



中山大學  
SUN YAT-SEN UNIVERSITY

# Web3与元宇宙的另一面 —— 风险与监管

吴嘉婧

中山大学 软件工程学院

2024 年 4 月 16 日

<http://xplanet.site>

# 提纲

- 1、元宇宙中的金融犯罪
- 2、元宇宙中的金融监管
- 3、元宇宙中的洗钱问题
- 4、监管与反洗钱：相关研究
- 5、监管与反洗钱：产品与工具

1

# 元宇宙中的金融犯罪

## ■ 诱发因素

### 1. 市场价值持续高涨

- Greyscale: 元宇宙物品销售（如虚拟土地、商品和服务等）已突破2亿美元
- Citibank: 预测到2030年，元宇宙的价值将高达13万亿美元

### 2. 数字资产的多样化

### 3. 概念新颖，辨识度低

### 4. 法律法规有待健全



#### Fungible

My \$10 is the exact same as your \$10



#### Semi-fungible

All general admission tickets get each person in to the same specific concert, but may not work for a different concert or date.



#### Non-fungible

Represents something unique and 1-of-1!

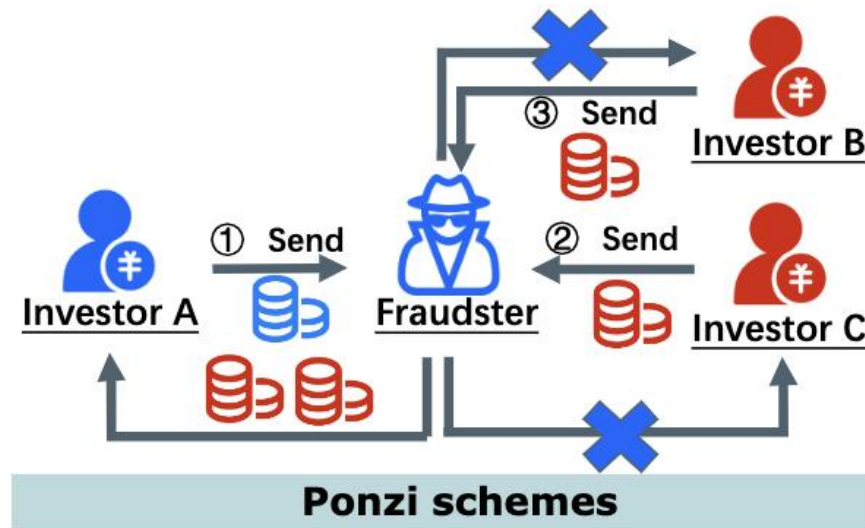
# 元宇宙中的金融犯罪



## ■ 旁氏骗局

### 1. 犯罪定义

- 一种空手套白狼的投资骗局：完全从新用户投入的资金中获得收入，通常依赖于收回的资金来弥补预付的资金

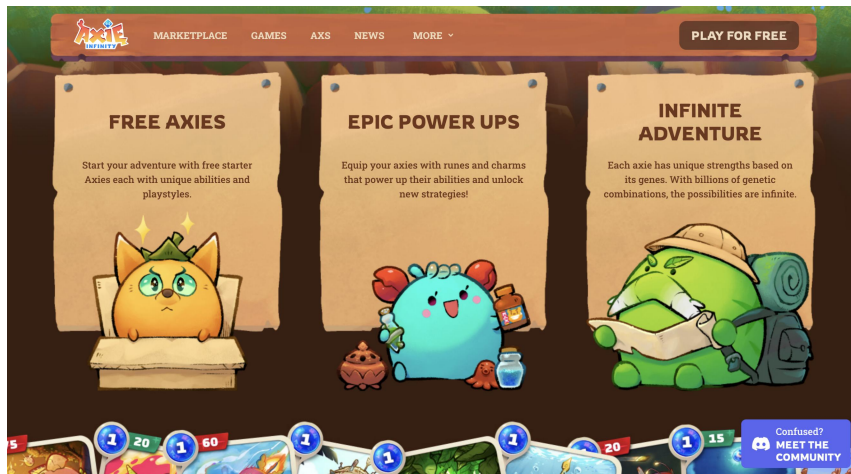


### 2. 表现形式

- 虚假包装（将物品资产化）
- 营销奖励（鼓励客户推荐购买）

### 3. 具体案例

- Axie Infinity



# 元宇宙中的金融犯罪



## ■ Rug Pull

### 1. 犯罪定义

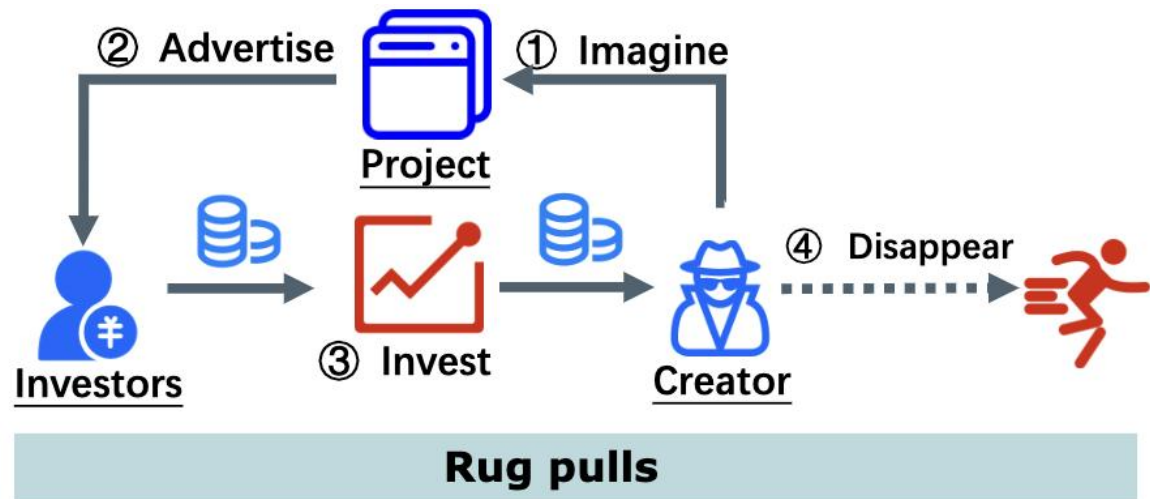
- 加密货币项目开发者带着投资者的钱潜逃的一种骗局

### 2. 表现形式

- 前期对项目进行宣传 and 承诺
- 后期毫无征兆地卷钱并逃跑

### 3. 具体案例

- Big Daddy Ape Club
- 获得了130万美元的投资金额，然后从大众的视野中消失



# 元宇宙中的金融犯罪



## ■ 钓鱼攻击

### 1. 犯罪定义

- 诱骗用户点击恶意链接，并恶意连接用户的 MetaMask 账户和资产

### 2. 表现形式

- 以广告的形式出现
- 钓鱼链接与官方域名相似

### 3. 具体案例

- The Sandbox Game
- 收到了声称为第二季发布出售土地的欺诈性网站



Ad · <https://www.decentraland.com/> :

#### Decentraland - Welcome to Decentraland

Decentraland is a virtual world where users can buy, develop, and sell Land. Gallery. Create, explore and trade in the first-ever virtual world owned by its users.

People also search for

<a href="#">decentraland game</a>	<a href="#">decentraland reddit</a>
<a href="#">decentraland (mana price prediction)</a>	<a href="#">decentraland casino</a>
<a href="#">where to buy decentraland</a>	<a href="#">decentraland rarible</a>
<a href="#">decentraland news</a>	<a href="#">is decentraland a good investment</a>

Ad · <https://www.decentrelond.net/> :

#### Decentraland 3D VR World - Decentraland Virtual World

Decentraland is controlled via the DAO, which owns the most important smart contracts. Using our service you can always get the most favorable conditions.

# 元宇宙中的金融犯罪



## ■ 虚假交易所

### 1. 犯罪定义

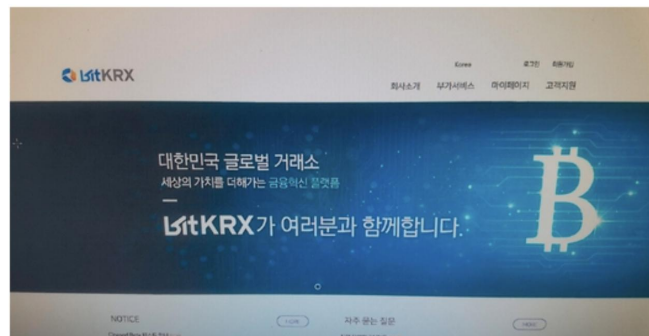
- 伪装成合法交易所，引诱交易者进行投资，待交易完成后直接消失

### 2. 表现形式

- 不惜使用假的名人代言
- 承诺惊人的投资回报率
- 拒绝提款

### 3. 具体案例

- BitKRX
- 伪装成大型、有信誉的交易平台 KRX





## ■ 赠品骗局

### 1. 犯罪定义

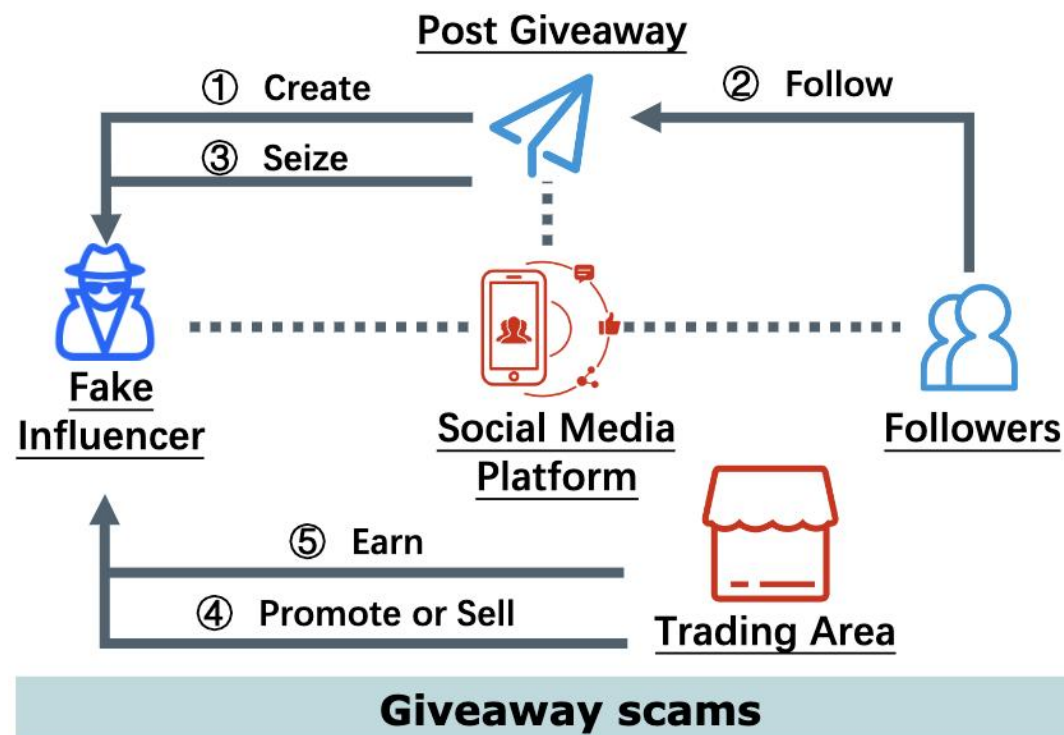
- 向被免费赠品诱惑的用户收取费用

### 2. 表现形式

- 宣传组织一次赠品活动
- 投资者向规定地址发送资产才能获取赠品

### 3. 具体案例

- Yuga Labs
- 推出 MetaRPG 和原生加密资产 ApeCoin 时，欺骗用户点击恶意链接并要求发送资金以获取赠品



## ■ 代码入侵

### 1. 犯罪定义

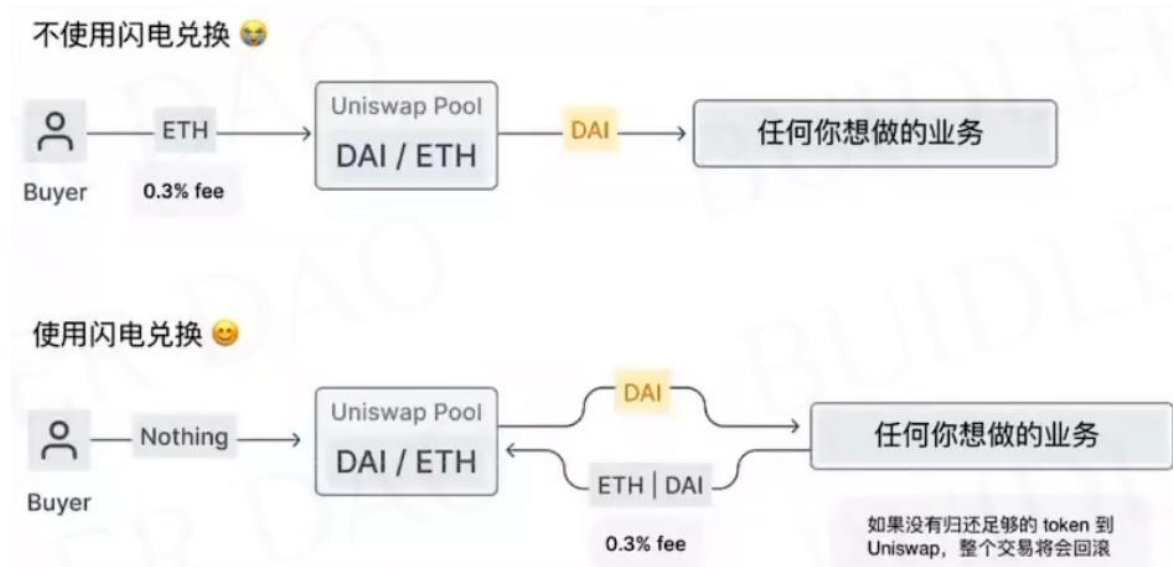
- 利用区块链协议或其智能合约中的漏洞对区块链系统的入侵

### 2. 闪电贷定义

- 无抵押贷款
- 通过区块链上的智能合约完成
- 贷款过程快，一个区块内完成贷款和还款

### 3. 闪电贷攻击案例：

- 币安智能链（BSC）上的DeFi项目Eleven Finance受到闪电贷攻击
- 攻击者最后归还闪电贷，将剩余的647573.8个BUSD转移到私人地址



## ■ 刷量

### 1. 犯罪定义

- 人为操纵数据来刷高数据，是一种欺骗性质的营销手段

### 2. NFT 刷量

- 为了上新 NFT 集合而虚构交易量
- 通过 NFT 交易刷量获取其他代币奖励

### 3. 具体案例

- Chainalysis 曾报道过两个钱包之间重复买卖相同的 3 个 NFT，交易了大约 650,000 ETH，花费 1.14 亿美元的交易费用
- 最后获得 NFT 交易平台价值约 1.855 亿美元的代币，带来了近 7100 万美元的利润



## ■ 洗钱

### 1. 犯罪定义

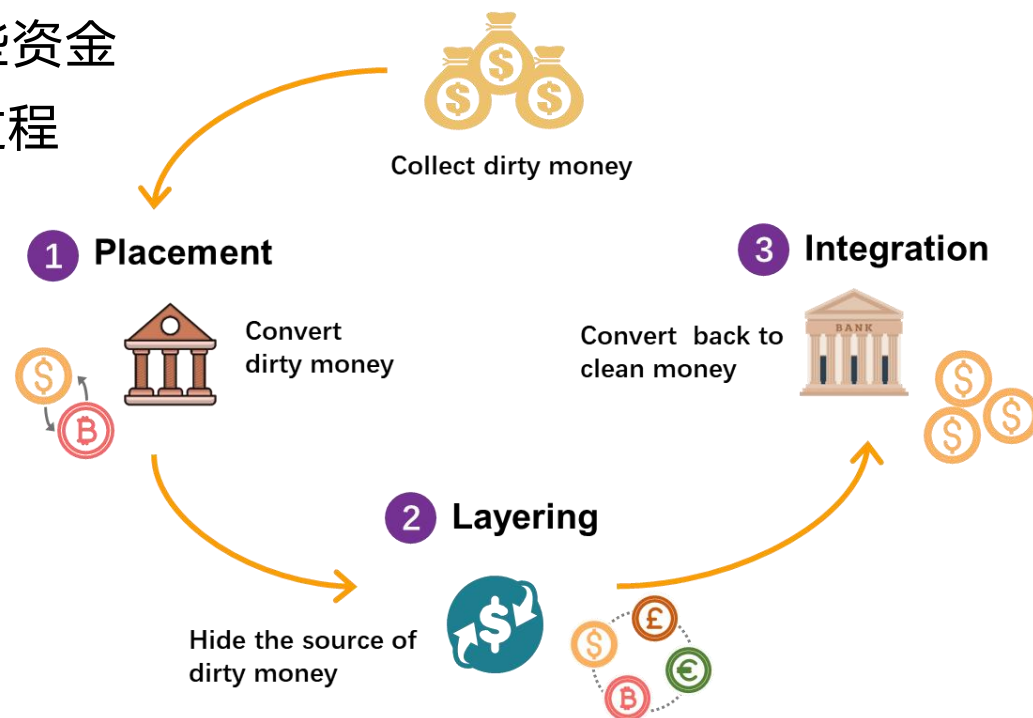
- 获取犯罪所得并掩饰其非法来源，以便利用这些资金从事合法或非法活动，让肮脏的钱看起来干净的过程

### 2. 洗钱三步骤

- 放置
- 分层
- 整合

### 3. 元宇宙背景下的洗钱

- 一般无需 know-your-customer (KYC) checks
- 土地资产和可穿戴设备成为洗钱的新途径



## ■ 非法服务和商店

### 1. 犯罪定义

- 不法分子可能会利用元宇宙商店销售非法服务和商品，用元宇宙商店里的物品来掩盖现实世界中的非法商品

### 2. 具体案例

- Youtube 上一段 30 秒的视频显示了 Snapchat 的屏幕截图，上面有机器人的声音覆盖，提供购买麻醉品和枪支等物品的服务，视频中没有透露地点，因此无法核实是否正在或曾经打算创建这种服务



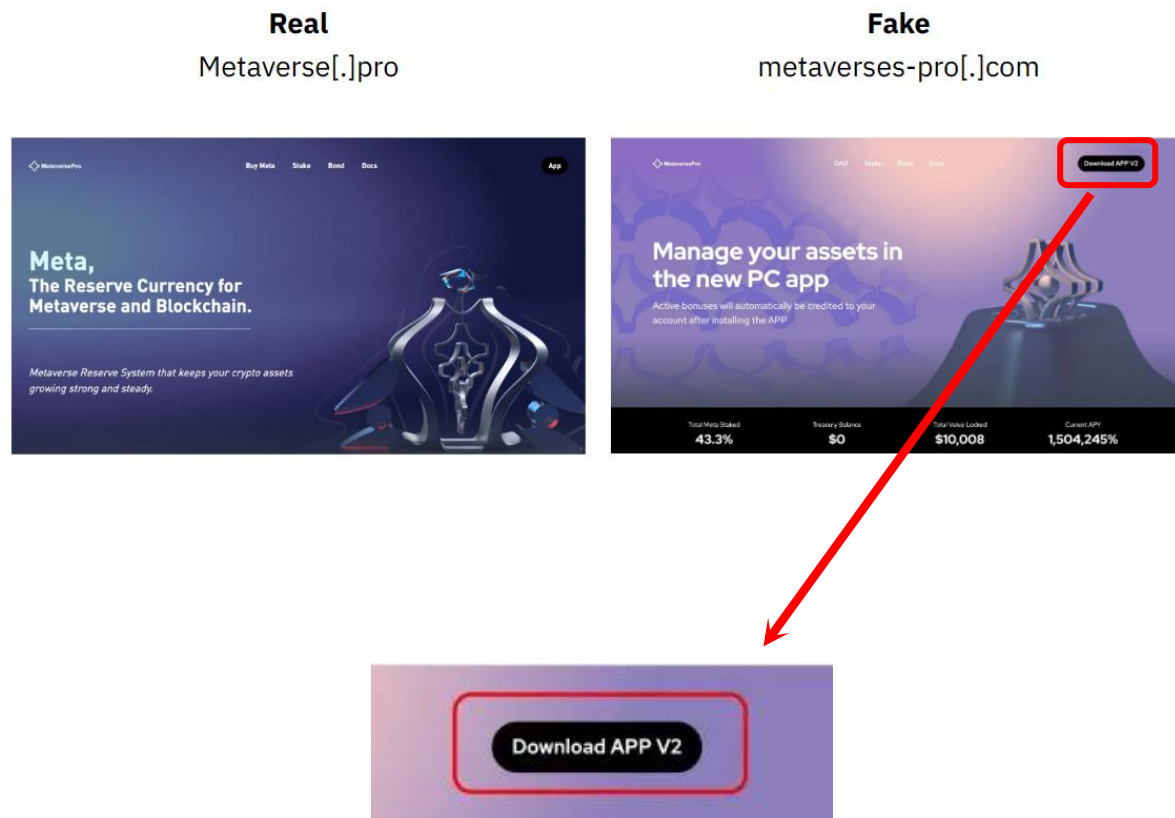
## ■ 虚假元宇宙

### 1. 犯罪定义

- 非法行为者通过宣布推出一个新的元宇宙项目或建立一个与合法项目相似的虚假 NFT 网站，来非法骗取用户的账户信息和加密资产

### 2. 具体案例

- MetaversePRO 的虚假克隆网站通过视觉效果让用户难以分辨，进而通过一步步的引导来骗取用户的加密资产



# 元宇宙中的金融犯罪



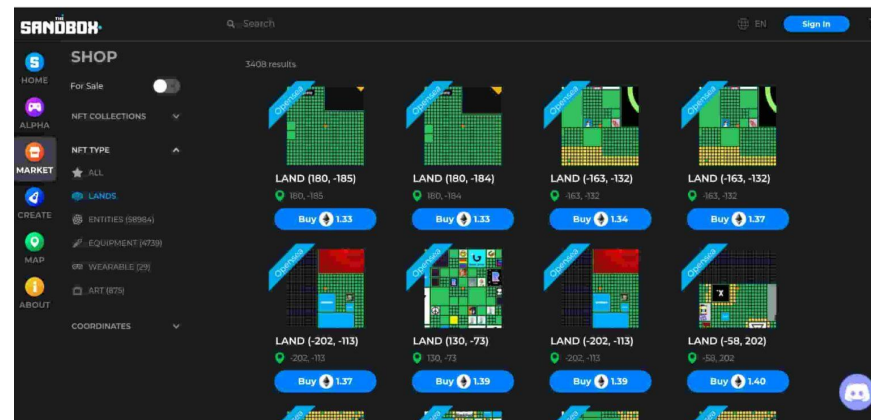
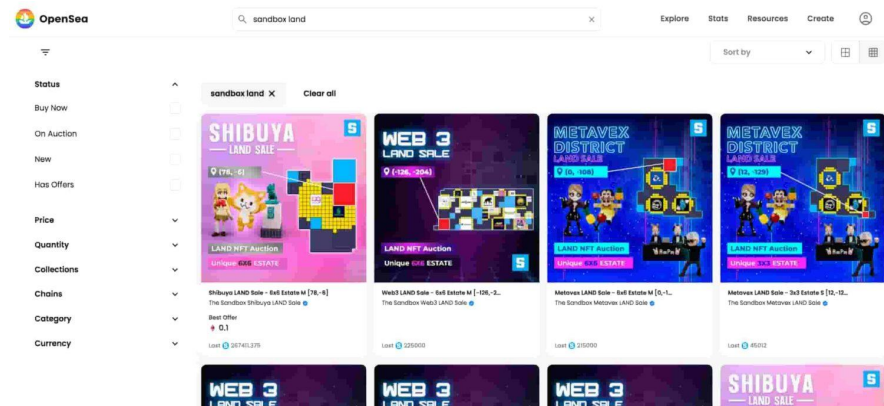
## ■ 虚假土地扩张

### 1. 犯罪定义

- 非法行为者通过推出虚假的新区域土地扩张或制造著名元宇宙项目土地资产的假版本来欺骗用户的购买

### 2. 土地资源

- Decentraland 启动了 90,601 块土地
- The Sandbox 拥有 166,464 块土地



## ■ 技术支持骗局

### 1. 犯罪定义

- 非法行为者通过冒充元宇宙项目的工作人员或者技术人员，来试图诱使新用户分享私钥或将他们的 MetaMask 钱包连接到非法恶意的网站

### 2. 表现形式

- 远程访问电脑
- 安装恶意软件
- 销售软件维护服务
- 推荐电脑保修计划
- 信用卡支付虚假服务
- 引导输入敏感信息





# 元宇宙中的金融犯罪



## ■ 研究现状

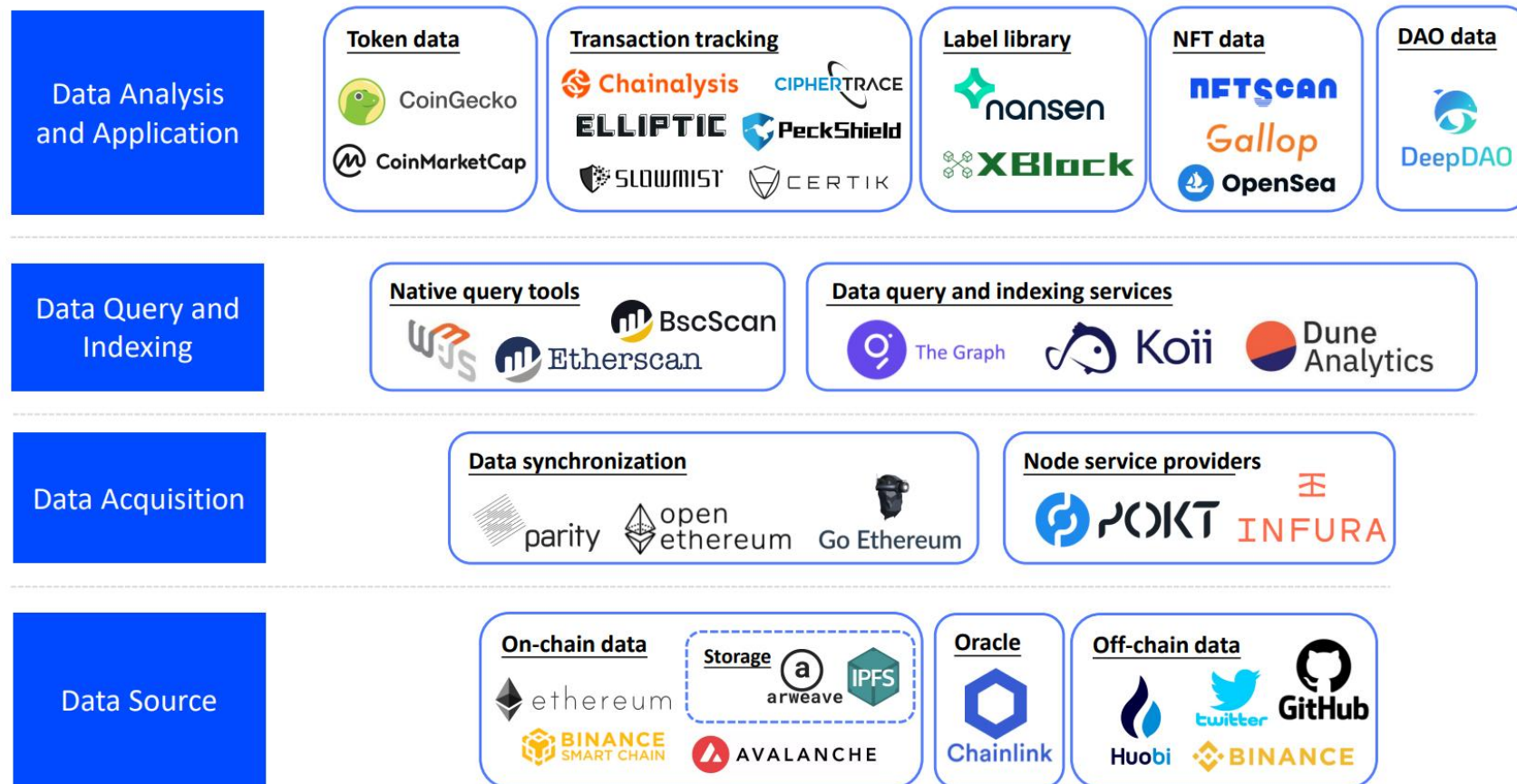
Crimes	Paper	Year
Scams	Cryptocurrency scams: analysis and perspectives	2021
Code Exploit	Cryptocurrency crime: Behaviors of malicious smart contracts in blockchain	2021
	Scams, frauds, and crimes in the nonfungible token market	2022
Wash Trading	Detecting and quantifying wash trading on decentralized cryptocurrency exchanges	2021
	Do cryptocurrency exchanges fake trading volumes? An empirical analysis of wash trading based on data mining	2022
	Detecting wash trading for nonfungible tokens	2022
Money Laundering	Identity, crimes, and law enforcement in the metaverse	2022

# 2

# 元宇宙中的金融监管

## ■ 数据驱动机遇：Web3.0 特性

- 公开透明
- 防伪造
- 不可篡改
- 可追溯



## ■ 数据来源

### 1. 链上数据

- 区块、转账交易、钱包地址、智能合约字节码、智能合约事件、数字资产信息等数据

### 2. 链下数据

- 中心化交易所的数据（如币安交易所）、社交媒体数据、GitHub网站数据等

```
name: "Golden carp"
description: "Oh, it's sparkly!\nキラキラ!"
image: "ipfs://bafybeidrduyubujutu745wtwua4urzfyfjdyfbragiwiivtpeuhbwcqnpqxy/golden-carp.png"
external_url: "https://www.sandbox.game/en/assets/golden-carp/9f8e8f95-af9a-4aa3-a1ec-48921375b01d/"
animation_url: "ipfs://bafybeidrduyubujutu745wtwua4urzfyfjdyfbragiwiivtpeuhbwcqnpqxy/golden-carp.gif"
sandbox:
  version: 2
  creator: "0xfe1824b88c1e91b027b2fb74b529c5229aa89d3a"
  classification:
    type: "Entity"
    theme: "None"
    categories:
      0: "Magic"
      1: "Nature"
      2: "Fantasy"
  voxel_model: "ipfs://bafybeidrduyubujutu745wtwua4urzfyfjdyfbragiwiivtpeuhbwcqnpqxy/golden-carp.vxc"
  creator_profile_url: "https://www.sandbox.game/en/users/hardbone01/04588f8c-13e5-444d-a43b-31e1689923a6/"
```

The Sandbox	NFT等交易数据存储在以太坊公链上，NFT的其余属性信息如图片存储在了IPFS
Decentraland	技术组件资源信息，开源（ <a href="https://github.com/decentraland/">https://github.com/decentraland/</a> ） Twitter了解项目的最新情况，（ <a href="https://twitter.com/decentraland">https://twitter.com/decentraland</a> ）

## ■ 数据获取：基于以太坊的元宇宙项目

### 1. 下载和直接解析区块文件

- 优点：简单、快速
- 不足：不能收集到完整的数据，内部事务无法直接获取

### 2. 部署以太坊客户端

- 优点：可直接获得以太坊的内部交易和外部交易
- 不足：获取的数据有限，如合约字节码数据等无法获取

### 3. 节点服务商

- 优点：缩小了金钱和技术等成本
- 实例：去中心化数据服务商 Pocket Network

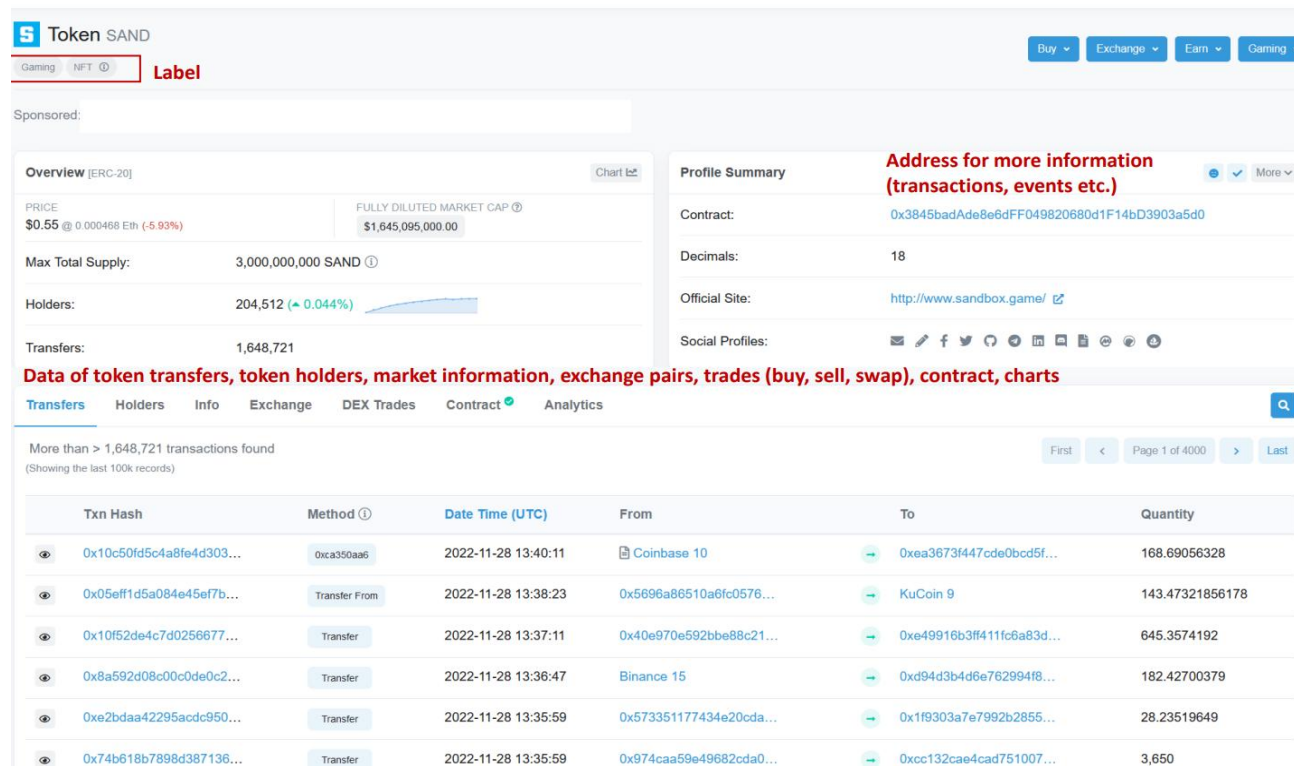
## ■ 数据查询与索引：底层公链的API和区块链浏览器

### 1. 以太坊提供的 web3 API

- 调用 `web3.eth.getTransaction()` 可以获取指定哈希交易的数据

### 2. 以太坊浏览器 Etherscan

- 可以直接通过网页搜索链上信息，包括链的数据，区块的数据、交易数据、智能合约数据、地址数据等



The screenshot displays the Etherscan interface for the Token SAND. It includes an overview section with price and market cap, a profile summary with contract address and decimals, and a table of recent transactions.

Txn Hash	Method	Date Time (UTC)	From	To	Quantity
0x10c50fd5c4a8fe4d303...	0xca30a6e	2022-11-28 13:40:11	Coinbase 10	0xea3673f447cde0bcd5f...	168.69056328
0x05eff1d5a084e45ef7b...	Transfer From	2022-11-28 13:38:23	0x5696a86510a6fc0576...	KuCoin 9	143.47321856178
0x10f52de4c7d0256677...	Transfer	2022-11-28 13:37:11	0x40e970e592bbe88c21...	0xe49916b3f411fc6a83d...	645.3574192
0x8a592d08c00c0de0c2...	Transfer	2022-11-28 13:36:47	Binance 15	0xd94d3b4d6e762994f8...	182.42700379
0xe2bd9aa42295acdc950...	Transfer	2022-11-28 13:35:59	0x573351177434e20cda...	0x1f9303a7e7992b2855...	28.23519649
0x74b618b7898d387136...	Transfer	2022-11-28 13:35:59	0x974caa59e49682cda0...	0xcc132cae4cad751007...	3,650

## ■ 数据查询与索引：提供数据查询和索引服务的服务商

### 1. Dunc Analytics 一个综合型的Web3数据平台

- 便于用户进行实时查询、分析以及通过仪表盘的可视化
- 注意：有用户在Dune上创建了NFT Wash Trader的仪表盘  
(<https://dune.com/cryptok/NFT-Wash-Trading>)

### 2. The Graph 一个去中心化的链上数据索引协议

- 用于查询像以太坊和 IPFS 网络
- 相关研究工作：Xia 等人 “Trade or trick? detecting and characterizing scam tokens on uniswap decentralized exchange,” 2021

## ■ 数据分析平台：封装的、可交付数字产品

参与者	代表性平台
代币数据平台	CoinMarketCap ( <a href="https://coinmarketcap.com">https://coinmarketcap.com</a> ) DeFiLlama ( <a href="https://defillama.com">https://defillama.com</a> ) (hack事件列表[1]) 等
链上交易追踪平台 (Srivasthav 综述[2])	Chainalysis ( <a href="https://www.chainalysis.com">https://www.chainalysis.com</a> ) CiperTrace ( <a href="https://ciphertrace.com">https://ciphertrace.com</a> )
标签库平台	Nansen ( <a href="https://www.nansen.ai/">https://www.nansen.ai/</a> ) Xblock ( <a href="http://xblock.pro/">http://xblock.pro/</a> )
NFT 数据平台	NFTscan ( <a href="https://www.nftscan.com/">https://www.nftscan.com/</a> ) Gallop 公司 ( <a href="https://www.higallop.com/">https://www.higallop.com/</a> ) (Cho等介绍与NFT 交易数据相关挑战以及数据预处理建议[3])
DAO 数据平台	DeepDAO ( <a href="https://deepdao.io/">https://deepdao.io/</a> )



# 3

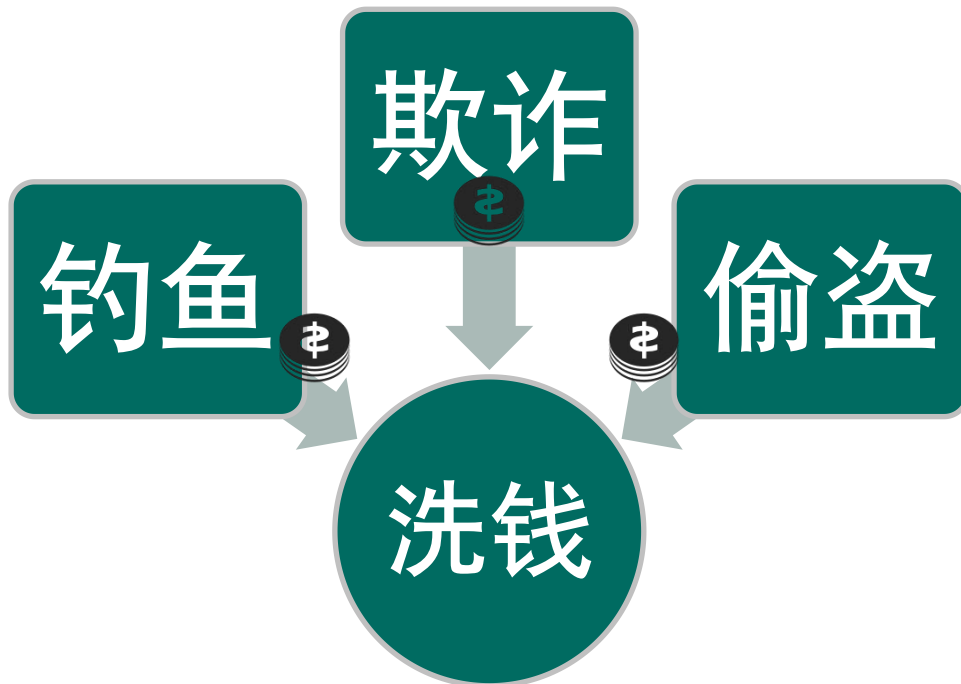
# 元宇宙中的洗钱问题



# 元宇宙洗钱高发



- 洗钱是众多上游犯罪对所得赃款进行处理的手段



- 作为上游犯罪的“链条下游”，通过加密货币交易的方式来洗白犯罪所得的黑币、黑钱已呈趋势

# 元宇宙洗钱高发



## ➤ 在技术方面：

### ● 去中心化

让其不受外汇管制，逃避金融监管。

### ● 分布式

让其在全球任何网络节点活动，监管难度很大。

### ● 匿名性

让其天然抗监管，难以追踪识别

## ➤ 在商业方面：

- 利用了人们的投机心理，以“风口”“暴富”为诱饵，招募众多人员注册匿名地址，为其洗钱提供便利





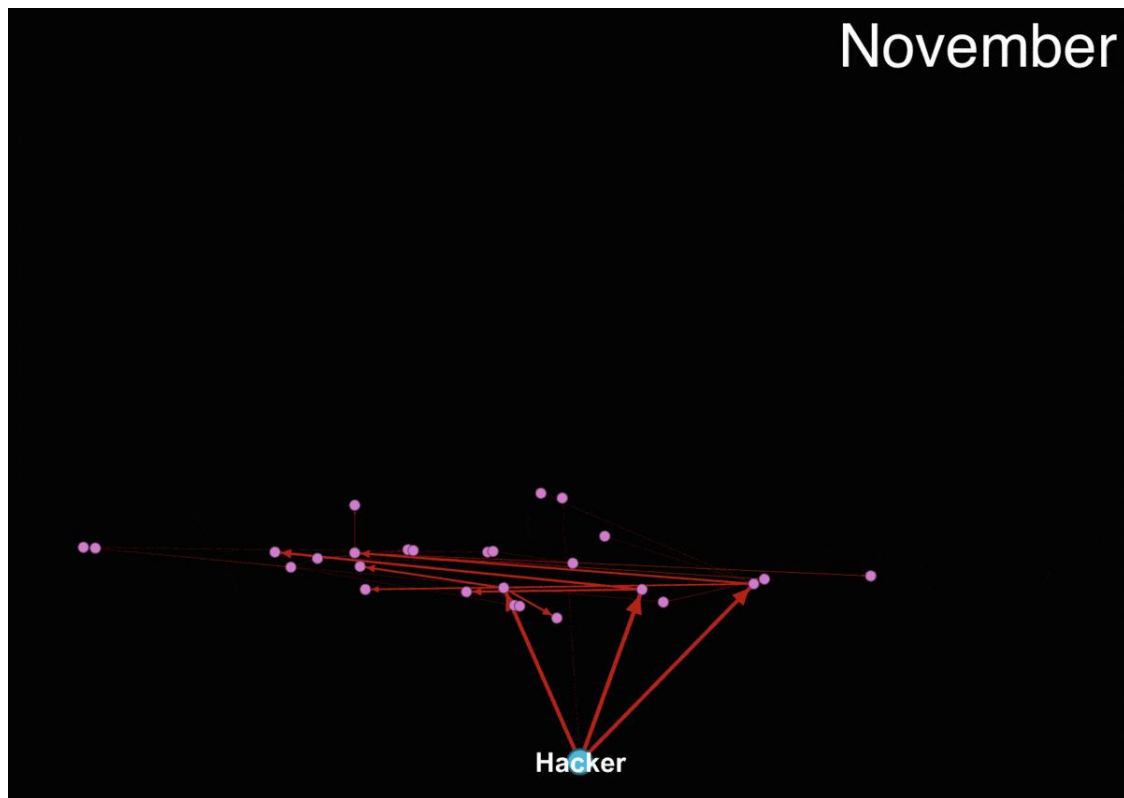
## ■ Upbit 交易所被盗安全事件

- 案件概述：2019 年11月，黑客从韩国upbit交易所热钱包中取走了 342,000 ETH，当时市值超过 4800 万美元
- 黑客账户：0xa09871 aeadf4994ca12f5c0b6056bbd1d343c029
- 洗钱时间：从 2019 年11月到 2020 年 5 月
- 洗钱规模：815 个账户（节点），1374 条交易（有向边）
- 洗钱模式：多个新地址拆分赃款，汇总去交易所套现
- 交易所AML：2020 年 5 月，中心化交易所 Binance 宣布冻结了黑客先前从Upbit盗取的ETH

# 元宇宙洗钱案例：Upbit 交易所被盗洗钱



## ■ Upbit交易所被盗洗钱动态图



Cylynx绘制的hacker每月洗钱动图

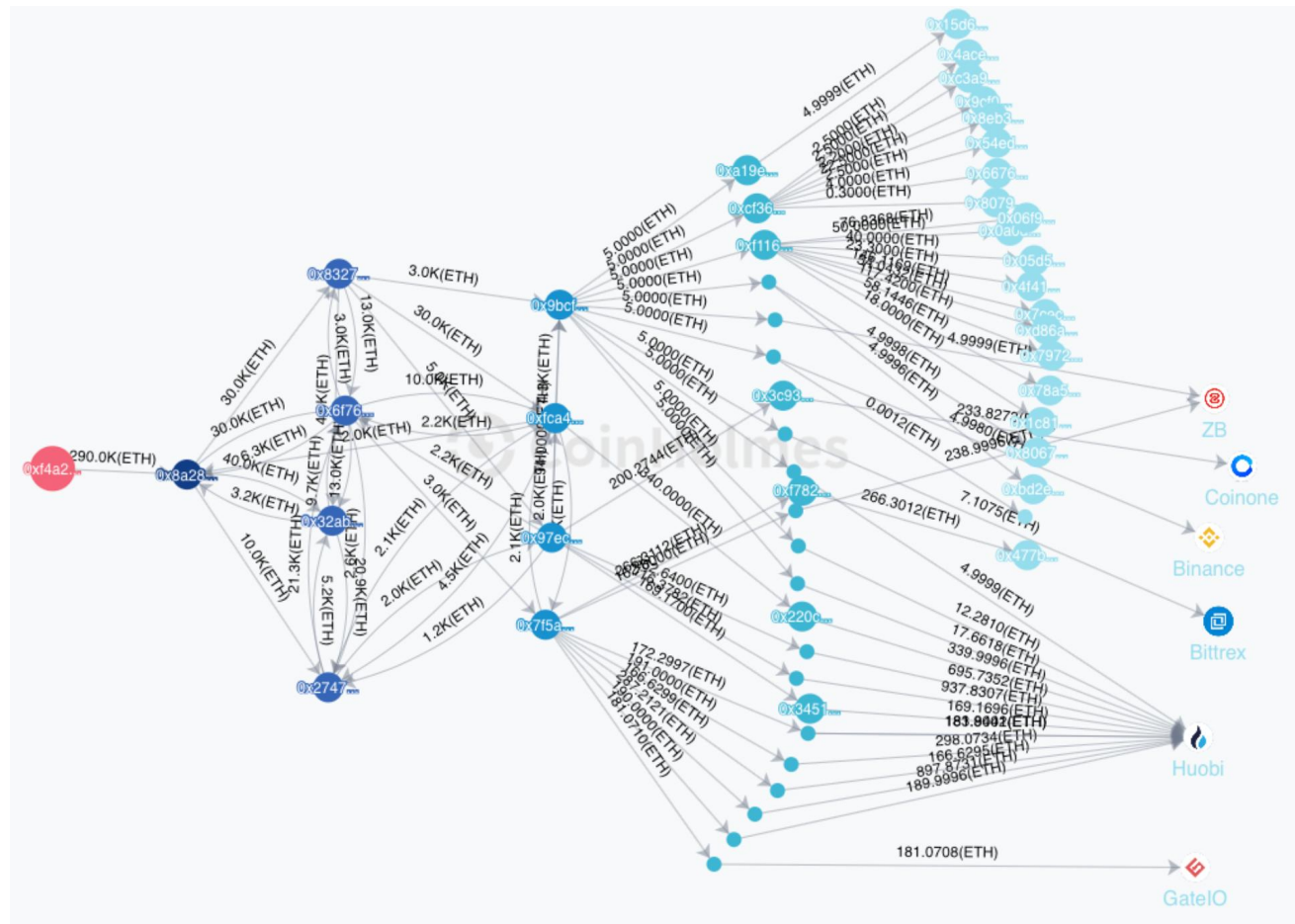
1	EXCHANGE	AMOUNT IN ETH	PERCENT
2	Binance	83280.19	22.07%
3	Undefined	57850.52	15.33%
4	Tokenlon	50743.93	13.45%
5	OKEX	48711.13	12.91%
6	Byex	39513.76	10.47%
7	Bitmax	34635.23	9.18%
8	Huobi Global	28457.35	7.54%
9	DDEX	12955.32	3.43%
10	Bibox	4665.61	1.24%
11	EtherDelta	4253.89	1.13%
12	Bity.com	3638.66	0.96%
13	FCoin	1844.02	0.49%
14	HitBtc	1079.69	0.29%
15	Bit-Z	817.6	0.22%
16	Poloniex	604.97	0.16%
17	Gate	520.62	0.14%
18	MXC	373.21	0.1%
19	Livecoin	335.4	0.09%
20	bgogo	323.0	0.09%

CLAIN统计的hacker洗钱出口

# 元宇宙洗钱案例：PlusToken 庞氏骗局洗钱



## PlusToken 资产转移过程图



多次周密的分散转移乃至混淆洗钱等操作，最终部分资金流入交易所

# 传统金融洗钱 vs 元宇宙洗钱？



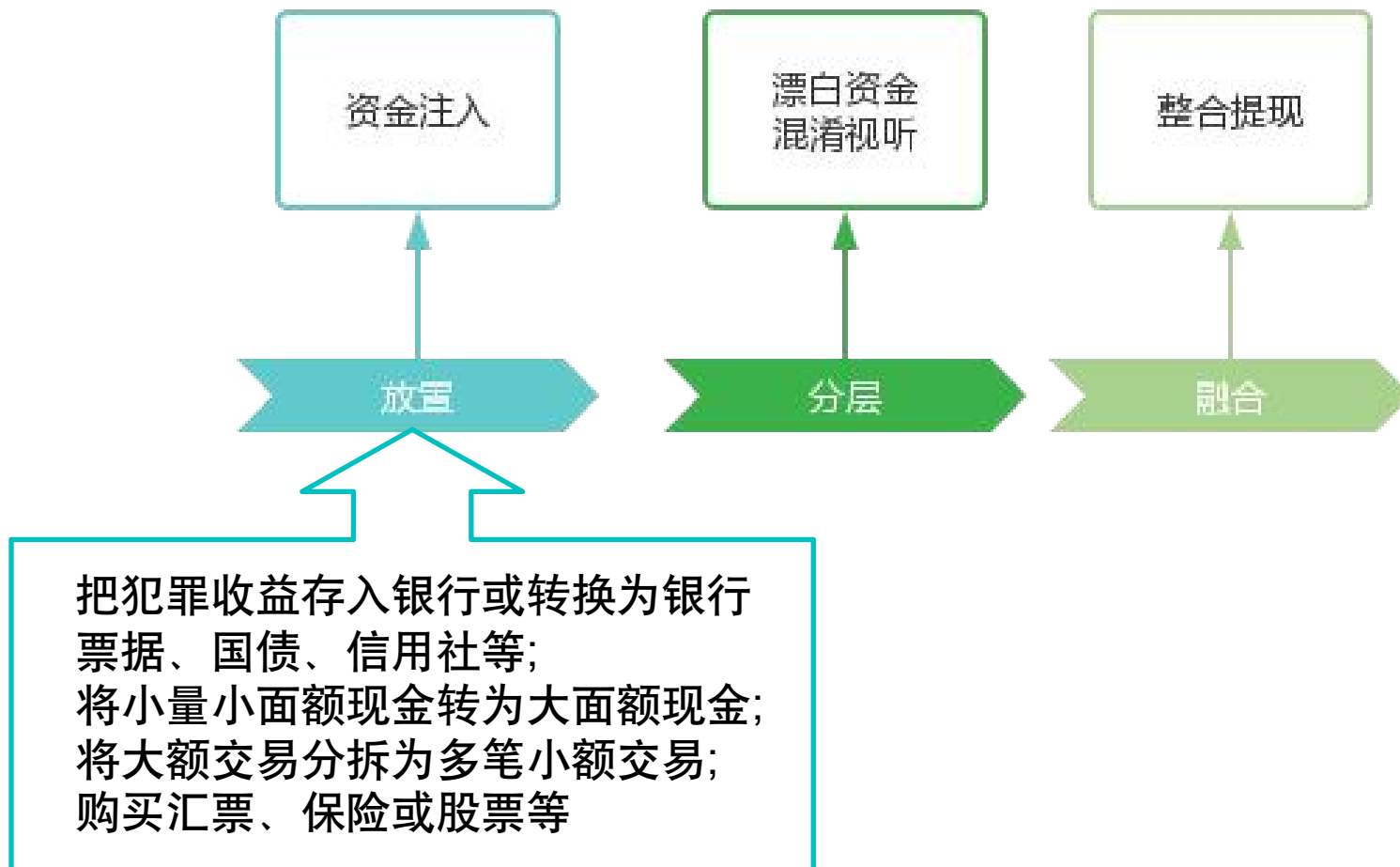
- 洗钱犯罪并不是一个新的问题，作为上游犯罪后所得赃款的后续处理手段，洗钱在传统金融行业中就有非常多的犯罪案例
- 传统金融洗钱：
  - 各种渠道收集的资产混合
  - 采取不同的手段进行多层次、分批次的财产转移
- 在传统金融行业中，各类机构例如银行等，也已经有许多运用各种方法进行反洗钱识别的研究



# 传统金融洗钱的基本过程



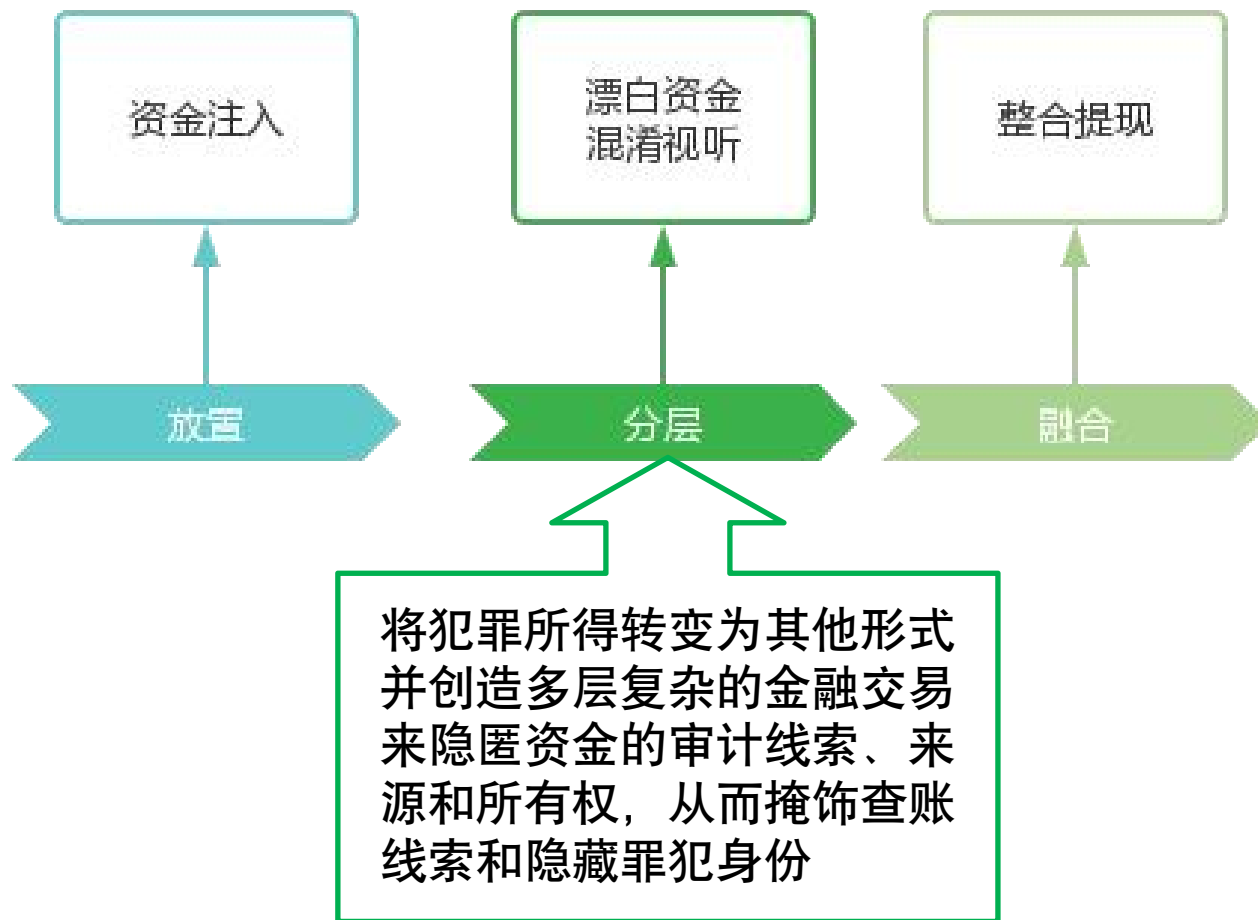
## ▶ 洗钱通常分为三个阶段



# 传统金融洗钱的基本过程



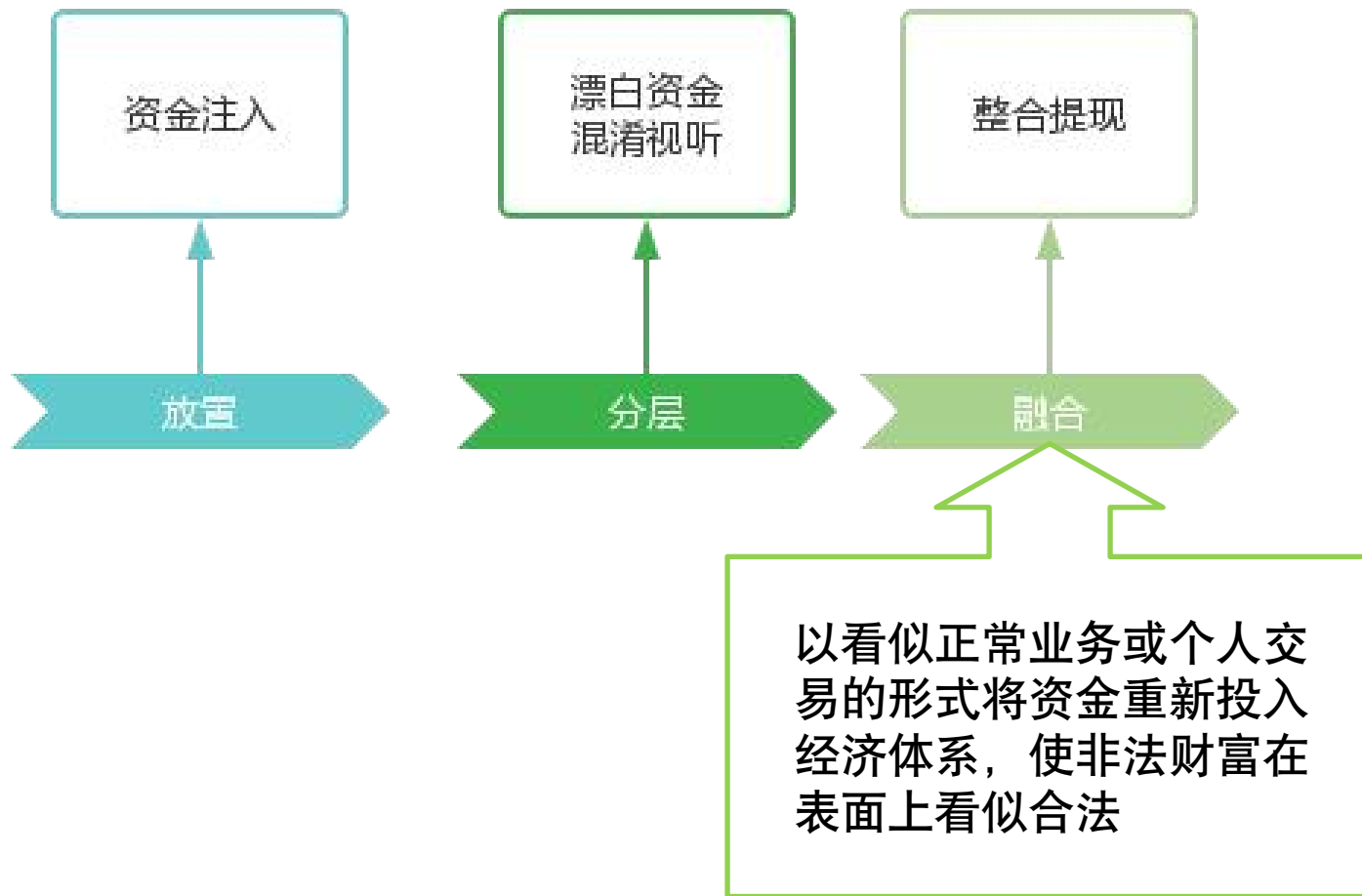
## ▶ 洗钱通常分为三个阶段



# 传统金融洗钱的基本过程



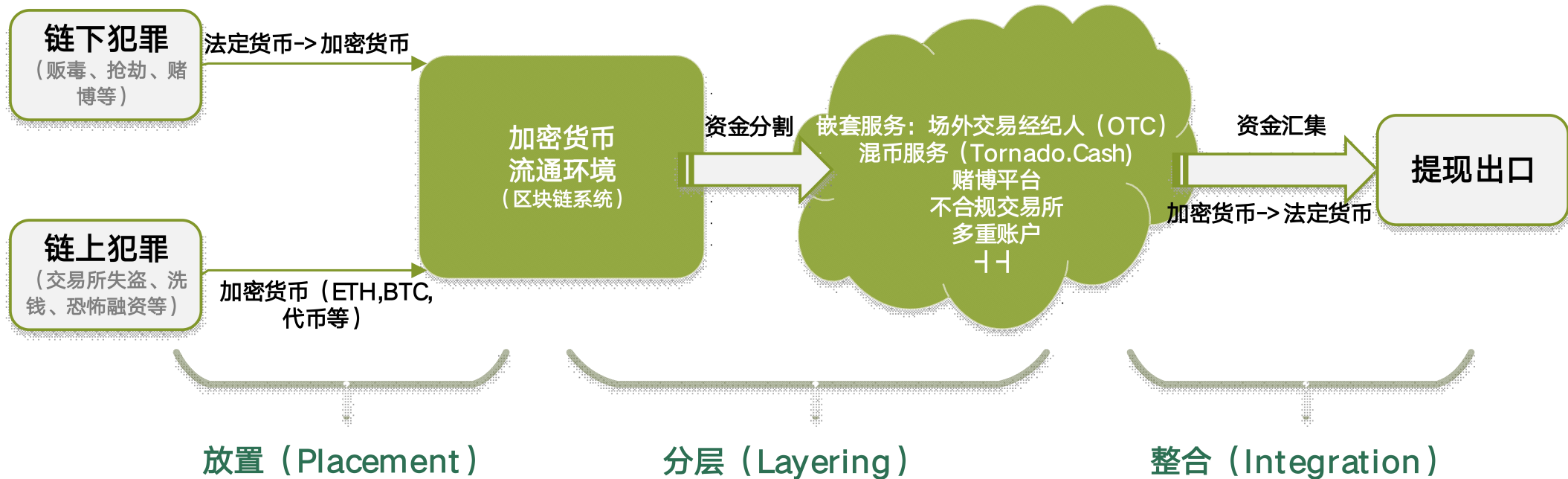
## ▶ 洗钱通常分为三个阶段



# 元宇宙洗钱的基本过程



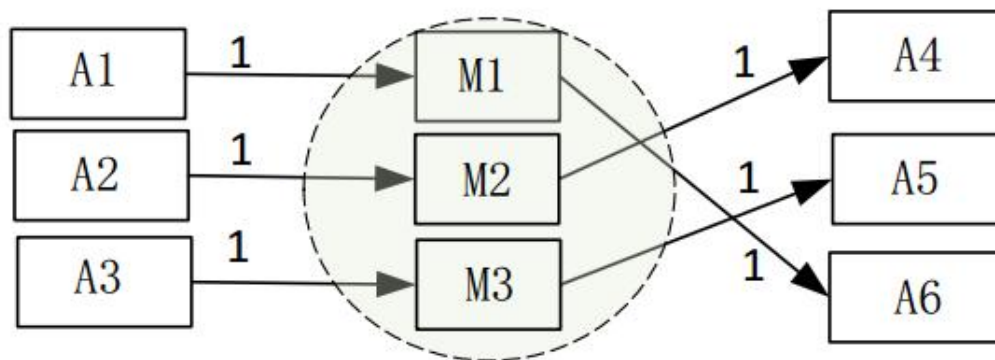
## 类似于传统金融洗钱，也是三个阶段



# 元宇宙新型洗钱手段：混币服务



- 混币服务是一种通过混淆交易记录以保护交易隐私的技术
- **方法：**多个用户间的资金快速高效混合，在现有的用户账户和混币后的新账户之间**创建随机的映射关系**
- 混币服务的**两面性**
- 混币服务既可以增强匿名性，被用于保护隐私被用于保护隐私被用于保护隐私
- 混币服务也可以被用于洗钱、犯罪等非法活动



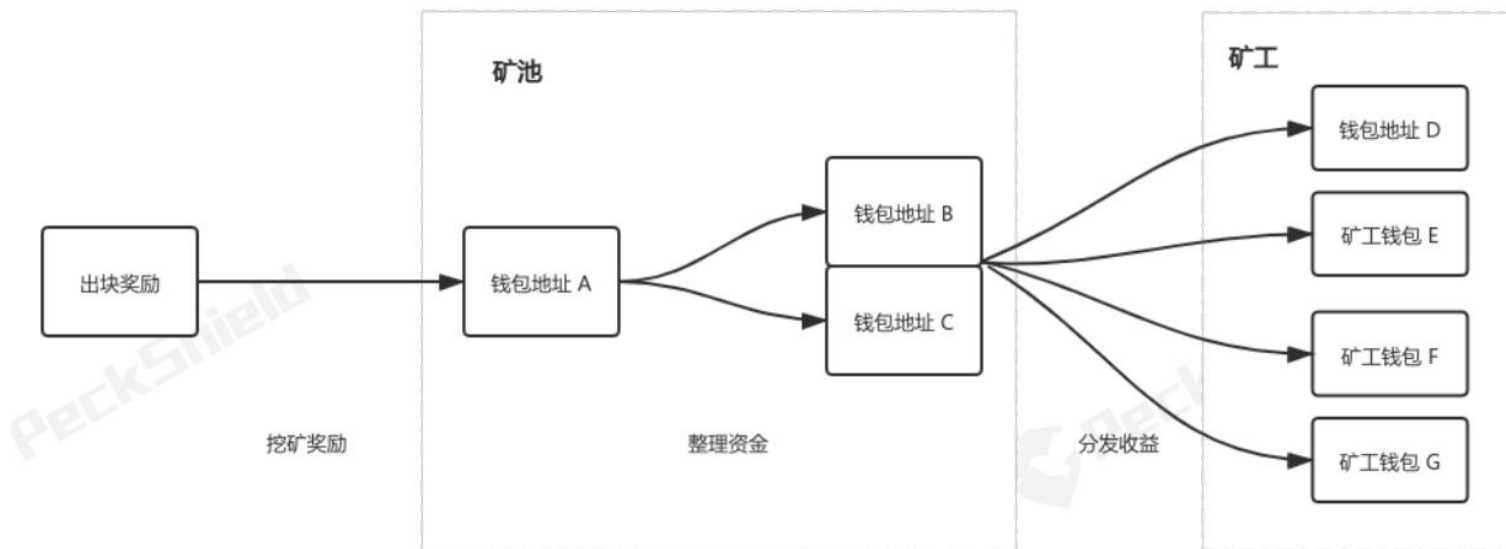
比特币混币服务

# 元宇宙新型洗钱手段：比特币矿工



## ➤ 最高检发布虚拟货币洗钱经典案例

- 陈某某获取链下犯罪非法所得的人民币90余万元
- 将90余万元转账给**比特币矿工**以换取比特币密钥
- 陈某某将比特币密钥发送给境外的同伙以获取洗白的比特币



矿工出块奖励资金流转

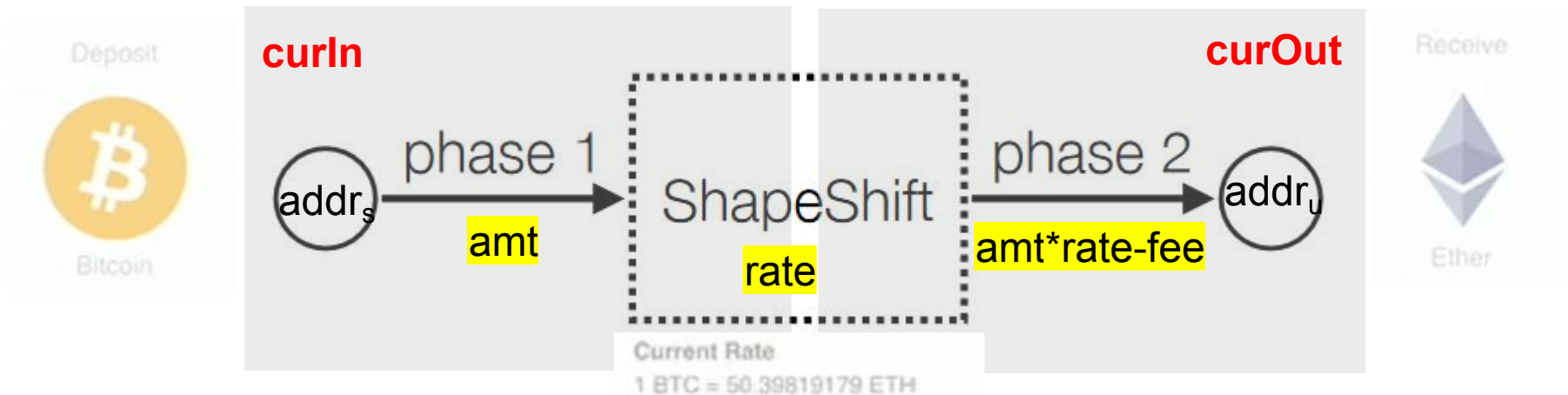
# 元宇宙新型洗钱手段：跨链洗钱



## 通过跨链交易来模糊资金路径

- **需求：** 由于众多区块链平台之间的相互独立性，通常需要通过跨链链间的资产转移
- **定义：** 将 A 链上的数据（或信息、资产）安全可信地转移到 B 链并在 B 链上产生预期效果
- **手段-跨链桥：** 跨链桥是目前最流行的跨链解决方案

技术方案：1. 锁仓+铸造/销毁类， 2. 流动性池类， 3. 原子置换类

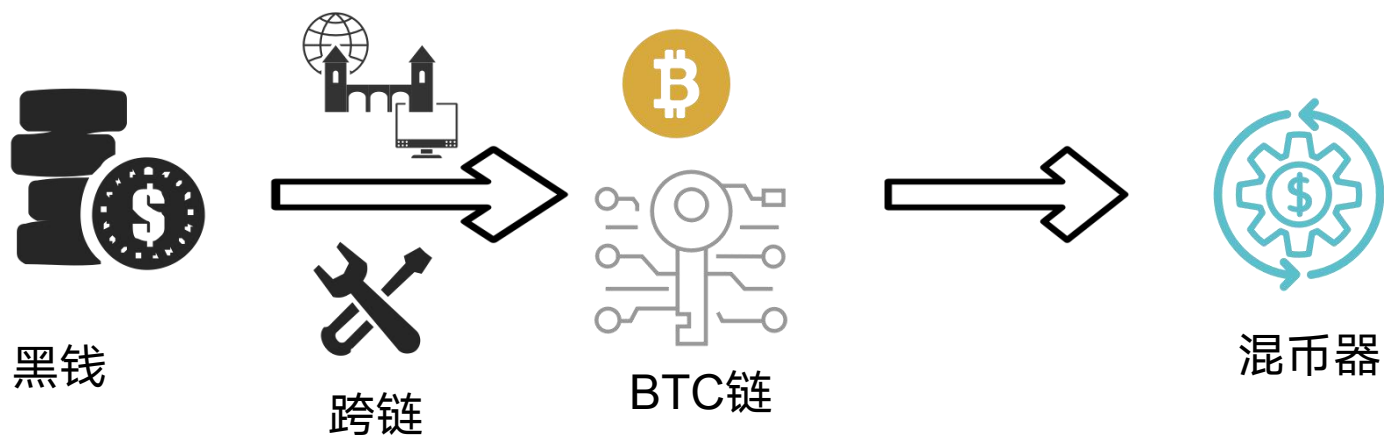


# 元宇宙洗钱手段：去中心化化工具洗钱



## ➤ 融合难追踪、更加复杂的去中心化金融DeFi工具模糊洗钱路径

- 罪犯利用跨链等工具将“黑钱”跨到BTC链上再转入ChipMixer等混币器
- 链上混币服务平台Tornado Cash已被美国制裁





# 元宇宙洗钱 vs 传统金融洗钱

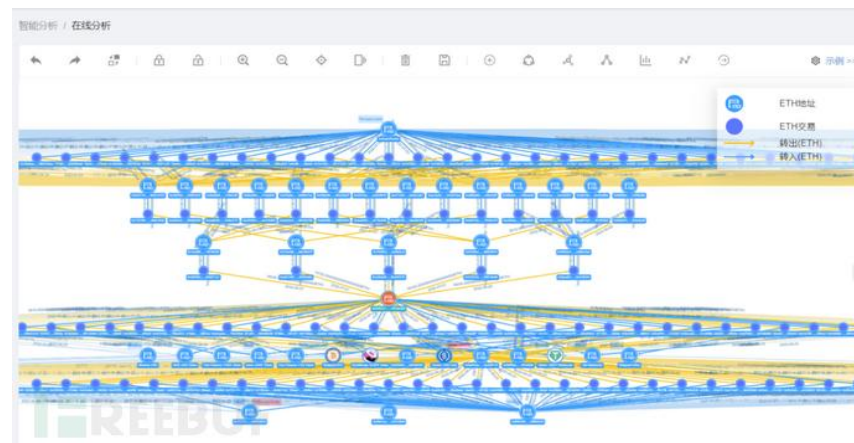


➤ 相比传统金融洗钱犯罪，元宇宙上的洗钱犯罪有着如下特点：

- 去中心化
- 匿名性
- 资产类型更为丰富
- 洗钱手段更为多样
- 洗钱链条更为复杂
- 查询调取更为繁琐



匿名性隐藏身份



复杂的洗钱链条

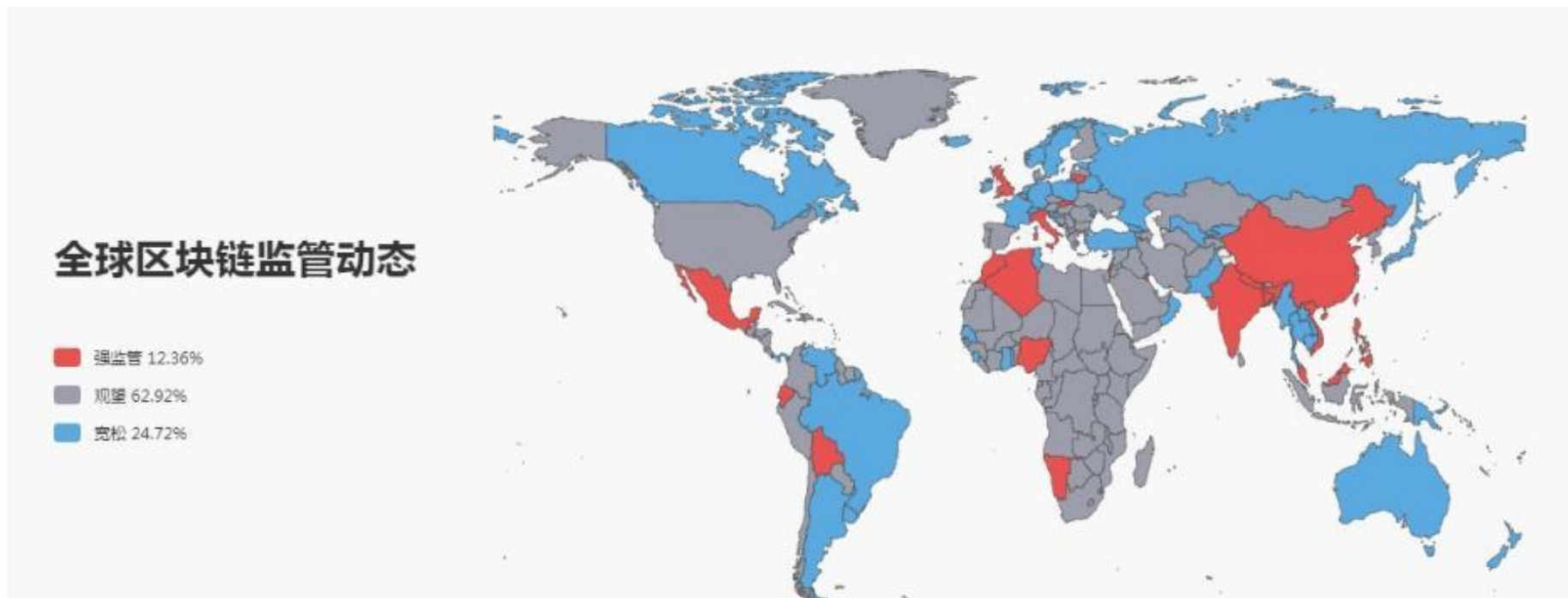
**上述特征使得区块链反洗钱的研究相比传统金融反洗钱研究面临着更大的挑战**

# 4

## 监管与反洗钱：相关研究

## ■ 全球区块链监管现状

- 大部分处于观望状态
- 中国、印度是少部分严格监管的国家



## ■ 印度政府：全面禁止加密货币

- 推出《禁止加密货币和官方数字货币监管2019年法案》
- 草案中，对“开采、生成、持有、出售、转让、处置、发行或交易加密货币”的人判处最高10年监禁
- 将加密货币彻底违法化



## ■ 印度央行：区块链监管沙盒

- 印度储备银行（RBI）已经宣布推出**区块链监管沙盒**条款
- 允许测试与区块链技术相关的各种应用，符合申请条件的“创新产品和服务”行业，包括零售支付、汇款服务、KYC核查、智能合约和网络安全产品等
- 凡是与加密货币相关的项目均被排除在外了

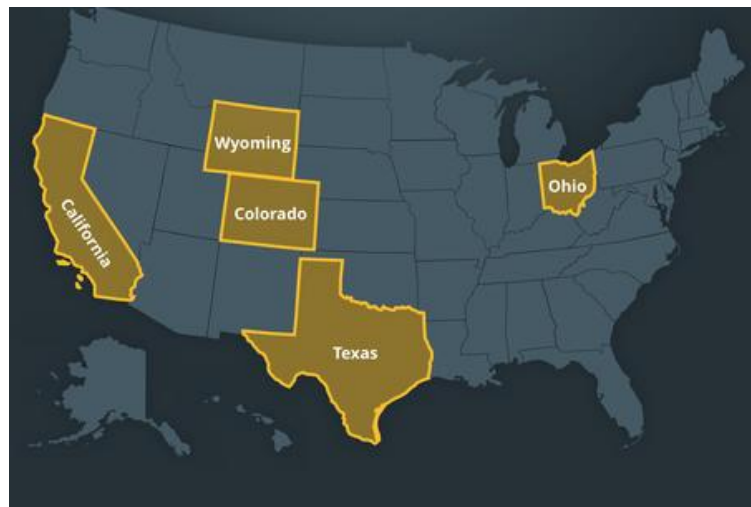


## ■ 美国区块链：证监会认定数字资产为证券

- 美国证监会（SEC）发布《关于数字资产证券发行与交易的声明》
- 明确了数字资产的监管要求：
  - 证券发行和销售
  - 投资于数字资产证券的工具
  - 数字资产证券的交易、流通

“你长得像一只鸭子，你走起路来也像一只鸭子，我必须要把你当作一只鸭子一样，来监管你。”

- **美国区块链：各州独立监管，联邦政府保持沉默**
  - 纽约州金融服务管理局提出“数字货币许可证制度”
  - 康涅狄格州《货币转移法案》：所有从事虚拟货币转移的商业行为都需遵守包括该法案规定的营业许可要求在内的全部内容
  - 《华尔街日报》：美国俄亥俄州将成为首个接受比特币缴税的州



## ■ 欧洲：各自为政，探索统一监管框架

- 德国：德国财政部在国会一份答复中称比特币为“数字货币”，某种程度上承认比特币的合法化
- 荷兰：禁止匿名的交易，强监管
- 英国：英国金融监管局设立监管沙盒，已批准四批公司
- 欧洲议会决议：探讨区块链技术的潜在监管，遵守欧盟通用数据保护条例（GDPR）以及防止与首次代币发行ICO相关的欺诈行为





## ■ 我国推出多条虚拟货币监管法律法规

- 人民银行：发布防范比特币风险通知，警示虚拟货币风险
- 公安部：防范以“虚拟货币”“区块链名义”进行风险集资
- 发改委：全面整治虚拟货币“挖矿”活动，加快存量项目有序退出，严禁新增挖矿相关项目
- 互联网金融协会：防范区块链ICO与虚拟货币交易活动的风险提示



关于防范以“虚拟货币”“区块链”名义进行非法集资的风险提示

时间：2018年08月28日

字体：大 中 小

分享



国家发展改革委等部门关于整治虚拟货币“挖矿”活动的通知

发改运行〔2021〕1283号



中国人民银行等五部委发布关于防范比特币风险的通知

中央政府门户网站 www.gov.cn 2013年12月05日 16时12分 来源：人民银行网站

【字体：大 中 小】【E-mail推荐】  发送 打印本页 关闭窗口



中国互联网金融协会  
National Internet Finance Association of China

您当前位置：协会动态 > 协会新闻

关于防范以区块链名义进行ICO与“虚拟货币”交易活动的风险提示

## ■ 区块链信息服务监管（网信办）

- 通过**备案制监管**，监管基于区块链的网站、APP等形式提供信息服务的主体
- 仅进行登记，不承担产品审查



## ■ 禁止代币融资

- 2017年9月4日《关于防范代币发行融资风险的公告》禁止ICO

## ■ 禁止虚拟货币交易

- 2021年5月下旬，中国人民银行发布《关于防范虚拟货币交易炒作风险的公告》
- 2021年5月21日，国务院金融稳定发展委员会召开会议，提出坚决防控金融风险，打击挖矿和交易等相关行为
- 2021年6月，央行约谈多家银行和支付机构，要求各单位不开展、不参与虚拟货币相关的业务活动

## ■ 对虚拟货币保持持续高压

- 2021年9月发布的《关于进一步防范和处置虚拟货币交易炒作风险的通知》中强调，**境外虚拟货币交易所**通过互联网向我国境内居民提供服务同样属于非法金融活动
- 随后，多家虚拟货币交易所**宣布清退中国大陆用户**，纷纷关闭在中国大陆的业务

为了您的资产不受损失

### 请中国大陆用户关注清退进度

12/14/11:00	12/15/11:00	12/31/24:00
关闭中国大陆用户充值功能	停止中国大陆用户的币币交易	下架OTC的CNY交易

请于15日前提币或者处置资产，如因在平台不能交易所带来的交易机会损失，与本平台无关

## ■ 联盟链技术被广泛应用

- 百度、腾讯、阿里等国内互联网企业都拥有自己的联盟链，并基于此研发NFT数字藏品
- 2023年3月3日，大数据流通与交易技术国家工程实验室与上海数据交易所正式启动国内首个数据交易链的建设工作



## ■ 钓鱼诈骗检测

- 传统的基于网站的钓鱼检测方法不能直接用于解决以太坊上的钓鱼检测问题
- 将以太坊的交易记录建模为一个有向交易网络，**自动学习诈骗地址的特征**，以区分网络钓鱼和非网络钓鱼地址

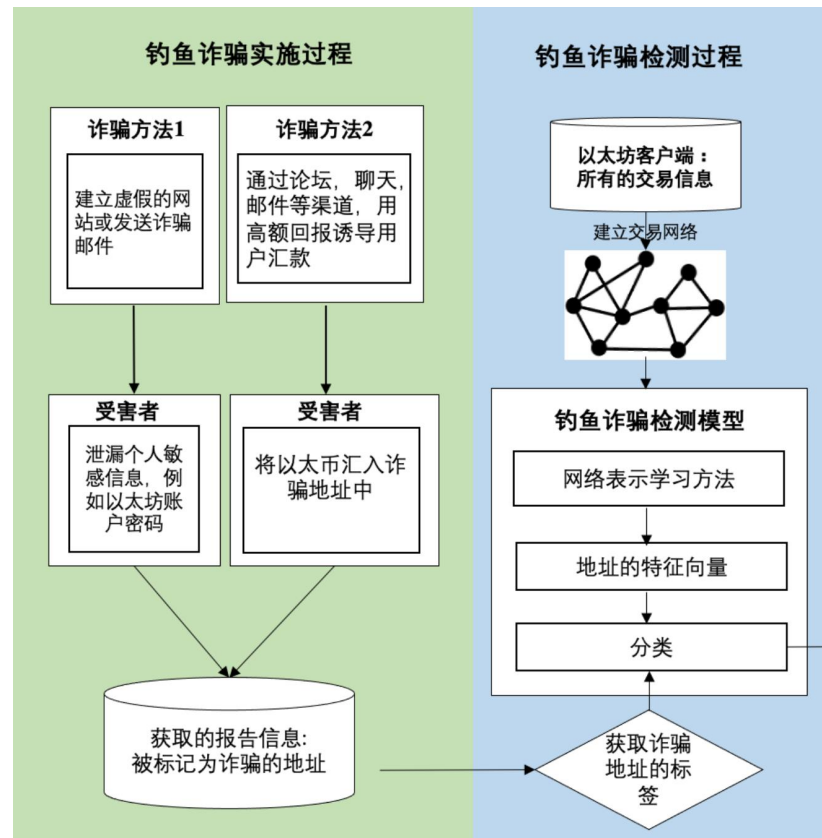
### Tech

#### Uniswap User Loses \$8M Worth of Ether in Phishing Attack

The attacker enticed users with a fake Uniswap airdrop message.

By Shaurya Malwa ⌚ Jul 12, 2022 at 7:56 p.m. Updated Jul 13, 2022 at 2:40 a.m.

### trans2vec算法



## ■ 庞氏骗局识别

- 区块链庞氏骗局、钓鱼诈骗丛生
- 如何通过代码、通过智能合约交易行为，对链上庞氏骗局、钓鱼诈骗进行提前检测与预警？
- 共**280704**个合约；给予代码特征，共识别出**386**个疑似的庞氏骗局合约。
- 论文发表于WWW互联网顶级会议

### The Rise of Cryptocurrency Ponzi Schemes

Scammers are making big money digital gold rush but don't unders

DAVID Z. MORRIS | MAY 31, 2017 | TECH

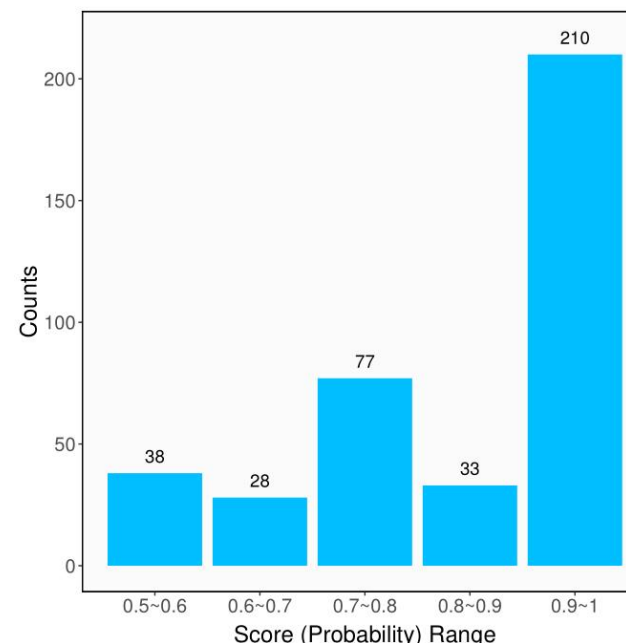
CRYPTOCURRENCY

#### Team Behind \$660M ICO In Vietnam Disappears

By PYMNTS  
Posted on April 13, 2018

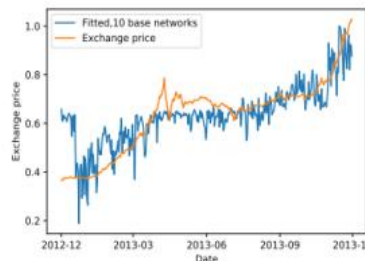


#### 'Gemcoin' Ponzi Scheme Operator Hit With \$74 Million Judgment

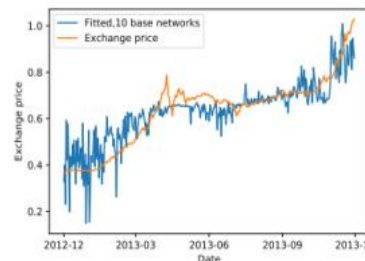


## ■ 虚拟货币市场操纵识别

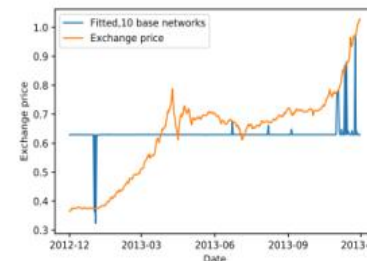
- 2014年全球超过70%的比特币交易
- 通过对交易所中买卖数据的分析
- 挖掘与现实世界中价格波动的内在联系
- 论文发表于顶级会议INFOCOM 2019



(a) EHG



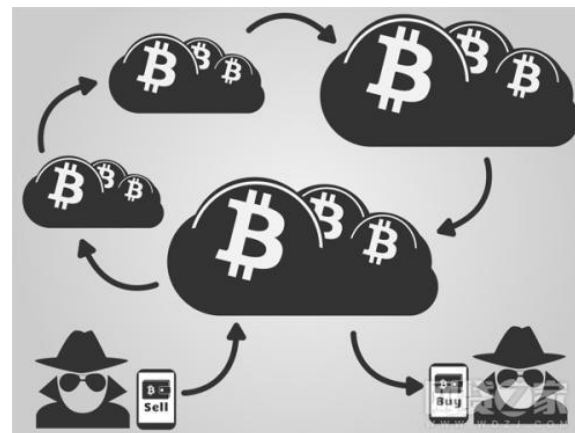
(b) ELG



(c) NMG

## ■ 混币服务地址识别

- 获取分析了比特币混币服务地址
- 对混币服务地址及4,500,000关联交易进行模式识别
- 可侦测未知的疑似洗钱行为





## ■ 面向账户类型的区块链反洗钱技术

### • 介绍：

- 根据账户的**特定类型**，来判断其是否存在洗钱的嫌疑，并采取相应的措施进行监控和调查。
- 这些账户类型通常都具有不同的**交易模式**、交易频率和交易金额等特征，因此可以通过监控这些特征，来检测是否存在洗钱行为。

### • 特点：

- **多维度分析**：考虑交易金额和频率等，结合账户的类型和交易对象等多个因素结合起来，提高检测洗钱行为的准确性。
- **风险评估精准**：通过对不同类型的账户进行分类，可以更加精准地进行风险评估，减少误判率和漏报率。
- **实时监控**：基于账户类型的反洗钱解决方案可以实时监控比特币交易，及时发现存在洗钱嫌疑的账户，采取相应的措施进行处置。



游戏



交易所



用户

...

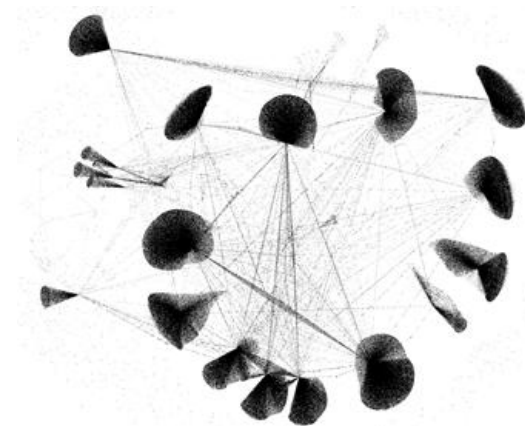
## ■ TTR交易追踪算法

### 需求：

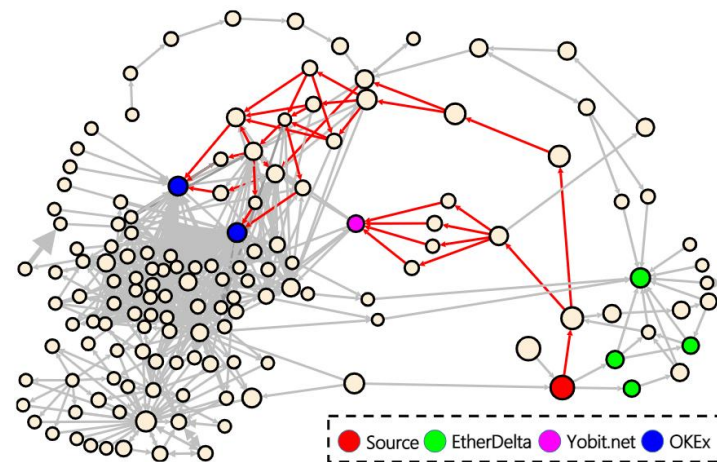
- 非法交易活动者在获取脏钱后，往往会参与洗钱以变现，而变现通常依赖交易所等服务
- 交易追踪旨在恢复洗钱过程，并为追赃提供证据
- 现有方法在效率和效果上都存在缺陷

### 怎么做：

- 从源节点出发寻找一个子图，尽可能包含源节点和目标节点之间的路径
- 平均追踪耗时为**30min**，而反洗钱专家需要1天以上



现有方法：慢、搜索范围大



业界需要：快、精准的追踪

## ■ TTR追踪核心算法

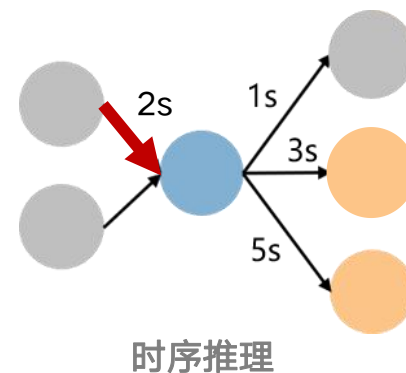
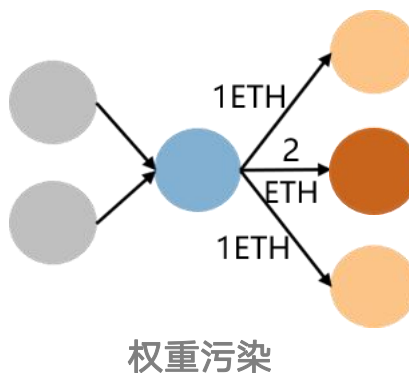
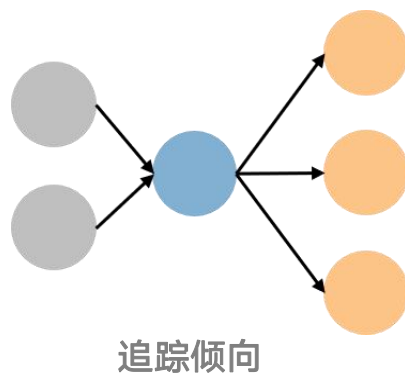
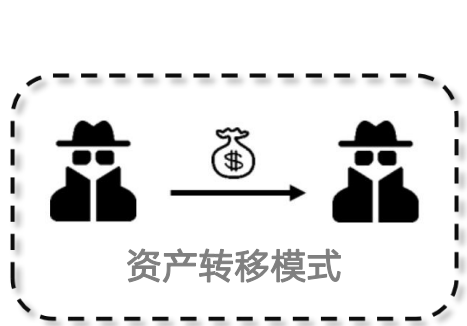
➤ 资产转移：指通过交易将资产发送到另一个账户

➤ 追溯策略

□ 追踪倾向：资金流来源和去向对不同任务而言重要性不同

□ 权重污染：沿着金额更大的资金链路更有可能找到资金链出口

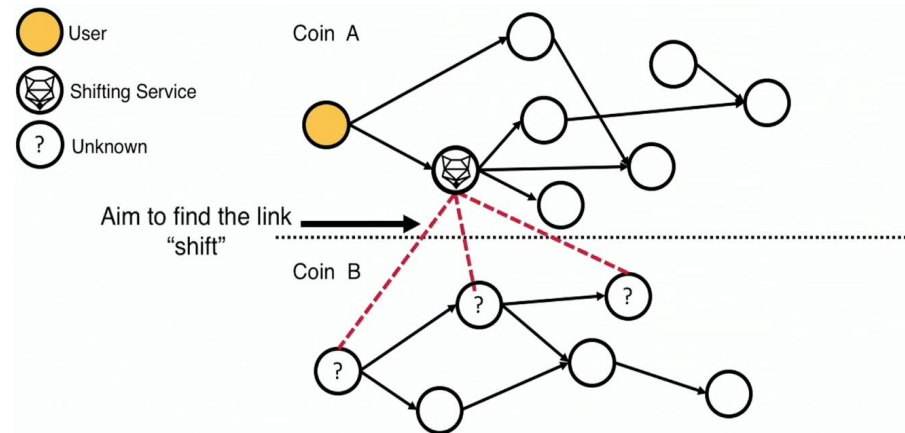
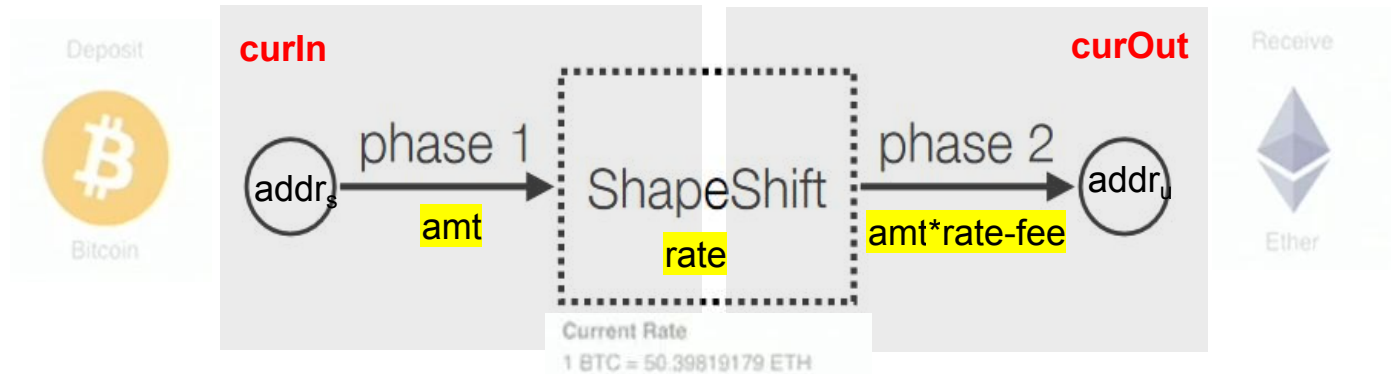
□ 时序推理：资金转移链路一定遵循时间顺序



## ■ 面向跨链桥的区块链反洗钱技术

### ➤ 背景介绍

- 中心化跨链交易所



## ■ 面向跨链桥的区块链反洗钱技术

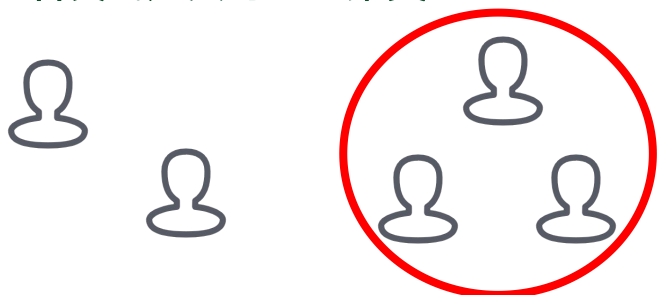
### ➤ 基于启发式方法

#### ① 基于API获取多链数据

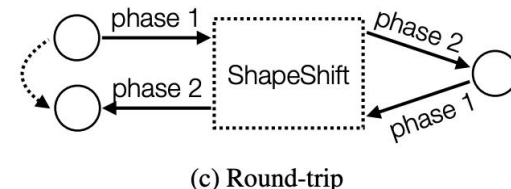
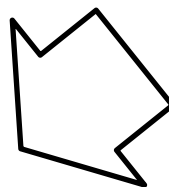
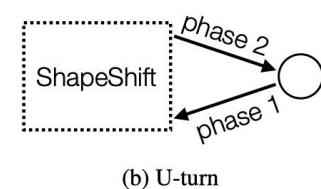
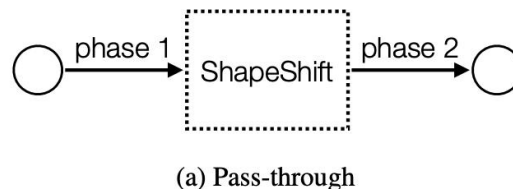
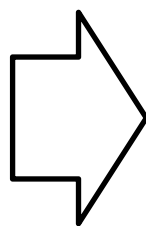
(curln, curOut, amt, t, id)

Currency	Abbr.	Total	curln	curOut
Ethereum	ETH	1,385,509	892,971	492,538
Bitcoin	BTC	1,286,772	456,703	830,069
Litecoin	LTC	720,047	459,042	261,005
Bitcoin Cash	BCH	284,514	75,774	208,740
Dogecoin	DOGE	245,255	119,532	125,723
Dash	DASH	187,869	113,272	74,597
Ethereum Classic	ETC	179,998	103,177	76,821
Zcash	ZEC	154,142	111,041	43,101

#### ③ 基于启发式方法对地址聚类



#### ② 分析交易过程中资金流动的方向和路径



### ➤ 贡献

- 第一篇研究跨链交易追踪，可解释性强，覆盖8条热门区块链
- 分析了跨链洗钱交易模式、跨链的非法用途

# 5

## 监管与反洗钱：产品与工具

## 1. 区块链监管分析软件：

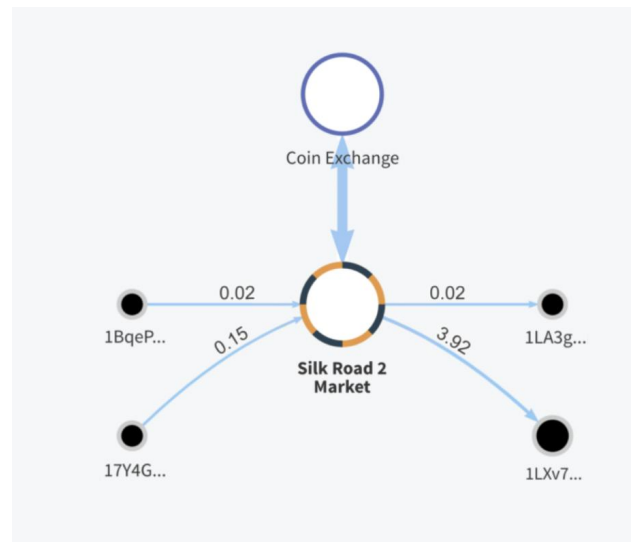
实时监控区块链上的交易，并通过分析数据来发现异常行为。例如，一些软件可以进行用户身份验证，自动跟踪资金流向和来源，识别大额转账和不合理的交易模式等。

(Chainalysis、Elliptic、Crystal、GraphSense等)

## 2. 反洗钱智能合约：

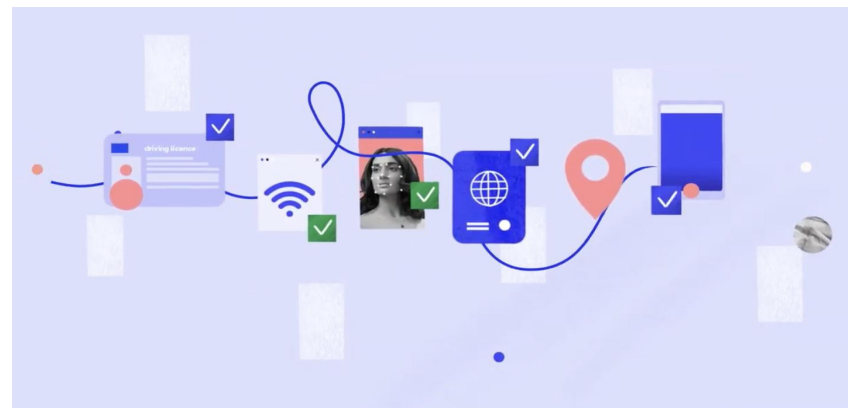
智能合约是区块链上的自动执行程序，可以根据预设条件自动执行相应的操作。一些智能合约可以用于反洗钱，例如根据监管机构的黑名单进行交易筛选和监控。

(KYC、AML、审计和信任)



Chainalysis

(<https://www.chainalysis.com/chainalysis-reactor/>)



Onfido

(<https://onfido.com/video/how-can-onfido-help/>)

## ■ 工业界区块链反洗钱解决方案：GraphSense

### • 定义和特点：

1. 加密资产分析平台
2. 强调完整的数据主权、算法透明度和可扩展性
3. 支持UTXO和账户模型

### • 功能：

1. 跨币种搜索
2. 交易追踪
3. 丰富的标签库等

### Features



#### Cross-currency search

Search by address, tag, transaction or block in several cryptocurrency ledgers.



#### Traverse transactions

Navigate in transaction network abstractions computed from various ledgers.



#### Inspect metadata

Inspect statistical properties of nodes and edges.



#### Find paths

Automatically search for transaction paths connecting two nodes.





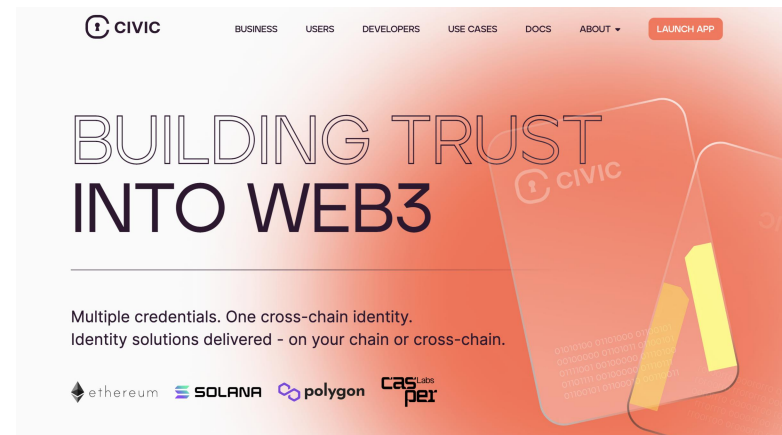
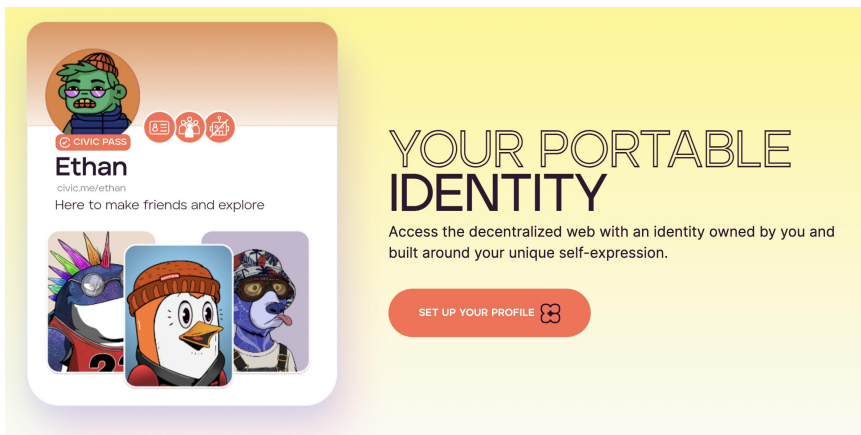
## ■ 工业界区块链反洗钱解决方案：CIVIC

### • 概念：

1. 提供跨链的身份验证
2. 提供对用户进行验证的功能，限制不符合规则的用户参与交易

### • 功能：提供可验证凭据的组合，对用户进行验证

1. 身份验证。使用政府颁发的身份证件验证用户的真实身份。
2. 年龄验证。确保用户在取消访问平台或社区之前满足规定的年龄标准。
3. 活体验证。用于确定用户是人还是机器人的视频自拍。
4. 验证码验证。确定用户是人还是机器人。
5. ...



## ■ MetaGuard区块链反欺诈安全卫士

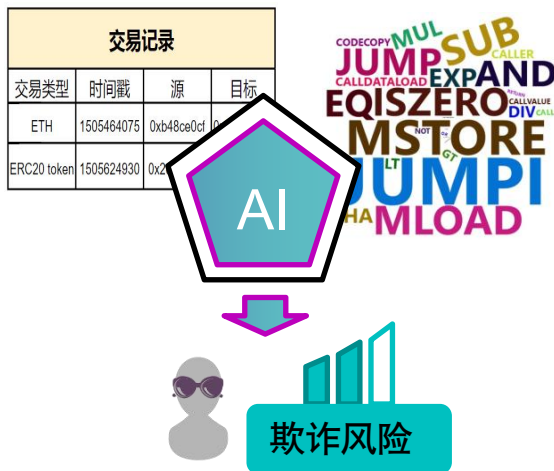
### 便捷的标签查询

超40万个标签的便捷查询



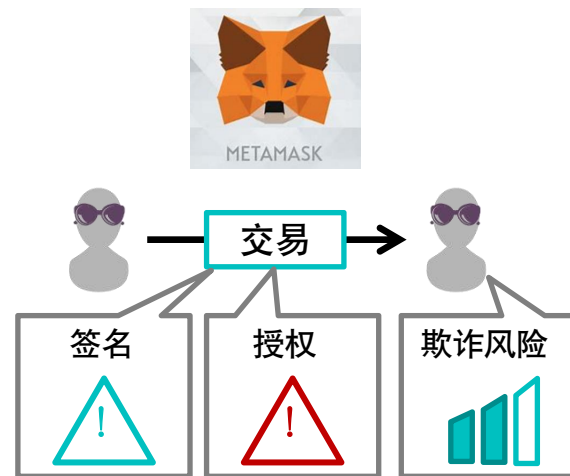
### 智能的诈骗检测

基于账户历史交易数据、合约操作码、人工智能算法在线推断欺诈嫌疑  
支持钓鱼诈骗、庞氏骗局的检测



### 实时的交易监听与预警

实时监听用户与区块链钱包插件的交互，  
对授权转账、签名进行弹窗提醒，并捕获交易账户进行欺诈风险推断



## ■ Xtracer追溯区块链交易利器

### 交易路径可视化

- ☆ 个性化交易追溯
- ☆ 前向资金流展示
- ☆ 后向资金流展示

### 交易数据可视化

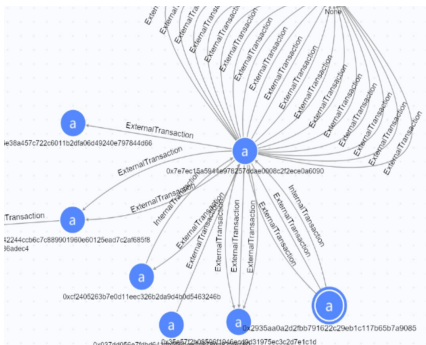
- ☆ 交易时间展示
- ☆ 交易类型展示
- ☆ 交易平台展示
- ☆ 多重交易展示

### 账户画像可视化

- ☆ 账户余额展示
- ☆ 账户标签展示
- ☆ 账户交易次数演变

### 入门教程可视化

- ☆ 产品介绍展示
- ☆ 如何查询展示
- ☆ 可视化分析展示
- ☆ 更多信息展示



#### 交易详情

起点  
[0x9a207194cbcd9f229694fdf5a28caab59157920d](#)

终点  
[0xb28bc69199a7abf00b9cb200356104ce1bdc4868](#)

具体信息  
交易哈希: [0x97b46f3f27fcea1b1152c386f...](#)  
时间: 2019-11-28 17:05:42  
类型: ExternalTransaction  
平台: ETH  
交易量: 0.000913502(ETH)

#### 账户详情

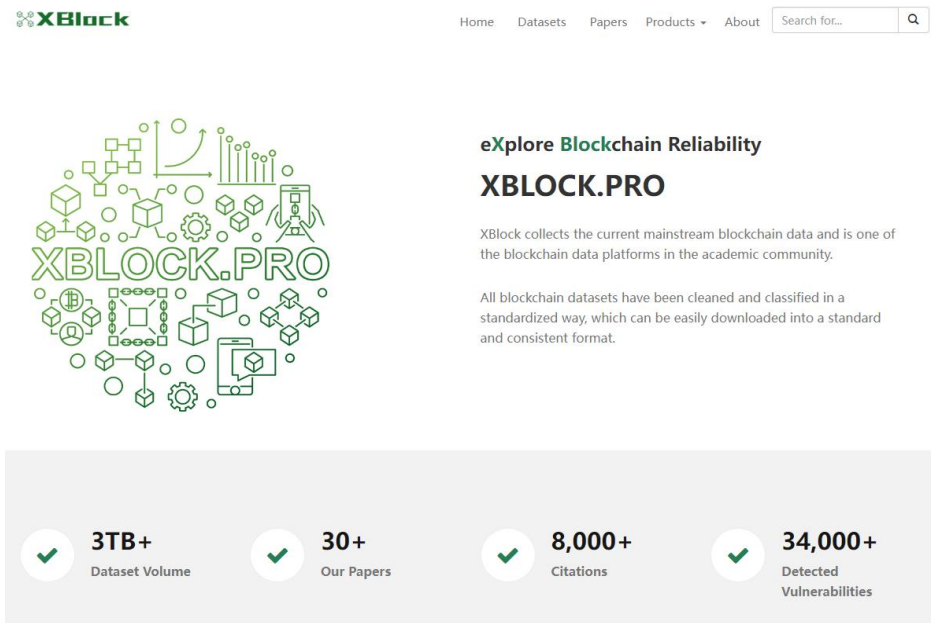
账户地址  
[0x9a207194cbcd9f229694fdf5a28caab59157920d](#)

余额  
Ether(ETH)  
102000000100000ETH  
Mystery Ghost Token(MGT)  
1000000000000MGT  
7Eleven(7E)  
1000000007E  
Coni(CONI)  
1000000000000000CONI  
UbiHacker1(UbiHacker1)



## ■ 区块链数据网站 XBlock.pro

- <https://xblock.pro>
- 收集了当前主流的区块链数据
  - 包括比特币、以太坊、EOS等多条公链
- 大型智能合约漏洞库



The screenshot shows the XBlock.pro website homepage. At the top, there is a navigation bar with links for Home, Datasets, Papers, Products, and About, along with a search bar. Below the navigation bar is a large graphic with the text 'XBLOCK.PRO' and various blockchain-related icons. To the right of the graphic, there is a section titled 'eXplore Blockchain Reliability XBLOCK.PRO' with a brief description: 'XBlock collects the current mainstream blockchain data and is one of the blockchain data platforms in the academic community.' Below this, it states: 'All blockchain datasets have been cleaned and classified in a standardized way, which can be easily downloaded into a standard and consistent format.'

✓ 3TB+ Dataset Volume	✓ 30+ Our Papers	✓ 8,000+ Citations	✓ 34,000+ Detected Vulnerabilities
--------------------------	---------------------	-----------------------	---------------------------------------

➤ 最大最全的区块链科研数据库

➤ 用户来源：北京大学、复旦大学、南洋理工大学等多所国内外高校，以及链安、IBM等知名公司

➤ 访问地区：国际化程度较高，近三个月约50%的访客ip来自海外

# 监管与反洗钱：产品与工具



## ■ 区块链数据网站 XLabelCloud

- 学术圈最大的开放标签数据库：**50万+**BTC/ETH/BSC的地址/交易标签
- 提供在线Chrome插件：实时检测网站中出现的地址标签
- **全自动化情报感知**：持续监听暗网、欺诈、钓鱼等非法活动网站

The screenshot displays the XLabelCloud interface. At the top, there is a large word cloud of various blockchain-related terms and project names. Below the word cloud, there is a search bar and a category dropdown menu set to 'Account'. A grid of labels is shown, each with a count in a green circle:

Armor.fi	13	ARCx	29	Arbitrum	36
ETH	268821	AtomSolutions	11	Asset Management	1
Art Blocks	4	Ampleforth	5	Allbit	2
Alchemist Coin	14	Alameda Research	2	AirSwap	16
Airdrop / Distributor	19	Zora	3	Zethr	6

On the right side, there is a transaction analysis panel for a specific transaction:

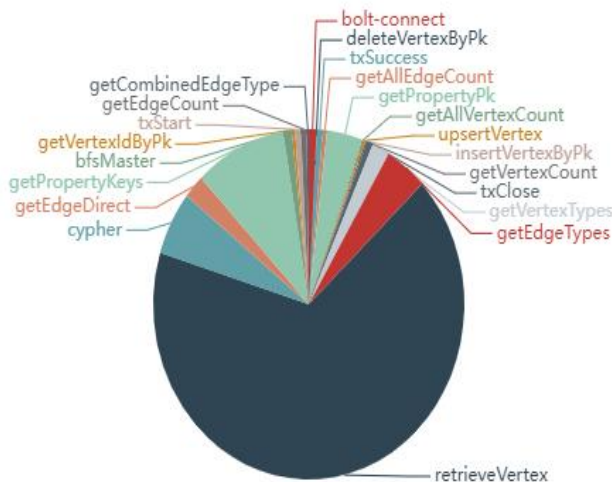
- Transaction Hash: 0xd16f3de6de2d230c0bc2681431bea94dbec0da4197f35382aacada5462e7e780
- Status: Success
- Block: 15607796 (118 Block Confirmations)
- Timestamp: 23 mins ago (Sep-25-2022 03:47:59 AM +UTC) | Confirmed within 16 secs
- From: thonman.eth
- To: Contract 0x335eef8e93a7a757d9e7912044d9cd264e2b2d8 (Sad Girls Bar: SadGirlsBar) | ETH,Token Contract,Phishing

## ■ 区块链数据网站 XNetSearch

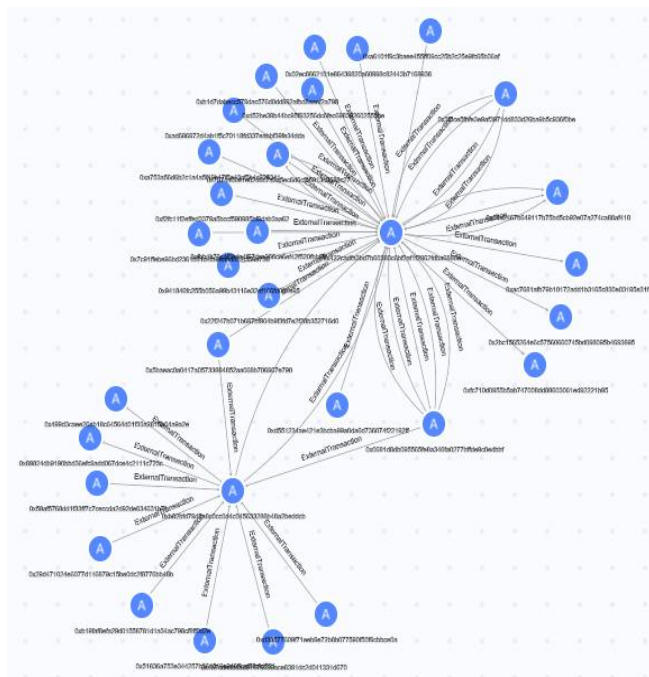
- 交易数据：**2.5亿**账户、**50亿**交易数据，超过3TB数据量
- 核心技术：
  - Galaxybase分布式图计算平台
  - 深层资金链路追踪
  - 交互式网络可视化



图模型

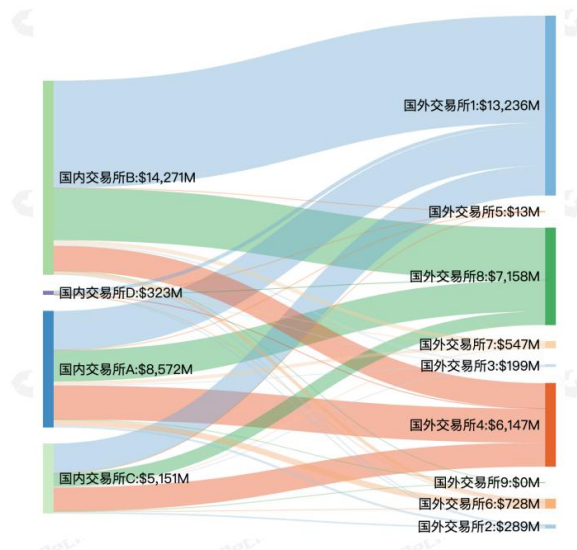


图计算性能分析



交互式链路追踪与可视化

## ■ 海量数据分析消耗算力



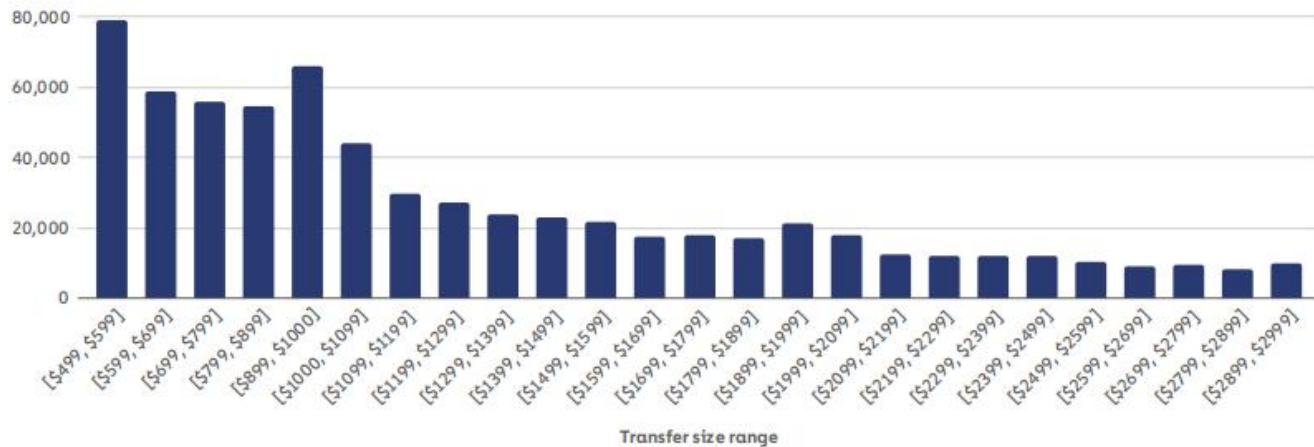
交易数量多，  
涉案金额大，  
数据复杂

Total cryptocurrency value received by illicit addresses | 2017–2021

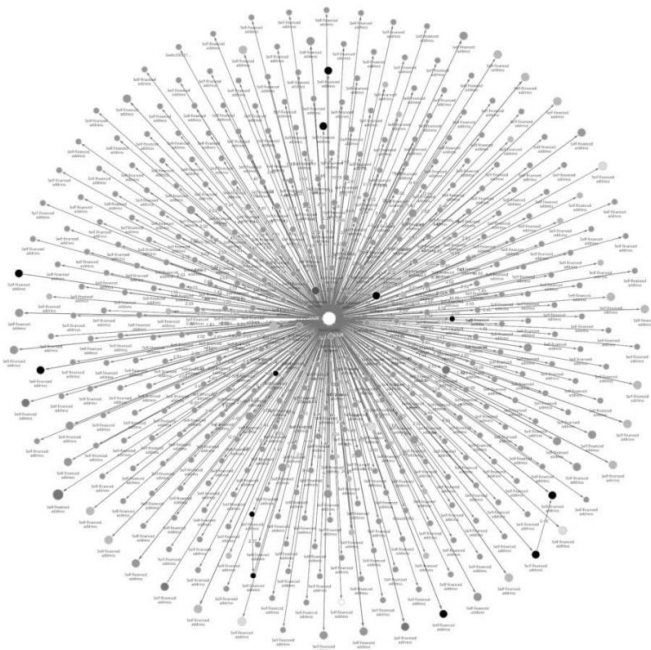


Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a darknet market.

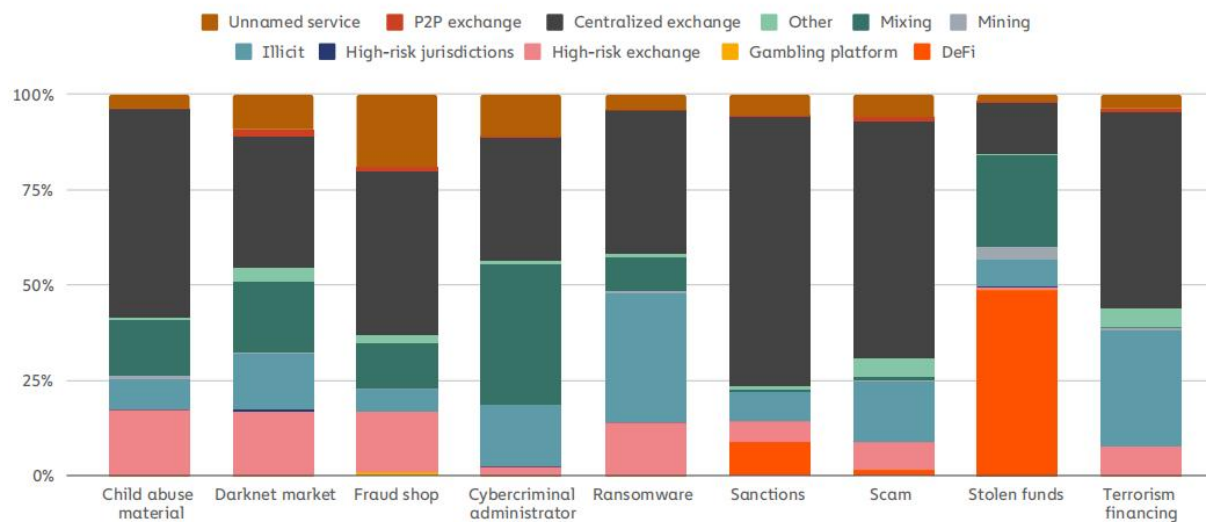
Number of transfers from illicit addresses to exchanges by transfer size | 2021



## ■ 区块链实体识别困难



Destination of funds leaving illicit addresses by crime type | 2021



网络结构复杂  
资金流向多样  
去中心化、匿名性  
难以实现对同一实体不同用户身份的追踪识别



## ■ 多部门协同监管：反洗钱和资金追回

- 技术支撑：结合人工智能方法的自动追踪和洗钱识别
- 网信+宣传：非法交易与内容的监听和审查
- 公安：实体身份和银行流水调查



- 区块链通过技术手段解决信任问题
- 适用于互不信任的多方进行协作的场景
- 区块链支撑的元宇宙未来潜力巨大
- 元宇宙上的欺诈与洗钱亟待监管
- 区块链的监管和反洗钱呼吁多部门合作

# 团队介绍



主讲人：吴嘉婧

- 香港理工大学电子与资讯工程学系博士学位
- 计算机学院 副教授，博导
- 研究方向：区块链反洗钱与反欺诈、区块链数据挖掘、网络科学、网络表示学习、图神经网络

## ■ 论文

- 发表区块链论文100余篇、ESI高被引5篇
- 2 篇论文进入全球引用最高区块链论文 TOP 10（引用次数3764、2992）

## ■ 项目

- 国家重点研发计划等研究课题20余项
- 腾讯、华为、蚂蚁金服等企业合作

## ■ 著作



## ■ 活动

- 区块链专刊20余个JSAC, TII, TSC, TETC, TVT
- BlockSys 2019, 2020, 2021, 2022
- IEEE Symposium on Blockchain 2021



谢谢!