以表示为:

$$\hat{y} = \text{mode}(\{\hat{y}_1, \hat{y}_2, \dots, \hat{y}_B\})$$

其中  $\hat{y}_b$  是第  $b$  棵树的预测。

$$\hat{y} = \frac{1}{B} \sum_{b=1}^B \hat{y}_b$$

其中  $\hat{y}_b$  是第  $b$  棵树的预测。

在每次分裂选择特征时, 随机森林从特征的一个随机子集中选择, 以增加森林的多样性并提高模型的泛化能力。

Askari 和 Hussain<sup>[101]</sup> 开发了一种使用直觉模糊逻辑和 C4.5 决策树的决策树 IFDTC4.5 来检测欺诈。在新加坡银行数据集上的实验显示, IFDTC4.5 的准确性随窗口大小的增加而提高, 作者认为它在计算上是高效的。这种提出的技术比现有技术如 SVM 和随机森林表现更好。Wang 等人<sup>[102]</sup> 应用决策树来解决供应欺诈问题。作者选择具有最大指数增益的基尼系数的特征。决策树在预测产品销售方面达到了 99.12% 的准确率。Cody 等人<sup>[103]</sup> 发现决策树学习可用于消费者能源消费中的欺诈检测。能源欺诈发生在消费者的智能电表报告与实际使用的能源不一致时。使用无噪音的数据集来学习消费模型, 并使用模拟的欺诈数据来验证模型。均方根误差的差异决定了行为是真实还是欺诈。结果显示决策树可用于数据组, 准确预测未来值。Sahin 等人<sup>[104]</sup> 提出了一种成本敏感的决策树方

法，在选择每个非终端代码的分割属性时最小化误分类成本之和。这种算法的动机是解决信用卡欺诈检测中的不平衡数据分布问题。该模型恢复了最多的财务损失。Khine 和 Khin<sup>[105]</sup> 采用在线提升方法，以极快决策树（EFDT）作为基础学习器。EFDT 以增量方式构建树，在选择最佳节点方面有最短延迟。作者得出结论，EFDT 在基准信用卡欺诈数据集上表现有效，并且对概念漂移有一定的内在接受能力。Save 等人<sup>[106]</sup> 发明了一种结合 Luhn 算法和 Hunt 算法的新型决策树模型。Luhn 算法用于检查账单地址是否与邮寄地址匹配。如果匹配，它将增加交易为真实交易的可能性。结果显示非常低的误报率。

表 3-6 金融欺诈与决策树/随机森林之间的联系

Table 3-6 The Linkage Between Financial Fraud and Decision Tree/Random Forest

欺诈类型	方法	结果
信用卡欺诈	成本敏感决策树	该算法有助于节省比其他算法更多的财务资源。
能源欺诈	决策树	决策树可应用于数据组，准确预测未来值。
信用卡欺诈	随机森林	准确率达 90%。
信用卡欺诈	极快决策树	在基准数据集上表现良好，且对概念漂移有良好抵抗力。
电子商务欺诈	基于模糊逻辑的决策树	该算法的结构使得处理过程在计算上高效。
供应链欺诈	决策树	准确率为 99.12%。

### 3.3.7 K 最近邻 (K Nearest Neighbor)

K 最近邻 (KNN) 是一种基于距离的分类和回归问题算法。它的假设是，相似的数据存在于相似的邻域中，并且它使用距离作为衡量相似性的手段。由于 KNN 是非参数的，它不会对数据做任何假设，也不需要训练集<sup>[104]</sup>。

给定一个训练数据集  $D = \{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$ ，其中  $x_i$  是特征向量， $y_i$  是对应的标签。对于一个新的实例  $x$ ，k-NN 算法执行以下步骤：

- (1) 计算实例  $x$  与训练集  $D$  中每个实例  $x_i$  之间的距离  $d(x, x_i)$ 。
- (2) 对所有计算得到的距离进行排序，并选择距离最近的  $k$  个点，形成集合  $N_k(x)$ 。
- (3) 对于分类问题：

$$\hat{y} = \operatorname{argmax}_j \sum_{i \in N_k(x)} I(y_i = j)$$

其中， $I$  是指示函数，如果  $y_i = j$  为真，则  $I(y_i = j) = 1$ ，否则为 0。

- (4) 对于回归问题：

$$\hat{y} = \frac{1}{k} \sum_{i \in N_k(x)} y_i$$

常用的距离度量包括欧氏距离、曼哈顿距离和明可夫斯基距离等。例如，欧

氏距离定义为：

$$d(x, x_i) = \sqrt{\sum_{j=1}^m (x_j - x_{ij})^2}$$

其中， $m$  是特征的数量， $x_j$  和  $x_{ij}$  分别是  $x$  和  $x_i$  在第  $j$  个特征上的值。

$k$  的选择会影响算法的结果。较小的  $k$  值意味着噪声将对结果有更大的影响，而较大的  $k$  值则使计算成本更高并可能导致过度平滑，从而忽略了局部结构的细节。

Badriyah 等人<sup>[107]</sup> 使用基于最近邻的方法和统计方法来检测欺诈的发生。数据集包含 33 个现有属性，结果显示 KNN 与支持向量机（SVM）和基于密度的方法相比，取得了最好的结果，准确率达到 99.9%，F 测量值为 99.6%。Makki 等人<sup>[108]</sup> 提出了一种新的 KNN 模型，使用余弦相似度来解决信用卡欺诈中的数据不平衡问题。该算法用两个向量之间的余弦相似度替换了 KNN 中使用的欧几里得距离。与简单投票或加权距离方法相比，使用余弦相似度在灵敏度方面更好。提出的 COS-KNN 在精确率-召回率曲线（AUPRC）和 F1 分数方面优于所有方法。Malini 和 Pushpa<sup>[109]</sup> 认为，KNN 和异常值检测方法可以降低误报率并提高欺诈检测率。在实验中，作者决定计算任何传入交易与新传入交易的最近点，较大的  $K$  值有助于减少数据中的噪音。结果显示 KNN 在检测信用卡欺诈方面准确且有效。Ganji 和 Mannem<sup>[110]</sup> 提出了一种逆向 KNN 算法来检测信用卡欺诈，因为它只需要扫描一次。作者声称该模型的优势包括两个方面：

- (1) 丢失和被盗卡特征使得模型更容易阻止欺诈交易。
- (2) 验证过程是顺序的，因此更容易检测到无效号码。

实验结果表明，提出的方法是高效且有效的。

表 3-7 金融欺诈与 K 最近邻的联系

Table 3-7 The Linkage Between Financial Fraud and KNN

欺诈类型	方法	结果
信用卡欺诈	KNN	KNN 占用的内存空间很少。
信用卡欺诈	KNN	KNN 在线环境中效率高。
信用卡欺诈	成本敏感 KNN	它的表现优于其他算法，除了决策树和单类 SVM。
保险欺诈	KNN	KNN 有助于特征选择过程，提高欺诈检测的准确性。

### 3.3.8 隐马尔可夫模型（Hidden Markov Model）

HMM（隐马尔可夫模型）是基于马尔可夫模型假设的统计模型。它包含一个可见的观测序列和一个不可见的状态序列<sup>[111]</sup>。由于通常无法知道交易是否欺诈，因此 HMM 的直觉适用于欺诈检测问题。交易序列模仿了个人的消费行为，是可观察的，因此可以将 HMM 应用于金融欺诈检测。

一个 HMM 可以通过以下元素定义：

- $N$ : 隐藏状态的数目。
- $M$ : 观测符号的数目。
- $A$ : 状态转移概率矩阵，其中  $A_{ij}$  表示从状态  $i$  转移到状态  $j$  的概率。
- $B$ : 观测概率矩阵，其中  $B_{ij}$  表示在状态  $i$  观测到符号  $j$  的概率。
- $\pi$ : 初始状态概率向量，其中  $\pi_i$  表示系统在时间  $t = 1$  时处于状态  $i$  的概率。

HMM 有两个基本假设：

- (1) 齐次马尔可夫性假设：隐藏的状态序列符合马尔可夫性质，即下一个状态的概率仅依赖于当前状态。

$$P(q_{t+1}|q_1, q_2, \dots, q_t) = P(q_{t+1}|q_t)$$

- (2) 观测独立性假设：任何时刻的观测仅依赖于该时刻的状态，与其他时刻的状态及观测无关。

$$P(o_t|q_1, q_2, \dots, q_t, o_1, o_2, \dots, o_{t-1}) = P(o_t|q_t)$$

在 HMM 中，通常有三个基本问题：

- (1) 评估问题：给定模型参数和观测序列，计算在该模型下观测序列的概率。通常使用前向算法或后向算法解决。
- (2) 解码问题：给定模型参数和观测序列，找到最有可能产生这些观测的隐藏状态序列。维特比算法是解决这个问题的常用方法。
- (3) 学习问题：给定观测序列，估计模型参数  $(A, B, \pi)$ ，使得在该模型下观测序列的概率最大。可以使用 Baum-Welch 算法（一种特殊的 EM 算法）来解决。

Robinson 和 Aria<sup>[112]</sup> 通过比较连续基于观察生成的 HMM 来构建他们的 HMM，以此来识别异常情况。他们使用 KL 散度来比较两个 HMM 连续接受概率的差异，并认为该方法在处理欺诈检测方面简单、高效且有效。

Sathyapriya 和 Thiagarasu<sup>[113]</sup> 为信用卡欺诈检测设计了一个三阶段的 HMM 模型：生成观测符号、HMM 训练和欺诈检测。在训练阶段，基于每个客户之前的购买模式和行为参数（如交易金额、地点、时间和产品）来构建个人支出模型。作者声称这种方法能够处理大量交易数据，具有良好的扩展性。

传统的特征工程方法没有将卖方的交易历史和交易历史视为一个序列。因此，Lucas 等人<sup>[114]</sup> 提出使用 HMM 生成基于历史的特征。该算法在面对面交易和电子商务交易中都显示出最佳稳定性，并且是训练速度最快的方法。

### 3.3.9 其他检测算法 (Other Fraud Detection Methods)

遗传算法用于通过构建染色体列表来解决优化问题。受自然选择的启发，通过模拟自然进化过程来获得最佳解决方案<sup>[115]</sup>。Yan 等人<sup>[116]</sup> 指出，传统的遗传算法容易陷入局部极值，因此他们提出了一种新的自适应遗传算法。作者决定根

**表 3-8 金融欺诈与隐马尔可夫模型的联系****Table 3-8 The Linkage Between Financial Fraud and HMM**

欺诈类型	方法	结果
信用卡欺诈	HMM	在在线欺诈检测中具有可扩展性。
电子商务欺诈	HMM	在金融欺诈检测中简单且高效。
信用卡欺诈和电子商务欺诈	多视角 HMM	该算法在检测电子商务欺诈方面稳定且快速。

据适应度从大到小对个体进行排名，并淘汰排名最低的四分之一。实验是在一家车辆保险公司的历史索赔数据上进行的。结果表明，提出的方法比传统的遗传算法具有更快的收敛速度和更好的预测准确性。

逻辑回归是一种统计模型，试图捕捉一个或多个二元因变量之间的关系。Alenzi 和 Aljehane<sup>[117]</sup> 使用包含欧洲信用卡持卡人交易的数据集。作者认为，逻辑回归比线性回归更先进，因为它能更好地分离重叠数据。尽管与 KNN 和 VC 分类器相比，逻辑回归的响应时间最长，但它达到了最佳的准确性。

模糊逻辑旨在模仿人类决策过程，同时承认其模糊性和不准确性。它类似于天气预报，其中下雨或晴天的概率总是在变化且不确定。Marah 等人<sup>[118]</sup> 采用模糊逻辑来检测国际电话中的欺诈行为。作者使用三角形会员函数来处理所有检测模式。他们从数据库中获得检测模式的最大值和最小值，然后计算会员值。欺诈检测系统表明，使用模糊逻辑在处理大量输入数据时变得更加灵活和可靠。

贝叶斯网络通过使用概率的概念来计算不确定性。Song 等人<sup>[119]</sup> 使用贝叶斯网络来检测散装货物盗窃中的欺诈行为。货物在运输过程中大多丢失。传统方法被证明是昂贵、精确和反应式的。贝叶斯网络可以发现风险组成部分之间的关系。它还具有很强的可解释性。曲线下面积得分达到 0.834%。因此，贝叶斯网络被证明是预防货物盗窃的有力工具。

**表 3-9 金融欺诈与其他检测算法的联系****Table 3-9 The Linkage Between Financial Fraud and Other Fraud Detection Methods**

欺诈类型	方法	结果
保险欺诈	模糊 C 均值聚类 (Fuzzy C-Means Clustering)	该模型通过控制不平衡的类分布来降低误报率。
信用卡欺诈	逻辑回归	响应时间最长但准确度最高。
汽车欺诈	自适应遗传算法	该模型收敛速度快，且不太容易陷入局部最小值。
货物欺诈	贝叶斯网络	准确度和召回值均大于 0.8。

## 3.4 金融欺诈检测中的挑战与未来发展展望

本节总结了金融欺诈检测技术和金融欺诈问题的研究成果，并将这些成果应用于加密货币欺诈检测。机器学习算法如 SVM、决策树/随机森林、KNN 和 HMM 在检测金融欺诈方面更为高效。

### 3.4.1 加密货币欺诈

加密货币作为区块链技术的产品，是一种基于分布式公共账本的新支付方式。发布在链上的交易对所有人都可见，但交易者可以保持匿名。萨尔瓦多最近成为第一个接受比特币作为法定货币的国家。此外，像 Doge 和 Shiba 这样的代币为其早期投资者创造了异常高的回报。零售投资者被新闻和常常不切实际的回报所吸引。零售资金的涌入为欺诈活动创造了温床。最著名的操纵手段是“拉高出货”骗局。Villegas-Ortega 等人<sup>[120]</sup> 描述说，从一开始，协调购买增加了交易活动并开始推高价格。零售投资者被拉升吸引并开始购买。最终，操纵者会以更低的价格抛售他们的头寸。如果没有实际项目支持代币，价格将跌至零。如果代币的钱包地址没有锁定，意味着所有者可以自由地将资金转移到另一个钱包，这种欺诈将转变为“拉毯子”骗局。在这个骗局中，投资者会损失所有资金。传统的股票操纵欺诈检测方法围绕价格、交易量和买卖订单频率。来自 Discord 和 Telegram 的文本数据更加重要，因为欺诈者喜欢玩弄投资者的情绪。尽管有“拉高出货”骗局，Jung 等人<sup>[121]</sup> 报告说，智能合约利用代码的不可变性吸引用户。然而，欺诈者可能修改参数以实现自己的利益。需要一个自动化代码审查系统来检测这种类型的欺诈。除了在一级市场上交易之外，Underwood.D.Barbara 指出<sup>[122]</sup>，大多数交易平台缺乏控制手段来避免滥用行为，如拉高出货活动。目前的形势要求监管机构和研究人员合作，以产生一个全面的欺诈检测系统。

### 3.4.2 加密货币欺诈类别

**金融欺诈:** 由于比特币可以在全球范围内即时转移，且政府无法监管持有比特币的加密货币钱包，因此欺诈者可能会利用加密货币进行金融犯罪，如洗钱、逃税和贿赂。

**庞氏骗局:** 许多去中心化应用程序，如游戏金融（玩家赚钱）和体育金融（运动赚钱），声称自己是金融创新，并承诺为用户带来高额投资回报。庞氏骗局需要新的采纳者来维持系统运行。以“Stepn”为例，这款移动赚取游戏宣称用户可以通过步行、慢跑或户外跑步来赚取代币。它还有一个愿景，就是吸引数百万人采纳更健康的生活方式，同时帮助实现碳中和。然而，Stepn 的奖励代币价格从 6 美元暴跌至 0.05 美元<sup>[123]</sup>。

**假冒服务:** 诈骗者假冒知名公司、投资经理、名人、网络“恋爱对象”、政府机构、执法部门和公用事业公司，向加密货币用户提供假服务。诈骗者可以使用各种方法诱骗受害者放弃他们的加密资产。Brandom, R 报道<sup>[124]</sup>，攻击者从 Decentraland 和 Bored Ape Yacht Club 窃取代币。Opensea 用户也有数百个非同质

化代币被盗。

**市场操纵:** 加密货币市场操纵包括拉高出货、前置交易、刷单和虚假交易。最突出的欺诈是拉高出货骗局。Nghiem 等人<sup>[125]</sup>描述说，诈骗者组织并利用媒体渠道人为地抬高代币价格，然后迅速出售以从买家那里获利。

**不道德推广:** 诈骗者支付给社交媒体影响者或名人，帮助他们推广投机性代币。

### 3.5 本章小结：从传统金融欺诈检测（FFD）到加密货币欺诈检测的知识转移

深度学习模型以橙色表示，机器学习模型以粉色表示。发现除了 KNN 之外的所有算法都可以用来检测信用卡欺诈和电子商务欺诈。KNN 可以检测保险欺诈，而 SVM 能够检测管理欺诈、财务报表欺诈和会计欺诈。加密货币欺诈检测中的金融犯罪可以被视为传统金融检测问题，因为除了欺诈者在加密货币中犯罪之外，它们本质上是相同的。庞氏骗局、假冒服务和不道德的推广都需要欺诈者/名人使用社交媒体或其他通信工具做出不切实际的高额回报承诺。所有这些类型的欺诈都面临伪装和高维特征的问题，因为在欺诈发生之前发出信号。可以借鉴电子商务欺诈检测的经验，因为它也面临伪装和高维特征的问题。对于市场操纵检测，比较“拉高出货”代币和合法代币的价格变动是非常重要的。因此，检测问题受到类别不平衡和标签稀缺的困扰。从图 3-2 可以看出，信用卡欺诈和电子商务/评论欺诈吸引了最多关注，深度学习算法在检测它们方面做出了最大的贡献。进一步得出结论，深度学习算法在检测加密货币欺诈方面有着广阔的未来。

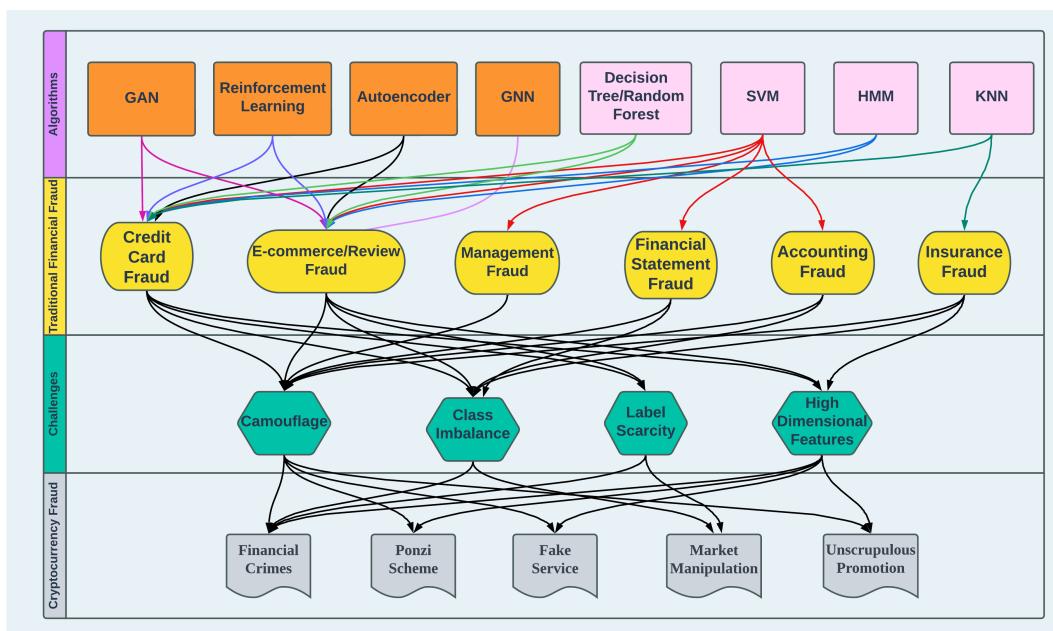


图 3-2 算法与加密货币欺诈之间的联系

Figure 3-2 The Linkage Between Algorithms and Cryptocurrency Fraud

## 第4章 在大语言模型框架下的加密货币属性判断以及投资决策

### 4.1 引言

高效市场假说提出，市场价格充分反映了所有可用信息，使市场参与者能够根据自身利益作出理性决策<sup>[126]</sup>。随着计算技术在金融行业的普及，信息获取方式发生了巨大变化。过去，市场情绪的衡量主要依赖于报纸、官方文件和每日更新的价格图表。然而，这一时代已然结束。在当今环境中，新闻无处不在，所以筛选出相关信息变得更加复杂。

大型语言模型（LLMs）的发展为这一挑战提供了解决方案。金融情绪分析的研究可以分为基于字典的、基于机器学习的和基于大型语言模型的三种主要方法。这些方法着眼于非市场因素，如公司报告、电话会议和新闻，目的在于及时提取积极、消极或中性的情绪评分。先前的研究显示，在资产估值高度不确定的时期，情绪对资产价格的影响更为显著<sup>[127]</sup>。

基于字典的方法因其计算效率高和一致性强而在文献中被青睐。有研究使用专门的词汇表来捕捉财务文件的基调，这些词汇表与诸如 10-K 报告回报、交易量、回报波动、欺诈、重大缺陷和意外收益等各种财务指标相关<sup>[128]</sup>。近期的研究对现有的情绪词典进行了改进和扩展，包括了双词组，以更细致地解释金融话语<sup>[129]</sup>。Correa 和 Mislang<sup>[130]</sup> 利用中央银行发布的金融稳定报告（FSRs）的文本，为 2005 年至 2017 年间的 30 个国家创建了专门的金融稳定情绪（FSS）指数。研究显示，FSS 指数不仅解释了信贷、资产价格、系统性风险和货币政策利率等金融周期指标的变化，而且还是银行危机的强有力预测指标。具体来说，FSS 上升一个百分点与危机发生概率增加二十九个百分点相关。

基于机器学习的方法通过将输入文本映射到基于上下文信息捕获的适当标签来学习分类文本。Leow 和 Chua<sup>[131]</sup> 引入了两种创新模型，情绪全天候（SAW）和情绪 MPT（SMPT），这些模型将机器学习技术与恒定再平衡（Constant Rebalancing (CRB)）和现代投资组合理论（Modern Portfolio Theory (MPT)）等经典金融理论结合起来，使用谷歌的 BERT 模型处理的 Twitter 情绪数据。这些模型通过遗传算法优化，以实现最大化累积回报和最小化波动性等目标。当它们在 2018 年 8 月到 2019 年 12 月的美国股票数据上训练，并在 2020 年 1 月到 4 月测试时，这些模型在夏普比率、累积回报和风险价值等指标上都超过了传统基准，如买入并持有的 SPY 指数、MPT 和 CRB。像潜在狄利克雷分配（LDA）这样的主题建模技术可用于自动分析和将金融新闻文章分类为“并购”、“收益报告”或“市场趋势”等各种主题。识别金融新闻中经常提到的指标可以为利益相关者提供市场当前关注点的见解。Li 等<sup>[132]</sup> 介绍了一种通过在线媒体文本挖掘来预测原油价格的新方法，使用深度学习技术，特别是卷积神经网络（CNN），来提取相关模式。该研究通过将从新闻文本情感和 CNN 提取的特征分组，并使用潜在狄利克雷分配（LDA）进行优化，通过滞后顺序和特征选择方法进一步优化这些

特征，从而提高了预测准确性，超越了传统基准，并展示了文本和金融特征的互补性。当 LDA 应用于稀疏和简短的新闻标题时，其局限性变得明显，因为这些标题通常是随意的和模糊的。因此，使用 LDA 进行原油价格基于文本的预测的现有研究面临着短文本数据和主题模型能力之间的不匹配，从而影响预测的准确性。Yun 和 Jia<sup>[133]</sup> 引入了两个创新的主题和情绪分析指标，并通过实证实验表明，使用这些指标的 AdaBoost.RT 应用程序提供了对短文本数据更细微的解释，并显著提高了预测性能，与其他基准相比。正如 Chiang 所表达的，ChatGPT 可以被认为是“模糊的网络 JPEG”。OpenAI 从包括社交媒体、维基百科和学术期刊在内的各种来源积累了大量知识，以创建一个体现压缩智慧的机器。<sup>[134]</sup>

然而，像 ChatGPT 这样的大型语言模型（LLMs）开启了一个新时代，LLMs 能够在复杂的信息环境中导航，得出细腻的判断。这种革命性的能力在金融文本解读领域尤其具有变革性，这是传统上由人类分析师承担的任务。随着 ChatGPT 的出现，这些复杂的分析现在可以以更低的成本执行，彻底改变了行业并释放了未开发的潜力。Wu 和 Mann<sup>[135]</sup> 介绍了 BloombergGPT，这是一种在金融自然语言处理（NLP）方面专门化的最新 LLM，其训练策略有效地结合了特定领域和通用数据，以实现平衡性能。该模型在一般 LLM 任务中树立了新的基准，并在金融应用中表现出色。Deng 和 Bendersky 在 Reddit 上使用一种精简的 LLM 进行金融情绪分析，其性能与使用最少的人工注释数据的监督模型相当，并在不同数据集上展现了良好的泛化能力<sup>[136]</sup>。虽然该模型的应用提出了关于负责任输出整合的伦理考虑，但这项工作突显了上下文学习在处理挑战性文本任务中的潜力，并为未来研究人机协作在提示设计和自动提示调整方面打下了基础。Huang 和 Yang 介绍了 FinBERT，这是一个金融领域适应的大型语言模型。作者得出结论，它在提取电话会议记录中的有用信息方面比其他方法更有效<sup>[137]</sup>。

本研究设定了两个主要目标：首先，利用大型语言模型（LLMs）分析公众对选定金融资产的感知，涉及黄金、原油、比特币、以太坊，以及微软和 Meta 平台公司的股票价格；其次，使用 LLMs 预测这些资产的每日价格。为此，研究从六大主流媒体来源汲取了 168,030 条新闻标题。研究采用了 Meta AI 开发的开源 LLM(Llama) 进行主题建模。为了高效管理其 130 亿个参数，研究中使用了 4 位量化技术。这些标题中的关键术语通过基于类别的词频-逆文档频率（TF-IDF）度量进行加权，随后通过 Llama 的 130 亿参数模型进行主题表示。对于预测任务，设计了一个专门的提示，采用思维链（Chain of Thought(COT)）框架，使 GPT-3.5 能够将每条新闻项目的影响分类为对资产价格的积极、消极或中性。

研究的贡献有三个方面：首先，通过使用 LLMs 分析 168,030 条新闻标题的大型语料库，更全面地捕捉了公众感知，扩展了现有关于经济预测中叙事情绪的文献<sup>[138–142]</sup>。其次，该研究回应了学术界对包括但不限于加密货币、黄金和原油等商品、股票价格和能源指数等多样化金融资产特性的关注<sup>[143–145]</sup>。第三，将 GPT 3.5 解读的情绪变量纳入资产价格预测模型中，发现新闻情绪与资产价格之间存在显著相关性。有趣的是，这种情绪变量对商品对（如原油和黄金）的解释

力大于加密货币对（如 ETH 和 BTC）或科技股对（如微软和 Meta）。通过展示 LLMs 在这一背景下的能力，该研究为未来研究人员探索更先进和可扩展的金融情绪分析和预测技术奠定了基础。

## 4.2 主题建模和预测框架

本研究提出的框架包含两个主要组成部分：第一部分使用 4 位量化的 Llama 2 13B 模型进行主题建模。大型语言模型（LLMs）中的量化方法是在模型精度和减少内存、加快推理速度之间的一种权衡，但实现最佳的位级缩放是具有挑战性的。Dettmers 和 Zettlemoyer<sup>[146]</sup>发现，4 位精度通常是平衡总模型位数和零次射击精度的最佳选择。第二部分利用以提示词为指导的 GPT-3.5 模型生成情绪变量。通过识别和分类主题，评估各种资产对之间的主题相似性，包括加密货币、商品和股票。随后，本研究提出了一个假设，关于在线新闻标题对资产价格预测的潜在影响。这项研究的最终目标是确定哪些资产对在媒体报道中与加密货币对展现出最大的主题相似性。如果股票对在新闻报道中与加密货币对展现出主题相似性，可能表明模型的可解释性（以 R 平方衡量）在这些资产类别之间是可比较的。

传统方法，如 Jianping Li 等人<sup>[147]</sup>所述，从主题数据中提取影响因素存在两个重大限制。首先，并非所有相关因素都能有效地被发掘出来。其次，全面因素列表的编制在很大程度上取决于主观人类偏好，因此引入了一定程度的偏见。为了缓解这些挑战，本文仅将主题建模作为数据表示的一种方法，作为高级推理的基础。

图 4-1 提供了使用在线新闻标题进行主题建模和预测资产价格的框架。主题建模包含六个步骤。第一步是使用 Sentence-BERT（双向编码器表示来自变换器）将新闻标题中的单词转换为机器可读的数值表示。随后，采用 Uniform Manifold Approximation and Projection (UMAP) 作为降维技术，从而促进后续的聚类任务。使用基于层次密度的空间聚类应用噪声（HDBSCAN）执行聚类，将降维后的嵌入分类为连贯的簇。接着，采用基于类别的词频-逆文档频率 (TF-IDF) 算法来最小化主题中停用词的出现。最终的输出包含每个主题的代表性词汇列表。然后部署一个大型语言模型来对这些主题进行标记，这种方式比人类解释更有一致性。

提示作为基础输入，引导大型语言模型生成既与上下文相关又具体的响应。图 4-2 阐述了实现指定任务中理想结果的最优提示配置。先前的研究，如 Takeshi Kojima 等人<sup>[148]</sup>所示，实证表明在提示中增加“让我们一步一步地思考”这句话显著提高了模型的性能，在 MultiArith 数据集上达到 78.7% 的最高准确率。类似地，另一项研究强调了“思维链”过程作为促进语言模型逻辑推理的有效机制的重要性<sup>[149]</sup>。综合这些发现，本研究将“思维链”和指导性示例纳入主题建模提示中。考虑使用 GPT 3.5 的财务影响至关重要，因为该模型每 1000 个输入令牌收费 0.0015 美元，每 1000 个输出令牌收费 0.002 美元。每个提示都专门针对个别新闻标题定制，以产生分析结果。然而，纳入带有指导性示例的提示将产生

可观的成本；因此，在执行这项研究时，提示词的简洁性是一个关键考虑因素。

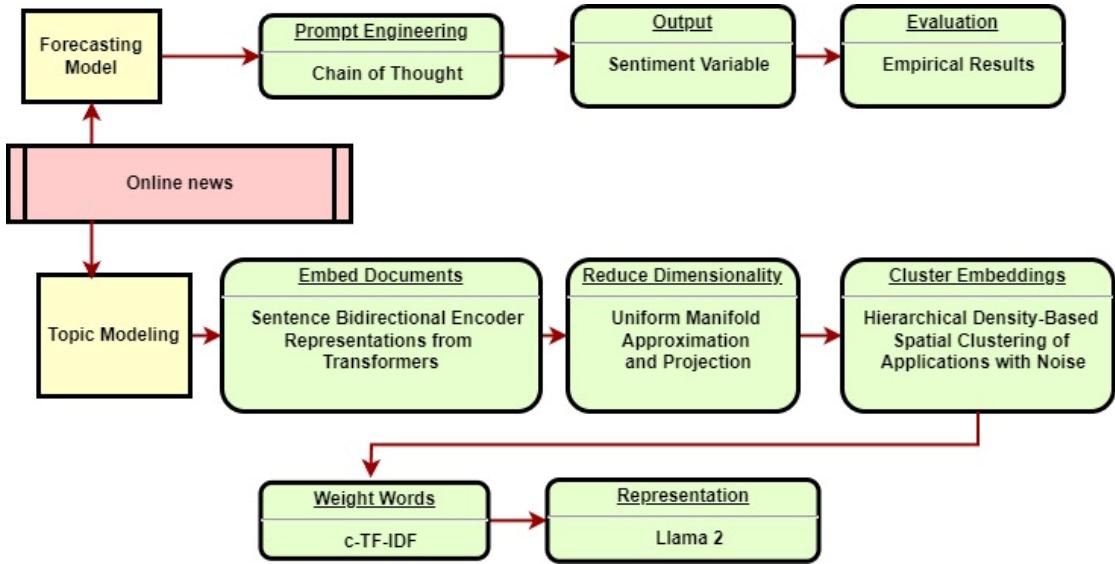


图 4-1 主题建模和预测框架

Figure 4-1 Framework for Topic Modeling and Forecasting

Topic Modeling Prompt	Forecasting Prompt
<pre> I have a topic that contains the following documents: [DOCUMENTS]  The topic is described by the following keywords: "[KEYWORDS]".  Based on the information about the topic above, let's think step by step, please create a short label of this topic. Make sure you to only return the label and nothing more.  ### EXAMPLE: I have a topic that contains the following documents: - Caroline Ellison, one of Sam Bankman-Fried's top deputies and also his ex-girlfriend, testified Wednesday that she felt relieved when his crypto empire started to collapse because it meant she could stop lying. - She noted the CoinDesk scoop that undid the company, saying the crypto news site's scoop was based on a balance sheet Alameda sent to lenders to mislead them into thinking the trading firm was on more solid financial footing than it really was – though the numbers were ugly enough to spark the collapse.  The topic is described by the following keywords: 'Caroline Ellison, top deputies, testified, crypto empire, collapse, lying, balance sheet, Alameda, mislead, trading firm, solid, financial footing'. ### </pre>	<pre> You are a financial expert with investment experience. Answer YES if it is good news for [ASSET] price, NO if it is bad news for [ASSET] price, or UNKNOWN if uncertain? {text_content} let's think step by step and only answer YES/NO/UNKNOWN". </pre>

图 4-2 左侧：带有思维链和指导性示例的主题建模提示。右侧：带有思维链的预测提示。

Figure 4-2 Left: Topic Modeling Prompt with Chain of Thought and Instruct example.

Right: Forecasting Prompt with Chain of Thought.

#### 4.2.1 具有普适性的大语言模型（4 比特量化技术）

大型模型需要大量的计算资源和内存，尤其是在 GPU 显存方面。不是所有的研究或应用场景都能负担得起高端硬件，比如 NVIDIA 的 A100 GPU。压缩模型可以使其在更普通的硬件上运行，提高模型的普适性和可访问性。并且较小的模型需要的计算资源少，推理（即模型做出预测的过程）速度更快。这对于需要实时分析和决策的金融应用来说尤其重要。本文使用的主题大语言模型有着 130 亿参数，需要执行 4 位比特量化技术，“压缩”模型以便运行它。本文使用的技术为 QLoRA (Quantized Lottery Ticket Rewinds and Adaptation<sup>[146]</sup>)，是一种高效的

微调方法，它能显著降低大型语言模型（LLMs）的内存占用，并保持完整的16位微调任务性能。在具体实现上，QLoRA通过一个冻结的4位量化的预训练语言模型传递梯度到低秩适配器（Low Rank Adapters，简称LoRA）中。QLoRA引入了多项创新技术来节省内存而不牺牲性能：

(1) **4位正态浮点量化（4-bit NormalFloat Quantization, NF4）**：正态浮点（NormalFloat, NF）数据类型是基于分位数量化（Quantile Quantization）构建的。对于零均值正态分布的输入权重，首先通过绝对最大值重标准化，将权重张量标准化到 $[-1, 1]$ 的范围。然后，估计标准正态分布的分位数，以获得量化数据类型。量化值 $q_i$ 的计算公式为：

$$q_i = \frac{1}{2} \left( Q_X \left( \frac{i}{2k+1} \right) + Q_X \left( \frac{i+1}{2k+1} \right) \right) \quad (4-1)$$

其中 $Q_X(\cdot)$ 是标准正态分布 $N(0, 1)$ 的分位函数。

(2) **双重量化（Double Quantization, DQ）**：双重量化是对第一次量化中的量化常数进行第二次量化的过程。双重量化后，每个参数的内存占用从 $32/64 = 0.5$  bits降低到 $8/64 + 32/(64 \times 256) = 0.127$  bits。减少的内存量为：

$$\text{内存减少} = 0.5 \text{ bits} - (0.127 \text{ bits}) = 0.373 \text{ bits} \quad (4-2)$$

(3) **QLoRA 的定义和操作**：对于量化基础模型的单个线性层，使用单个LoRA适配器，QLoRA定义如下：

$$Y_{BF16} = X_{BF16} \text{doubleDequant}(c_{FP32}^1, c_k^2, W_{NF4}) + X_{BF16} L_{BF16}^1 L_{BF16}^2 \quad (4-3)$$

其中，`doubleDequant(·)`定义为：

$$\text{doubleDequant}(c_{FP32}^1, c_k^2, W_k) = \text{dequant}(\text{dequant}(c_{FP32}^1, c_k^2)W_{4\text{bit}}) = W_{BF16} \quad (4-4)$$

对于参数更新，只需要计算适配器权重的误差梯度 $(\frac{\partial E}{\partial L_i})$ ，而不需要计算4位权重的误差梯度 $(\frac{\partial E}{\partial W})$ 。但是，计算 $\frac{\partial E}{\partial L_i}$ 需要通过去量化，从存储数据类型 $W_{NF4}$ 转换为计算数据类型 $W_{BF16}$ ，以BFLOAT16精度计算导数 $\frac{\partial X}{\partial W}$ 。

#### 4.2.2 Sentence BERT

Sentence-BERT（SBERT）因其生成语义丰富且计算效率高的嵌入而受到赞誉，特别适合于新闻标题嵌入等工作。在这些领域中，嵌入的速度和语义完整性对于新闻主题的实时分析和分类至关重要。SBERT是对像BERT和RoBERTa这样的预训练模型的精致改进，经过精心设计，能够生成固定大小、语义上有意义的句子嵌入，并提高了计算效率<sup>[150]</sup>。该模型的架构包括一个池化操作，并采用专门的神经网络框架，孪生网络和三重网络进行微调。

SBERT利用各种目标函数进行优化。例如，分类目标是通过在加权和 $W_t \cdot (u, v, |u - v|)$ 上应用softmax激活来制定的，其中 $u$ 和 $v$ 代表句子嵌入， $W_t$ 是一

一个可训练的权重矩阵。这里的目标是最小化交叉熵损失，以使嵌入与实际的类别标签紧密对齐，表示为：

$$\text{Loss}_{\text{class}} = - \sum_{i=1}^N y_i \log(p_i)$$

，其中  $N$  是类别数量， $y_i$  是真实标签， $p_i$  是预测概率。

另一方面，回归目标专注于利用句子嵌入  $u$  和  $v$  之间的余弦相似度来最小化均方误差损失，公式表达为：

$$\text{Loss}_{\text{reg}} = \frac{1}{N} \sum_{i=1}^N (y_i - \cos(u, v))^2$$

最后，三元目标函数表述为

$$\max(\|s_a - s_p\| - \|s_a - s_n\| + \epsilon, 0)$$

，旨在最小化锚定句子  $s_a$  和正句子  $s_p$  之间的欧式距离，同时与负句子  $s_n$  相比，这一过程受到边界值  $\epsilon$  的限制。

#### 4.2.3 Uniform Manifold Approximation and Projection (UMAP)

均匀流形近似和投影（UMAP）是一种深植于黎曼几何和代数拓扑的降维技术。UMAP 算法的运作方式首先是在高维空间构建一个加权的 k 最近邻（k-NN）图，其中每个节点代表一个数据点，边权重基于相似性函数计算<sup>[151]</sup>。这个函数通常表示为：

$$\text{sim}(x, y) = \frac{1}{1 + a \cdot \|x - y\|^b}$$

，其中  $a$  和  $b$  是超参数， $\|\cdot\|$  表示距离度量。同时，构建一个相应的低维图，旨在尽可能接近地近似高维图。该优化步骤的关键在于最小化交叉熵损失函数，表述为：

$$\mathcal{L} = - \sum_{x,y} w_{xy} \log(u_{xy}) + (1 - w_{xy}) \log(1 - u_{xy})$$

，其中  $w_{xy}$  和  $u_{xy}$  分别代表高维和低维图中的边权重。通过随机梯度下降或类似的优化算法来减少这个损失函数，最终得到一个低维表示，有效地保留了原始高维数据中的局部和全局结构。

#### 4.2.4 HDBSCAN: Hierarchical Density-Based Spatial Clustering of Applications with Noise

HDBSCAN，即带噪声的层次密度基空间聚类（Hierarchical Density-Based Spatial Clustering of Applications with Noise），是一种高级聚类算法，以其在不需要事先指定聚类数量的情况下检测不同密度的聚类而闻名。与许多聚类算法不

同, HDBSCAN 能够识别出不同形状和大小的聚类, 使其成为适用于广泛数据分析任务的强大选择<sup>[152]</sup>。

HDBSCAN 算法的核心是测量数据点之间的距离, 常用的距离度量包括欧几里得距离或曼哈顿距离。两点  $P(x_1, y_1)$  和  $Q(x_2, y_2)$  之间的欧几里得距离公式为:

$$d(P, Q) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

计算距离后, 基于与其邻近点的距离估计点  $x$  的密度。核密度估计 (KDE) 的公式为:

$$\hat{f}(x) = \frac{1}{n} \sum_{i=1}^n K_h(x - x_i) = \frac{1}{nh} \sum_{i=1}^n K\left(\frac{x - x_i}{h}\right)$$

其中  $K$  是核函数,  $n$  是数据点的数量,  $h$  是带宽。

在计算距离之后, 根据数据点之间的距离度量构建最小生成树 (MST)。MST 中一条边  $e$  的权重由它连接的点之间的距离给出, 即  $w(e) = d(P, Q)$ 。

构建 MST 之后, 通过分析 MST 并创建树状图来形成聚类层次结构。两个聚类  $C_i$  和  $C_j$  合并的不相似度  $\delta$  由两个聚类中点之间的最大距离给出:

$$\delta(C_i, C_j) = \max_{x \in C_i, y \in C_j} d(x, y)$$

然后通过在产生最持久聚类的点处切割树状图, 从树状图中提取稳定的聚类。聚类的稳定性基于其在一系列数据规模上的持久性来评估, 聚类  $C$  的稳定性由

$$S(C) = \sum_{x \in C} \lambda(x)$$

给出, 其中  $\lambda(x)$  是层次结构中点  $x$  成为聚类  $C$  成员的层级。

#### 4.2.5 C-TF-IDF: class-based Term Frequency-Inverse Document Frequency

BERTopic 采用了 TF-IDF 的一种变体, 称为 c-TF-IDF, 通过将关注点从单个文档调整到聚类或主题层面, 以更好地从词袋矩阵中划分主题。在这种改进的公式中, 类别  $c$  中词项  $x$  的频率表示为

$$\mathbf{tf}_{x,c} = \text{词项 } x \text{ 在类别 } c \text{ 中的频率}$$

此外, 词项  $x$  在所有类别中的频率表示为  $\mathbf{f}_x$ 。每个类别中的平均词数由  $\mathbf{A}$  表示, 用于构建一种修改过的逆文档频率 (idf) 变体, 表达为

$$\text{idf variant} = \log\left(1 + \frac{\mathbf{A}}{\mathbf{f}_x}\right)$$

这种 idf 变体通过在对数中包含 1 来确保正值。然后, 类别中一个词项的 c-TF-IDF 权重计算为

$$\mathbf{W}_{x,c} = \mathbf{tf}_{x,c} \times \text{idf variant}$$

将类别中的词频与修改后的 idf 结合起来，以确定词项  $x$  在类别  $c$  中的重要性分数。通过将聚类视为用于导出类别内词频的单一文档，并应用 L1 范数以适应不同的主题大小，c-TF-IDF 及其随后的权重提供了与传统 TF-IDF 相比更精确的主题表示。

### 4.3 实验数据

为了确保全面而稳健的分析，从六个著名新闻媒体收集了数据：CNN、《纽约时报》、《华尔街日报》、路透社、《金融时报》和 BBC。这些不同来源的多样性使得观点更加平衡，能够容纳对相似事件的不同视角，从而使得机器分析更接近于人类对新闻的解读。

计算了每日平均分数，以规范化不同叙述并确保解释的一致性。文本数据来源于 Factiva，这是一个在金融新闻分析领域享有盛誉的平台。需要特别指出的是，尽管报道资产的开始日期可能有所不同，收集的数据始终涵盖了 2016 年至 2023 年的时期。还剔除了仅讨论价格变动的新闻文章，并将标题长度限制在至少十个词，因为任何比这更短的标题可能无法提供有用信息。

除了新闻数据外，还从雅虎财经获取了交易量、收盘价和市场资本化等财务细节。同时纳入了芝加哥期权交易所的 VIX 指数进行分析，这是基于市场对情绪的敏感性和当前不确定性之间存在相关性的证据<sup>[127]</sup>。

#### 4.3.1 科技股对比-微软和 Meta

关于微软的主题描绘了该公司采取的一系列战略举措和适应性措施。一个突出的方面是微软对 LinkedIn 的收购，这标志着其在专业网络和社交媒体领域的显著扩张和整合。同时，描述主题还强调了对微软云服务的关注，展示了该公司持续强化和推广其云计算服务的重点，这在现代数字基础设施中至关重要。此外，微软应对全球挑战的方式也被描绘出来，例如 COVID-19 大流行。这展示了该公司在适应办公环境以应对大流行带来的前所未有的挑战方面的响应能力，强调了在运营中的韧性和连续性。另外，描述中还包含了网络安全的元素，可能表明微软在防御日益演变的威胁和漏洞方面的积极策略，强调了对安全和稳健技术生态系统的承诺。

Meta 的主题叙述描述了与社会元素、法规和创新追求的多方面互动。一个突出的特点是探讨争议和监管导航，以围绕隐私问题及其相应的法律和解为例。通过 Meta 广告和欧盟隐私法规中提到的俄罗斯干预 2016 年美国总统选举的情况进一步凸显了该公司与更广泛的社会和地缘政治动态的复杂纠缠。创新和面向未来战略也是 Meta 描绘的重点，明显提及了元宇宙和虚拟现实。这展示了 Meta 在重新定义数字互动和体验方面的努力，预示着虚拟连接的新前沿。此外，描述还展示了 Meta 在应对当代全球挑战（如 COVID-19 大流行期间的错误信息传播）方面的参与，反映了该公司在信息流和社会影响方面的关键作用。

微软和 Meta 在各自的表现中展示了既有的分歧焦点，也有共同的战略基础。

他们共有的是与全球逆境的密切关联，体现在微软对大流行相关的适应措施以及 Meta 在 COVID-19 大流行期间应对错误信息传播方面的参与。两家公司都展现出战略远见，微软体现在收购行为上，Meta 则在虚拟现实和元宇宙方面的创新探索上表现出色。然而，在战略重点上的差异也是显著的。微软似乎更倾向于在其运营生态系统中进行整合、技术提升和网络安全方面的努力。相比之下，Meta 的叙述富含监管参与、社会影响和开创性创新，反映了与外部实体的更广泛的互动和面向未来的探索。因此，尽管在共同的全球参与上有所交集，这两家公司在其发展路径和重点领域上展现了各自独特的战略方向。

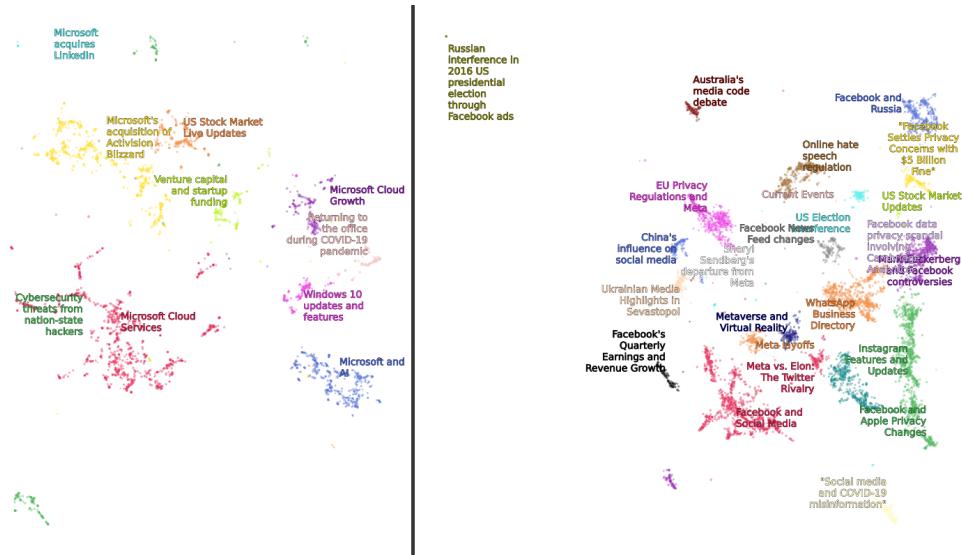


图 4-3 左侧：与微软相关的话题。右侧：与 Meta 相关的话题。

Figure 4-3 Left: Topics related to Microsoft. Right: Topics related to Meta.

### 4.3.2 大宗商品对-黄金和原油

黄金的话题主要围绕各种市场表现、全球经济指标和货币汇率展开。值得注意的是，重点放在区域市场表现上，包括亚洲、澳大利亚和加拿大等地，这表明在对黄金进行分析和讨论时存在地理多元化。与“加密货币市场波动”的交叉点体现了传统资产与数字资产之间微妙的对话，将黄金描绘为在加密货币动荡局势中可能的稳定器。这种对比促进了围绕风险管理、多元化策略和当代投资范式的讨论。与此同时，黄金与“全球冠状病毒传播追踪”话题的互动体现了其在全球逆境中作为投资者避风港的角色，揭示了黄金与更广泛的经济健康和投资者情绪在危机时期的交织关系。

相反，原油的话题具有更专业的关注，主要集中在石油和能源领域。主题涵盖从原油价格和库存的具体讨论到能源部门内更广泛的市场趋势。地缘政治因素也在原油话题中占据重要地位，涵盖中东、非洲和俄罗斯等地区和国家。俄罗斯媒体对原油的报道可能反映了该国的战略目标和经济考虑。作为俄罗斯经济的重要组成部分，俄罗斯媒体对原油趋势、价格和地缘政治谈判的描绘可能反映了该国更广泛的经济战略以及地缘政治联盟或紧张关系。例如，媒体报道可能包

括俄罗斯在石油输出国组织（OPEC+）协议、制裁以及与其他重要石油生产国的合作或竞争方面的立场。此外，俄罗斯和中国媒体报道之间的合作或互动可能揭示了这两个国家在能源领域内双边关系的方面。作为能源的重要消费国和主要生产国，中国和俄罗斯在全球能源格局中有着重要的关系。他们的媒体报道可能共同揭示了能源战略和地缘政治考虑中的共生动态、共同目标或分歧。

黄金和原油的讨论都涉及理解全球经济和政治对它们的市场的影响。它们都关注不同地区如何影响它们的价格和需求。然而，关于它们各自讨论的具体内容存在明显差异。原油的讨论更为专业，主要集中在石油行业本身。它们谈论的内容包括石油生产、供应以及政治事件如何直接影响石油市场。另一方面，黄金的讨论更加多样化。它们不仅讨论黄金市场，还包括关于新兴金融趋势如加密货币（比特币等数字货币）的对话。



图 4-4 左侧：与黄金相关的话题。右侧：与石油相关的话题。

Figure 4-4 Left: Topics related to Gold. Right: Topics related to Oil.

### 4.3.3 加密货币对 - 比特币和以太坊

比特币，经常被称为传统价值储存的数字替代品，与黄金等诸多特性相似，例如稀缺性和对抗通货膨胀的潜力。”比特币作为价值储存与传统资产的对比”的叙事逐渐变得更加重要，因为投资者考虑到这种加密货币在投资组合多元化方面的潜力，类似于黄金等传统避险资产。然而，不能低估”比特币对汇款市场的影响”，因为它为传统银行系统提供了去中心化的替代方案，降低了全球工作者汇款回家的成本和交易时间。在”经济危机”期间，比特币的非主权性质允许个人规避不稳定的本地货币。尽管如此，”监管挑战和比特币的未来”问题仍然严峻，加密货币的颠覆潜力面临着多种监管响应，旨在平衡防范金融犯罪和促进技术创新。这个复杂的监管环境无疑将塑造比特币在全球金融体系中走向主流接受或潜在边缘化的道路。

以太坊，作为“加密货币市场趋势”的先驱，已经成为数字资产世界的基石，不仅因为其货币以太币，还因为其强大的平台，使开发人员能够构建去中心化应用程序。这种多功能性是“加密货币市场增长”背后的重要推动因素，因为以太坊的自动执行合同将协议条款直接编写成代码，具有远远超出简单交易的潜在应用，影响到金融、房地产和法律等多样化领域。此外，以太坊的框架催生了“加密艺术和非同质化代币（NFTs）”运动，彻底改变了数字艺术和收藏品的创作、购买和销售方式。通过允许艺术家和创作者在没有中间商的情况下实现作品的货币化，以太坊的 NFT 重新定义了数字时代的所有权，使其成为快速发展的加密货币在更广泛经济叙事中的关键参与者。

尽管比特币和以太坊的话题都涉及这些加密货币的经济和市场影响，但比特币的讨论更侧重于其货币特性、监管方面以及对经济状况的响应。与此同时，以太坊的话题聚焦于其开启新应用、促进市场增长以及促进数字所有权和创造力新形式的方面。

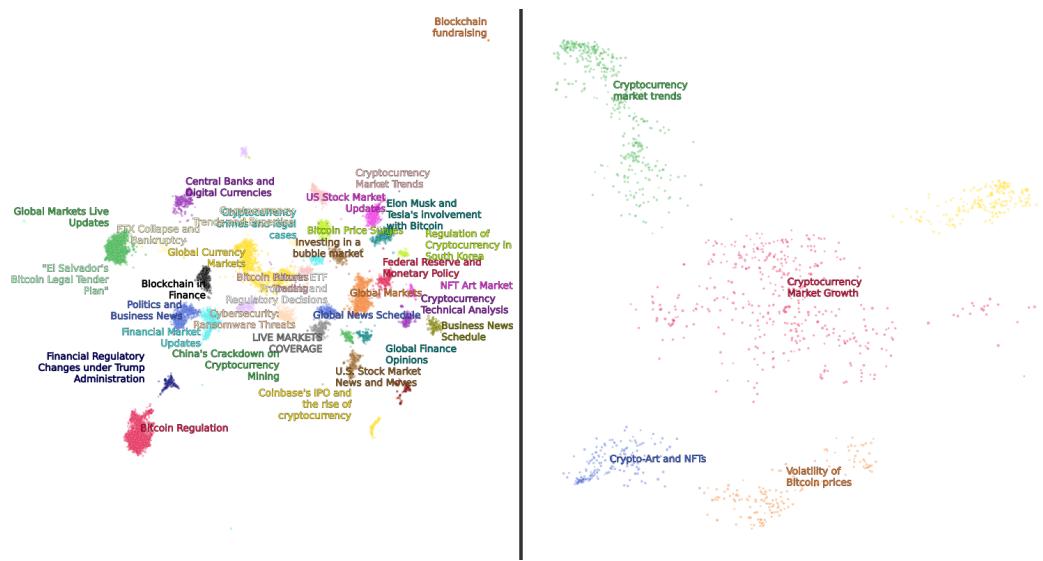


图 4-5 左侧：与比特币相关的话题。右侧：与以太坊相关的话题。

Figure 4-5 Left: Topics related to Bitcoin. Right: Topics related to Ethereum.

#### 4.3.4 以太坊的属性

在研究股票对如微软和 Meta，以及大宗商品对如黄金和原油的特征时，出现了明显的特点，这些特点对于评估以太坊是安全还是商品的性质至关重要。代表科技股的微软和 Meta 以其持续创新和技术进步而闻名。这包括微软进军云计算和网络安全领域，以及 Meta 探索虚拟现实和元宇宙。这两家公司还深度参与监管和社会问题，应对复杂的隐私问题和虚假信息等问题，反映出它们融入更广泛社会和地缘政治动态的特点。此外，它们的战略涉及重大收购和市场扩展，正如微软收购 LinkedIn 和 Meta 进军新数字领域所示。这些公司还展现出高度的响应能力，根据全球挑战的需求调整其运营，以应对 COVID-19 大流行等情况。

另一方面，黄金和原油等大宗商品主要在市场表现、经济指标和供需动态方面讨论。黄金通常被视为在波动市场中的稳定器，包括与加密货币动荡局势的对比。原油的讨论侧重于石油行业的具体方面，包括生产、供应和地缘政治影响，反映了其在全球政治和经济中的关键作用。

将豪威测试应用于以太坊时，本研究观察到与股票特征更为相似，而不是大宗商品。该测试用于确定资产是否符合安全性的条件，考虑因素包括投资资金并期望主要来自他人努力的利润。在以太坊的情况下，投资者将资本投入，期望获得的收益在很大程度上取决于平台更广泛的开发社区的努力，类似于股票价值取决于底层公司的表现。此外，以太坊的价值与其平台的成功紧密相连，类似于股票投资中所见的共同企业方面。在以太坊的增长和价值方面的推动者或第三方的角色，类似于公司管理层对股票的影响，进一步符合豪威测试对安全性的标准。

总之，以太坊的特点和其投资动态的性质更接近于微软和 Meta 等科技股，而不是黄金和原油等大宗商品。它的价值不是来自实际属性或固有的物质效用，而是来自技术创新、平台增长的潜力和开发社区的集体努力。豪威测试的结果加强了这一观点，将以太坊定位在安全性领域，因为它的投资结构和从共同企业的努力中获利的期望。

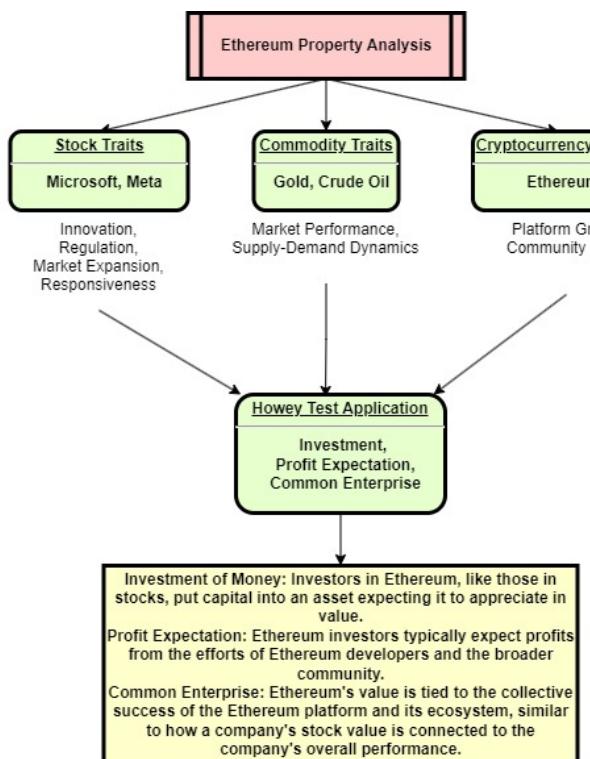


图 4-6 以太坊属性分析。

Figure 4-6 Ethereum Property Analysis

## 4.4 模型与结果

在统计分析中，重点是理解每日对数收益作为因变量  $y$  的影响因素。为了实现这一目标，采用了一个数学上表述如下的普通最小二乘（OLS）回归模型：

$$y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \epsilon$$

- $y$  代表因变量，即‘每日回报率’。
- $\beta_0$  是回归线的截距。
- $\beta_1, \beta_2, \beta_3$  是自变量的系数。
- $X_1, X_2, X_3$  是自变量，分别对应‘API\_Response\_Score(情绪变量)’、‘Word\_Count(字数)’和‘VIX\_Index (VIX 指数)’。
- $\epsilon$  是误差项，捕捉到预测值与实际值之间的残差或偏差。

**表 4-1 实证结果**  
**Table 4-1 Empirical Results**

	BTC	ETH	Gold	Oil	Microsoft	Meta
Intercept	-0.0362	-0.0064	-0.0006	-0.0371	0.0002	-0.0112
API Response Score	0.0604 *** (0.01)	0.0474 *** (0.014)	0.0013 *** (0.000)	0.0698 *** (0.005)	0.0056 ** (0.003)	0.0255 *** (0.006)
Word Count	0.0313 *** (0.012)	0.0151 (0.04)	-0.0002 (0.000)	0.0056 (0.006)	0.0064 (0.008)	-0.0001 (0.007)
VIX Index	-0.0089 (0.01)	-0.1180 *** (0.028)	-0.000 (0.000)	-0.022 *** (0.006)	-0.0219 *** (0.005)	-0.0141 ** (0.006)
R-squared	0.03	0.038	0.217	0.148	0.019	0.016

\*  $p \leq 0.1$

\*\*  $p \leq 0.05$

\*\*\*  $p \leq 0.01$

表 3-1 呈现了一项统计分析，研究了 GPT 3.5 的 API 响应对各种金融资产的影响。分析中包括的资产有比特币 (BTC)、以太坊 (ETH)、黄金、原油、微软和 Meta。API 响应分数表示 GPT 3.5 对金融新闻的判断以及是否被视为相应资产的正面信号。API 响应分数的系数对于所有资产都是正的，并在 1% 的水平上具有统计显著性（用 \*\*\* 表示），这表明 API 的更有利判断与相应资产价值的增加相关。对于 BTC 和 ETH，字数变量在 1% 和 5% 的水平上具有统计显著性，这意味着金融新闻的长度可能对这些加密货币的价值产生积极影响。然而，对于其他资产，字数似乎没有显著影响。

恐慌指数 (VIX Index)，通常被称为“恐惧指标”，与 BTC、ETH、原油、微软和 Meta 的价值呈负相关，具有不同水平的显著性 (ETH 在 1%、原油和微软

在 5%、Meta 在 10%）。这表明随着市场波动性的增加，这些资产的价值会受到负面影响。VIX 指数与 ETH 和科技股都呈负相关，但对黄金没有显著影响。这可能意味着在市场波动性较高的时期，ETH 和科技股的价值往往会下降，这是与传统商品如黄金不共享的特征。

R 平方值对于 BTC、ETH、微软和 Meta 都相对较低，表明该模型仅解释了这些资产价值变化的一小部分。然而，对于黄金和原油，R 平方值较高，特别是对于黄金，这表明该模型更适用于预测这些资产价值的变化。

总体而言，结果表明 GPT 3.5 对金融新闻的 API 响应是资产价值的重要预测因素，尤其是对于加密货币和科技公司的股票。

#### 4.4.1 知识截止日期的稳健性检验

为了评估模型的效力和稳定性，进行了一个两阶段的评估：第一阶段涉及分析模型在预定义的知识截止日期（2021 年 9 月 1 日）之前数据上的表现。在此阶段，使用了一个不包含任何截止日期之后信息的数据集，以确保在受控环境中对模型的预测能力进行无偏评估。第二阶段将这个分析扩展到截止日期之后的时期。这种方法允许比较模型在样本内（训练）的表现与样本外（测试）的效果。稳健性检验涉及对两个阶段的均方误差（MSE）和平均绝对误差（MAE）进行精细的计算。这些指标为评估模型的预测准确性提供了定量基础。此外，还使用 t 检验探索了截止日期前后预测误差的分布，为模型在不同时间段的一致性提供了统计证据。

Financial Asset	MSE Before	MAE Before	MSE After	MAE After
BTC	0.00195	0.0295	0.00106	0.0229
ETH	0.0084	0.0610	0.00235	0.0342
GOLD	0.000	0.0002	0.000	0.0003
OIL	0.0006	0.0153	0.0006	0.0176
Microsoft	0.0003	0.0120	0.0004	0.0152
META	0.0004	0.0137	0.0012	0.0225

表 4-2 金融资产的稳定性检验

Table 4-2 Robustness Check for Financial Assets

表格的结果表明，对于像 BTC、ETH、OIL、Microsoft 和 META 这样的资产，MSE 和 MAE 值都有明显的降低。这种降低意味着模型的预测逐渐接近实际值，表明了模型性能的提高。

唯一不符合这一趋势的是黄金，它的 MAE 值有所增加，而 MSE 略有下降。黄金的这种混合结果可能指向数据或市场行为的特定特征，这些特征可能会影响模型的预测能力，与其他资产相比有所不同。

在通过 t 值和 p 值评估统计显著性时，可以观察到黄金的指标明显不同，t 值为 -1.89，p 值为 0.06，接近统计显著性的边缘，暗示着截止日期前后模型误差

Financial Asset	T-Value	P-Value
BTC	0.43	0.67
ETH	1.14	0.25
GOLD	-1.89	0.06
OIL	0.62	0.54
Microsoft	0.96	0.34
META	0.25	0.81

表 4-3 金融资产的统计显著性

Table 4-3 Statistical Significance for Financial Assets

分布可能发生了变化。而其他资产的 p 值都远远超过了传统的 0.05 阈值，表明它们在两个时期的误差分布变化缺乏统计显著性。

## 4.5 结论

本研究通过深入的主题建模分析，对资产如以太坊（ETH）本质的理解提供了新的视角，揭示了它与霍威测试下定义的技术股特性之间的紧密联系。霍威测试作为判定证券身份的法律标准，凸显了以太坊的讨论主题——集中在其实用性、创新性及开发社区的集体贡献上——与技术股的属性相较于传统商品有更多的共鸣。这种洞察为利用大型语言模型（LLM）进行财务情绪分析和资产价格预测提供了关键的理论基础和分析框架。

进一步深入研究的预测领域，本研究表明 GPT-3.5 对财经新闻的解读对多元资产的估值产生了显著影响，这些资产包括加密货币、商品和技术股。分析发现新闻情绪的 API 响应分数与资产价值之间存在正相关关系，这强调了 LLM 在挖掘市场深层次洞察方面的巨大潜力。然而，不同资产类别对新闻情绪的响应程度存在明显差异，这表明资产类型——无论是加密货币、商品还是技术股——对新闻情绪的敏感度各不相同。

从管理层面来看，这些发现强调了将 LLM 融入财务分析和决策制定流程中的战略价值。金融机构和投资者可以通过这些先进的模型加深对市场动态的理解，并且提升其预测市场走势的能力，进而制定出更加精准和高效的投资策略。尽管如此，由于新闻情绪对不同资产类别的影响存在差异，这提示在应用 LLM 于不同的金融环境时，需要采取更为细致和定制化的方法。

然而，本研究的局限性也是显而易见的。一些资产的 R 平方值相对较低，意味着模型只能解释资产价格变动的一小部分因素。此外，本研究依赖于公开可获取的数据和固定的知识截止日期，这可能无法全面反映金融市场的复杂性和动态变化。因此，在解释和应用这些研究成果时，需要充分考虑这些因素，以确保分析结果的准确性和实用性。

## 4.6 本章小结

研究发现以太坊等资产与科技股特征在 Howey 测试下更加一致，强调了大型语言模型在金融分析中的潜在重要性。此外，研究证明了 GPT 3.5 对金融新闻情感的解读对各种资产的估值产生了重要影响，尤其是对加密货币和科技股。然而，不同资产类别对新闻情感的敏感性存在差异，需要在不同金融背景下采用定制的方法。

## 第5章 深度学习视角下的NFT价值研究

### 5.1 引言

非同质化代币（NFTs）代表了一类独特的代币，它们不可互换并具有固有的独特性。一个相关的例子是购买具有特殊序列号的美元纸币或邮票，因为一些人愿意为这些独特的物品支付溢价。在数字领域，NFTs 附带一份真品证书，并可以采取各种数字格式。NFTs 是通过在流行的区块链上部署一个代币来创建的，如 Polygon、Ethereum 或 Solana，代币的名称和符号由创建者确定。与代币相关的智能合约生成一个独特的哈希，并将其链接到被出售的商品。要购买 NFT，用户必须使用中心化交易所如 Nifty Gateway 或去中心化交易所如 LooksRare 或 X2Y2 以及加密钱包。NFT 的价值是基于其美学、实用性或它产生的互联网热度等因素来评估的，它解决了数字世界中的所有权问题。

每个 PFP（头像图片）系列都是基于特定主题开发的，系列中 PFP 的数量和铸造价格由相应的开发者确定。在发布过程中，用户无法选择要铸造的 PFP；然而，他们可以通过 OpenSea 等平台进行二级市场交易。本研究旨在从深度学习的角度评估市场泡沫期间的整个收藏系列。虽然开发者可以通过附加实用性和路线图来增加价值，但 PFP 的基本价值在于其独特性。

本文首先调查 OpenSea 主要 NFT 市场潜在泡沫的时间。为此，本研究应用泡沫检测算法，并使用后向序列增强的 Dickey-Fuller (BSADF) 检验来精确确定潜在泡沫的时间框架。本研究专注于这一时期交易量最大的头像图片 (PFP) 项目，并通过应用预训练模型 Visual Geometry Group (VGG)-19 来进行美学分析，以识别 PFP 系列内的相似性。本文的假设认为，用户更喜欢具有低相似性得分的 PFP 系列，表明其独特性。本文采用 t 分布的随机邻居嵌入 (t-SNE) 来评估不同收藏之间的风格相似性。此外，我们还探索了美学、知识产权 (IP) 权利与发布后表现指标之间的关系，包括首日回报、30 天回报和 1 年回报。

本研究做出了三方面的贡献。首先，这是第一个使用深度学习技术来调查 PFP 的美学特征的研究。其次，它将知识产权 (IP) 权利和美学特征整合为发布后表现的决定因素。第三，研究揭示了那些将 IP 权利分配给持有者的 PFP 项目在财务表现上具有可比性，而那些相似性得分低的项目则倾向于获得更高的回报。

#### 5.1.1 相关研究

本研究为新兴的非同质化代币（NFT）定价文献做出了贡献。Okonkwo<sup>[153]</sup> 认为 NFT 为版权持有者提供了商业化其知识产权的机会。Dowling 的研究<sup>[154]</sup> 旨在检验波动性冲击对 NFT 市场的影响，并通过小波相干分析研究市场之间的共动性。为了比较市场，从 2019 年 7 月到 2021 年 1 月期间使用了五个指数（比特币、以太坊、Decentraland、Cryptopunks 和 Axie Infinity）。值得注意的是，Dowling

发现与加密货币定价相比, NFT 定价展现出独特的波动性传导特征。Ko 等人<sup>[155]</sup> 将 NFT 整合到传统资产中, 如股票、债券、美元、商品指数和加密货币, 使用马科维茨均值-方差框架构建投资组合。结果表明, 将 NFT 纳入基于传统资产的投资组合中, 增强了投资者的多样化机会。此外, Maouchi 等人<sup>[156]</sup> 分析了九种 DeFi 代币、三种 NFT、比特币和以太坊, 以研究数字金融泡沫。运用实时泡沫检测方法, 该研究得出结论, DeFi 和 NFT 的快速增长可能导致潜在的溢出效应, 影响其他加密货币和金融市场。Kapoor 等人<sup>[157]</sup> 利用机器学习算法来预测基于 Twitter 的各种特征 (包括帖子、用户名和关注者数量) 的 NFT 价值。作者们认为社交媒体特征显著影响 NFT 的价值, 并观察到赞和回复数量、被列数以及 Twitter 用户名中 NFT 的存在是最有影响力的因素。Mekacher 等人<sup>[158]</sup> 采用统计方法来衡量稀有性与市场表现之间的关系。作者得出结论, 一个系列内物品的异质分布对其成功至关重要。

## 5.2 NFT 的买卖机制

NFT (非同质性代币) 是一种独特的数字资产, 它利用区块链技术来证明所有权和确保每个 NFT 的独一无二性。与传统的数字物品不同, NFT 具有不可替代性, 每个 NFT 都有独特的识别码和元数据, 区分于所有其他的 NFT。这些特性使得 NFT 成为数字艺术、音乐、收藏品和其他形式的创意作品的理想载体, 因为它们可以确保创作内容的真实性和所有权。NFT 的买卖机制涉及几个主要步骤:

### (1) 创建 (铸造) NFT

- 创造性工作: 艺术家或创作者将他们的创作内容转换为 NFT。
- 铸造过程: 在这一步骤中, 将创作内容的信息上传到区块链上, 这一过程创建了代表作品所有权和真实性的独一无二的数字证书。

### (2) 上架 NFT

- 选择市场: 创作者选择一个 NFT 市场来上架他们的作品, 例如 OpenSea、Blur、Rarible 等。
- 定价和销售方式: 创作者为 NFT 设定价格, 并选择销售方式, 可以是固定价格或通过拍卖。

### (3) 购买 NFT

- 浏览和选择: 买家在市场上浏览并选择他们感兴趣的 NFT。
- 支付和交易: 交易通常使用加密货币进行, 一旦决定购买, 买家将通过智能合约支付购买价格。

### (4) 转移所有权

- 自动化的过程: 交易完成后, NFT 的所有权自动转移给买家。NFT 的转移主要通过智能合约在区块链上执行。在大多数平台, 如以太坊, 这一过程通常涉及调用智能合约的 ‘transferFrom’ 方法, 这个方法会检查调用是否有权限转

移NFT，然后更新NFT的所有权记录。

- 不可篡改的记录：所有权转移和交易历史都在区块链上有不可篡改的记录。

#### (5) 次级市场交易

- 再次销售：NFT的当前所有者可以在次级市场上出售他们的NFT。
- 市场多样性：次级市场为NFT生态提供了丰富的购买和出售机会。

#### (6) 版税和智能合约

- 版税系统：NFT可以编程以确保原始创作者在每次NFT转售时获得版税。
- 智能合约的力量：通过智能合约，版税支付自动执行，无需手动处理。

### 5.2.1 NFT交易所

中心化交易所，如OpenSea，以其用户友好的界面和全面的服务吸引了广泛的用户群体，而去中心化交易所，如Blur，则凭借其高效的交易处理和低成本吸引了更专业的用户。随着NFT市场的不断成熟和扩展，理解这些平台的特点和它们在市场中的作用，对于评估NFT作为一个新兴资产类别的未来潜力至关重要。

OpenSea，作为一个领先的中心化NFT交易平台，提供了一个全面且用户友好的界面，使得艺术家、收藏家和一般用户可以轻松地浏览、购买、出售和拍卖NFT。OpenSea通过其集中化的架构，能够有效地处理大规模的交易并提供额外的安全保护，尽管这也意味着用户必须信任平台并遵守其规定和费用结构。

相比之下，Blur，作为一个去中心化的交易平台，主要关注于为用户提供一个高效和低成本的交易体验。它适用于那些对区块链和NFT市场有更深层次理解的用户，强调的是速度、效率以及用户对自己资产的控制权。虽然去中心化的模式降低了资金被单一实体控制的风险，但它也要求用户对自己的资金和交易安全负有更高的责任。它还支持Blend协议用NFT背书借款。它的特点是不依赖预言机来决定利率或评估NFT价值，而是通过市场条件自动调整。这种模式允许持续的借贷而无需固定到期日，增加了借款人的便利性。借款可能因荷兰式拍卖机制触发的再融资或没人愿意接手债务时被清算。Blend的这种点对点借贷模型和对市场动态的适应性，提供了一个灵活且高效的NFT抵押借款解决方案。

### 5.3 研究数据与方法

本研究采用统计模型和深度学习技术进行实证研究。研究方法包括两个主要阶段。在第一阶段，通过对nftgo.io从2021年4月12日至2022年4月11日期间的总市值数据进行分析，进行后向序列增强的Dickey-Fuller(DF)检验。选择在泡沫期间活跃的PFP项目进行进一步分析。在第二阶段，使用Visual Geometry Group(VGG)-19模型提取所选PFP的特征。利用曼哈顿距离度量方法计算图像之间的相似性，该方法在高维应用中效果显著。此外，使用t分布随机

邻居嵌入 (TSNE) 技术来度量风格相似性，以对 PFP 系列进行聚类。最后，运用对知识产权的理解进行发布后回报分析。利用 NFTGO 获得的平均和初始销售价格计算首日、一月和一年的回报。考虑到 PFP 销售中观察到的高额回报，使用对数变换来减轻每个回报中可能的偏斜。

根据文献的方法，基于后向序列增强的 Dickey-Fuller (BSADF) 检验计算 NFT 市场中泡沫的发生。BSADF 检验在金融时间序列分析中特别有用，因为它可以考虑数据中的非平稳性和内生性。通过使用后向递归残差，它可以检测时间序列中的多个结构性断点。模型可以描述如下：

$$\Delta y_t = \alpha + \beta y_{t-1} + \sum_{i=1}^{p-1} \gamma_i \Delta y_{t-i} + \sum_{i=1}^{q-1} \delta_i \Delta y_{t-i} + \sum_{j=1}^{k-1} \lambda_j D_j y_{t-1} + \epsilon_t \quad (5-1)$$

其中  $\Delta y_t$  是被检验平稳性的时序序列的因变量的一阶差分， $y_{t-1}$  是滞后的因变量， $\sum_{i=1}^{p-1} \gamma_i \Delta y_{t-i}$  是  $p$  阶自回归项， $\sum_{i=1}^{q-1} \delta_i \Delta y_{t-i}$  是  $q$  阶移动平均项， $\sum_{j=1}^{k-1} \lambda_j D_j y_{t-1}$  是后向递归残差， $\epsilon_t$  是误差项。

根据文献的建议<sup>[159]</sup>，BSADF 检验的统计量为：

$$BSADF_t = \frac{T + \gamma}{\alpha_t} \quad (5-2)$$

其中  $T$  是样本大小， $\gamma$  是回归方程中估计系数的函数， $\alpha_t$  是回归的标准误差。

使用现有的 R 包进行超参数调整和可视化<sup>[160]</sup>。输入有 5 个超参数：数据 (y)，滞后阶数 (ADF lag)，信息标准 (IC)，自举重复次数 (nboot) 和最小窗口大小 (swindow0)。由于数据仅涵盖 1 年且频率为 5 天，因此选择 ADF lag 为 1 以获得较小的窗口大小。选择 nboot 为 99 来运行测试并通过自举模拟临界值。同时选择 BIC 以进行一致估计。

在分析的第二阶段，本研究使用 VGG-19 计算图像相似性得分并使用 T-SNE 进行风格相似性聚类。VGG-19 架构以其简单和有效性而闻名，它采用了统一且重复的小型卷积滤波器 (3x3) 结构，步长为 1 像素，这允许学习到更多区分性特征。与使用较大滤波器相比，小型滤波器的使用还有助于减少参数数量并减轻过拟合，这在有限数据量训练时尤其重要<sup>[161]</sup>。使用 VGG-19 从一个 PFP 系列中提取所有特征向量，然后计算它们之间的曼哈顿距离作为独特性的指标。

VGG-19 是一种深度卷积神经网络，它的设计结构相对简单，主要由连续的卷积层和池化层组成，后接全连接层。VGG-19 特别的地方在于它使用了很多层 (共 19 层)，这也是“19”这个数字的来源。

1. 卷积层 (Convolutional Layer)：每个卷积层可以表示为：

$$\mathbf{H}_l = f(\mathbf{W}_l * \mathbf{H}_{l-1} + \mathbf{b}_l)$$

其中，\* 表示卷积操作， $\mathbf{H}_{l-1}$  是第  $l-1$  层的输出， $\mathbf{W}_l$  和  $\mathbf{b}_l$  分别是第  $l$  层的卷积核 (权重) 和偏置， $f$  是非线性激活函数 (如 ReLU)， $\mathbf{H}_l$  是第  $l$  层的输出。

2. 池化层 (Pooling Layer): 池化层通常用于降低特征维度和减少计算量。最常见的是最大池化，可以表示为：

$$\mathbf{P}_l = \text{maxpool}(\mathbf{H}_l)$$

其中， $\mathbf{P}_l$  是池化后的输出。

3. 全连接层 (Fully Connected Layer): 全连接层可以表示为：

$$\mathbf{F}_l = f(\mathbf{W}_l \cdot \mathbf{F}_{l-1} + \mathbf{b}_l)$$

其中， $\cdot$  表示矩阵乘法， $\mathbf{F}_{l-1}$  是上一层的输出， $\mathbf{W}_l$  和  $\mathbf{b}_l$  是全连接层的权重和偏置， $\mathbf{F}_l$  是该层的输出。

T-SNE 是一个将高维数据可视化为二维映射的极佳工具<sup>[162]</sup>。算法首先通过使用高斯核计算高维空间中数据点之间的成对相似度：

$$p_{ij} = \frac{\exp(-|\mathbf{x}_i - \mathbf{x}_j|^2 / 2\sigma_i^2)}{\sum_{k \neq l} \exp(-|\mathbf{x}_k - \mathbf{x}_l|^2 / 2\sigma_i^2)} \quad (5-3)$$

其中  $\mathbf{x}_i$  和  $\mathbf{x}_j$  是高维空间中的数据点， $\sigma_i$  是点  $i$  的高斯分布方差。然后对成对相似度进行标准化以获得联合概率分布：

$$p_{ij} = \frac{p_{ij} + p_{ji}}{2n} \quad (5-4)$$

其中  $n$  是数据点的数量。

在低维空间中，T-SNE 使用学生 t 分布核来计算数据点之间的成对相似度：

$$q_{ij} = \frac{(1 + |\mathbf{y}_i - \mathbf{y}_j|^2)^{-1}}{\sum_{k \neq l} (1 + |\mathbf{y}_k - \mathbf{y}_l|^2)^{-1}} \quad (5-5)$$

其中  $\mathbf{y}_i$  和  $\mathbf{y}_j$  是低维空间中的数据点。

T-SNE 的目标是最小化联合概率分布  $p_{ij}$  和条件概率分布  $q_{ij}$  之间的 Kullback-Leibler 散度：

$$C = \sum_{i \neq j} p_{ij} \log \frac{p_{ij}}{q_{ij}} \quad (5-6)$$

T-SNE 使用随机梯度下降 (SGD) 最小化这个成本函数。算法迭代地更新低维表示  $\mathbf{y}_i$  以最小化成本函数  $C$ 。更新基于成本函数相对于低维表示的梯度：

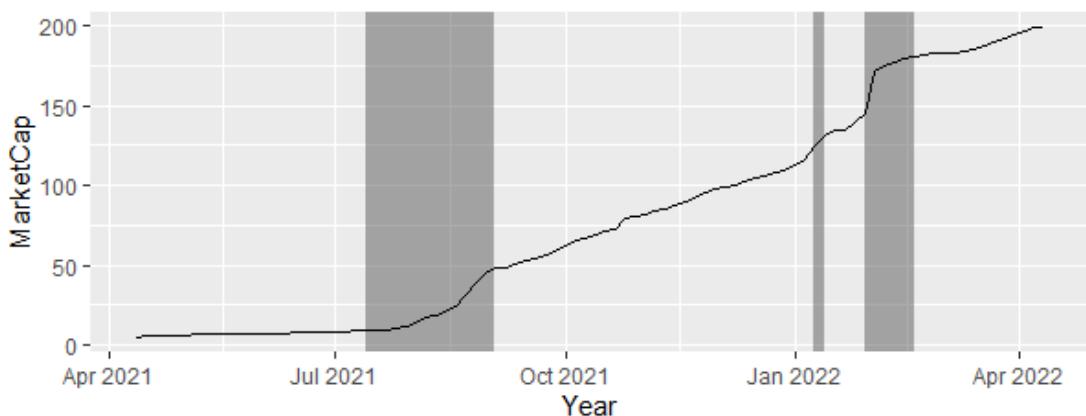
$$\frac{\partial C}{\partial \mathbf{y}_i} = 4 \sum_j (p_{ij} - q_{ij})(1 + |\mathbf{y}_i - \mathbf{y}_j|^2)^{-1} (\mathbf{y}_i - \mathbf{y}_j) \quad (5-7)$$

使用 Python 包 sci-kit Learn 从每个系列中随机挑选 50 张图像进行 TSNE 可视化<sup>[163]</sup>。通过将困惑度微调至 10，图像获得了清晰的聚类。

## 5.4 实证研究

### 5.4.1 PFP 项目的选择

图 5-1 显示，NFT 市场的泡沫期发生在 2021 年 7 月、2021 年 8 月、2022 年 1 月和 2022 年 2 月。研究将聚焦于这些时间段内铸造并拥有最大市值的 PFP 项目。泡沫检测算法用于对这些项目进行案例研究，并将它们标记为市场推动者。这些 PFP 来源于 OpenSea，NFT 的主要市场。选定的 PFP 项目包括：3Landers(1223)、Auzki(1214)、coolcats(500)、creatureworld(550)、deadfellaz(700)、flufworld(450)、in-visible fren(700)、karafuru(700)、ON1 force(536)、pudgy penguins(750)、supducks(500)、world of women(3446)、bored ape yacht club(9997)。



**图 5-1 NFT 市场中的泡沫期（实线是 1 年 NFT 市场总值的扩散，阴影区域是潜在泡沫，阴影区域是 PSY 统计量超过其 95% 自举临界值的时期）**

**Figure 5-1 Bubble Periods in NFT Marketplace (The solid line is the 1-year NFT market cap spread and the shade area is the potential bubble, the shaded areas are the periods where the PSY statistic exceeds its 95% bootstrapped critical value)**

### 5.4.2 风格相似性、知识产权和发布后市场表现

通过 t 分布随机邻居嵌入 (t-SNE)，可以洞察到收藏品之间的相似性，因为高维空间中的邻近点可以转换到低维空间。在图 5-2 中，观察到不同收藏系列之间明显的聚类，例如 Pudgy Penguins 和 Coolcats、3Landers 和 Supducks、Creature World 和 Deadfellaz，当多个 PFP 重叠时，明显的聚类现象尤为突出。在图 5-3 中，当 Pudgy Penguins 和 Coolcats 授予持有者知识产权 (IP) 时，它们显示出类似的价格表现。然而，3Landers 和 Creature World 明确表示其持有者没有 IP 权利。与风格相似的 PFP 系列相比，3Landers 的一年回报显著低于 Supducks，而 Creature World 的一年回报相比于 Deadfellaz 则相对较低。有趣的是，3Landers 和 Creature World 展现出非常高的 30 天回报和非常低甚至负的一年回报，这表明可能存在操纵市场和倾销的行为。



图 5-2 PFP 风格聚类  
Figure 5-2 PFP Style Clustering

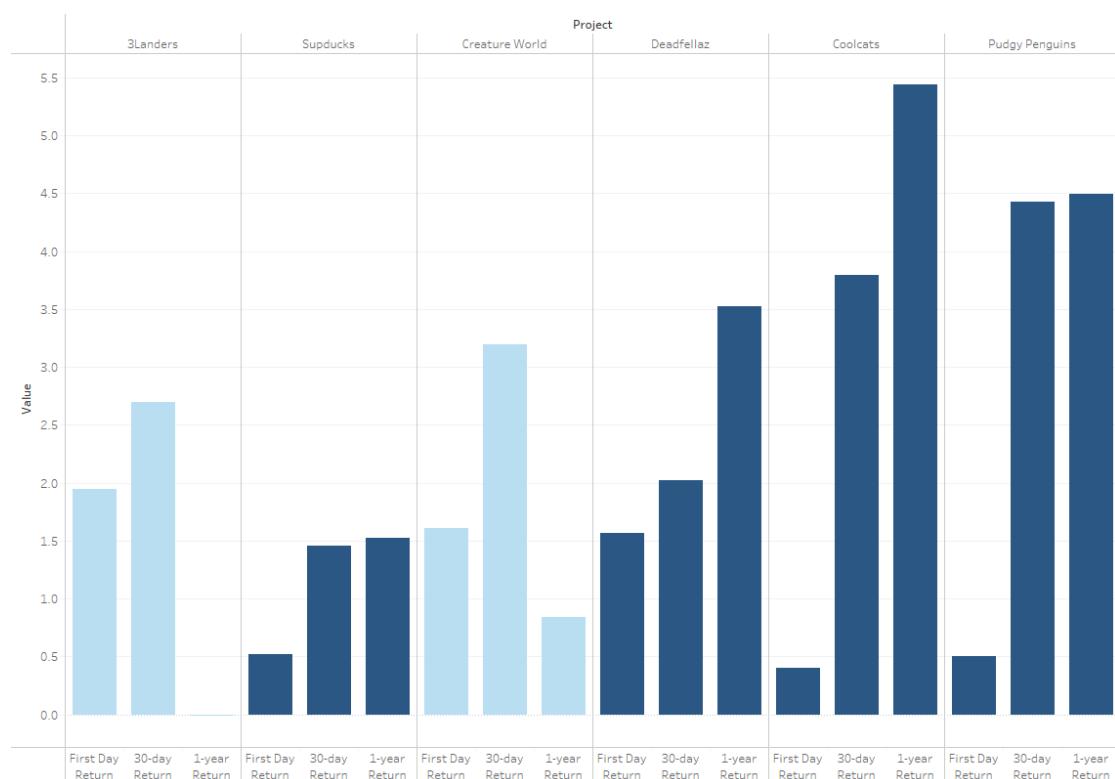


图 5-3 具有相似风格的 PFP 系列间的发布后表现。浅蓝色 = 无知识产权。深蓝色 = 有知识产权。)

Figure 5-3 Bubble Periods in NFT Marketplace (Post-launch performance between PFP collections with similar styles. Light blue = No IP rights. Dark blue = IP rights.

### 5.4.3 图像相似性（独特性）、知识产权和发布后表现

PFP系列图像相似性计算得分，代表了独特性这一PFP的主要卖点之一。在分析的13个PFP项目中，有四个项目要么含糊其辞，要么明确指出持有者没有知识产权（IP）权利。为了增强PFP销售表现的可比性，对销售价格进行了对数变换以消除异常值。值得注意的是，在拥有IP权利和没有IP权利的PFP项目之间观察到一种二元性。具体来说，在图5-4中，没有IP权利的PFP项目，例如Karafuru和ON1Force，在其曼哈顿距离较大时展现出更高的首日回报。有趣的是，具有更大独特性的PFP项目，如Azuki和World of Women，并没有显示出相应高的首日回报。这种二元性的一个可能解释是，没有IP权利的PFP项目可能有更积极的营销活动来弥补其缺乏IP保护的不足。在图5-5中，没有IP权利的PFP项目展现出一致的30天回报，而拥有IP权利的PFP项目并没有显示出独特性与30天回报之间的明显关系。在图5-6中，观察到拥有IP权利和没有IP权利的PFP项目之间存在类似的二元性，后者展示出更低的一年回报。此外，具有更大独特性的PFP项目往往具有更高的一年回报。总结来说，没有IP权利的PFP项目在首日回报上与独特性呈正相关，而拥有IP权利的PFP项目之间则观察到负相关。就30天回报而言，没有IP权利的PFP项目倾向于展现更一致的回报，而拥有IP权利的PFP项目表现出更大的变化性。

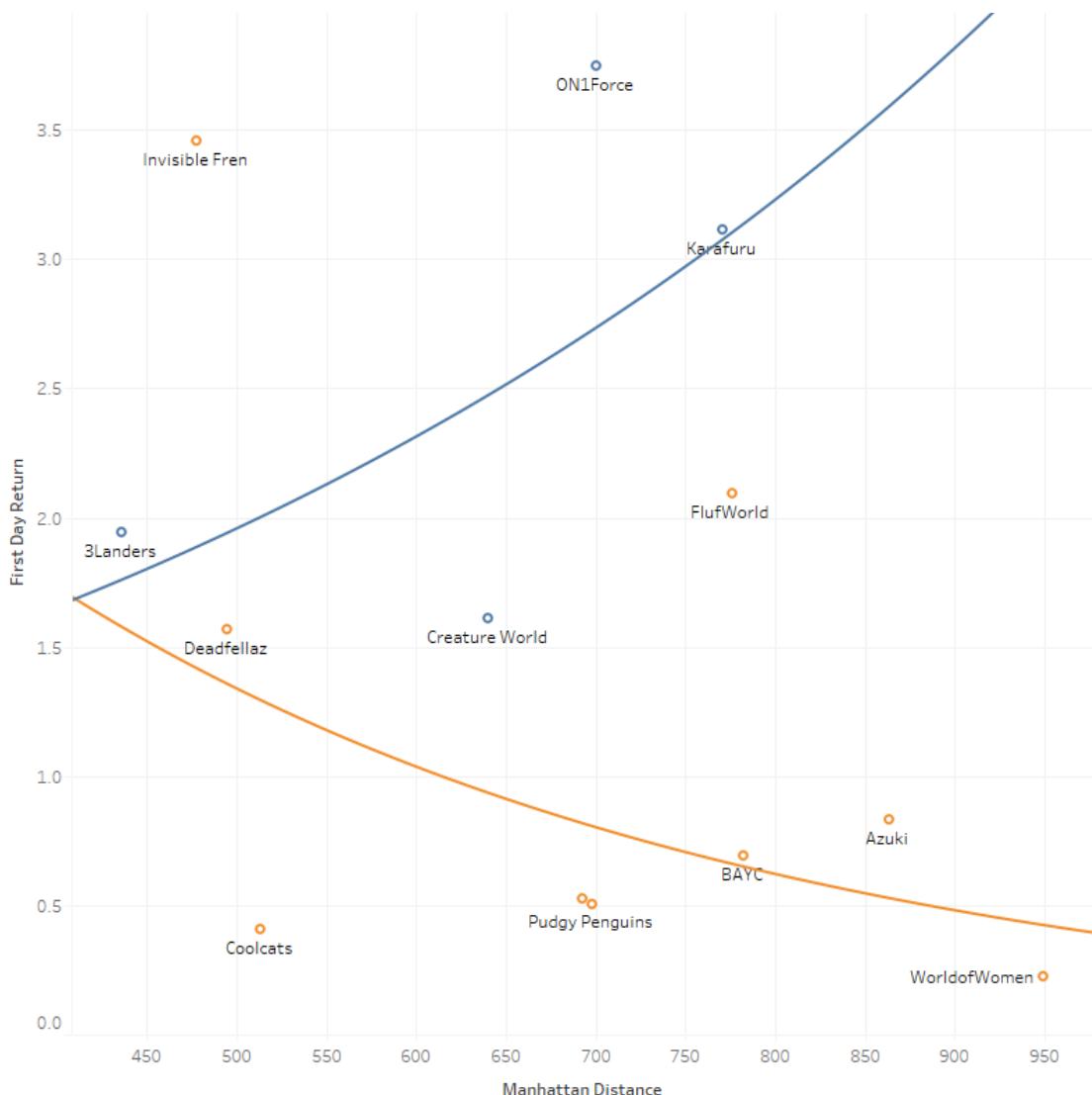


图 5-4 发布后表现与首日回报之间的关系。具有更高曼哈顿距离的 PFP 系列更为独特。蓝色 = 无知识产权的 PFP 项目。橙色 = 拥有知识产权的 PFP 项目。

蓝色线条 =  $0.85 \times \exp(0.0016687 \times \text{曼哈顿距离})$ , R 平方 = 0.3704, P 值 = 0.3913

橙色线条 =  $4.82 \times \exp(-0.00256 \times \text{曼哈顿距离})$ , R 平方 = 0.2479, P 值 = 0.1726

**Figure 5-4 Post-launch performance between uniqueness and first-day returns. PFP collections with higher Manhattan Distance are more unique. Blue = PFP projects with No IP rights. Orange = PFP projects with IP rights.**

Blue line =  $0.85 \times \exp(0.0016687 \times \text{Manhattan distance})$ , R-Squared = 0.3704, P-value=0.3913

Orange line =  $4.82 \times \exp(-0.00256 \times \text{Manhattan distance})$ , R-Squared = 0.2479, P-value=0.1726

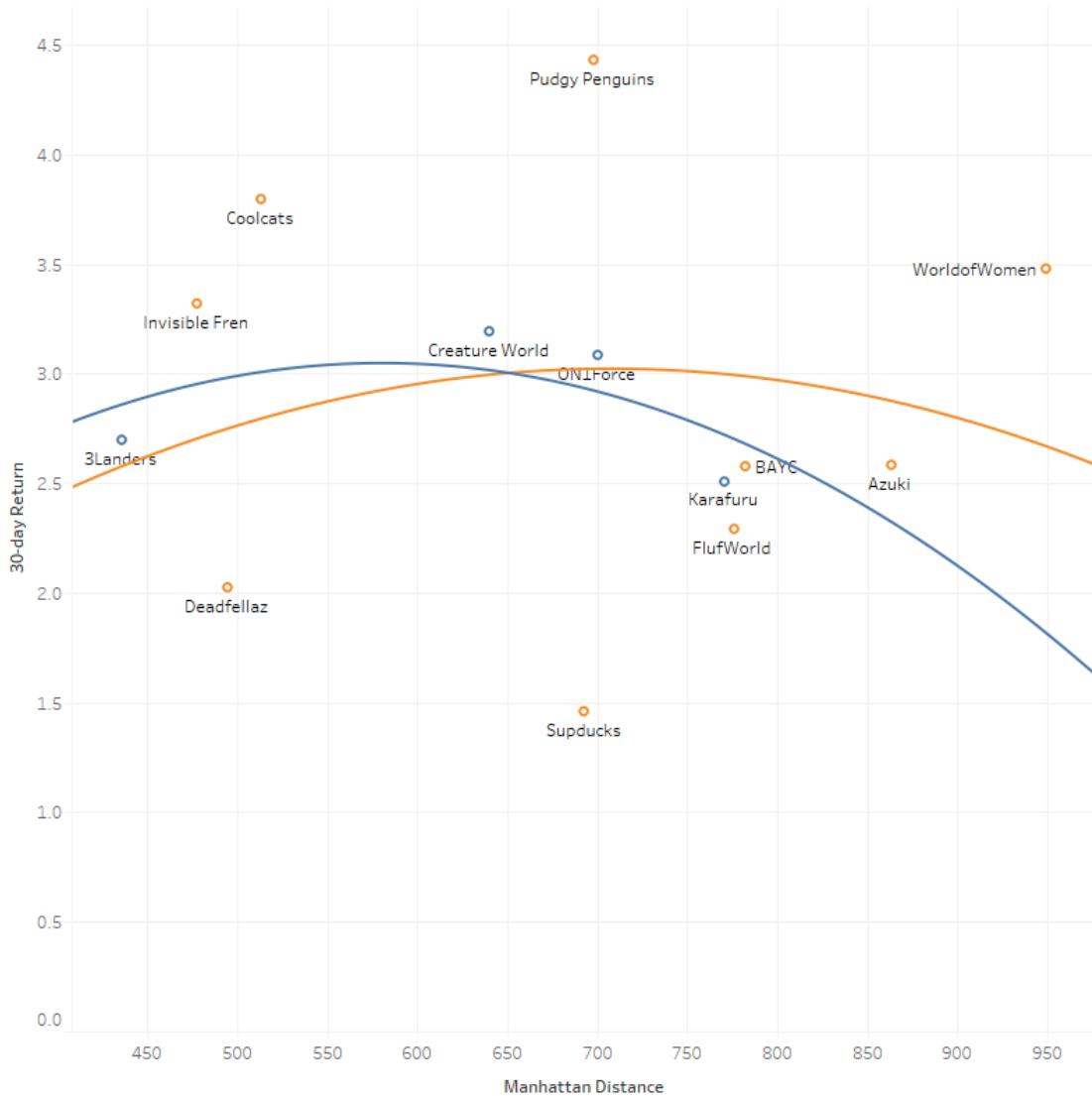


图 5-5 发布后表现与 30 天回报之间的关系。具有更高曼哈顿距离的 PFP 系列更为独特。

蓝色 = 无知识产权的 PFP 项目。橙色 = 拥有知识产权的 PFP 项目。

蓝色线条 =  $-9.04e-6 \times \text{曼哈顿距离}^2 + 0.01 \times \text{曼哈顿距离}$ , R 平方 = 0.9961, P 值 = 0.0039

橙色线条 =  $-6.04e-6 \times \text{曼哈顿距离}^2 + 0.008 \times \text{曼哈顿距离}$ , R 平方 = 0.9056, P 值 = 0.0002

**Figure 5-5 Post-launch performance between uniqueness and 30-day returns. PFP collections with higher Manhattan Distance are more unique.Blue = PFP projects with No IP rights. Orange = PFP projects with IP rights.**

**Blue line =  $-9.04e-6 \times \text{Manhattan Distance}^2 + 0.01 \times \text{Manhattan Distance}$ , R-Squared = 0.9961, P-value=0.0039**

**Orange line =  $-6.04e-6 \times \text{Manhattan Distance}^2 + 0.008 \times \text{Manhattan Distance}$ , R-Squared = 0.9056, P-value=0.0002**



图 5-6 发布后表现与一年回报之间的关系。具有更高曼哈顿距离的 PFP 系列更为独特。蓝色 = 无知识产权的 PFP 项目。橙色 = 拥有知识产权的 PFP 项目。  
 蓝色线条 =  $0.80 \times \ln(\text{曼哈顿距离}) - 4.68$ , R 平方 = 0.1323, P 值 = 0.6363  
 橙色线条 =  $1.08 \times \ln(\text{曼哈顿距离}) - 3.21$ , R 平方 = 0.0214, P 值 = 0.7070

Figure 5-6 Post-launch performance between uniqueness and one-year returns. PFP collections with higher Manhattan Distance are more unique. .Blue = PFP projects with No IP rights. Orange = PFP projects with IP rights.  
 Blue line =  $0.80 \times \ln(\text{Manhattan Distance}) - 4.68$ , R-Squared = 0.1323, P-value=0.6363  
 Orange line =  $1.08 \times \ln(\text{Manhattan Distance}) - 3.21$ , R-Squared = 0.0214, P-value=0.7070

## 5.5 结论

本文专注于识别 2021 年 7 月至 2022 年 2 月期间 NFT 市场中四个泡沫时期里具有市场影响力的 PFP（个人形象头像）项目。通过应用泡沫检测算法，选出了 OpenSea（NFT 的主要市场）中市值最大的 13 个 PFP 项目。分析集中在探究这些项目在知识产权、图像相似性和上市后表现方面的相似性和差异。

T-SNE 分析显示了不同 PFP 项目间明显的聚类，表明存在具有不同特征的 PFP 类别。聚类模式也暗示风格相似的 PFP 往往有相似的上市后表现。然而，也发现某些 PFP 项目由于缺乏知识产权可能导致潜在的炒作和抛售行为。

深度学习分析表明，缺乏知识产权的 PFP 项目，如 Karafuru 和 ON1Force，在曼哈顿距离较大时展现出更高的首日回报。在 30 天内，缺乏知识产权的 PFP 项目往往显示出更一致的回报，而拥有知识产权的 PFP 项目则表现出更大的变化性。然而，具有更高独特性的 PFP 项目无论是否拥有知识产权，一年回报率都倾向更高。

该研究由于没有考虑其他金融资产、团队专业知识和社交媒体活动对 PFP 上市后表现的影响而受到限制。未来的研究可能会纳入这些变量，以构建更全面的 PFP 项目定价模型。

## 5.6 本章小结

本研究分析了 2021 年 7 月至 2022 年 2 月期间 NFT 市场中 13 个主要 PFP 项目的特性，发现风格相似的 PFP 在发布后表现上有类似趋势。分析还指出，没有知识产权的 PFP 项目在短期内可能表现更好，但独特性更高的项目在长期回报上更为优秀。



## 第6章 社交媒体舆情对首次交易所发行（IEO）的影响：市场营销与操纵策略的分析

### 6.1 引言

自新冠大流行开始以来，全球加密货币市场经历了显著增长，其市值从2017年的8000亿美元飙升至2023年的1.1万亿美元。尽管比特币占据了超过一半的市场份额，但其他加密货币也占据了市场相当部分的份额。

首次代币发行（ICO）已成为一种创新的融资机制，使组织能够通过出售加密保护的数字资产，即代币或硬币，给投资者筹集资金<sup>[164]</sup>。这些资产基于区块链技术，提供了从个人信任到数学算法信任的范式转变<sup>[165]</sup>。

ICO 与众筹在利用互联网平台进行筹资方面有相似之处，宣传视频和文章是吸引投资者的关键。然而，ICO 与传统众筹不同，它提供的代币不仅可以访问产品和服务，还具有未来增长的潜力。这一点，加上缺乏严格的监管和对该领域的全面理解，使得 ICO 领域被比喻为“wild west”。

与此相反，首次交易所发行（IEO）是在加密货币交易所的监督下进行的，为区块链项目提供了一个受监管的平台，用于筹集资金和推出其代币。据加密货币交易所币安所述，IEO 受到严格审查，包括评估商业模式、团队专业知识、实际用例和详细的白皮书<sup>[166]</sup>。因此，投资者可能因其受监管的性质而偏好 IEO 而非 ICO。

本文探讨了情感和社交机器人在 IEO 前期的作用及其对 IEO 后期表现的影响。尽管声称受到更多监管，IEO 仍然是未注册的证券，交易所从这些项目的交易费中获利。即使是“受监管最严格”的交易所 FTX，也被媒体披露非法使用100亿美元的客户资金<sup>[167]</sup>。这项研究旨在调查是否出现了传统金融中低交易量的便士股票（penny stock）上常见的哄抬抛售（pump-and-dump）计划的迹象。在加密货币市场，欺诈者在社交媒体上制造炒作以吸引注意力。正如诺贝尔奖得主赫伯特·A·西蒙所言，“信息的丰富创造了注意力的贫乏”；注意力本身就是货币。一旦欺诈者通过社交媒体收集到足够的注意力，他们就可以在 IEO 阶段后抬高价格，然后逐渐将它们抛售给投资者。

在 IEO 前期，利益相关方通过发布宣传文章和鼓励讨论来制造炒作并吸引关注，从而构建项目的“第一印象”。Telegram 和 Discord 等新兴社交媒体平台尚未成为主流，大多数讨论活动仍然集中在 Twitter 上。这种现象在加密货币市场和传统金融领域均有出现。Lidingo Holding 专注于为上市公司提供投资者关系和推广研究服务，也曾涉足股市的哄抬抛售策略<sup>[168]</sup>。该研究并非旨在验证每条信息的真实性，而是旨在衡量那些 Twitter 账户的机器人行为以及这些信息背后的情绪。该研究收集了2017年至2022年所有币安 IEO 项目在推出前一个月的超过11,000条推文，并进行了描述性分析。通过主题建模，该研究探讨了币安与首次交易所发行（IEO）项目之间的关系，并将主题分类为与币安相关、与

项目相关和与机器人相关。研究发现，进行空投的项目中机器人评论普遍存在，部分项目如“Loka”表现出强烈的哄抬抛售迹象。Botometer 算法被用来生成机器人分数，情感分析则采用了 python 库 TweetNLP 中的 RoBERTa（强大优化的 BERT 预训练方法）来生成情绪分数<sup>[169]</sup>。研究开发了两个附加的社交指标：一个是对机器人影响情绪的惩罚分数，另一个是机器人分数与情绪分数之间的交互作用项。通过回归分析，研究探讨了社交因素对 IEO 后期表现的预测力。研究发现，机器人分数与 30 天回报之间存在负相关，而与 30 天波动性之间存在正相关。此外，观察到交互作用项在决定 30 天波动性方面具有最强的预测力。

该研究在三个方面为文献做出了贡献。首先，研究对币安这一最大加密货币交易所的所有初始交易所发行（IEO）进行了全面调查，而不仅仅关注市值较小的首次代币发行（ICO）项目，认识到市值较高的 IEO 项目对投资者构成更大的风险。其次，研究提出了一个分析 IEO 启动前社交媒体活动的框架，运用两种算法生成机器人分数和情绪分数，并研究了机器人活动对情绪的潜在影响，计算了交互作用项和惩罚分数来衡量影响。第三，研究利用各种经济指标评估了 IEO 后期的表现，是首次探讨机器人活动与 IEO 后期表现关联的研究。

IEO 被宣传为具有高市值的稳健技术和商业投资，不会发生哄抬抛售事件。然而，研究的发现表明，通过利益相关方的精心规划，这类事件仍有可能发生。因此，该研究为投资者提供了一个模型，以分析 IEO 项目的质量并保护自己免受可能的哄抬抛售计划的伤害。研究强调，收集 IEO 前期的讨论和评估机器人参与度能有效检测潜在的哄抬抛售事件。

## 6.2 相关文献

初始代币发行（ICO）和初始交易所发行（IEO）已成为加密领域流行的筹资机制。然而，它们并非没有风险。虽然一些项目真正展示了技术创新，但很多其他项目是承诺高回报的庞氏骗局。哄抬抛售计划是加密领域常见的欺诈形式。这些计划通过广泛的宣传讨论人为地抬高代币价格，以混淆人们的判断。零售投资者因对技术创新的看法而买入，推高了价格。随后，价格被抬高，之后又被抛售给毫无戒备的买家。这种复杂的庞氏骗局需要大量的宣传努力来吸引投资者，使骗局看起来吸引人。

由币安支持的 IEO 项目 Axie Infinity 就是其中一个例子。该项目承诺了一个人们可以同时工作和玩耍的乌托邦式的世界愿景。它甚至在由风险投资公司 Andreessen Horowitz 领投的 B 系列轮中筹集了 1.52 亿美元。投资页面声明，玩家可以通过在游戏中赢得战斗来赚取 SLP 代币，以及购买游戏内物品的 AXS 代币。该项目甚至声称游戏正在取代传统的就业形式。然而，《时代》杂志发布的一份报告揭示了 Axie Infinity 的经济结构是不可持续的，代币价值依赖于新人入场<sup>[170]</sup>。

### 6.2.1 初始代币发行

Hasti Chitsazan 和 Tajeddin 采用信号理论和 ICO 过程的阶段性视角, 对 78 项经验研究进行了系统回顾, 这些研究时间跨度为 2017 年 1 月至 2022 年 1 月, 研究内容包括 ICO 成功的概念、理论和决定因素。该综述探讨了 ICO 成功的六个主要决定因素: 创始人、ICO、创业企业、市场、投资者和背景。创始人通过有意选择这一融资方式来启动 ICO 过程, 并选择类型和质量的信号, 以鼓励投资者参与并支持不同背景下的 ICO 项目。在此综述的基础上, 提出了一个 ICO 成功模型, 追踪了 ICO 过程中各个阶段的成功因素。最后, 强调了未来研究的议程以及对政策、理论和实践的影响。<sup>[171]</sup> Momatz 首次提供了在创业金融背景下信号传递中的道德风险证据, 通过研究代币发行或初始代币发行 (ICOs)。在竞争获取增长资本的过程中, 创业者传递质量信号的能力至关重要。然而, 缺乏验证内生信号的机构可能导致信号传递中的道德风险。与此假设一致, 人工智能语言分析表明, 代币发行者系统性夸大了在白皮书中披露的信息。夸大的创业者能够在更短的时间内筹集更多资金, 表明投资者最初并未识破这一做法。最终, 投资者通过与其他投资者进行交易来了解夸大偏见, 导致投资者失望, 加剧了加密货币贬值和平台失败的风险。<sup>[172]</sup> Wang 和 Qin 构建了一个文档分析深度回归模型 (DADRM), 以创新地从白皮书中提取深层文本和布局特征。基于真实数据集, 进行了比较研究, 评估了所提出的框架在预测 ICO 成功 (以融资金额为指标) 方面的有效性。经验结果显示, 该模型既提取文本内容又保留文档的原始二维结构, 可以显著减少预测误差。基于该提出的模型, ICO 平台和投资者都可以预测加密货币项目的融资金额, 并减轻信息不对称。此外, 该研究还表明, 商业文件中的内容以及文件的呈现方式都会影响投资者的决策。<sup>[173]</sup>

Fisch 等人利用一组包括 517 名 ICO 投资者的主要数据集, 通过因子分析识别和分类了投资 ICO 的动机。发现投资者的动机包括意识形态、技术和财务动机。在动机的相对重要性方面, 技术动机被认为是 ICO 投资者最关注的, 其次是财务和意识形态动机。通过进行回归分析, 以不同的动机来区分投资者, 研究发现不同动机的投资者在风险感知、信息来源和对严格监管的需求等方面存在显著差异。<sup>[174]</sup> Xu 和 Zhao 揭示了先前的研究主要使用与项目相关的因素来预测 ICO 成功, 而忽略了团队信息和专家评估等社会因素。受到企业的知识基础理论 (KBT) 启发, 旨在研究团队知识和专家评估对 ICO 成功的影响。本研究的一个主要贡献是基于 KBT 设计了新颖的知识度量标准。此外, 提出了一个深度学习模型——基于注意力的双向递归神经网络 (A-BiRNN), 用于自动从在线评论中提取特征。研究在实际数据集上验证了所提出的模型, 并实验结果显示, 所提出的预测模型的准确性超过了现有模型超过 6%, 突显了所提出方法在预测 ICO 成功方面的有效性。本研究的结果为投资者和 ICO 平台提供了有关评估加密货币项目质量的有用思路, 从而改善了 ICO 市场中的信息对称性。此外, 本研究还展示了在 ICO 市场评估企业绩效方面应用 KBT 的价值。所提出方法的广义价值应该在更多的商业背景下进行测试, 如众筹和点对点 (P2P) 借贷。<sup>[175]</sup>

Lyandres 和 Rabetti 整合了包括 11 个 ICO 聚合器在内的 19 个数据来源，构建了一个全面的初始代币发行（ICO）数据集。通过对 ICO 数据质量的首次系统分析，缓解了现有 ICO 数据的严重限制。利用这个数据集研究了 ICO 融资成功的决定因素，以及 ICO 后的运营绩效，并提供了一些关于初始和长期 ICO 成功的新颖决定因素的证据。最后，研究表明，ICO 后的运营绩效与同时期代币回报呈正相关，一般与代币回报的波动性呈负相关，表明 ICO 后的运营绩效具有财务影响。<sup>[176]</sup> Aylin 等人对 ICO 成功的决定因素以及 ICO 的售后表现进行了全面分析。证据表明，拥有更高评级、计划代币销售期限较短、代币销售份额较小、拥有更多专家和开发团队成员的 ICO 更有可能成功，并筹集更多资金。研究还展示了发行价格和市场情绪在解释长期的 ICO 后绩效方面起着重要作用。然而，在加密货币市场的繁荣与低迷期间，成功的 ICO 和 ICO 后绩效的关键因素存在差异<sup>[177]</sup>。Davydiuk 等人提供了证据表明，创业者使用保留来减轻信息不对称。由于底层技术和缺乏监管，ICO 市场非常适合从经验角度研究这个问题。利用手工收集的数据集，显示保留更多代币的 ICO 发行者在融资努力方面更加成功，并更有可能开发出可行的产品。此外，发现在市场拥挤且投资者没有足够时间进行尽职调查时，保留成为更强的信号。研究表明，企业家通过在 ICO 市场中自持代币来传递其项目质量，这与 ICO 的成功呈正相关<sup>[178]</sup>。

### 6.2.2 哄抬抛售操纵系统

由于对市场操纵和欺诈的担忧，对 ICO 中哄抬抛售计划的研究有所增加。Hamrick 等人发现这种计划在 Discord 和 Telegram 上广泛存在，庄家明牌哄抬价格更为成功。他们建议监管机构通过关注最多的交易所和哄抬渠道来干预未来的计划<sup>[179]</sup>。Nghiem 和 Ferrara 提出了一种方法，利用基于神经网络的架构，使用市场和社交媒体信号来预测每次炒作前的目标加密货币，并提供了关于它们黑匣子性质的可解释见解。此外，构建了能够在揭示加密货币的身份后预测炒作引发的最高价格的模型，误差在 6.1% 以内。研究了最佳的时间窗口，并描述了使用社交数据来预测加密货币交易中的操纵的局限性。实验结果证明了使用公开可用数据识别加密货币炒作和倒卖欺诈的可行预测专家系统的存在<sup>[125]</sup>。Balciar 和 Ozdemir 研究了比特币与替代币市场在细分层面上的非对称波动传染效应。采用了频率联系方法，对从 2017 年 9 月 1 日至 2022 年 3 月 2 日的 11 种主要加密货币的日常数据进行了分析。尝试揭示在加密市场中存在的“错失机会恐惧”心理效应和“炒作和倒卖计划”。为此，估计了比特币对替代币的波动传染以及在牛市和熊市中的加密货币的自身风险传染效应。比特币对替代币的波动传染结果对于主要加密货币是否存在这种理论存在不确定性。然而，通过加密货币的自身波动传染效应进行的实证研究充分证实了除了 USDT 外，所有加密货币都存在“错失机会恐惧”效应和“炒作和倒卖计划”的存在。<sup>[180]</sup> Morgia 和 Stefa 对互联网社区组织的两种市场操纵行为进行了深入分析：炒作和倒卖以及群体炒作。炒作和倒卖计划是股票市场上的一种古老欺诈行为，现在在加密货币市场这个监管较松散的市场上重新焕发生机。高度协调的群体通常在 Telegram 和 Discord

上有组织地安排这种欺诈行为。在超过3年的时间内监控了这些群体，检测到了约900个个别事件。报告了与炒作和倒卖群体相关的三个案例研究。利用我们独特的已验证炒作和倒卖数据集，构建了一个机器学习模型，能够在炒作和倒卖开始的25秒内检测到，达到94.5%的F1分数。后来，其他Reddit社区在加密货币市场上复制了这一操作。目标是狗狗币(DOGE)和瑞波币(XRP)。研究重构了这些操作是如何发展的，并讨论了与标准的炒作和倒卖的差异和类似之处。<sup>[181]</sup> Chullamonthon和Tangamchit的研究聚焦于股价操纵行为，通过结合无监督深度学习和监督深度学习方法来提高操纵行为检测的准确性。使用泰国证券交易所的实际案例进行验证，新的集成模型在检测股价操纵方面表现出更高的检测率，能够识别出所有真实操纵案例并降低误报率。采用了长短时记忆(LSTM)网络和支持向量机(SVM)等技术来构建这一有效的检测方法。<sup>[182]</sup>

### 6.2.3 社交机器人

社交机器人可以通过传播虚假和误导性信息，或人为地传播积极情绪来操纵关于金融资产(如股票或加密货币)的公共舆论。Mbona和Eloff的研究应用本福特定律于Twitter数据集来区分人类和恶意机器人账户。虽然有效，但该定律的局限性在于它只适用于仅含有数字的数据集<sup>[183]</sup>。Mazza和Tesconi通过大规模定量分析，探究了这些不同账户的特征，特别关注了以往研究较少的Twitter国家支持的网络水军。通过分析账户的信誉度、主动性和适应性，研究发现可以有效区分这些不同的账户。实验结果表明，结合这三种特质可以更准确地进行分类，进一步的分析还揭示了在识别不同类型账户时，某些特征(如转推模式和URL共享)的重要性。<sup>[184]</sup> Beatson和Elliot探讨了社交媒体中机器人(bot)检测方法的有效性，并指出现实中实时检测几乎不可能，因此普通Twitter用户难以判断哪些账户是机器人，也无法知道他们在网上被操纵的程度。文章通过构建两种不同的机器人检测方法来展示检测的挑战：第一种方法基于固定标准，采用常见的机器人识别标识；第二种方法采用更灵活的调查方法，揭露参与协调努力影响在线辩论的机器人。研究还提出了一个评估框架，定义了四个关键标准来评估这些方法的效果，并以准确性为核心标准进行了比较。研究结果显示，不同的机器人检测方法会呈现出显著不同的结果，只有通过Twitter的官方确认(如账户暂停或声明)才能真正让用户知道一个账户是否为机器人。这一发现对社交媒体用户对他们通过社交媒体接收的信息以及政治过程的信任水平可能产生重大影响。<sup>[185]</sup> Heidari等人分析了社交媒体机器人如何利用推文情感来产生逆火效应(backfire effect)和确认偏误(confirmation bias)，从而创造虚假趋势或改变公众舆论，探讨了情感特征对社交媒体机器人检测机器学习模型准确性的影响。研究分析了基于情感特征的机器人检测问题，并基于在线评论的文本信息创造新特征。此外，文章提出了一种定量方法来创造新特征，并比较了用于机器人检测的机器学习模型。特别地，研究实现了针对荷兰语的新模型，并基于新的情感特征实现了超过87%的荷兰推文检测准确率，展示了基于推文文本的心理和社会因素的新情感特征为社交媒体机器人检测开辟了潜在的研究领域。<sup>[186]</sup>

Cai 和 Wang 的研究结合机器学习和因果回归方法，探讨社交机器人如何影响社交媒体信息传播机制。研究基于利益相关者视角和情感传染理论提出问题和假设，分析了与 COVID-19 相关的两个时间段内的微博公共舆论数据。通过比较分析，研究发现社交机器人在某些话题中发挥重要作用，倾向于传播负面情绪信息，但在传播负面情绪方面能力不如人类用户。此外，使用格兰杰因果关系测试（Granger causality）确认人类和机器人情绪在时间序列中可以相互预测<sup>[187]</sup>。Pastor-Galindo 和 Perez 根据行为将 Twitter 用户分类为三组：可能是人类、可能是半机器人和可能是机器人，发现每组具有不同的行为和不同的网络影响力。可能是人类的影响力最大，可能是半机器人产生大量内容，可能是机器人虽然分享较少，但位于战略位置并参与的推文比预期的多。所有组别都讨论相同的话题，可能是为了侵占趋势话题标签，其中可能是半机器人在传播内容方面特别有效<sup>[188]</sup>。

### 6.3 研究方法

#### 6.3.1 IEO 前期社媒舆情和 IEO 后期表现的时间线

本研究的目标是在币安 IEO 项目上市前尽可能多地收集 Twitter 上的讨论。为此，本研究从 coincodex.com 上 IEO 结束日期前的一个月内提取用户名、日期和推文数据。使用大小写的代币/硬币符号和完整的项目名称进行搜索。对于数据抓取过程，本文使用 Twitter 官方 API，并使用一个名为 TweetNLP 的 Python 包来分析用户情绪。为了确定机器人的参与度，本文使用 Botometer。图 6-1 展示了分析 IEO 中哄抬抛售计划的时间线。

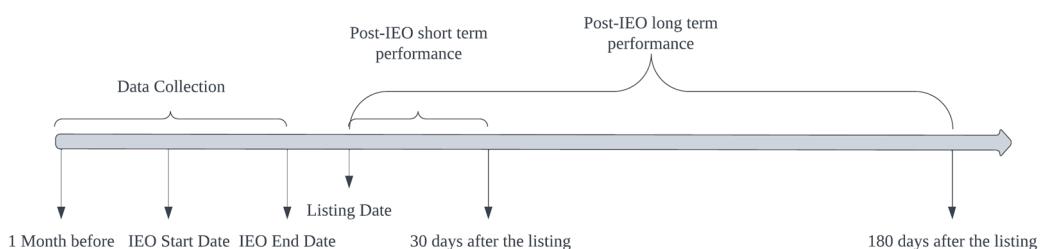


图 6-1 IEO 前期社媒舆情和 IEO 后期表现的时间线)

Figure 6-1 Timeline for Analyzing Pre-IEO Discussion and Post-IEO Performance

#### 6.3.2 数据收集

为了确保对公众情绪的分析有一个标准化和一致的基础，本研究选择收集币安上所有 IEO 项目一个月的 Twitter 舆情数据。数据集包含了 2017 年至 2022 年间 53 个项目的超过 110,000 条由独立账户发布的推文。在机器人检测任务中，本文排除了重复账户并采用平均机器人分数来代表机器人在 IEO 项目中的参与度。通常情况下，利益相关者会发布目标代币以及他们想要推广的其他代币，并

且推文中经常包含私人聊天群组链接以获得个人收益。为了捕捉真实的情绪，本文移除链接和不相关的代币来过滤抓取的数据。此外，本研究只包括评论数超过1000的项目。最终，选定了22个IEO项目进行分析。

### 6.3.3 探索性分析-主题建模

币安作为一个著名的加密货币交易平台，对初始交易所发行(IEO)抱有浓厚的兴趣，并因此在Twitter上进行广泛的市场营销活动。此分析的单位是单个推文。为了分析IEO启动前的主题和讨论，本研究采用了Bidirectional Encoder Representations from Transformers Topic(BERTopic)，这是一种用于通过高级嵌入生成主题的算法<sup>[189]</sup>。一个包含11,000条独特推文的数据集被输入模型，为每个IEO项目生成四个主题。Axie Infinity仅有两个主题，因为大量信息重复。该算法采用基于类别的词频-逆文档频率(TF-IDF)来选择主题。具体来说，它将单一类别或簇内的所有文档视为一个统一的文档，并对这个集合单位应用TF-IDF。结果是每个类别的长文档，其生成的TF-IDF分数表明了主题内的重要词汇。基于类别的TF-IDF公式如下：

$$C - TF - IDF_i = \frac{t_i}{w_i} \times \log\left(\frac{m}{\sum_j^n t_j}\right)$$

其中，每个类别*i*中每个词*t*的频率被计算并通过总词数*w*进行标准化，从而调整类别中频繁词的影响。然后，为了衡量一个词在所有类别中的重要性，将文档总数*m*除以该词在所有类别*n*中的总频率。

在此主题分析中有两个目标。第一个目标是探索币安与初始交易所发行(IEO)项目之间的关系。第二个目标是初步了解与这些IEO项目相关的机器人评论。基于这些目标，将主题分为三类：与币安相关、与项目相关和与机器人相关。

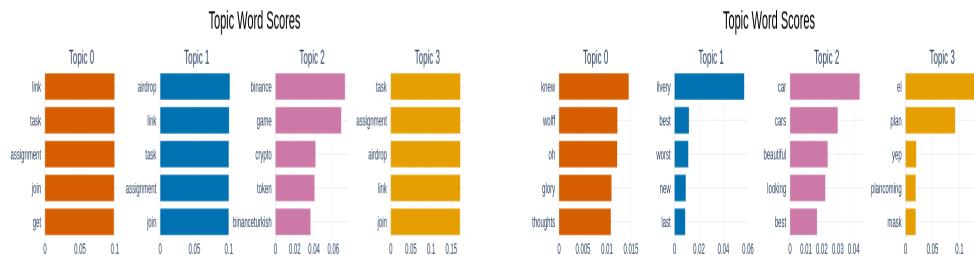
本研究使用以下标准确定分类。对于与币安相关的主题，识别关键词如“币安”和“发射台(launchpad)”，并将代币与这些关键词关联。对于与项目相关的主题，如果主题提到了一个项目名称如“sandbox”，一个区块链游戏，并包含了描述项目的词汇如“games”，“regulatory”，“kids”，和“fintech”，则关联的代币会被归类为与项目相关。最后，本文将包含无意义热词如“good”，“yeah”，“try”，“nice”，“airdrop”，和“tickets”的主题定义为与机器人相关。关键词如“pump”和“dump”出现在FET和SFP代币的主题表示中；值得注意的是，虽然这两个代币最初价格上涨，但其180天回报率随后表现下降。

值得一提的是，在加密货币的背景下，空投指的是向特定加密货币的现有持有者分发免费代币或硬币，通常作为市场营销或促销策略。有空投的项目可能会吸引大量机器人评论。如图6-2所示，这一现象在“Alice”，“Axie Infinity”，和“Loka”等区块链游戏中尤为明显，因为游戏中的空投通常提供对某些功能的早期访问。在评论中使用热词“thanks”是用户对收到空投表示感谢的一种方式。

例如，“Loka”有一个0.365898的机器人评分，这反映在与其相关的主题中。与“Loka”相关的所有四个主题都展示了机器人相关活动的迹象，其IEO后的表现展示了强烈的哄抬抛售行为迹象。表6-1展示了基于主题的代币分类。

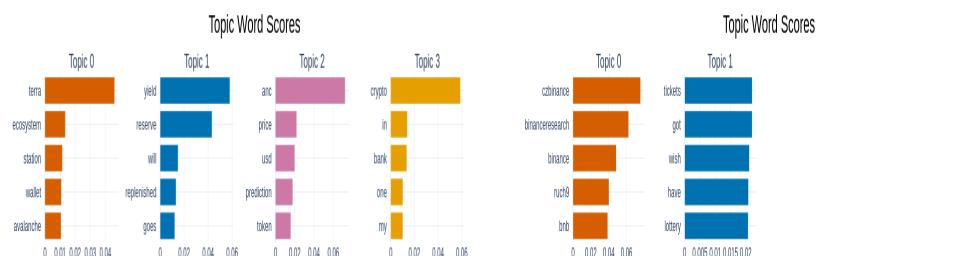
Topics	Tokens
Binance-Related Topics	ALICE,AXS,BETA,C98,CTK,CTSI,SFP,WRX
Product-Related Topics	ALPINE,ANC,BTTOLD,C98,CTK,GAL,GMT,QI,SAND,SFP,WING
Bot-Related Topics	BETA,BTTOLD,C98,CTK,CTSI,DEGO,FET,GAL,GMT,HFT,HOOK,LOKA,QI,SFP,TKO,WING,WRX,WING

表6-1 代币分类  
Table 6-1 Categorization Of Tokens



(a) ALICE

(b) ALPINE



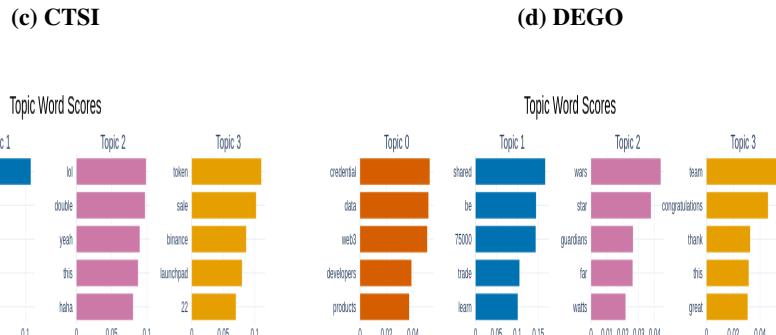
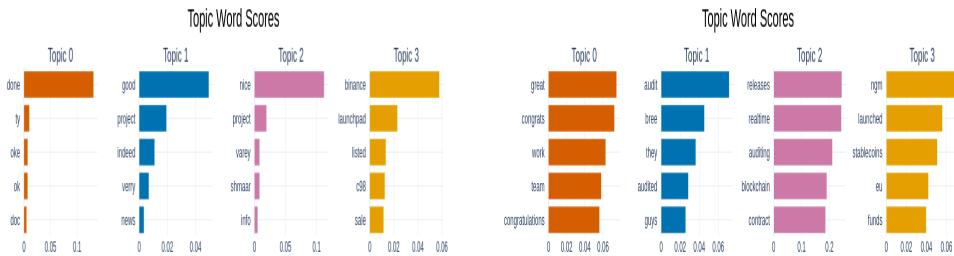
(c) ANC

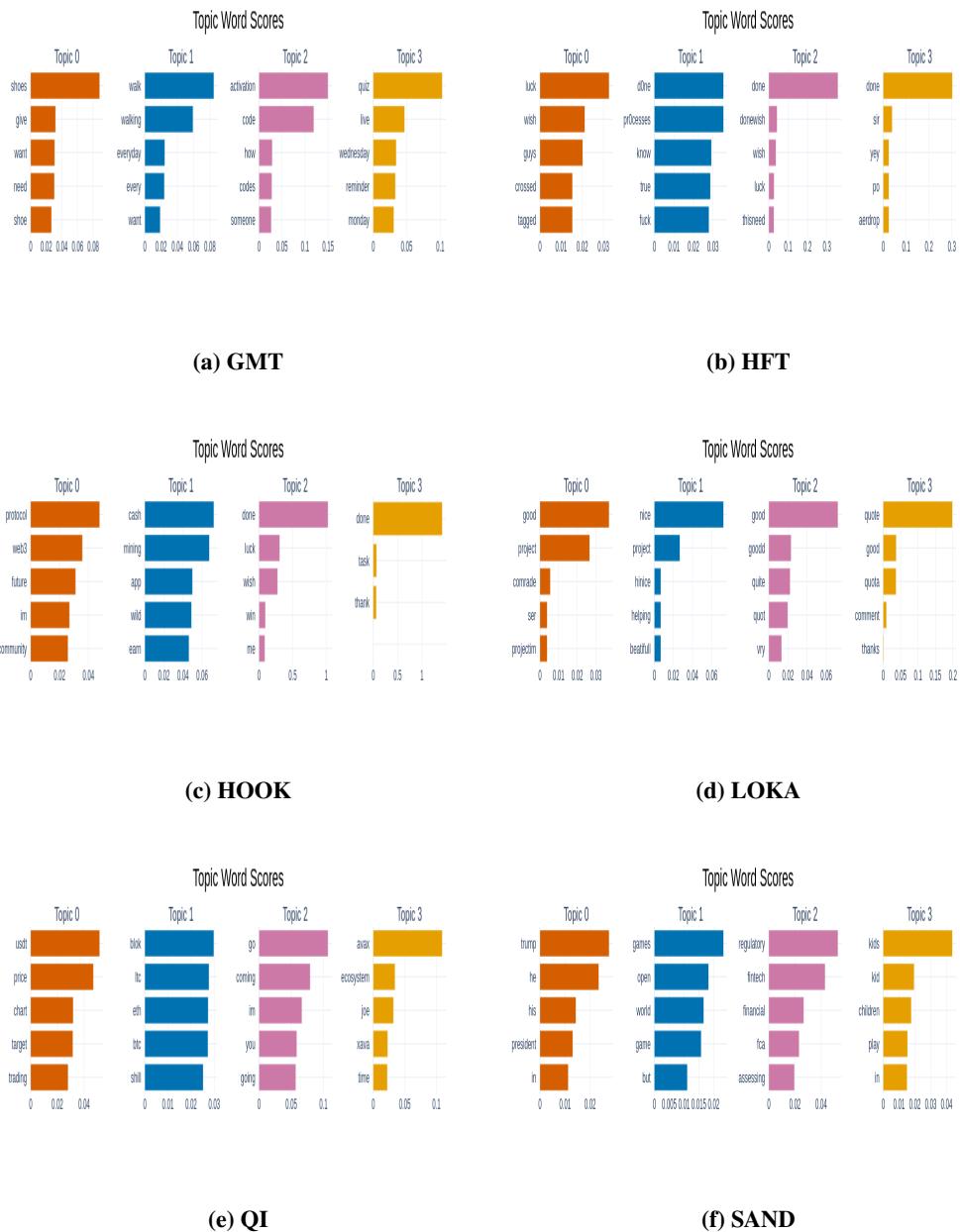
(d) AXS



(e) BETA

(f) BTTOOLD





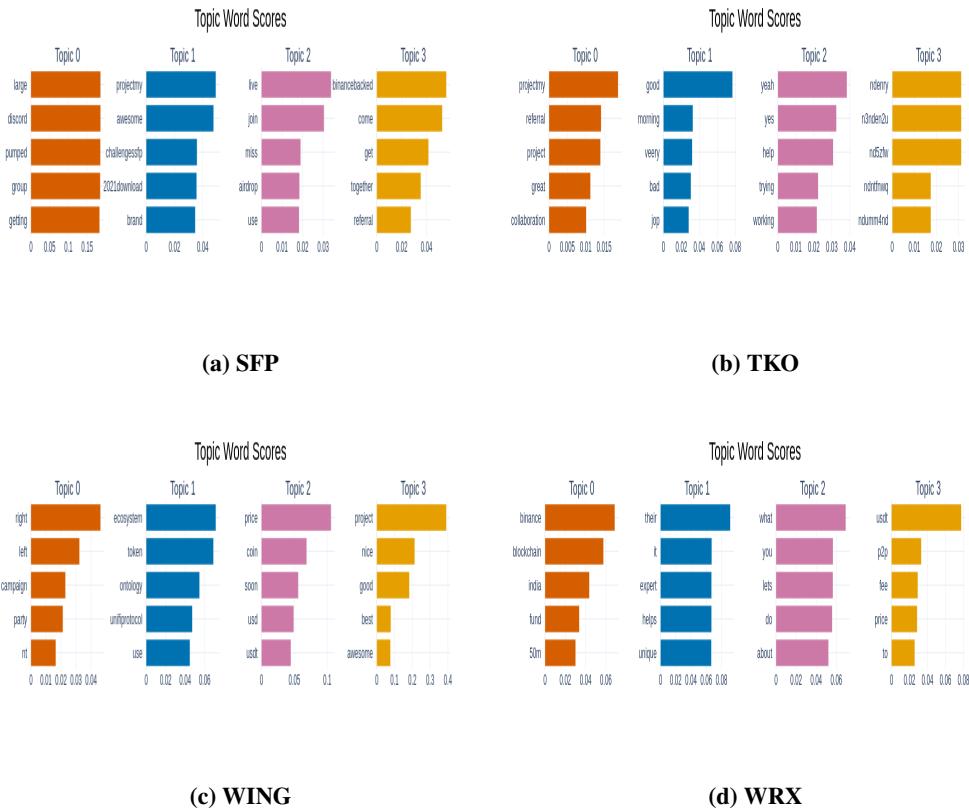


图 6-2 每个 IEO 项目下推文集合的前 4 个最常见主题 (AXS 的前 2 个最常见主题)

Figure 6-2 Top 4 most frequent topics that best represent the collection of tweets under each IEO project (Top 2 most frequent topics for AXS to avoid redundancy)

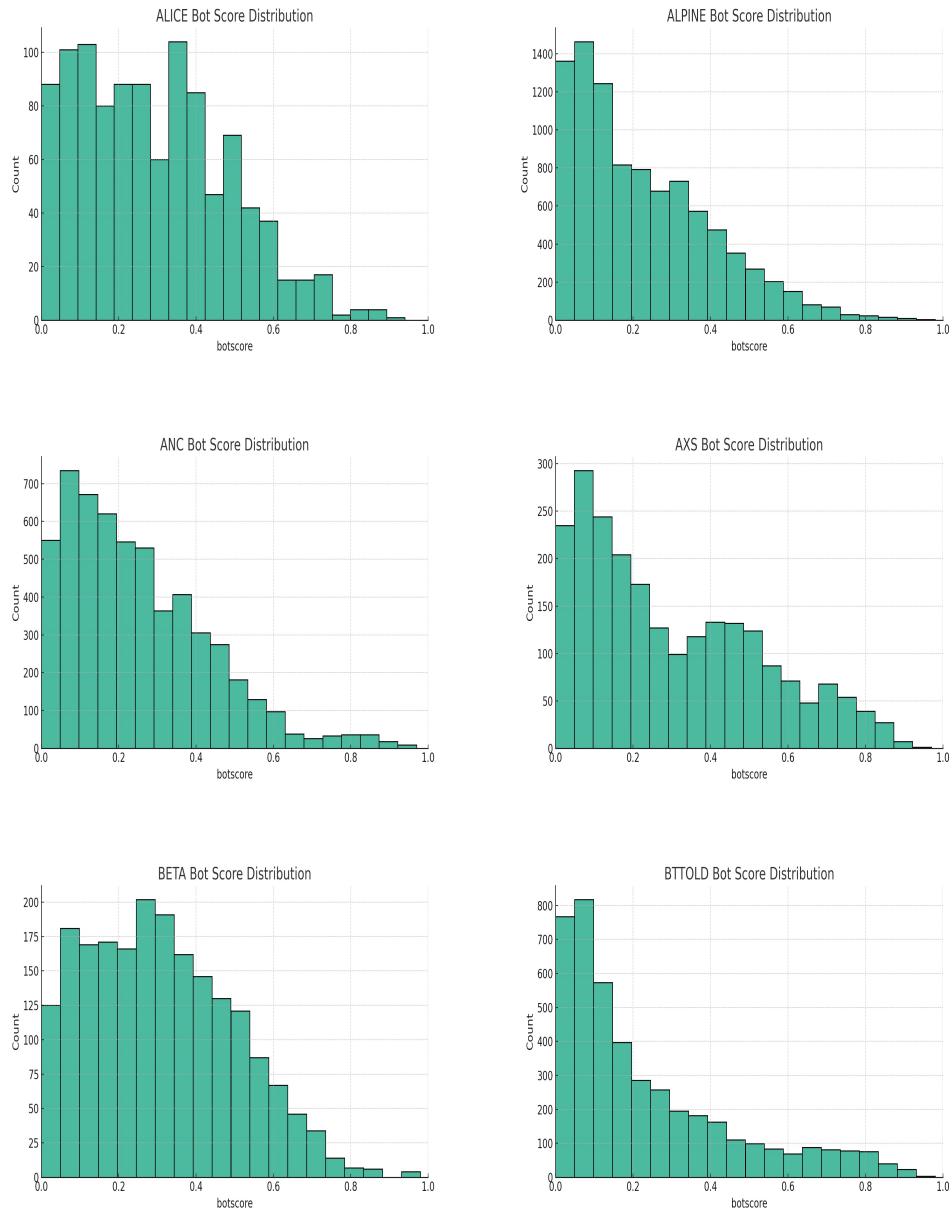
### 6.3.4 探索性分析-社交机器人（水军）得分分布

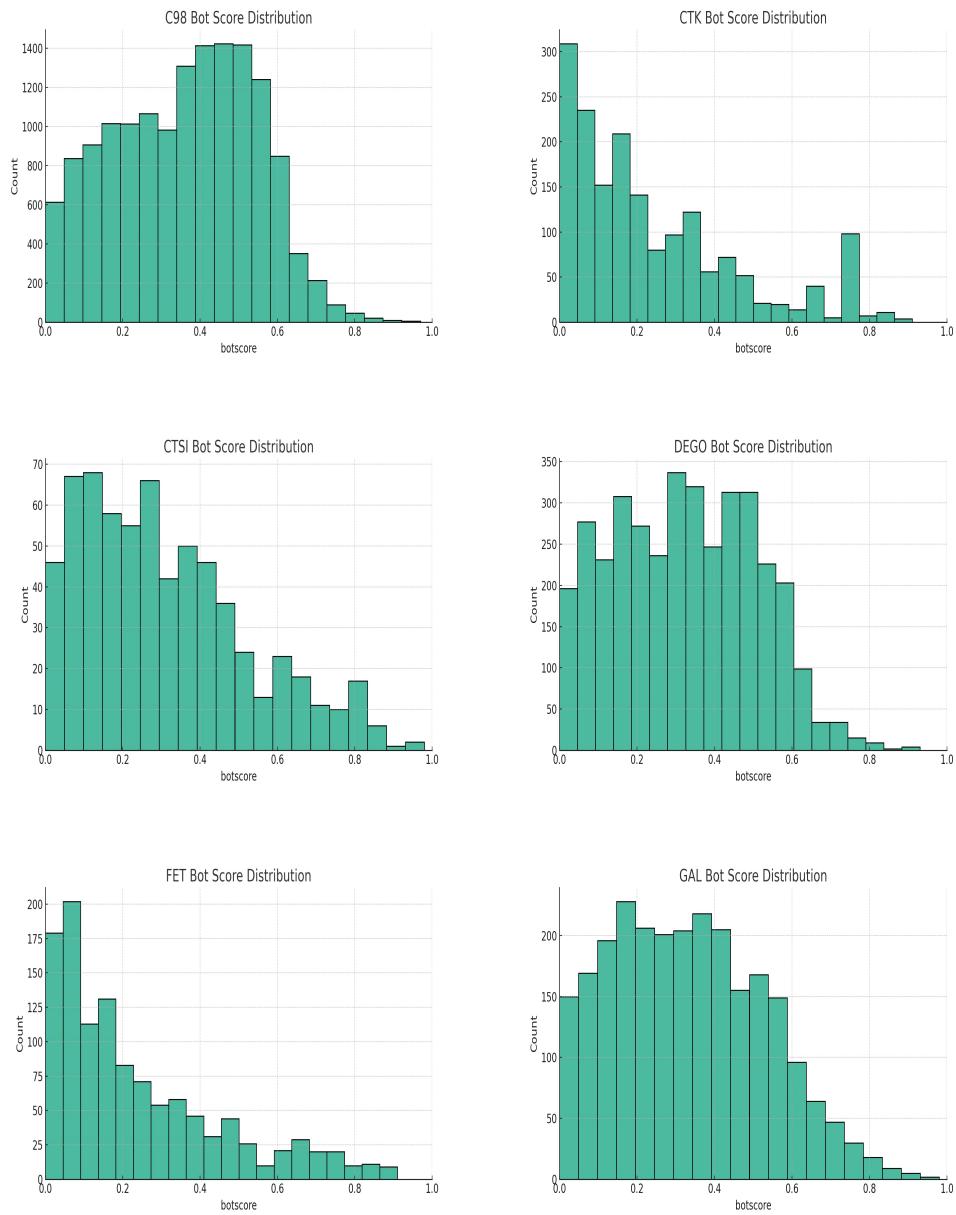
图 6-3 展示了每个 IEO 项目的机器人得分分布。对这些分布的视觉分析揭示了不同项目之间的显著变化。一些项目表现出机器人得分集中在较低的值上，这表明主要是人类活动。相反，其他项目则显示出更均匀的分布或机器人得分集中在较高的值上，这表明有大量的机器人活动。

### 6.3.5 探索性分析-卡方检验

情绪得分被归类为三种类别：负面 (-1)，中性 (0)，和积极 (1)。此外，根据阈值将机器人得分也归类为三种类别：人类 (机器人得分 < 0.5)，半机器人 ( $0.5 \leq$  机器人得分 < 0.7)，和机器人 (机器人得分  $\geq 0.7$ )。然后进行卡方检验来评估这两个分类变量之间的依赖性。

如表 6-2 所示，数据集显示不同项目的卡方和 P 值各有不同。例如，“Alpine”项目显示出较高的卡方值 83.28 和显著小的 P 值  $8.24 \times 10^{-11}$ ，表明有强烈的统计证据反对独立性的零假设。这意味着对于该项目，研究中的变量之间存在显著关联。相反，“Hook”项目的卡方值低至 0.36，P 值高达 0.836，表明缺乏统计证据来拒绝零假设，从而暗示该项目的变量之间可能独立。







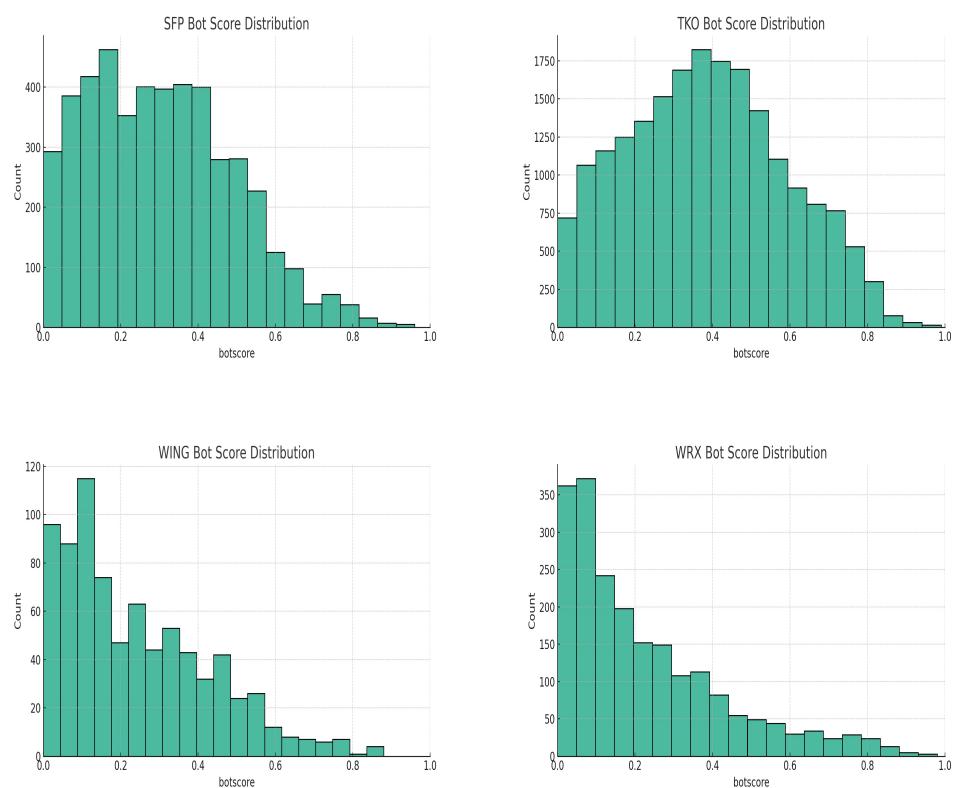


图 6-3 每个 IEO 项目的推文的水军得分分布。

**Figure 6-3 Bot score distribution for tweets mentioning each IEO project.**

结果表明,不同项目的变量之间存在不同程度的关联。值得注意的是,这些关系纯属观察性质,仅凭卡方检验无法得出因果关系的结论。

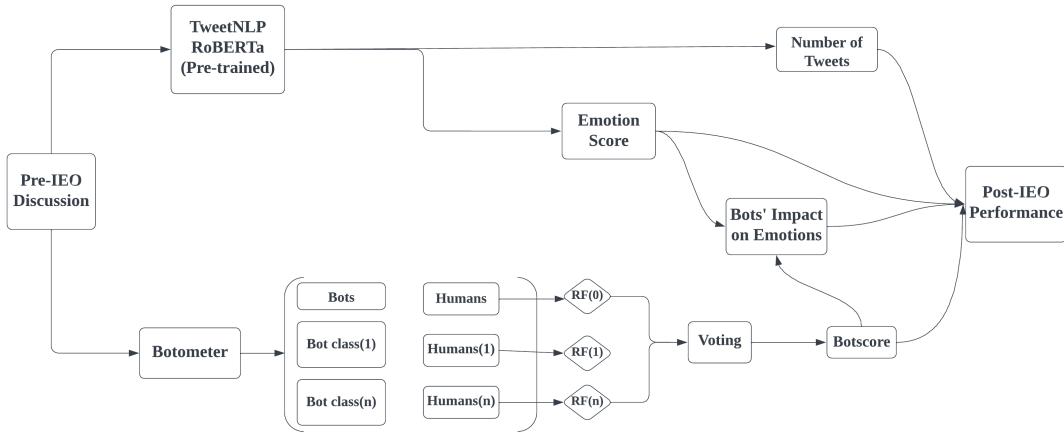
表 6-2 IEO 项目的卡方检验

Table 6-2 Chi-Square Test for IEO projects

Project Name	Chi-Square	P-Value
Hook	0.36	8.360000e-01
Alice	4.45	1.080000e-01
Alpine	83.28	8.240000e-11
ANC	10.66	4.850000e-03
CTK	70.36	5.270000e-16
BETA	16.51	2.590000e-04
BTTOLD	9.99	6.780000e-03
c98	180.96	5.060000e-40
CTSI	12.69	1.760000e-03
DEGO	48.88	2.440000e-11
FET	2.07	3.550000e-01
GAL	13.48	1.180000e-03
GMT	27.66	9.850000e-07
HFT	2.36	3.070000e-01
LOKA	64.66	9.100000e-15
QI	1.77	4.130000e-01
SAND	3.50	1.740000e-01
SFP	18.87	8.000000e-05
TKO	54.16	1.730000e-12
WING	2.70	2.590000e-01
WRX	4.49	1.060000e-01
AXS	61.35	4.760000e-14

## 6.4 研究框架

社交媒体营销可以为 IEO 项目实现筹资目标、建立品牌认可度以及吸引投资者。本研究提出了一种利用监督和非监督机器学习算法的研究框架。这些算法为每条推文生成一个情绪得分和一个机器人得分,并应用一个交互项和一个惩罚函数来评估机器人对每条推文的影响。图 5-4 提供了研究框架的概览。



**图 6-4 IEO 前期社交媒体舆情和 IEO 后期表现的研究框架。**最顶端的随机森林，标记为  $RandomForest_0$  ( $RF_0$ )，代表人类检测子系统的基线分类器。每个专门分类器  $RandomForest_i$  ( $RF_i$ ) 都是在一个均衡的数据集上训练的。该数据集包括来自机器人类别 ( $BC_i$ ) 和从所有数据集中相同数量的人类账户采样实例。

**Figure 6-4 Framework for Pre-IEO discussion and Post-IEO performance.** The topmost random forest, denoted as  $RandomForest_0$  ( $RF_0$ ), represents the baseline classifier for the human detection subsystem. Every specialized classifier  $RandomForest_i$  ( $RF_i$ ) in the ensemble shown in the figure is trained on a balanced dataset. This dataset includes an equal number of examples from both the bot class ( $BC_i$ ) and human examples sampled from human accounts across all datasets.

#### 6.4.1 情绪测量

TweetNLP 方法利用预训练技术，包括 RoBERTa 和跨语言模型 RoBERTa (XLM-R)，以实现强大的语言建模和跨语言解释。RoBERTa 是作为对 BERT 的增强而开发的，比所有后 BERT 方法表现更优。此外，RoBERTa 是在一个大数据集 (CC-News) 上训练的，结果是更准确、更稳健的语言建模<sup>[190]</sup>。

XLM-R 是在 CommonCrawl 数据集上训练的，涵盖了 100 种不同语言的 2.5TB。该模型在分类、序列标注和问答等任务上超越了以前的多语言模型，如 mBERT 和 XLM。<sup>[191]</sup>

通过 TweetNLP 对 Twitter 数据进行情绪分析，以检测给定推文的情绪是积极的、消极的还是中性的，分别用 1、-1 和 0 表示。这种方法非常适合分析大量的文本数据并识别公众舆论趋势。

#### 6.4.2 测量水军的活跃度

Kraaijeveld 和 Smedt 的研究使用基于规则的方法发现至少有 1-14% 与加密货币相关的推文是由“机器人”账户发布的。这些机器人账户通常与错误信息的传播有关<sup>[192]</sup>。为了检测这些账户，Sayyadiharikandeh 和 Menczer 使用了 Botometer，这是一个针对 Twitter 账户的机器人检测工具<sup>[193]</sup>。该工具采用了“专业化分类器集成” (ESC) 的方法，用于检测社交媒体上的机器人账户。这种方法的灵感来

自于两个实证发现：首先，人类账户在不同领域比机器人账户更加同质化；其次，不同类别的机器人账户具有不同的信息特征集。基于这两点，研究者们提出了为不同机器人类别建立专门模型的方法，并将这些模型汇总成一个集成，通过投票机制结合它们的输出。ESC方法使用100个决策树估计器的随机森林模型，并通过Platt缩放校准得分，用于识别可能的机器人账户。

Platt缩放校准是一种将分类模型的输出转换为类概率分布的方法。它通过拟合一个逻辑回归模型来实现，公式如下：

$$P(y = 1|x) = \frac{1}{1 + e^{(A \cdot f(x) + B)}}$$

其中：

- $P(y = 1|x)$  是给定输入  $x$  属于标签为 1 的类的预测概率。
- $f(x)$  是分类器对输入  $x$  的原始输出。
- $A$  和  $B$  是在拟合分类器输出到逻辑回归模型时学习的参数，它们优化了预测概率以使其尽可能接近验证数据中的实际标签分布

专门分类器集合通过投票方式来计算每个账户的机器人得分。为了训练这些专门的分类器，研究者们将机器人账户按其行为分成几类，包括简单机器人、垃圾邮件发送者、假粉丝、自我声明的机器人、政治机器人等。使用5折交叉验证，ESC在域内检测中取得了高准确率。这个集合用最高得分的规则来综合所有机器人得分，并决定该账户是机器人还是人类。如果一个账户的机器人得分很低，那么这意味着这是一个真正的人类账户。

对于人类分类器  $RF_0$ ：

$$s'_i = 1 - s_i$$

对于其他所有分类器  $RF_i$ ：

$$s'_i = s_i$$

每个专门的分类器  $RF_i$  都是在一个平衡的数据集上训练的，这个数据集包含相等数量的某个特定机器人类别  $BC_i$  的账户和从所有数据集中采样的人类账户。换句话说，每个分类器都在50%的机器人和50%的真实人类账户上进行训练，目的是让它们能够准确区分这两种类型的账户。这些公式用于调整集成中分类器的得分。对于人类分类器，得分是反转的，反映出账户为人类的信心。对于其他分类器，得分保持不变，指示账户是机器人的可能性。得分  $s'_i$  代表每个分类器的调整后得分。所有分类器中的最高得分表明账户最有可能属于的类别。

根据研究<sup>[194,195]</sup>建立了0.5和0.7的阈值。研究<sup>[196]</sup>使用了0.5的阈值，而其他研究<sup>[197,198]</sup>则采用了0.7的阈值。在本研究中，为了确保全面分析，合并了这两个阈值进行计算。

为了量化机器人（水军）账户的存在，采用了这些阈值将Twitter用户分类为三类：机器人得分超过0.7的用户被归类为机器人账户；机器人得分在0.5

到 0.7 之间的用户被认为是类似机器人的账户；机器人得分低于 0.5 的用户被识别为人类用户。设计了一个函数来调整不同级别的类似机器人账户的感知情绪值。假设如果账户的行为像机器人，其感知情绪值就不如人类账户那么重要。因此，对与类似机器人账户相关的情绪得分应用了惩罚。考虑机器人得分集合  $B_i = b_1, b_2, \dots, b_n$  和情绪得分集合  $E_i = e_1, e_2, \dots, e_n$ 。S 将是表示这种关系的得分：

$$S = \begin{cases} (1 - B_i)^2 E_i, & B_i \geq 0.7 \\ B_i^2 E_i, & 0.5 \leq B_i < 0.7 \\ B_i E_i, & \text{其他.} \end{cases} \quad (6-1)$$

其次，本文设计了一个交互项，记为 R，来探究机器人活动和情绪反应的复合效应。公式如下：

$$R = B_i \times E_i$$

评估感知情绪得分 (S) 和交互项 (R) 的预测效力，与实际情绪得分相比，对于初始交易所发行 (IEO) 后的市场表现。

#### 6.4.3 IEO 发售后的哄抬抛售

正如文献<sup>[199]</sup> 所指出，在 2017-2018 年的以太坊泡沫期间，大部分交易发生在泡沫前期和泡沫期间，这表明加密货币市场有很强的投机性。当前文献对哄抬抛售事件缺乏明确的定义。尽管如此，基本模式很明显：初始的交易量哄抬吸引个人投资者，随后 IEO 项目内部人抛售代币。这一现象因两个原因需要更强的监管。首先，IEO 项目通常被认为比传统的初始代币发行 (ICO) 项目更可信，投资者依赖交易所对项目质量进行严格的尽职调查。其次，IEO 项目的市值远大于 ICO 项目，可能造成的市场伤害更高。

为了衡量 IEO 后期的表现，利用了 ICO 文献中提出的四个指标<sup>[172,200,201]</sup>：首日回报、30 天回报、30 天波动率和 180 天回报。这些指标的数据来自 Coinmarketcap。考虑到加密货币市场的高波动性，计算时使用了对数回报。

对于每个 IEO 公司，记为  $i$ ，首日回报表示首个交易日的回报，计算为收盘价  $P_c$  与开盘价  $P_o$  的比率的自然对数：

$$\text{First day return} = \ln \frac{P_c}{P_o}$$

为了计算 30 天的波动率，收集了 30 天的代币价格，并使用 365 的平方根计算日波动率，考虑到加密货币一年交易 365 天。让  $P_{av}$  表示代币的平均价格， $P_i$  表示第  $i$  天的代币价格：

$$30\text{dayVolatility} = \sqrt{365} \times \sqrt{\sum (P_{av} - P_i)^2 / 30}$$

选择首日回报来衡量炒作，以及30天和180天回报来分别评估中期和长期投资回报。30天波动率指标用于评估投资项目的风险水平，高的30天波动率表明代币价格有显著波动，因此风险水平高。

## 6.5 研究结果

### 6.5.1 机器人水军、情绪以及IEO售后市场表现

本章探索机器人水军、情绪和初始交易所发行(IEO)售后市场表现之间的实证关系。分析的单位是IEO项目。本文采用普通最小二乘回归分析，将情绪值、机器人得分和推文数量作为自变量。

分析中的因变量对应于IEO售后的指标，即首日回报、30天回报、30天波动率和180天回报。尝试使用不同的情绪值(E, R和S)来确定最佳预测因子。此外，使用最小和最大标准化处理推文数量，以便于解释结果和比较不同特征的相对重要性。

本研究假设高机器人得分和情绪将在短期内催化价格飙升，导致波动性增加。然而，从长期来看，预计回报将随之减少。

表 6-3

模型1 使用常规情绪得分(E)。模型2 使用惩罚情绪得分(S)。模型3 使用交互项(R)。  
括号中为标准误差。N=22  
\* 在90%的水平上显著。  
\*\* 在95%的水平上显著。

Table 6-3

Model 1 uses the regular emotion score(E). Model 2 uses the penalized emotion score(S). Model 3 uses the interaction term(R). Standard errors are in parentheses. N=22  
\* Significant at the 90% level.  
\*\* Significant at the 95% level.

	First Day Return		
	Model 1	Model 2	Model 3
Bot score	-0.8414 (0.559)	-0.8321 (0.510)	-0.7658 (0.525)
Counts	0.1581 (0.267)	0.118 (0.27)	0.1269 (0.274)
Sentiment	0.4353 (0.337)	1.7357 (1.197)	1.1925 (0.961)
$R^2$	0.109	0.126	0.104

表 6-4

模型 1 使用常规情绪得分 (E)。模型 2 使用惩罚情绪得分 (S)。模型 3 使用交互项 (R)。

括号中为标准误差。N=22

\* 在 90% 的水平上显著。

\*\* 在 95% 的水平上显著。

Table 6-4

Model 1 uses the regular emotion score(E). Model 2 uses the penalized emotion score(S). Model 3 uses the interaction term(R). Standard errors are in parentheses. N=22

\* Significant at the 90% level.

\*\* Significant at the 95% level.

	30 Day Volatility		
	Model 1	Model 2	Model 3
Bot score	3.4516*	4.4419**	4.7462**
	(1.876)	(1.772)	(1.4085)
Counts	1.3212	1.3591	1.4085
	(0.897)	(0.938)	(0.947)
Sentiment	1.3855	2.7249	1.4251
	(1.131)	(4.164)	(3.318)
$R^2$	0.809	0.799	0.797

表 6-5

模型 1 使用常规情绪得分(E)。模型 2 使用惩罚情绪得分(S)。模型 3 使用交互项(R)。

括号中为标准误差。N=22

\* 在 90% 的水平上显著。

\*\* 在 95% 的水平上显著。

Table 6-5

Model 1 uses the regular emotion score(E). Model 2 uses the penalized emotion score(S). Model 3 uses the interaction term(R). Standard errors are in parentheses. N=22

\* Significant at the 90% level.

\*\* Significant at the 95% level.

	30 Day Return		
	Model 1	Model 2	Model 3
Bot score	-3.5540** (1.292)	-2.8117* (1.244)	-2.6795* (1.280)
Counts	0.5578 (0.618)	0.5264 (0.658)	0.5423 (0.669)
Sentiment	1.6635 (0.779)	4.5767 (2.920)	3.2399 (2.343)
R <sup>2</sup>	0.278	0.210	0.190

表 6-6

模型 1 使用常规情绪得分 (E)。模型 2 使用惩罚情绪得分 (S)。模型 3 使用交互项 (R)。

括号中为标准误差。N=20

\* 在 90% 的水平上显著。

\*\* 在 95% 的水平上显著。

Table 6-6

Model 1 uses the regular emotion score(E). Model 2 uses the penalized emotion score(S). Model 3 uses the interaction term(R). Standard errors are in parentheses. N=20

\* Significant at the 90% level.

\*\* Significant at the 95% level.

	180 Day Return		
	Model 1	Model 2	Model 3
Bot score	-4.0845 (3.012)	-3.6545 (2.728)	-3.4108 (2.769)
Counts	1.4908 (1.442)	1.5790 (1.473)	1.6442 (1.489)
Sentiment	0.0686 (1.839)	-1.034 (6.422)	-1.4067 (5.21)
R <sup>2</sup>	0.256	0.257	0.259

### 6.5.2 实验结果

实验发现社交媒体上的水军活动对 IEO 售后市场表现有显著影响。在首日回报的情况下，发现机器人得分和因变量之间有负相关性。此外惩罚情绪得分的 R 平方值被发现高于常规情绪值。在 30 天波动率的情况下，机器人得分对因变量有显著的正面影响。包含交互项的模型 3 显示出比模型 2 更低的 P 值 (0.016)。推文数量和情绪值也表现出与因变量的正相关性。这些发现揭示社交媒体上水军的活动的增加会导致更大的价格波动。

在 30 天回报率的情况下，发现机器人得分与因变量之间有显著的负相关性。当项目利益相关者试图获得利润时，他们可能会采用增加社交媒体上水军活动的市场操纵策略。使用常规情绪得分的模型 1 显示出最低的 P 值 (0.012)。推文数量和情绪值也表现出与因变量的正相关性。

最后，在 180 天回报率的情况下，没有一个独立变量被证明是统计上显著的。这可能是因为 180 天的时间范围远远超出了 IEO 前期媒体造势的影响范围，期间会有许多其他因素会影响价格。尽管如此，机器人得分与因变量呈负相关，表明社交媒体上水军活动仍对 IEO 的长期结果有持久影响。

## 6.6 结论

本文进行了对 Twitter 上 IEO 前机器人式讨论的调查,从而为 ICO 成功、社交媒体机器人检测,以及加密货币炒作和抛售研究的现有文献做出贡献。该研究首次审查全球最大加密货币交易所 Binance 上所有发行的 IEO 项目。交易所层面的炒作和抛售事件与频繁的社交媒体机器人活动有着密切联系。纽约州总检察长的报告揭示<sup>[202]</sup>,投资者对 IEO 项目的信息披露获取渠道有限,且只有少数交易所监控机器人活动。虽然加密货币交易所明面表示市场操纵和金融欺诈是严重问题,但实施政策来解决这些问题的交易所却寥寥无几。

与传统初创公司不同,加密初创公司只能通过社交媒体与投资者进行沟通,Twitter 是进行营销活动的最重要平台。在注意力经济中,对新初创公司而言,吸引投资者的注意力可能是一个挑战,使得区分营销和恶意市场操纵变得困难。为了研究 IEO 前社交媒体活动与 IEO 后表现之间的关系,设计了三个具有不同情绪值的模型。这一启发式方法关注于识别社交媒体中的机器人式活动集中度及其与价格变动的关系。研究发现,更高的机器人评分与 30 天回报率有显著的负相关关系,同时对 30 天波动率有显著的正影响。这种关系表明,拥有高机器人式评论的 IEO 项目风险更大。

研究认识到,影响 IEO 价格轨迹的动态因素是多方面且复杂的,超出了当前分析的范围。投资资金的水平、团队成员的经验、白皮书的质量,以及整体金融市场状态(无论是熊市还是牛市)等关键因素,在塑造 IEO 表现方面都起着重要作用。在研究的背景下,特别关注了 IEO 前活动的影响。虽然研究的发现提供了有价值的洞察,但应在这一有限的背景下理解。未来的研究可以通过将更全面的变量集成入分析中,对这些发现进行有益的扩展。

## 6.7 本章小结

本文调查了 IEO 售前的社交媒体机器人(水军)活动与 IEO 售后市场表现之间的关系,首次全面审视了币安交易所的所有 IEO 项目。研究表明,社交媒体上的机器人活动与 IEO 项目的市场表现密切相关,尤其是机器人得分与项目短期回报和波动性有显著关联。本研究的发现对投资者和监管机构具有重要的实践意义。



## 第 7 章 总结与展望

### 7.1 本文总结

区块链数字货币的发展已成为当今金融科技领域的一个标志性事件。这一新兴领域的不断演化不仅揭示了其潜在的巨大价值，也暴露出许多挑战与风险。为此，本文基于深度学习和社交媒体传播理论，从不同区块链数字货币的视角下对其进行属性分析，价值确认，以及风险预警。具体地，本文的主要研究内容和贡献如以下四个内容：

#### (1) 金融诈骗检测方法综述

首先对传统金融诈骗及用于检测此类诈骗的主流学习算法进行了分析。接着，介绍了当前存在的加密货币诈骗问题，并将针对传统金融诈骗的处理经验汇集到一个创新的加密货币诈骗检测框架。这篇综述确定了四种主要的金融诈骗类型——消费者服务与商品诈骗、投资诈骗、公司诈骗及保险诈骗，并将加密货币诈骗归类为一种投资诈骗。研究发现，生成对抗网络 (GAN)、强化学习、自编码器和图神经网络能够有效应对加密货币诈骗检测面临的诸多挑战。此外，详细综述了 111 篇具有代表性的文献，为加密货币诈骗检测的深度学习解决方案提供了宝贵的参考。

#### (2) 在大语言模型框架下的加密货币属性判断以及投资决策

通过将以太坊与像微软和 Meta 这样的科技股票，以及黄金和原油这类传统商品进行比较，评估了以太坊作为证券或商品的分类。采用霍威测试 (Howey Test)，发现以太坊更接近于科技股票，这是由于它依赖于技术创新和社区努力。研究使用普通最小二乘法 (OLS) 回归模型来分析各种因素对这些资产日志收益率的影响，包括 GPT-3.5 的 API 响应评分这样的独特变量。结果揭示了 GPT-3.5 对情绪解读的显著相关性与各种金融资产的价值之间的联系，包括科技股、商品和加密货币。该研究还包括了稳健性检验，确认了模型在不同时间段的预测准确性。最终，以太坊与科技股更为一致，突显了大型语言模型在金融市场分析中的实用性。

#### (3) 深度学习视角下的 NFT 价值研究

将 PFPs (Picture For Proof) 与其他 NFT 类别区分开，因为 PFPs 主要受审美和社区参与度的驱动。本工作采用了 Backward Sup Augmented Dickey-Fuller (BSADF) 测试来检测时间序列市值数据中的泡沫。选取了 13 个项目进行分析。研究使用 t 分布随机邻域嵌入 (T-SNE) 可视化进行风格相似性分析，并利用视觉几何组 (Visual Geometry Group, VGG) -19 作为特征提取器，用于收藏品内的图像相似性分析。结果表明，拥有知识产权 (IP) 且图像相似性低的 PFP 收藏品在长期内展现出最大的财务收益。

#### (4) 社交媒体舆情对首次交易所发行 (IEO) 的影响：市场营销与操纵策略

## 的分析

首次代币发行（ICOs）容易受到“抬价-抛售”骗局的影响，骗子通过在社交媒体上传播虚假信息来抬高代币价格。然而，首次交易所发行（IEOs）被认为更可靠，因为交易所会对项目进行尽职调查。本研究通过分析 54 个 IEO 项目的不同账户在 IEO 前一个月发布的超过 11,000 条推文，调查了 IEOs 在减轻“抬价-抛售”骗局方面的有效性。选取了至少有 1000 条推文的 22 个项目，并使用主题建模进行描述性分析。使用 Botometer 生成每个推文账户的机器人评分，并利用预训练的双向编码器表示来自变压器（BERT）模型进行情感分析。引入了惩罚性情感得分和交互项，并使用普通最小二乘法（OLS）回归模型来识别机器人评分、情感值与 IEO 后表现之间的关系。研究发现，机器人评分与 30 天回报率呈负相关，与 30 天波动率呈正相关，这表明 IEOs 中存在“抬价-抛售”骗局。建议投资者、交易所和监管机构应采取措施评估 IEOs 相关的风险，并设计适当的干预措施以防止市场操纵。

## 7.2 研究展望

基于区块链数字货币的发展及其在金融科技领域的重要性，结合对金融诈骗检测、加密货币属性判断、NFT 价值研究和社交媒体影响的深入分析，未来的研究可以在以下四个方面展开：

### （1）多模态加密货币诈骗检测机制

随着金融诈骗的手段日益高明，未来的研究应专注于开发更先进的诈骗检测算法。可以探索结合多模态数据源（如交易数据、用户行为、社交媒体动态等）的深度学习模型，以实现更为全面和精确的诈骗行为识别。

### （2）深度学习在加密货币市场分析中的应用拓展

在加密货币属性判断以及投资决策方面，未来可以进一步利用大语言模型，对市场情绪、政策变动等外部因素进行更深入的分析。此外，可以通过增强模型的解释性，帮助投资者和管理者更好地理解模型决策背后的逻辑。

### （3）NFT 市场的细分化价值评估

对于 NFT 市场，未来研究可以继续深化 PFPs 等特定类别的价值分析。考虑到 NFT 的多样性和艺术属性，可以探索结合艺术学、社会学等跨学科知识的深度学习模型，以更准确地评估和预测 NFT 作品的长期价值。

### （4）加强社交媒体舆情在金融市场中的作用研究

社交媒体在塑造投资者行为和市场动态方面的作用不断增强。未来研究可以关注如何更有效地利用社交媒体数据来预测市场走势，以及如何设计有效的监管措施来减少信息操纵和误导性信息传播对市场的负面影响。同时，研究应关注机器人和虚假账户对市场的潜在影响，以及如何通过技术手段减轻这些影响。

通过以上研究方向的深入探索，可以进一步增强对区块链数字货币市场的理解，优化金融诈骗检测机制，加强市场监管，促进金融科技领域的健康和可持

续发展。



## 参考文献

- [1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [M/OL]. 2008. <https://bitcoin.org/bitcoin.pdf>.
- [2] Yukun, Liu, Aleh T. Risks and returns of cryptocurrency [J/OL]. National Bureau of Economic Research, 2018(24877). DOI: [10.3386/w24877](https://doi.org/10.3386/w24877).
- [3] Ur R, Vo X V. Cryptocurrencies and precious metals: a closer look from diversification perspective [J]. Resources Policy, 2020, 66(101652).
- [4] Hassan M B H, M. Kabir, Rashid M M. Using precious metals to hedge cryptocurrency policy and price uncertainty [J]. Economics Letters, 2021, 206(109977).
- [5] Liu J J, Jian, Gou S. Decomposing interconnectedness: A study of cryptocurrency spillover effects in global financial markets [J]. Finance Research Letters, 2024, 61(104950).
- [6] Niyati A A S, Bhanja, Arif Billah D. Aggregate, asymmetric and frequency-based spillover among equity, precious metals, and cryptocurrency [J]. Resources Policy, 2023, 80(103145).
- [7] Walid Mensi H U K X V V, Mariya Gubareva, Kang S H. Tail spillover effects between cryptocurrencies and uncertainty in the gold, oil, and stock markets [J]. Financial Innovation, 2023, 9(92).
- [8] Wang L R W Q, Q. Non-fungible token (nft): Overview, evaluation, opportunities and challenges. [M]. arXiv preprint, 2021.
- [9] Matthieu, Nadini F D M L M a B, Laura , Alessandretti. Mapping the nft revolution: market trends, trade networks, and visual features [J]. Scientific Reports, 2021, 11(20902).
- [10] Tuba Yilmaz S S, Velasco C. What makes nfts valuable to consumers? perceived value drivers associated with nfts liking, purchasing, and holding [J]. Journal of Business Research, 2023, 165(114056).
- [11] Kin-Hon Ho Y H, Monica Law, Chan T T. Spillover analysis on nfts, nft-affiliated tokens and nft submarkets [J]. Finance Research Letters, 2024, 60(104598).
- [12] Wang Y. Volatility spillovers across nfts news attention and financial markets [J]. International Review of Financial Analysis, 2022, 83(102313).
- [13] Houda BenMabrouk F S, Syrine Sassi, Abid I. Connectedness and portfolio hedging between nfts segments, american stocks and cryptocurrencies nexus [J]. International Review of Financial Analysis, 2024, 91(102959).
- [14] Ahmet Faruk Aysan M C, Cepni O. Not all words are equal: Sentiment and jumps in the cryptocurrency market [J]. Journal of International Financial Markets, Institutions and Money, 2024, 91(101920).
- [15] Lee K, Jeong D. Too much is too bad: The effect of media coverage on the price volatility of cryptocurrencies [J]. Journal of International Money and Finance, 2023, 133(102823).
- [16] Arianna Agosto P C, Pagntoni P. Sentiment, google queries and explosivity in the cryptocurrency market [J]. Physica A: Statistical Mechanics and its Applications, 2022, 605 (128016).
- [17] Kulbhaskar A K, Subramiam S. Breaking news headlines: Impact on trading activity in the cryptocurrency market [J]. Economic Modelling, 2023, 126(106397).
- [18] Ante L. How elon musk's twitter activity moves cryptocurrency markets [J]. Technological Forecasting and Social Change, 2023, 186(122112).

- [19] Kirsty Moreland. What is proof-of-work (pow)? [EB/OL]. 2019. <https://www.ledger.com/academy/blockchain/what-is-proof-of-work>.
- [20] Kirsty Moreland. What is proof-of-stake (pos)? [EB/OL]. 2019. <https://www.ledger.com/academy/blockchain/what-is-proof-of-stake>.
- [21] Schilling L, Uhlig H. Some simple bitcoin economics [J]. Journal of Monetary Economics, 2019.
- [22] Yermack D. Chapter 2 - is bitcoin a real currency? an economic appraisal [M]. Handbook of Digital Currency, 2015.
- [23] Vranken H. Sustainability of bitcoin and blockchains [J]. Current Opinion in Environmental Sustainability, 2017.
- [24] Dirk G. Baur K H, Lee A D. Bitcoin: Medium of exchange or speculative assets [J]. Journal of International Financial Markets, Institutions and Money, 2018.
- [25] Reilly White N I, Yorgos Marinakis, Walsh S. Is bitcoin a currency, a technology-based product, or something else? [J]. Technological Forecasting and Social Change, 2020.
- [26] Han-Min Kim G W B, Lee G. Predicting ethereum prices with machine learning based on blockchain information [J]. Expert Systems with Applications, 2021.
- [27] Nadler P, Guo Y. The fair value of a token: How do markets price cryptocurrencies? [J]. Research in International Business and Finance, 2020.
- [28] Lin William, Cong Y, Ke, Tang, Xi, Zhao. Inclusion and democratization through web3 and defi? initial evidence from the ethereum ecosystem [J]. National Bureau of Economic Research, 2023.
- [29] Ting Chen Y Z C X L J C S L X L X Z, Zihao Li. Understanding ethereum via graph analysis [C]. ACM Transactions on Internet Technology, 2020.
- [30] Saleh F. Blockchain without waste: Proof-of-stake [J]. The Review of Financial Studies, 2021.
- [31] Jingxing (Rowena) Gan G T, Netessine S. Decentralized platforms: Governance, tokenomics, and ico design [J]. Management Science, 2023.
- [32] Chod J, Lyandres E. A theory of icos: Diversification, agency, and information asymmetry [J]. Management Science, 2021.
- [33] Andreas Barth S M, Valerie Laturus, Wagner A F. Conflicted analysts and initial coin offerings [J]. Management Science, 2023.
- [34] Jingxing (Rowena) Gan G T, Netessine S. Initial coin offerings, speculation, and asset tokenization [J]. Management Science, 2020.
- [35] Holden R, Malani A. An examination of velocity and initial coin offerings [J]. Management Science, 2022.
- [36] Sarah Alsultan A K, Markellos R N. Can we price beauty? aesthetics and digital art markets [J]. Economics Letters, 2024.
- [37] Te Bao M M, Wen Y. Herding in the non-fungible token (nft) market [J]. Journal of Behavioral and Experimental Finance, 2023.
- [38] Nicola Borri Y L, Tsivinski A. The economics of non-fungible tokens [EB/OL]. 2022. <https://cowles.yale.edu/sites/default/files/2022-10/EconomicsNFTs.pdf>.
- [39] Guadamuz A. The treachery of images: non-fungible tokens and copyright [J]. Journal of Intellectual Property Law Practice, 2021.
- [40] Kathleen Bridget Wilson A K, Ghaderi H. Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity [J]. Business Horizons, 2022.

- 
- [41] Peng , Peng W L, Yuehong , Chen, Wang J Z. Attention-based cnn–lstm for high-frequency multiple cryptocurrency trend prediction [J]. Expert Systems with Applications, 2024.
  - [42] Jiyang Cheng D K M M, Sunil Tiwari, Shahzad U. Forecasting bitcoin prices using artificial intelligence: Combination of ml, sarima, and facebook prophet models [J]. Technological Forecasting and Social Change, 2024.
  - [43] Chakraborty M, Subramaniam S. Does sentiment impact cryptocurrency? [J]. Journal of Behavioral Finance, 2024.
  - [44] An Pham Ngoc Nguyen M B M C, Tai Tan Mai. Volatility and returns connectedness in cryptocurrency markets: Insights from graph-based methods [J]. Physica A: Statistical Mechanics and its Applications, 2023.
  - [45] Omar H, Lasrado L A. Uncover social media interactions on cryptocurrencies using social set analysis (ssa) [J]. Procedia Computer Science, 2023.
  - [46] Administration I T. Impact of covid pandemic on ecommerce [M/OL]. 2020. <https://www.trade.gov/impact-covid-pandemic-ecommerce>.
  - [47] Pwc. Pwc’ s global economic crime and fraud survey [M/OL]. 2022. <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>.
  - [48] Al-Hashedi K G, Magalingam P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019 [J]. Computer Science Review, 2021, 40(100402).
  - [49] Waleed Hilal S A G. Financial fraud: A review of anomaly detection techniques and recent advances [J]. Expert Systems with Applications, 2022, 193(116429).
  - [50] Becker G S. Crime and punishment: An economic approach [M/OL]. 1974. <http://www.nber.org/books/beck74-1>.
  - [51] Experian. Fraud rate rises 33 2020. <https://www.experianplc.com/newsroom/press-releases/2020/fraud-rate-rises-33-during-covid-19-lockdown>.
  - [52] Hubler M. Guide financial statement fraud [M/OL]. 2016. <https://www.purdueglobal.edu/blog/business/guide-financial-statement-fraud>.
  - [53] Hajek P, Henriques R. Mining corporate annual reports for intelligent detection of financial statement fraud –a comparative study of machine learning methods [J]. Knowledge-Based Systems, 2017, 128: 139-152.
  - [54] Minhas S, Hussain A. From spin to swindle: Identifying falsification in financial text [J]. Cognitive Computation, 2016, 8: 729–745.
  - [55] Maniraj S, Saini A, Ahmed S, et al. Credit card fraud detection using machine learning and data science [J]. International Journal of Engineering Research, 2019, 8: 110-115.
  - [56] Makki S, Assaghir Z, Taher Y, et al. An experimental study with imbalanced classification approaches for credit card fraud detection [J]. IEEE Access, 2019, 7: 93010-93022.
  - [57] Zhang G, Li Z, Huang J, et al. efraudcom: An e-commerce fraud detection system via competitive graph neural networks [C]. New York: ACM Transactions on Information Systems (TOIS), 2022.
  - [58] Luca M, Zervas G. Fake it till you make it: Reputation, competition, and yelp review fraud [J]. Management Science, 2016, 62: 3412-3427.
  - [59] Sithic H L, Balasubramanian T. Survey of insurance fraud detection using data mining techniques [M]. arXiv preprint, 2013.
  - [60] Wang Y, Xu W. Leveraging deep learning with lda-based text analytics to detect automobile insurance fraud [J]. Decision Support Systems, 2018, 105: 87-95.

- [61] Villegas-Ortega J, Bellido-Boza L, Mauricio D. Fourteen years of manifestations and factors of health insurance fraud, 2006–2020: a scoping review [J]. *Health & justice*, 2021, 9(1): 1-23.
- [62] Schölkopf B, Platt J C, Shawe-Taylor J, et al. Estimating the support of a high-dimensional distribution [J]. *Neural computation*, 2001, 13(7): 1443-1471.
- [63] Ruff L, Vandermeulen R, Goernitz N, et al. Deep one-class classification [C]. PMLR, 2018: 4393-4402.
- [64] Erfani M, Shoeleh F, Ghorbani A A. Financial fraud detection using deep support vector data description [C]. IEEE, 2020: 2274-2282.
- [65] Deng Q. Application of support vector machine in the detection of fraudulent financial statements [C]. IEEE, 2009: 1056-1059.
- [66] Pai P F, Hsu M F, Wang M C. A support vector machine-based model for detecting top management fraud [J]. *Knowledge-Based Systems*, 2011, 24(2): 314-321.
- [67] Renjith S. Detection of fraudulent sellers in online marketplaces using support vector machine approach [M]. arXiv preprint, 2018.
- [68] Rtyali N, Enneya N. Enhanced credit card fraud detection based on svm-recursive feature elimination and hyper-parameters optimization [J]. *Journal of Information Security and Applications*, 2020, 55: 102596.
- [69] Subudhi S, Panigrahi S. Quarter-sphere support vector machine for fraud detection in mobile telecommunication networks [J]. *Procedia Computer Science*, 2015, 48: 353-359.
- [70] Qin R. Identification of accounting fraud based on support vector machine and logistic regression model [J]. *Complexity*, 2021, 2021.
- [71] Phua C, Lee V, Smith K, et al. A comprehensive survey of data mining-based fraud detection research [M]. arXiv preprint, 2010.
- [72] Pang G, Shen C, Cao L, et al. Deep learning for anomaly detection: A review: volume 54 [C]. ACM New York, NY, USA, 2021: 1-38.
- [73] Ng A, et al. Sparse autoencoder [J]. CS294A Lecture notes, 2011, 72(2011): 1-19.
- [74] Vincent P, Larochelle H, Bengio Y, et al. Extracting and composing robust features with denoising autoencoders [C]. Proceedings of the 25th international conference on Machine learning, 2008: 1096-1103.
- [75] Zhou C, Paffenroth R C. Anomaly detection with robust deep autoencoders [C]. Proceedings of the 23rd ACM SIGKDD international conference on knowledge discovery and data mining, 2017: 665-674.
- [76] Doersch C. Tutorial on variational autoencoders [M]. arXiv preprint, 2010.
- [77] Dong M, Yao L, Wang X, et al. Opinion fraud detection via neural autoencoder decision forest [J]. *Pattern Recognition Letters*, 2020, 132: 21-29.
- [78] Pumsirirat A, Liu Y. Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine [J]. *International Journal of advanced computer science and applications*, 2018, 9(1).
- [79] Misra S, Thakur S, Ghosh M, et al. An autoencoder based model for detecting fraudulent credit card transaction [J]. *Procedia Computer Science*, 2020, 167: 254-262.
- [80] Wong M L, Seng K, Wong P K. Cost-sensitive ensemble of stacked denoising autoencoders for class imbalance problems in business domain [J]. *Expert Systems with Applications*, 2020, 141: 112918.

- [81] Zamini M, Montazer G. Credit card fraud detection using autoencoder based clustering [C]. 2018 9th International Symposium on Telecommunications (IST), 2018: 486-491.
- [82] Anh N T N, Khanh T Q, Dat N Q, et al. Fraud detection via deep neural variational autoencoder oblique random forest [C]. 2020 IEEE-HYDCON, 2020: 1-6.
- [83] Sanchez-Lengeling B, Reif E, Pearce A, et al. A gentle introduction to graph neural networks [J]. Distill, 2021, 6(9): e33.
- [84] Wang H, Wang J, Wang J, et al. Learning graph representation with generative adversarial nets [J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 33(8): 3090-3103.
- [85] Liu Z, Dou Y, Yu P S, et al. Alleviating the inconsistency problem of applying graph neural network to fraud detection [C]. Proceedings of the 43rd international ACM SIGIR conference on research and development in information retrieval, 2020: 1569-1572.
- [86] Cheng D, Wang X, Zhang Y, et al. Graph neural network for fraud detection via spatial-temporal attention [J]. IEEE Transactions on Knowledge and Data Engineering, 2020.
- [87] Wang D, Lin J, Cui P, et al. A semi-supervised graph attentive network for financial fraud detection [C]. 2019 IEEE International Conference on Data Mining (ICDM), 2019: 598-607.
- [88] Zheng P, Yuan S, Wu X, et al. One-class adversarial nets for fraud detection: volume 33 [C]. Proceedings of the AAAI Conference on Artificial Intelligence, 2019: 1286-1293.
- [89] Chen J, Shen Y, Ali R. Credit card fraud detection using sparse autoencoder and generative adversarial network [C]. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018: 1054-1059.
- [90] Ba H. Improving detection of credit card fraudulent transactions using generative adversarial networks [M]. arXiv preprint, 2010.
- [91] Charitou C, Garcez A d, Dragicevic S. Semi-supervised gans for fraud detection [C]. IEEE, 2020: 1-8.
- [92] Charitou C, Dragicevic S, Garcez A d. Synthetic data generation for fraud detection using gans [M]. arXiv preprint, 2021.
- [93] Pandey A, Bhatt D, Bhowmik T. Limitations and applicability of gans in banking domain. [C]. ADGN@ ECAI, 2020.
- [94] Mnih V, Kavukcuoglu K, Silver D, et al. Playing atari with deep reinforcement learning [J]. arXiv preprint arXiv:1312.5602, 2013.
- [95] Shen H, Kurshan E. Deep q-network-based adaptive alert threshold selection policy for payment fraud systems in retail banking [C]. Proceedings of the First ACM International Conference on AI in Finance, 2020: 1-7.
- [96] Zhao M, Li Z, An B, et al. Impression allocation for combating fraud in e-commerce via deep reinforcement learning with action norm penalty. [C]. IJCAI, 2018: 3940-3946.
- [97] Zhinin-Vera L, Chang O, Valencia-Ramos R, et al. Q-credit card fraud detector for imbalanced classification using reinforcement learning. [C]. ICAART (1), 2020: 279-286.
- [98] Mead A, Lewris T, Prasanth S, et al. Detecting fraud in adversarial environments: A reinforcement learning approach [C]. 2018 Systems and Information Engineering Design Symposium (SIEDS), 2018: 118-122.
- [99] Dou Y, Ma G, Yu P S, et al. Robust spammer detection by nash reinforcement learning [C]. Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2020: 924-933.
- [100] El-Awady K. Adaptive stress testing for adversarial learning in a financial environment [M]. arXiv preprint, 2021.

- [101] Askari S M S, Hussain M A. Intuitionistic fuzzy logic based decision tree for e-transactional fraud detection [J]. Science Direct, 2020.
- [102] Wang H, Yang F, Shen S. Supply fraud forecasting using decision tree algorithm [C]. IEEE, 2021: 344-347.
- [103] Cody C, Ford V, Siraj A. Decision tree learning for fraud detection in consumer energy consumption [C]. IEEE, 2015: 1175-1179.
- [104] Sahin Y, Bulkan S, Duman E. A cost-sensitive decision tree approach for fraud detection [J]. Expert Systems with Applications, 2013, 40(15): 5916-5923.
- [105] Khine A A, Khin H W. Credit card fraud detection using online boosting with extremely fast decision tree [C]. 2020 IEEE Conference on Computer Applications (ICCA), 2020: 1-4.
- [106] Save P, Tiwarekar P, Jain K N, et al. A novel idea for credit card fraud detection using decision tree [J]. International Journal of Computer Applications, 2017, 161(13).
- [107] Badriyah T, Rahmaniah L, Syarif I. Nearest neighbour and statistics method based for detecting fraud in auto insurance [C]. IEEE, 2018: 1-5.
- [108] Makki S, Haque R, Taher Y, et al. A cost-sensitive cosine similarity k-nearest neighbor for credit card fraud detection [C]. Big Data and Cyber-Security Intelligence, 2018.
- [109] Malini N, Pushpa M. Analysis on credit card fraud identification techniques based on knn and outlier detection [C]. IEEE, 2017: 255-258.
- [110] Ganji V R, Mannem S N P. Credit card fraud detection using anti-k nearest neighbor algorithm [J]. International Journal on Computer Science and Engineering, 2012, 4(6): 1035-1039.
- [111] Eddy S R. Hidden markov models [J]. Current opinion in structural biology, 1996, 6(3): 361-365.
- [112] Robinson W N, Aria A. Sequential fraud detection for prepaid cards using hidden markov model divergence [J]. Expert Systems with Applications, 2018, 91: 235-251.
- [113] Sathyapriya M, Thiagarasu D V. Implementation of big data technology for credit card fraud detection system using hidden markov model [J]. International Journal of Scientific Research in Computer Science Applications and Management Studies, 2018, 7(3).
- [114] Lucas Y, Portier P E, Laporte L, et al. Towards automated feature engineering for credit card fraud detection using multi-perspective hmms [J]. Future Generation Computer Systems, 2020, 102: 393-402.
- [115] Mukhopadhyay D M, Balitanas M O, Farkhod A, et al. Genetic algorithm: A tutorial review [J]. International journal of grid and distributed computing, 2009, 2(3): 25-32.
- [116] Yan C, Li M, Liu W, et al. Improved adaptive genetic algorithm for the vehicle insurance fraud identification model based on a bp neural network [J]. Theoretical Computer Science, 2020, 817: 12-23.
- [117] Alenzi H Z, Aljehane N O. Fraud detection in credit cards using logistic regression [J]. International Journal of Advanced Computer Science and Applications, 2020, 11(12).
- [118] Marah H M, Elrajubi O M, Abouda A A. Fraud detection in international calls using fuzzy logic [C]. International Conference on Computer Vision and Image Analysis Applications, 2015: 1-6.
- [119] Song R, Huang L, Cui W, et al. Fraud detection of bulk cargo theft in port using bayesian network models [J]. Applied Sciences, 2020, 10(3): 1056.
- [120] Villegas-Ortega J, Bellido-Boza L, Mauricio D. Fourteen years of manifestations and factors of health insurance fraud, 2006–2020: a scoping review [J]. Health & justice, 2021, 9(1): 1-23.

- [121] Jung E, Le Tilly M, Gehani A, et al. Data mining-based ethereum fraud detection [C]. 2019 IEEE International Conference on Blockchain (Blockchain), 2019: 266-273.
- [122] Underwood. D Barbara. Virtual currencies integrity initiative report. office of the new york state attorney general [M/OL]. 2018. [https://ag.ny.gov/sites/default/files/vmii\\_report.pdf](https://ag.ny.gov/sites/default/files/vmii_report.pdf).
- [123] Cointelegraph. What is stepn: A beginner's guide on the web3 lifestyle app [M/OL]. 2022. <https://cointelegraph.com/metaverse-for-beginners/what-is-stepn-gmt-a-beginners-guide-on-the-web3-lifestyle-app>.
- [124] Brandom, R. \$1.7 million in nfts stolen in apparent phishing attack on opensea users. the verge [M/OL]. 2022. <https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft>.
- [125] Nghiem H, Muric G, Morstatter F, et al. Detecting cryptocurrency pump-and-dump frauds using market and social signals [J]. Expert Systems with Applications, 2021, 182: 115284.
- [126] Malkiel B G. The efficient market hypothesis and its critics [J]. Journal of economic perspectives, 2003: 59-82.
- [127] Birru J, Young T. Sentiment and uncertainty [J]. Journal of Financial Economics, 2022: 142-3.
- [128] Loughran T, McDonald B. When is a liability not a liability? textual analysis, dictionaries, and 10-ks [J]. The Journal of Finance, 2011.
- [129] García H X, Diego, Rohrer M. The colour of finance words [J]. Journal of Financial Economics, 2023.
- [130] Correa G K L J M, R., Mislang N. Sentiment in central banks' financial stability reports [J]. Review of Finance, 2021.
- [131] Edmund Kwong Wei Leow B P N, Chua M C H. Robo-advisor using genetic algorithm and bert sentiments from tweets for hybrid portfolio optimisation [J]. Expert Systems with Applications, 2021, 179.
- [132] Li W S, Xuerong, Wang S. Text-based crude oil price forecasting: A deep learning approach [J]. International Journal of Forecasting, 2019, 35: 1548-1560.
- [133] Yun Bai H Y, Xixi Li, Jia S. Crude oil price forecasting incorporating news text [J]. International Journal of Forecasting, 2022, 38(1): 367-383.
- [134] Chiang T. Chatgpt is a blurry jpeg of the web [M/OL]. 2023. <https://www.newyorker.com/tech/annals-of-technology/chatgpt-is-a-blurry-jpeg-of-the-web>.
- [135] Wu I O L S D V D M G S , S., Mann G. Bloomberggpt: A large language model for finance [M]. Arxiv, 2023.
- [136] Deng B V H F B S, X., Bendersky M. What do llms know about financial markets? a case study on reddit market sentiment analysis [C]. ACM, 2023.
- [137] Huang H W, Allen H., Yang Y. Finbert: A large language model for extracting information from financial text [J]. Contemporary Accounting Research, 2023: 806-841.
- [138] Sharpe N R S, Steven A., Hollrah C A. The power of narrative sentiment in economic forecasts [J]. 39, 2023, 3: 1097-1121.
- [139] Wei G S, Mingzhe, Stasinakis C. Forecasting and trading bitcoin with machine learning techniques and a hybrid volatility/sentiment leverage [J]. Journal of Forecasting, 2023, 42: 852-871.
- [140] Lin F J Z Y, J., Chen L. Real-time macroeconomic projection using narrative central bank communication [J]. Journal of Applied Econometrics, 2023: 202-221.

- [141] Sutherland, S C. Forward guidance and expectation formation: A narrative approach [J]. *Journal of Applied Econometrics*, 2023: 222-241.
- [142] Khanh Quoc Nguyen T H N, Do B L. Narrative attention and related cryptocurrency returns [J]. *Finance Research Letters*, 2023: 104174.
- [143] Kumar J R B F, S., Billah M. Interconnectivity and investment strategies among commodity prices, cryptocurrencies, and g-20 capital markets: A comparative analysis during covid-19 and russia-ukraine war [J]. *International Review of Economics Finance*, 2023, 88: 547-593.
- [144] Abdullah M A F C, Mohammad, Sulong Z. Asymmetric efficiency and connectedness among green stocks, halal tourism stocks, cryptocurrencies, and commodities: Portfolio hedging implications [J]. *Resources Policy*, 2023, 81: 103419.
- [145] Arfaoui N M A B S M N, N., Karim S. Interdependence of clean energy and green markets with cryptocurrencies [J]. *Energy Economics*, 2023, 120.
- [146] Dettmers T, Zettlemoyer L. The case for 4-bit precision: k-bit inference scaling laws [C]. PMLR, 2023.
- [147] Jianping Li M L X Z, Guowen Li, Wei L. A novel text-based framework for forecasting agricultural futures using massive online news headlines [J]. *International Journal of Forecasting*, 2022: 35-50.
- [148] Takeshi Kojima M R Y M, Shixiang Shane Gu, Iwasawa Y. Large language models are zero-shot reasoners [J]. arXiv preprint, 2021: 11916.
- [149] Wei W X S D B M C E L Q, J., Zhou D. Chain of thought prompting elicits reasoning in large language models [J]. arXiv preprint, 2022: 11903.
- [150] Reimers N, Gurevych I. Sentence-bert: Sentence embeddings using siamese bert-networks [C]. ACL, 2019.
- [151] Leland McInnes J H, Melville J. Umap: Uniform manifold approximation and projection for dimension reduction [J]. 2018.
- [152] Stewart G, Al-Khassaweneh M. An implementation of the hdbscan\* clustering algorithm [J]. *Applied Sciences*, 2022: 2405.
- [153] Okonkwo I E. Nft, copyright and intellectual property commercialization [J]. *International Journal of Law and Information Technology*, 2021.
- [154] Dowling M. Is non-fungible token pricing driven by cryptocurrencies? [J]. *Finance Research Letters*, 2022: 102097.
- [155] Ko B S Y L H J, Hyungjin, Lee J. The economic value of nft: Evidence from a portfolio analysis using mean-variance framework [J]. *Finance Research Letters*, 2022: 102784.
- [156] Maouchi L C, Youcef, Montasser G E. Understanding digital bubbles amidst the covid-19 pandemic: Evidence from defi and nfts [J]. *Finance Research Letters*, 2022: 102584.
- [157] Kapoor G D M M Y R G M K P, A. Tweetboost: Influence of social media on nft valuation [C]//In Companion Proceedings of the Web Conference 2022. ACM, 2022.
- [158] Mekacher B A N M M M A L A L M B A, A. How rarity shapes the nft market [J]. 2022.
- [159] Phillips S S, Peter CB, Yu J. Specification sensitivity in right-tailed unit root testing for explosive behaviour [J]. *Oxford Bulletin of Economics and Statistics*, 2014, 76: 315-333.
- [160] Phillips, P. C. B., Shi, S. Real-time monitoring of asset markets: Bubbles and crisis [EB/OL]. 2020. <https://cran.r-project.org/web/packages/psymonitor/index.html>.
- [161] Simonyan K, Zisserman A. Very deep convolutional networks for large-scale image recognition [M]. arXiv preprint, 2014.

- [162] Van der Maaten L, Hinton G. Visualizing data using t-sne [J]. Journal of machine learning research, 9.
- [163] Pedregosa F, Varoquaux G, Gramfort A, et al. Scikit-learn: Machine learning in python [J]. Journal of machine learning research, 2011, 12(Oct): 2825-2830.
- [164] Li J, Mann W. Initial coin offering and platform building [J]. SSRN Electronic Journal, 2018: 1-56.
- [165] Andreas Antonopoulos. Bitcoin security model: trust by computation [EB/OL]. 2014. <http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html>.
- [166] Binance Academy. What is an initial exchange offering (ieo) [EB/OL]. 2020. <https://academy.binance.com/en/articles/what-is-an-initial-exchange-offering-ieo>.
- [167] Chris Prentice, Angus Berwick and Hannah Lang. Exclusive how ftx bought its way to become the 'most regulated' crypto exchange [EB/OL]. 2022. <https://www.reuters.com/technology/exclusive-how-ftx-bought-its-way-become-most-regulated-crypto-exchange-2022-11-18/>.
- [168] Aral S. The hype machine: how social media disrupts our elections, our economy, and our health—and how we must adapt. [J]. 2021.
- [169] Camacho-Collados J, Rezaee K, Riahi T, et al. TweetNLP: Cutting-Edge Natural Language Processing for Social Media [C]//Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing: System Demonstrations. Abu Dhabi, U.A.E.: Association for Computational Linguistics, 2022.
- [170] Andrew R. Chow and Chad De Guzman . A crypto game promised to lift filipinos out of poverty. here's what happened instead [EB/OL]. 2022. <https://time.com/6199385/axie-infinity-crypto-game-philippines-debt/>.
- [171] Hasti Chitsazan A B, Tajeddin M. Initial coin offerings (icos) success: Conceptualization, theories and systematic analysis of empirical studies [J]. Technological Forecasting and Social Change, 2022, 180: 121729.
- [172] Momtaz P P. Entrepreneurial finance and moral hazard: evidence from token offerings [J]. Journal of Business Venturing, 2021, 36(5): 106001.
- [173] Jiayue Wang W X Y T, Runyu Chen, Qin Y. A document analysis deep learning regression model for initial coin offerings success prediction [J]. Expert Systems with Applications, 2022, 210: 118367.
- [174] Christian Fisch S V J B, Christian Masiak. Motives and profiles of ico investors [J]. Journal of Business Research, 2021, 125: 564-576.
- [175] Wei Xu R C, Ting Wang, Zhao J L. Prediction of initial coin offering success based on team knowledge and expert evaluation [J]. Decision Support Systems, 2021, 147: 113574.
- [176] Lyandres B P, Evgeny, Rabetti D. Initial coin offering (ico) success and post-ico performance [J]. Management Science, 2022: 8658-8679.
- [177] Aslan A ♦, Aylin, Akdeniz L. Determinants of ico success and post-ico performance [J]. Borsa Istanbul Review, 2023: 217-239.
- [178] Davydiuk D G, Tetiana, Rosen S. De-crypto-ing signals in initial coin offerings: Evidence of rational token retention [J]. Management Science, 2023.
- [179] J.T. Hamrick A M A F N G T M M V, Farhang Rouhi. An examination of the cryptocurrency pump-and-dump ecosystem [J]. Information Processing Management, 2021, 58(4): 102506.
- [180] Balcilar M, Ozdemir H. On the risk spillover from bitcoin to altcoins: The fear of missing out

- and pump-and-dump scheme effects [J]. *Journal of Risk and Financial Management*, 2023, 16(1): 41.
- [181] La Morgia A M F S, Massimo, Stefa J. The doge of wall street: Analysis and detection of pump and dump cryptocurrency manipulations [C]//ACM Transactions on Internet Technology. Association for Computing Machinery, 2023.
- [182] Chullamonthon P, Tangamchit P. Ensemble of supervised and unsupervised deep neural networks for stock price manipulation detection [J]. *Expert Systems with Applications*, 2023: 119698.
- [183] Mbona I, Eloff J H. Feature selection using benford' s law to support detection of malicious social media bots [J]. *Information Sciences*, 2022, 582: 369-381.
- [184] Mazza M A S C, Michele, Tesconi M. Investigating the difference between trolls, social bots, and humans on twitter [J]. *Computer Communications*, 2022, 196: 23-36.
- [185] Beatson R G M C C, Oliver, Elliot M. Automation on twitter: Measuring the effectiveness of approaches to bot detection [J]. *Social Science Computer Review*, 2023: 181-200.
- [186] Uzuner M H H J J O. An empirical study of machine learning algorithms for social media bot detection [C]//2021 IEEE International IOT, Electronics and Mechatronics Conference. IEEE, 2021.
- [187] Cai H L X M Y C, Meng, Wang W. Network distribution and sentiment interaction: Information diffusion mechanisms between social bots and human users on social media [J]. *Information Processing Management*, 2023: 103197.
- [188] Pastor-Galindo F G M, Javier, Pérez G M. Profiling users and bots in twitter through social media analysis [J]. *Information Sciences*, 2022: 161-183.
- [189] Grootendorst M. Bertopic: Neural topic modeling with a class-based tf-idf procedure [M]. arXiv preprint, 2022.
- [190] Liu M O N G J D M J D C O L M L L Z, Yinhan, Stoyanov V. Roberta: A robustly optimized bert pretraining approach [M]. arXiv preprint, 2019.
- [191] Conneau K K N G V C G W F G E G M O L Z, Alexis, Stoyanov V. Unsupervised cross-lingual representation learning at scale [J]. 2019.
- [192] Kraaijeveld O, Smedt J D. The predictive power of public twitter sentiment for forecasting cryptocurrency prices [J]. *Journal of International Financial Markets, Institutions and Money*, 2020.
- [193] Sayyadilarikandeh O V K C Y A F, Mohsen, Menczer F. Detection of novel social bots by ensembles of specialized classifier [J]. In Proceedings of the 29th ACM international conference on information knowledge management, 2020: 2725-2732.
- [194] Chengcheng Shao O V K C Y A F, Giovanni Luca Ciampaglia, Menczer F. The spread of low-credibility content by social bots [J]. *Nature Communications*, 2018.
- [195] Alessandro B, Ferrara E. Social bots distort the 2016 u.s. presidential election online discussion [J]. *First monday*, 2016.
- [196] Vosoughi Soroush D R, Aral S. The spread of true and false news online [J]. *Science*, 2018.
- [197] Nir Grinberg L F B S T, Kenneth Joseph, Lazer D. Fake news on twitter during the 2016 u.s. presidential election [J]. *Science*, 2019.
- [198] Yang E F, Kai-Cheng, Menczer F. Botometer 101: Social bot practicum for computational social scientists [J]. *Journal of Computational Social Science*, 2022.

- [199] Bonifazi E C D U, Gianluca, Virgili L. A social network analysis-based approach to investigate user behaviour during a cryptocurrency speculative bubble [J]. Journal of Information Science, 2021: 01655515211047428.
- [200] Momtaz P P. Initial coin offerings [J]. Plos one, 2020, 15(5): e0233018.
- [201] Fisch C, Momtaz P P. Institutional investors and post-ico performance: an empirical analysis of investor returns in initial coin offerings (icos) [J]. Journal of Corporate Finance, 2020.
- [202] Letitia James. Attorney general james recovers 1.7million from cryptocurrency platform for operating illegally [EB/OL]



## 致 谢

此处填写致谢。

2023 年 6 月



## 作者简历及攻读学位期间发表的学术论文与其他相关学术成果

### 作者简历：

2016 年 08 月——2018 年 09 月，在纽约大学文理学院获得学士学位。

2018 年 09 月——2020 年 05 月，在福德汉姆大学商学院获得硕士学位。

2021 年 08 月——2024 年 07 月，在中国科学院大学经济与管理学院攻读博士学位。

### 已发表（或正式接受）的学术论文：

- (1) Tian, Yingjie, Xie, Yuhao, Su, Duo, Zhao, Xiaoxi."Picture For Proof (PFPs): Aesthetics, IP and post launch performance." *Finance Research Letters* 55 (2023): 103974.(SCI 2 区, IF: 10.4)
- (2) Tian, Yingjie, and Xie, Yuhao. "Artificial cheerleading in IEO: Marketing campaign or pump and dump scheme." *Information Processing and Management* 61.1 (2024): 103537. (SCI 1 区, IF:8.6)

### 在投的学术论文：

- (1) Tian, Yingjie, Xie, Yuhao, Gong, Yezhi."Toward the Future in Financial Fraud Detections: A Survey." *Expert Systems With Applications*. (SCI 1 区, IF: 8.5, 二审)
- (2) Xie, Yuhao, and Tian, Yingjie. "Dissecting Ethereum's Market Identity: A Cross-Asset Analysis with Large Language Model." *Information Systems Research*. (UTD24, 一审)

