NebulaGraph

https://nebula-graph.com.cn

图技术在稳定币监管下的深度应用

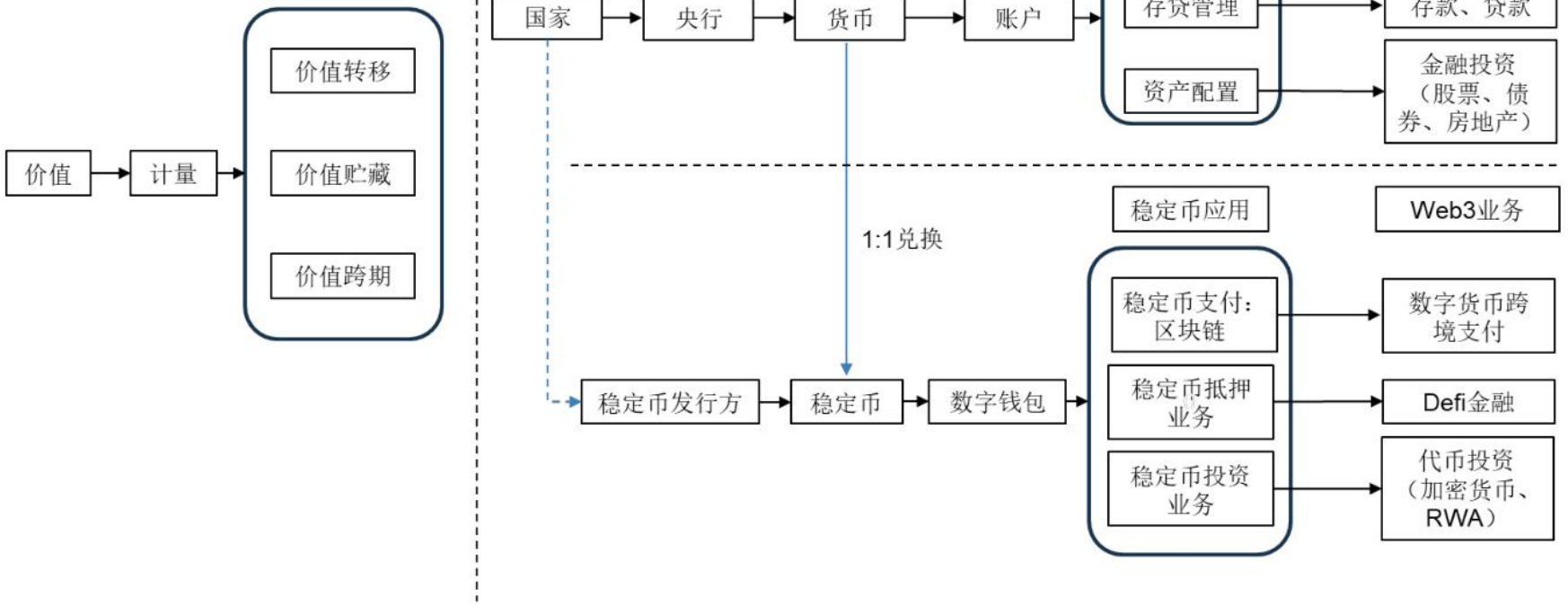
解决方案架构师：鲍翰林

01 稳定币的发展与挑战

什么是稳定币

稳定币（Stablecoin）是一种基于区块链技术的加密数字货币，通过锚定法定货币、大宗商品、主流加密资产，或依赖算法机制调节供应量，实现价格的相对稳定。**从本质上看，稳定币是法币信用在数字空间的延伸，通过链上发行和流通机制拓展法币的信用边界。**

稳定币与金融体系的关系

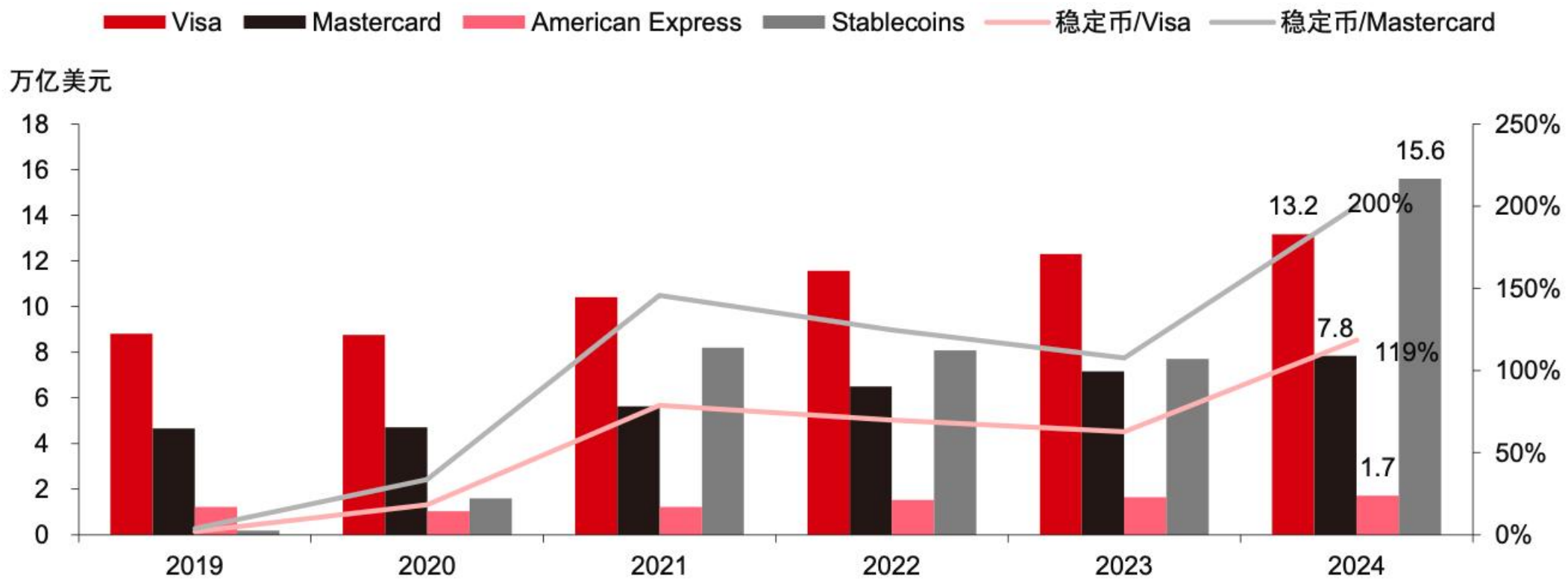


资料来源：中信证券研究部

稳定币交易量高速增长

截至 2024 年末，全球稳定币总市值超 2000 亿美元。

2024年稳定币交易额达 15.6 万亿美元，首次超过 Visa 和 Master，给传统金融业务带来挑战。



资料来源：ARK Invest《Big Ideas 2025》，中信证券研究部

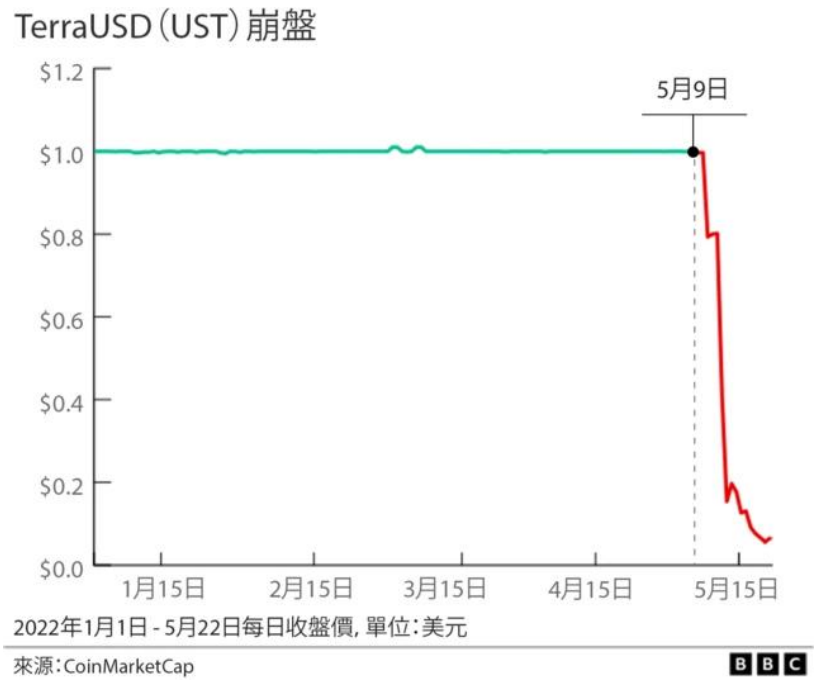
Terra崩盘始末

LUNA币依托的 Terra 区块链平台是韩国人权道亨（Do Kwon）2018 年建立的，发行后最初两年价格一直在一美元以下浮动。2021 年 12 月开始崭露头角，币价开始上涨，从 5 美元升到22年 4 月的 116 美元，一度接近120美元，市值 410 亿美元，在所有加密币中排第五名。

在 LUNA 币之后，Terra 又发行了一个跟美元 1：1 对标的稳定币 UST，LUNA 可以跟 UST 相互兑换。

5月8日，Terra 挪动1.5亿美元 UST 调整流动性，但 10 分钟后一个新地址突然抛售 8400 万美元的 UST，随即引发抛售浪潮和恐慌情绪。当天，UST 价格顽固地滞留在 95 美分水平，进一步刺激了抛售潮。局势很快失控。UST 与美元加速脱钩，9 日崩盘，48 小时贬值 99%。

5月17日，LUNA 币价格几乎归零。



监管从重点关注违法行为逐步转向构建完善监管框架

稳定币的创设初衷在于构建法定货币与数字资产间的交易桥梁，然而传统金融市场风险外溢及链上风险频发，导致稳定币存在与法定货币脱锚风险，且其发行方储备资产的不透明性亦构成重大隐患。

没有透明储备，没有风控机制的稳定币容易崩盘

资料来源：wind，各公司官网，中信证券研究部

全球稳定币行业迈入合规化发展新阶段

条例关键词：

- 锚定法定货币
- 需牌照
- 100% 资产储备，充分披露
- 定期提交审计报告
- 遵守 KYC/AML

长远意义：

- 巩固香港金融中心地位：虚拟资产国际中心
- 以香港做为试点

中国香港《稳定币条例》核心内容

监管要点	具体内容
监管机构	• 香港金融管理局金融管理专员
监管对象	• 聚焦法币稳定币，指锚定一种或多种官方货币维持价值的稳定币
受监管的活动	• 在香港发行法币稳定币 • 在香港或香港以外发行港元稳定币 • 向香港公众积极推广其法币稳定币的发行
发牌准则	• **储备资产的管理及稳定机制**：稳定币储备资产任何时候都必须大于等于其流通面值，必须隔离管理、充分披露 • **赎回**：必须按面值赎回，且流程透明、费用合理 • **实体运营**：必须在香港设有实体公司 • **财政资源**：最低缴足股本必须 2500 万港元 • **适当人选**：控权人/高管必须为合格的“适当人选”，负责管理与营运的人员必须具备所需知识和经验 • **审慎及风险管理**：必须健全风险管理制度，必须设有适当的管控制度，防止及打击洗钱等活动
开放式牌照	• 牌照持续有效(未撤销时)，持牌人接受持续监管。
销售限制	• 仅限持牌发行人、持牌虚拟资产交易平台、获证监会批准的法团及认可机构销售
监管权力	• 金融管理专员有权要求提交文件、发出指示、调查等持续监管权力
刑事罚则	• 无牌活动/非指定销售：罚款 500 万港元及监禁 7 年 • 欺诈交易：罚款 1000 万港元及监禁 10 年 • 欺诈性陈述：罚款 100 万港元及监禁 7 年

资料来源：招商银行研究院

传统风控合规与 Web3 风控合规的差异

基于链上数据的分析本质是“关系密集型、路径驱动型”，而传统以表为中心的系统在建模、查询、计算、可视化方面均存在瓶颈，难以支撑复杂实体关系的挖掘与风险洞察，**图数据库成为风控刚需**。

百亿级公链数据

多条公链上的交易、合约和资产信息数据量庞大且关系复杂，天然构成一张动态关系图。所有基于公链的交易均透明可视，可追溯。

例如反洗钱场景，在传统的银行侧，跨行追查成本较高，但在链上的追查成为必备的基础能力。甚至在每一笔交易时需要识别是否有隐藏风险。

传统技术难以将链上地址与链下用户高效融合，严重限制了数据分析的深度与广度。

更复杂的KYC

黑产常通过“一人多地址”“地址共用”、“跨链跳转”、“多次流转”等方式隐藏真实控制人。

尽管香港条例强制要求用户身份与链上地址绑定，**但某跨境洗钱案中，单个犯罪者操控超过 200 个钱包地址分散资金。**

传统技术依赖静态规则和简单关联分析，无法动态识别此类集群化行为。

更深的资金链路追踪

欺诈及洗钱的结合风险通常相伴而生，犯罪分子通过超过20层以上的交易链路、跨链桥，实现快速的多链资产转移，资金路径被切割成碎片化轨迹。

BIS 数据显示，43% 的洗钱交易因风控响应延迟得逞。

传统技术难以在快速变化的数据中穿透多层链路进行分析，及时监控风险，挽回用户损失。

02 基于图技术的风控合规解决方案

NebulaGraph

基于图技术的风控合规解决方案全景图

https://nebula-graph.com.cn

业务目标

扎实做好风控与合规，为业务发展保驾护航

业务阶段

事前预警 → 事中决策 → 事后分析

应用场景

事前预警	事中决策	事后分析	
同一客户识别	风险账号冻结	风险交易中断	地址关联分析
风险账户识别	反薅羊毛	资金流向追踪	交易关联分析
批量注册识别	反盗号	多账户协同交易识别	资金追缉

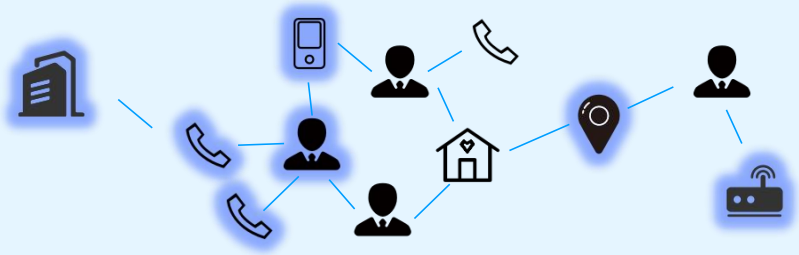
图技术

团伙挖掘能力	实时决策能力	数据探索能力
图特征	图指标	图算法

隐藏链式发现　环路模式发现　出入度分析　社区发现算法　相似度算法

图模型

构建图关系底座



数据层

外部数据　介质数据　KYC数据　链上数据　行为数据　……

基于链上和链下数据搭建统一图模型

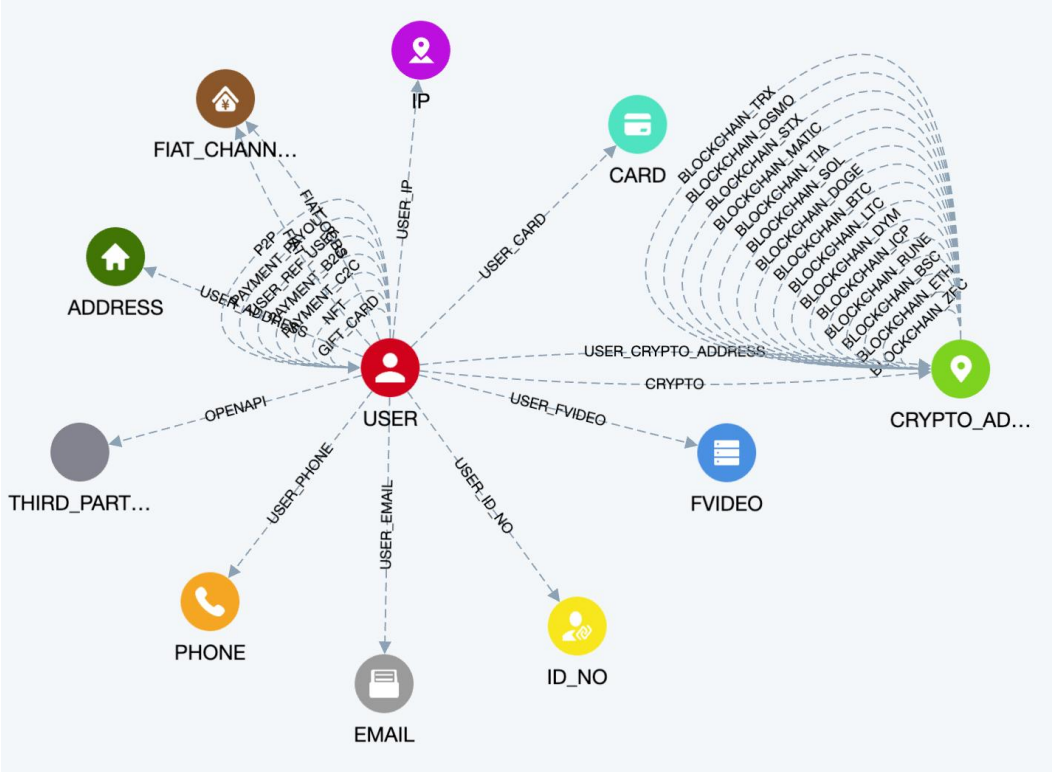
融合多数据源数据，提高网络的关联程度，丰富实体的属性，为关系网络特征挖掘提供良好的数据基础

支持分布式存储千亿点万亿边，可承载内外部多链数据的存储与计算

- 链上交易数据
- 登录/设备数据
- 推荐/拉新记录
- Web3社交平台
- ……

离线全量导入

实时增量导入



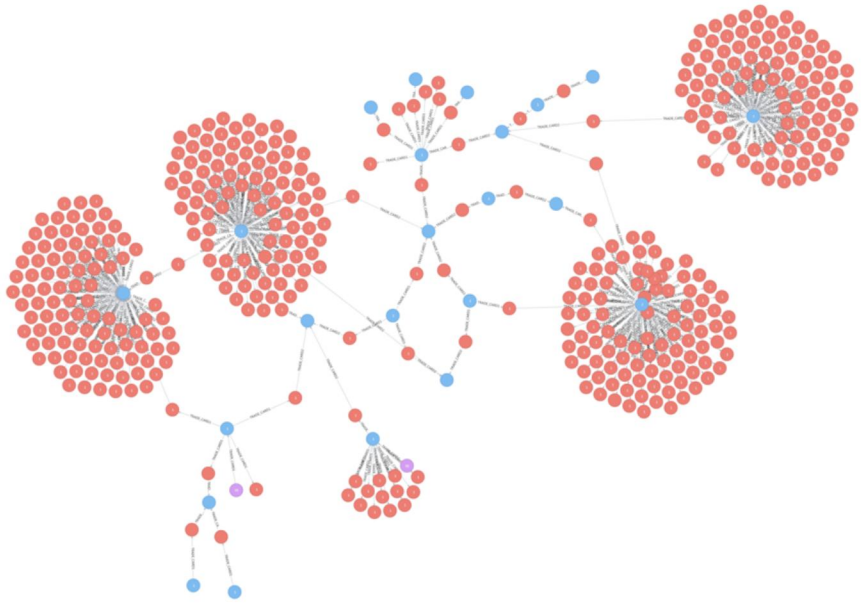
融合链上加密地址（CRYPTO_ADDRESS）信息以及链上交易记录（如BLOCKCHAIN_XXX ）和内部的用户（USER）相关信息，如身份信息（如ID_NO 、EMAIL 、PHONE ），支付渠道（如CARD 、FIAT_CHANNEL ）以及金流数据（如P2P、PAYMENT_B2C）进行分析，同时还涵盖了用户的多种媒介数据和行为数据（如IP、FVIDEO ）

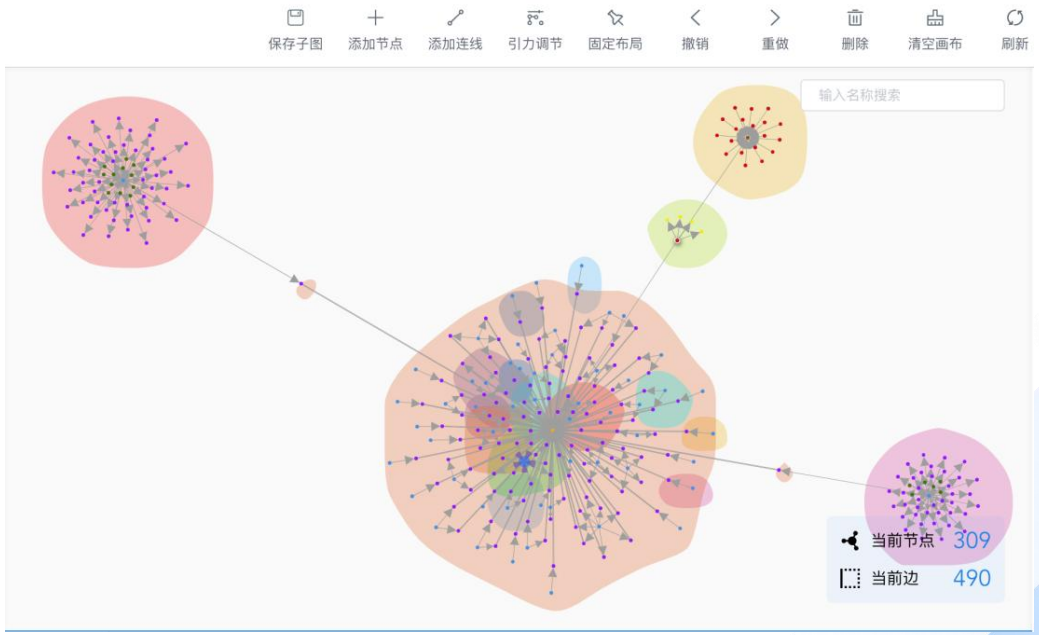
使用高性能图计算引擎挖掘高风险社区/团体

将用户账户、提币地址、充值地址、设备、IP、交易信息等关键实体构建为图谱网络，并采用 **WCC/Louvain 社区发现算法**，将图划分为多个**结构紧密的风险社区**。这些社区中的账户彼此之间在设备、资金流向、行为路径上具有高度关联。有效识别其中的同一客户、同一机构、黑产团伙。

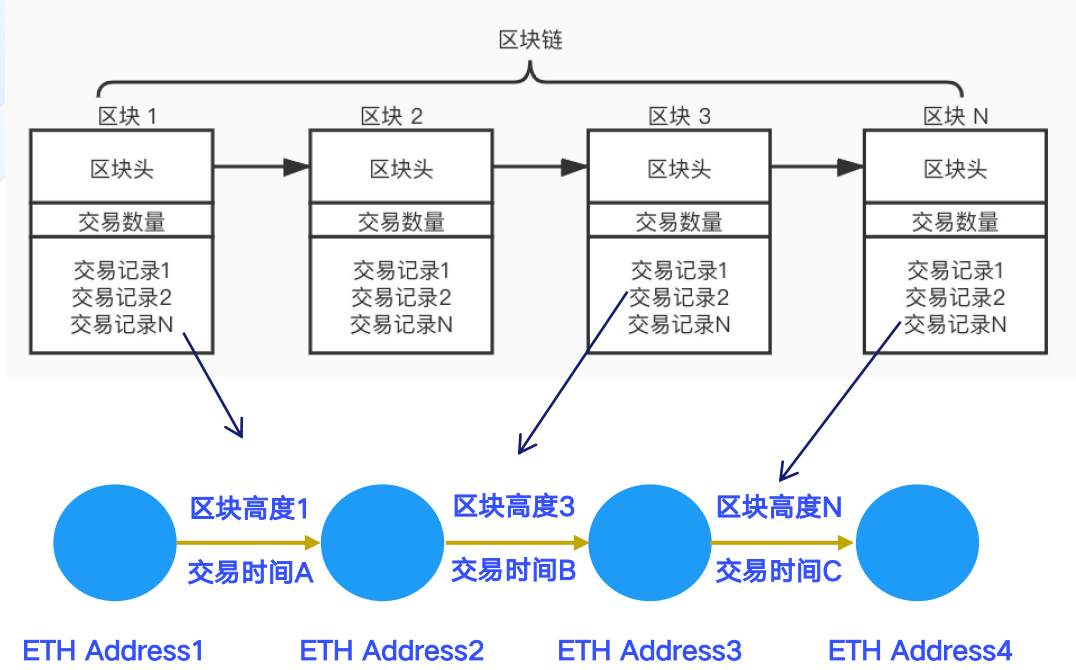
在此基础上，我们可以基于少量已知的高风险实体（如涉诈钱包、黑产登录IP、被盗账号）进行**标签传播**，使同一社群中具有强连接关系的用户受到**“风险扩散”**的影响。

相较 GraphX，图算法性能在不同算法上有 10-100倍 以上性能提升；内存开销节省 5x 左右；ISO-GQL编写分布式图算法，极大降低业务人员使用难度





大规模数据下的多层链路指标计算



链上追踪往往与时序以及区块高度等信息的递增相关，查询路径中需剔除重复出现点

GQL:

```
match p = ACYCLIC  (a:ETH)-[:`FROM`]->(:Transfer)
((t1:Transfer)-[:`TO`]->(temp:ETH)-[:`FROM`]->(t2:Transfer)
where t2.区块高度>=t1.区块高度 and t2.交易时间 >=t1.交易时间){1,3}
(:Transfer)-[:`TO`]->(b:ETH)  return p
```

客户端
直接获取结果

GQL直接实现复杂业务逻辑，单次调用图库，时延低

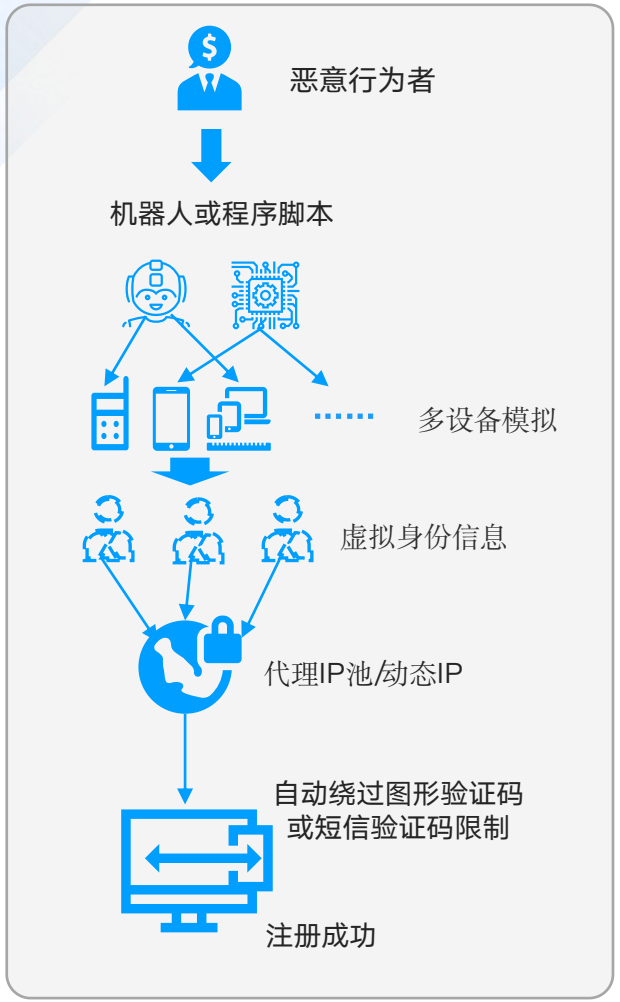
- **快速识别关联风险，多层链路穿透**
  实时查询用户与黑名单、链式集群等的多跳关系，精准识别潜在风险地址。
- **低延迟高并发，满足实时风控**
  支持毫秒级复杂关系查询，保障实时决策效率。
- **证据链留存**
  记录相关交易路径及关联关系，作为证据链留存。

深度	关系型数据库执行时间(s)	图数据库执行时间(s)	返回记录数
2	0.0016	0.001	~250
3	3.0267	0.0168	~11000
4	154.3505	0.1359	~60000
5	未完成	0.2132	~80000

深度	并发数	QPS	平均时延（ms）
1	500	124081.01	1.4
2	500	143352.06	1.27
3	500	6345.76	47
4	500	227.24	126

数据集：亿级反欺诈测试数据

传统的批量注册场景风控分析



产生一些列的数据特征

数据类型	特征描述
注册信息	相似或批量生成的邮箱/手机号、重复使用的身份证、银行卡
IP地址	注册IP频繁变动，或多个账户共用同一IP段（代理池）
设备信息	相同或极为相似的设备指纹、浏览器指纹、模拟器特征
时间特征	注册时间高度集中，注册行为呈现秒级间隔或固定时间差
行为路径	注册→KYC→首充→交易路径一致，行为模板化

根据行为特征进行风控

静态规则

- 同一IP连接的注册数量
- 单个地址连接的黑点数量
- 同一设备的注册数量
- 。。。。。

指纹识别

- 对设备信息/浏览器指纹做唯一性校验

黑名单机制

- 对IP、设备号、邮箱域名等维度定期维护黑名单

流量限速

- 控制单位时间内注册请求频率

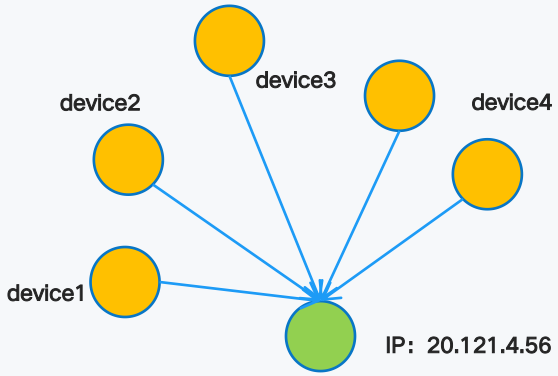
存在的挑战

- **跨维度难以联动分析**：无法灵活地将“IP”、“设备”、“KYC信息”、“行为轨迹”等多维数据动态关联分析
- **识别存在滞后性**：规则触发往往依赖行为完成后的回溯，难以实时阻断
- **多账号关系难以挖掘**：传统技术很难发现“多账户背后的同一操控者”

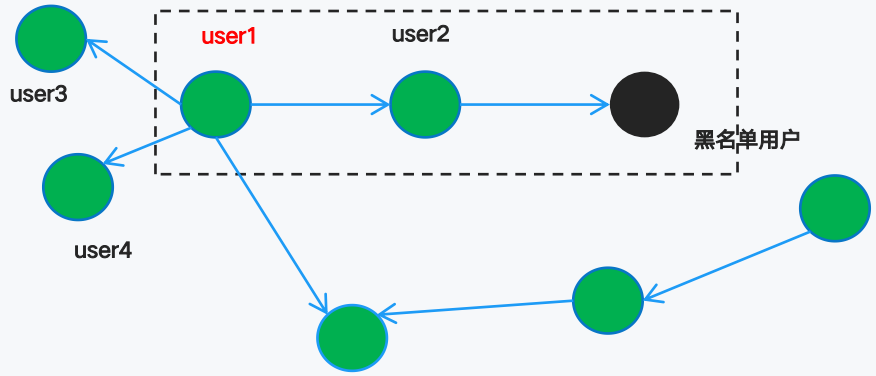
基于图技术的多维数据动态关联分析

基于图规则功能，业务可以快速实现复杂的关联欺诈逻辑的可视化快速开发，校验申请人提供的信息和数据库中的不一致地方，与风控决策平台结合，实现实时查询，动态关联分析

多注册设备连接到同一IP



注册地址三跳内有黑点链接



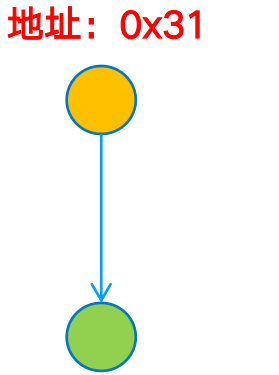
深入分析关联关系：图模型可以直观地展示IP、设备、KYC、行为轨迹关系，帮助发现潜在的注册链条、识别“谁与谁共用IP”、“设备是否被多个账号共用”等等。

动态更新和实时反应：在用户注册的瞬间，图数据库会将其提交的IP、设备、手机号、邮箱等多维信息实时写入图中，并立刻与已存在的黑名单节点或高风险账号图谱进行结构匹配。

批量注册--利用图结构实时识别风险并阻断

单地址信息正常

注册号	注册时间	链上地址	IP地址
1	T	0x31	19.10.12.4

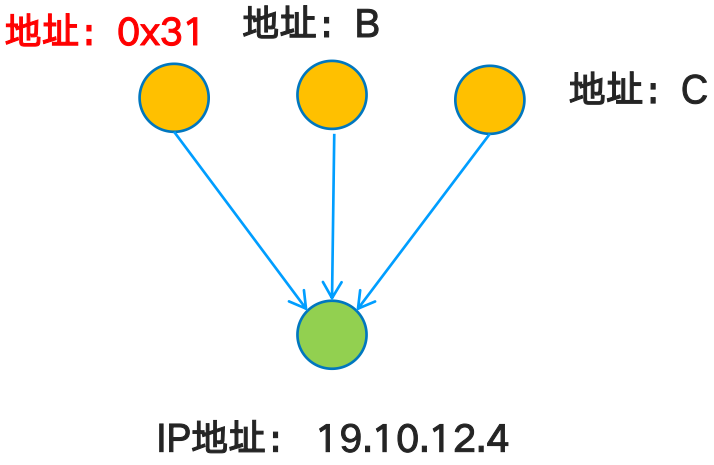


优质客户

放行操作
发放空投/奖励

基于全局信息，实时写入图数据库，并根据内嵌图规则，发现为批量注册账号

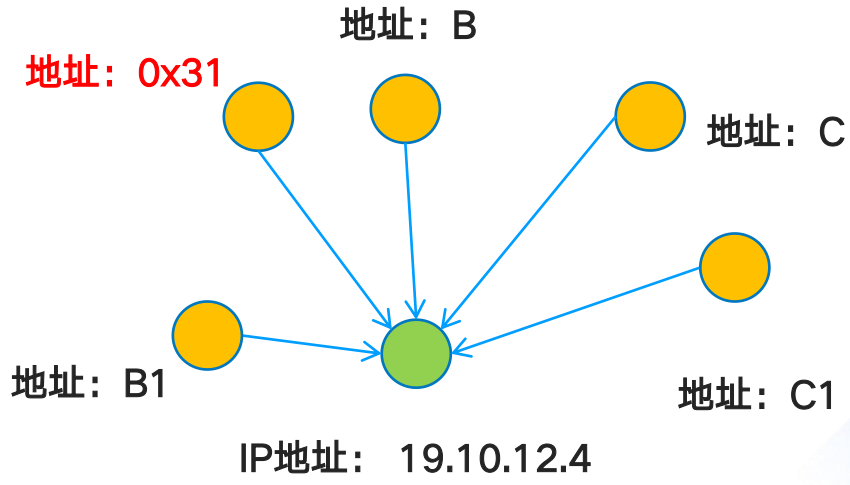
注册号	注册时间	链上地址	IP地址
2	T+1	B	19.10.12.4
3	T+1	C	19.10.12.4



疑似欺诈用户

限制功能
拒绝任务奖励发放

注册号	注册时间	链上地址	IP地址
4	T+3	C1	19.10.12.4
5	T+3	B1	19.10.12.4



欺诈黑名单用户

标记为风险地址
冻结资金/限制提现

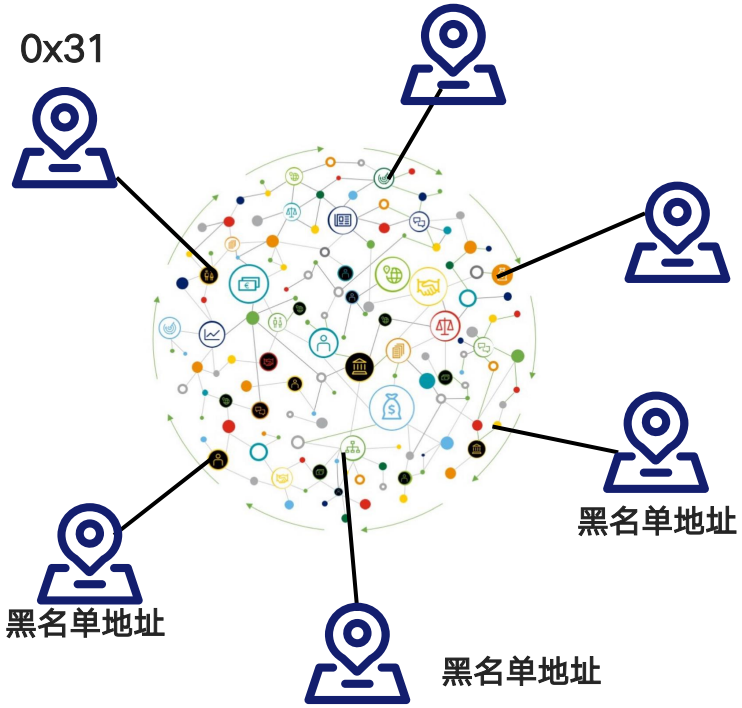
批量注册--利用图算法快速识别黑产团伙

复杂关系识别困难：黑产行为往往涉及多个账号之间复杂的资金流转和协同作案，传统的规则检测方法很难揭示账户间隐秘的关联。

大规模数据处理难度：随着交易量和用户数量的增长，黑产行为可能跨越多个交易平台、多个账户，依赖单点的分析方法难以有效处理和发现这些跨平台的风险。

单点判断无风险

优质用户地址



群体判断高风险

风险地址

群体规则

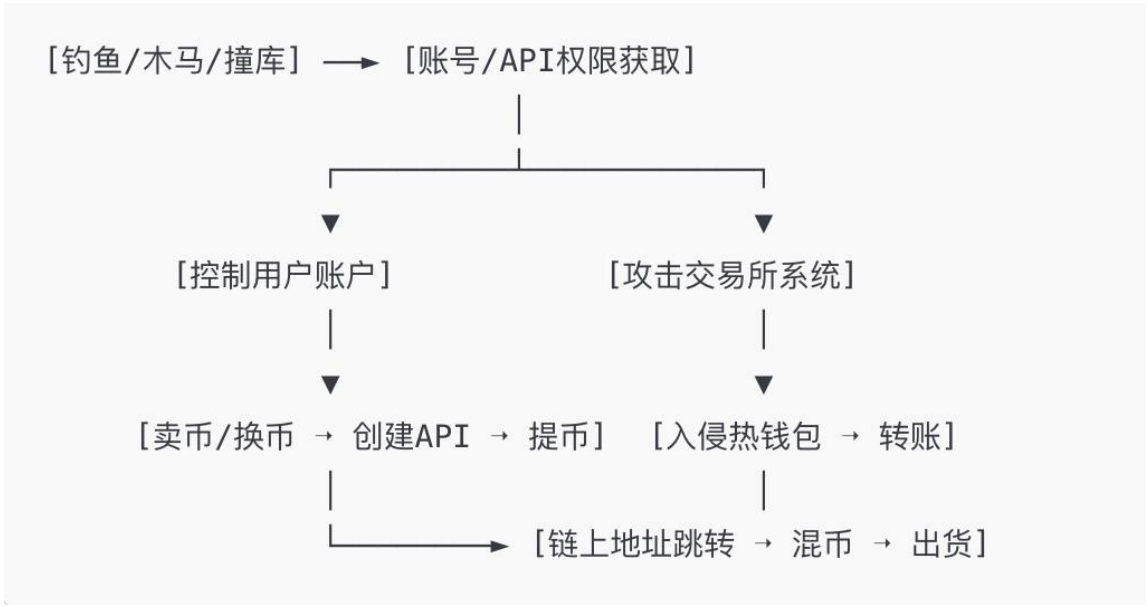
- 社区中有多个地址存在同一时间段内批量操作行为
- 社区中多个地址资金最终流向同一节点
- 社区外部连接比小于一定比例（比如 <20%）
- 社区中存在多个中介中心度高数值节点
- 社区内部平均度（连接数）高于阈值（比如 >10）

全面覆盖风险网络：图算法能够帮助构建用户和账户的全网视图，从而覆盖所有潜在的风险行为，从单一账户的异常到多账户协同作案的复杂行为都能得到全面监控。

交易风控场景分析

黑客盗币逻辑流程图

- 异地登录：短时间内IP跨度大或来自可疑地区
- 设备指纹异常：从未用过的设备、环境登录
- 快速操作路径：登录 ➡ API创建 ➡ 卖币 ➡ 提币，一气呵成
- 提币地址异常：从未使用过地址，或与其他黑产账号共享地址
- 提币金额接近上限：且分批操作规避规则



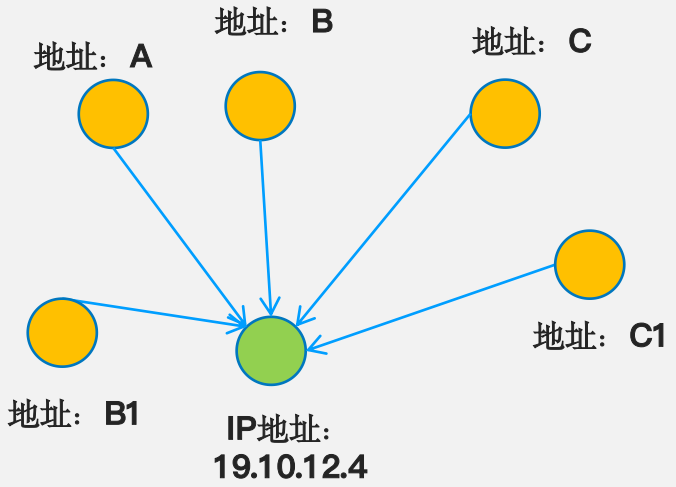
面临挑战

- **多跳地址难穿透：** 黑客往往通过多跳钱包地址中转，规避风控识别
- **聚合钱包难识别：** 不同用户提现到中转地址，最终流向同一个聚合地址
- **实时性处理难度大：** 高频交易、操作行为实时性要求高，传统规则反应不及

交易风控--基于图规则的实时风控监测

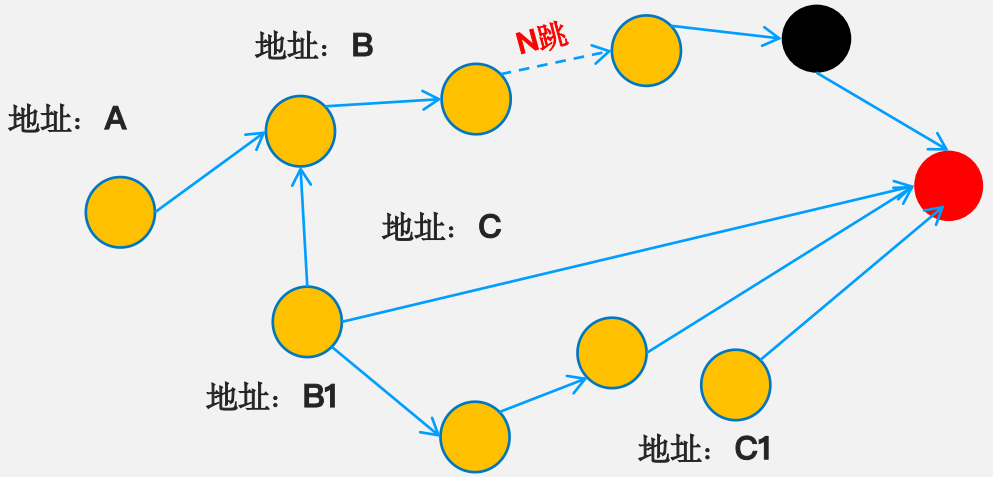
基于**手机号、IP 地址、登录设备、钱包地址、提币地址、身份信息、交易行为链和行为时间特征**构建**黑产盗号交易风控图谱**。复杂的地址与账户图谱结构在抽象化之后，可通过识别典型的**黑产行为模式**，配置对应的**图规则**进行实时风控。

登录类行为模式



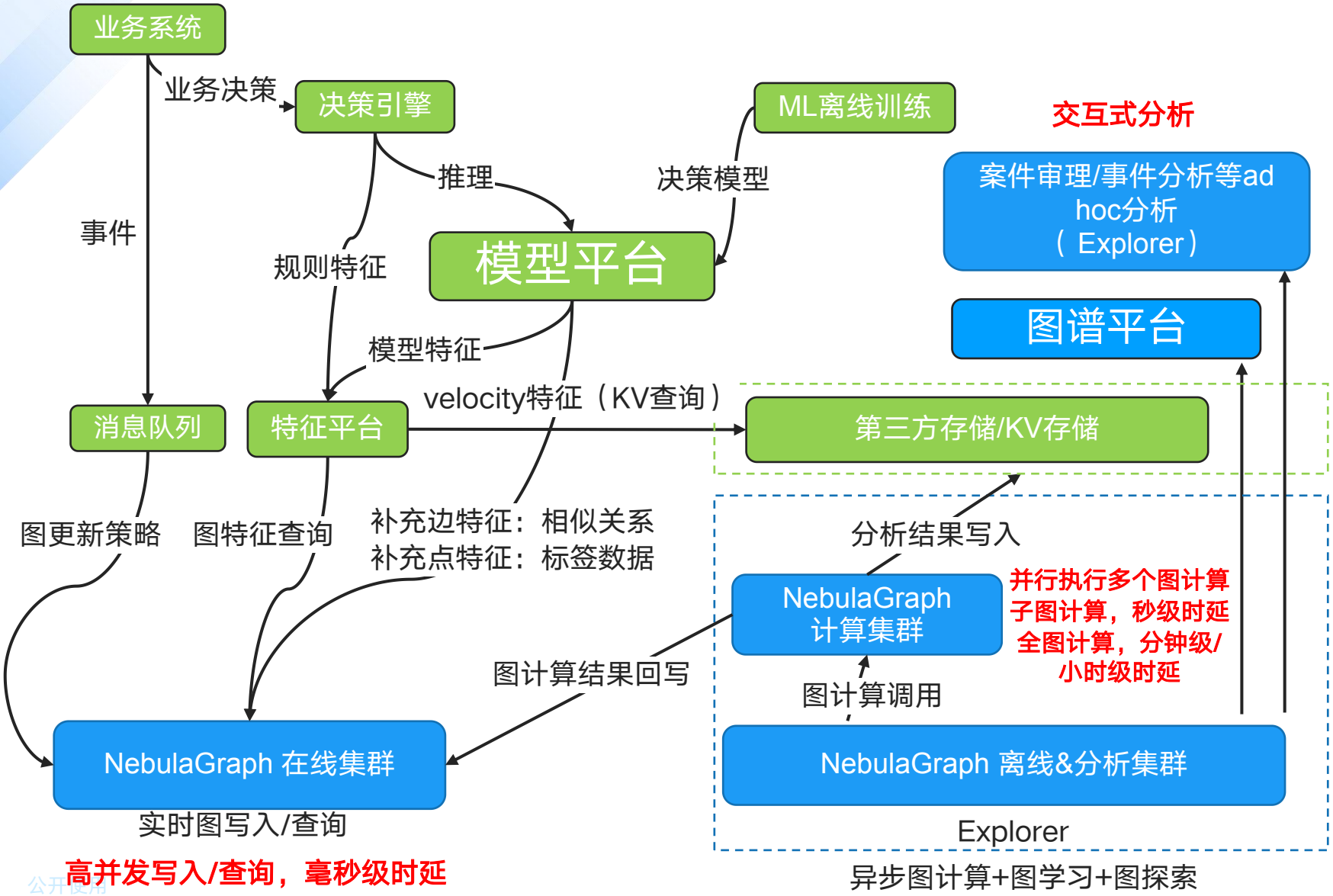
5分钟内同一个IP集中登录多个地址

资金流转行为模式



多钱包通过不同的路径汇入同一“黑产收款地址”

实时 / 准实时 / 离线多种技术场景组合架构



1. 两套集群，同时支持实时业务和离线分析业务。

2. 在线集群处理高并发写入和高并发查询业务。

3. 通过集群同步功能将数据准实时同步到离线集群。

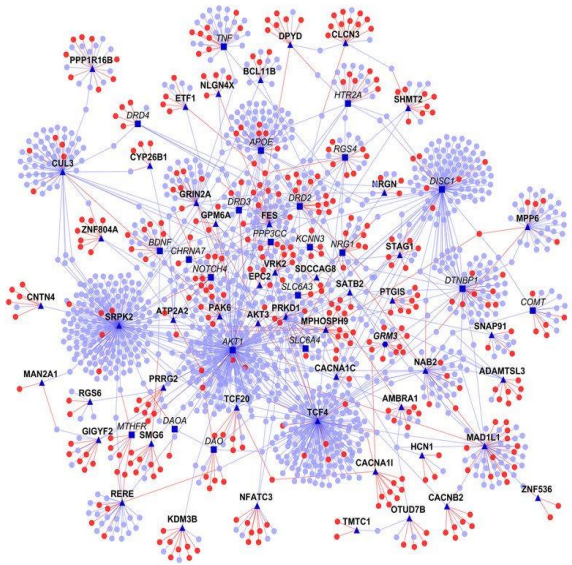
4. 离线集群处理异步图计算等复杂计算业务，结果写回在线集群。

5. 离线集群支撑子图/全图计算。

6. Analyticd 集群支持图计算，针对全图的计算可以在闲时按需拉起。

基于图特征的动态策略生成

借助数据丰富程度增加与机器学习策略，生成新的关联关系，丰富图特征策略，提升反欺诈效果



特征更丰富，准确率更高

- 在统计特征之余，补充关系维度特征
- 关系特征往往更真实，造假成本更高

可解释

- 打破传统AI黑盒模式，图特征可解释

图特征提取

补充点/边特征数据

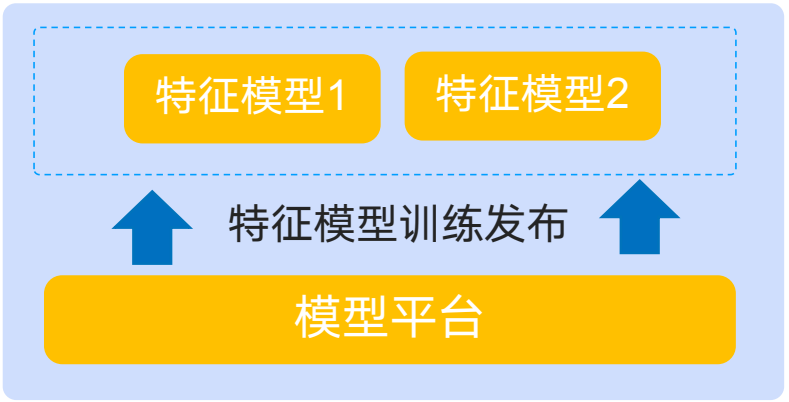
补充特征

- 除实体间实际关系外，补充相似关系特征
- 补充点的标签特征

增强图查询/计算能力

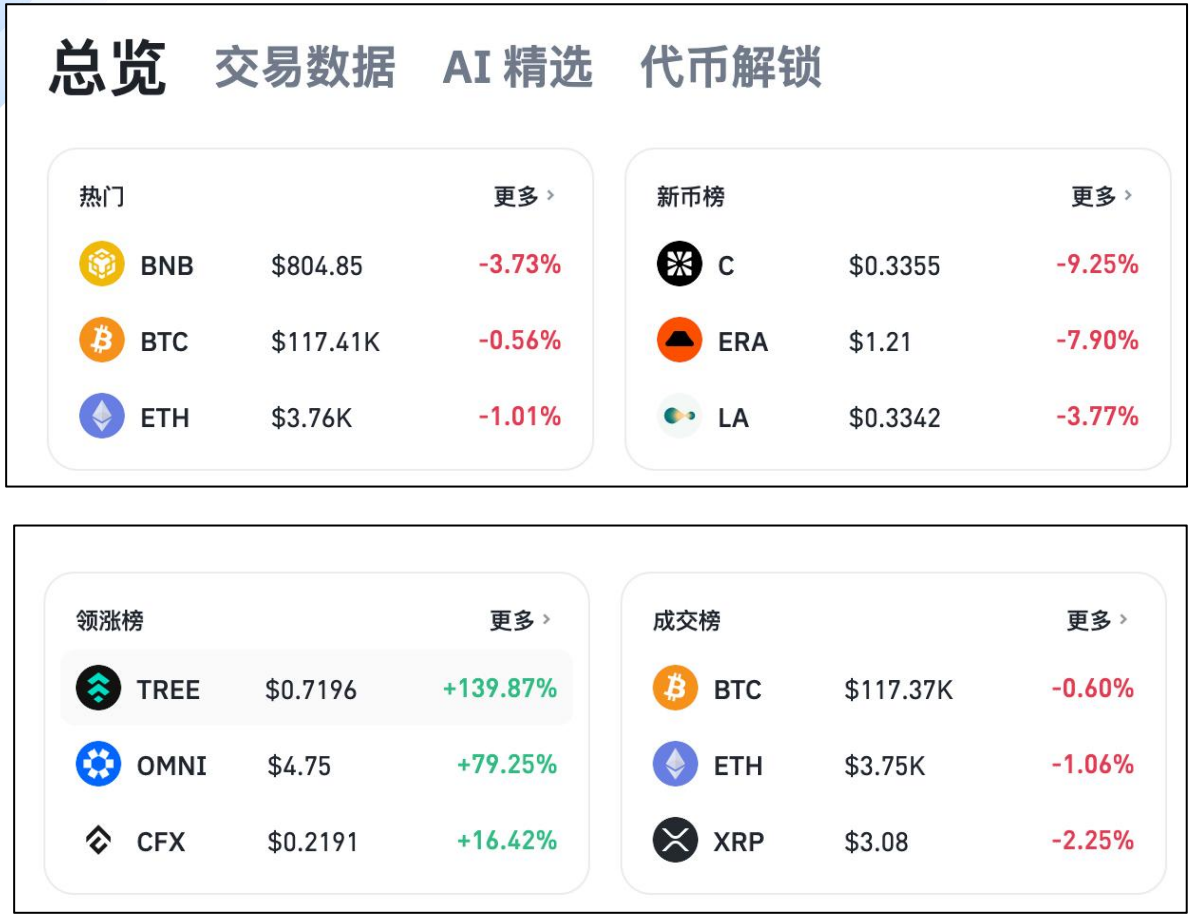
- 基于更多关联关系，增加查询/计算维度

特征平台



03 客户案例

基于百亿规模图谱的 CSI 平台



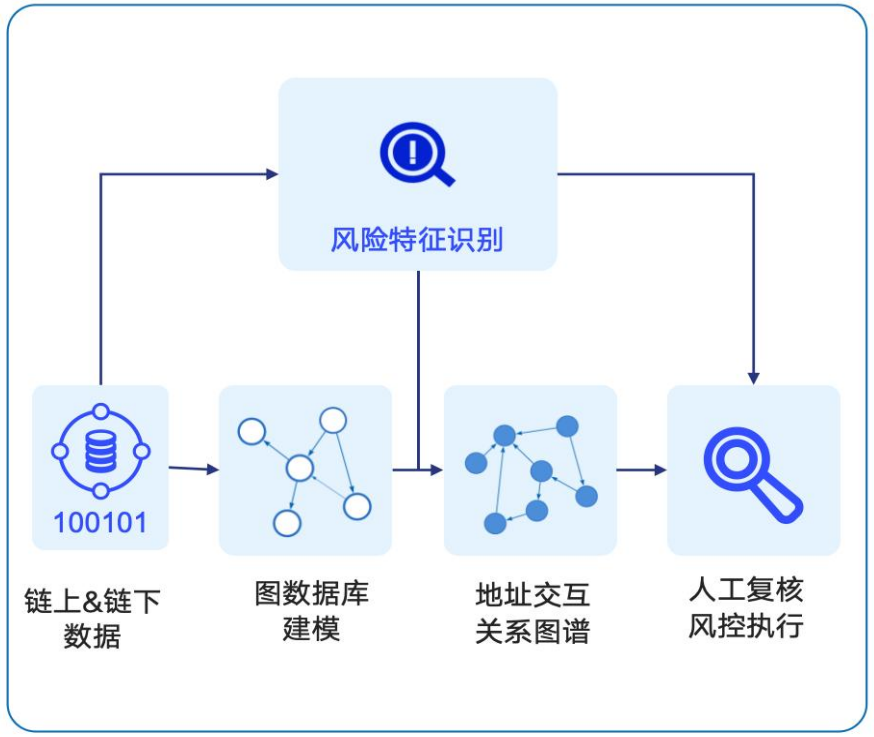
业务背景

- **行业监管趋于规范化**：随着加密资产和DeFi的快速发展，全球各地的监管机构对这一领域的关注度不断提高。例如，美国证券交易委员会（SEC）、欧洲证券和市场管理局（ESMA）等机构都在加强对加密资产的监管。
- **AML和KYC要求**：反洗钱（AML）和了解客户（KYC）要求越来越严格。许多国家和地区要求加密交易所实施严格的 AML 和 KYC 措施，防止非法资金流动。
- **交易量巨大**：每天上百亿美金交易量，如何基于海量交易数据识别其中的可疑交易，防止洗钱及非法活动。

业务挑战

- 在 AML 和 KYC 措施要求日益严格的背景下，如何有效且高效地执行用户身份验证和资金流动监测，防止非法资金流入，成为一个巨大的挑战。
- 随着加密市场交易量日益增长，每天数百亿美元的交易量使得交易所面临着海量数据的处理与分析挑战。如何从中识别出潜在的可疑交易活动（如洗钱、市场操控等）是一个技术难题。

基于百亿规模图谱的 CSI 平台



基于 NebulaGraph 的解决方案

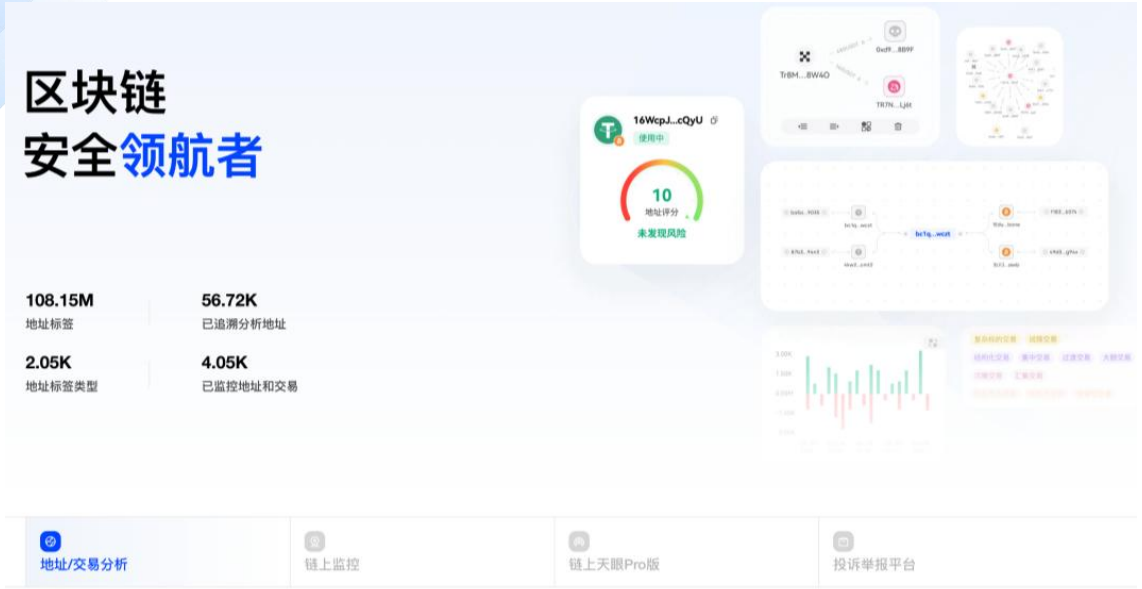
- 基于介质数据、链上数据、用户数据、交易数据等构建 40 亿点，400 亿边的风控合规图谱
- 交易链路穿透：根据给定的地址信息，秒级返回地址之间的交易链路
- 离线计算：全量链上链下数据离线分析，挖掘可疑交易结构
- 可视化分析：业务人员结合重点名单，进行人工研判

应用价值

- **精准的风险监控：**通过实时处理海量数据，快速发现可疑交易和异常资金流动，有效提升黑产识别和响应速度。
- **高效的跨账户关联分析：**精准识别账户间的复杂关系，提升跨平台风险识别能力，防范黑产网络和非法行为。
- **增强合规透明度与审计能力：**通过自动化合规数据整合和报告生成，提升监管合规的透明度，确保合规审计的可解释性和可追溯性。

基于标签地址的链上追踪

加密世界积累了海量的原生链上数据，谁能做到有效的的搜集获取，谁就能拥有交易层面的先发优势



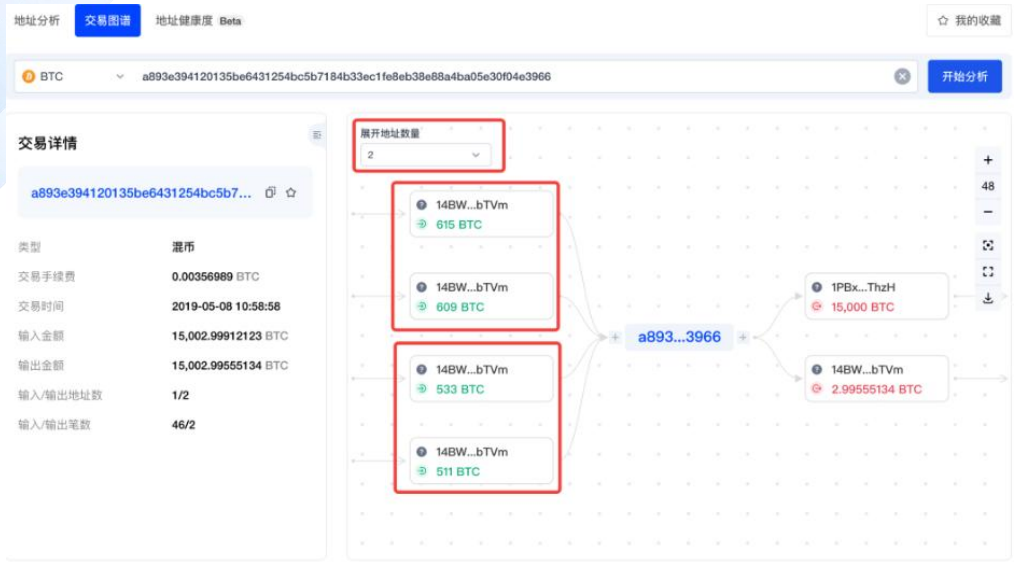
业务背景

- 标记并过滤了 30亿 +个地址和海量、即时的链上底层数据，并对这些地址进行标签分类，可以让用户进行原生的交易数据分析与图谱溯源
- 依托地址标签、已追溯分析地址、已监控地址和交易等数据积累，可以进一步提供地址健康度、地址分析、交易图谱等链上数据服务

业务挑战

- 如何在大体量的链上数据基础上，从数据线团中抽丝剥茧，最大程度处理并挖掘出价值
- 多链复杂交易、多跳匿名路径使得传统方式链上交易路径难以追踪
- 深度链路探索时延高，响应慢，难以触达终端地址

基于标签地址的链上追踪



一站式图平台解决方案

- 图建模：地址、交易、合约等异构图同一建模
- 图实时计算：基于图数据库计算链路路径
- 图算法：路径识别、社区检测快速识别资金汇集等情况
- 图可视化：可视化追溯交易链路
- 图+AI：基于图特征训练标签模型，支持自动迭代

应用价值

- 拓展了监控资产类型：基于图数据库存储关系优势，链上天眼的「地址/交易分析」功能在原先比特币主链、以太坊主链、OKC主链（OKC）的基础上，**大大拓展了监控资产类型**
- 「地址健康度」画像，辅助判断风险：通过丰富的图规则与指标，图算法，**挖掘可疑地址的交易结构特征**
- 深度链上交易图谱分析：基于图数据库强大的深度关系计算能力，探寻层层关联转账交易等行为，**提升了交易链路探查深度**

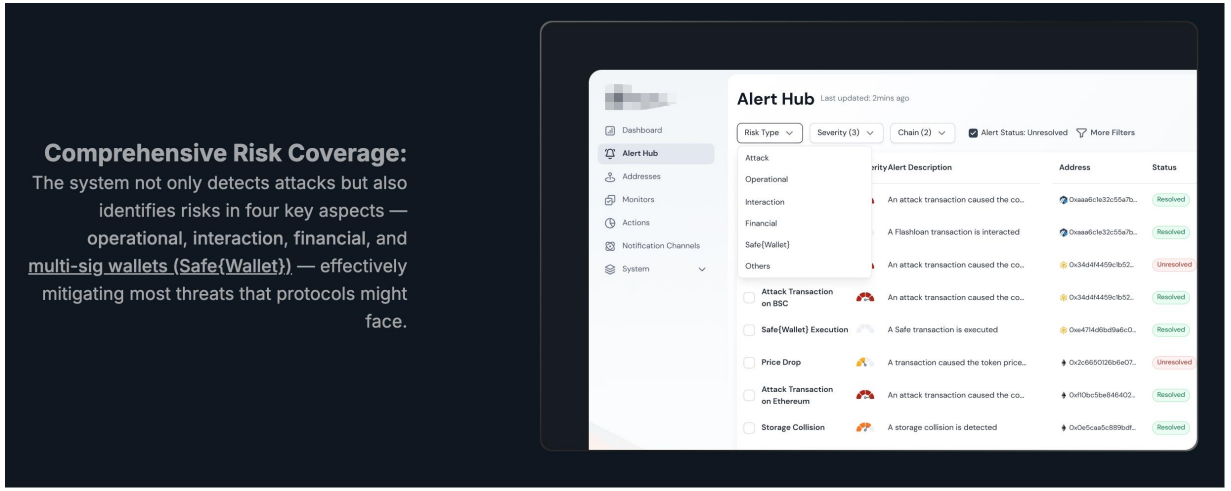
NebulaGraph

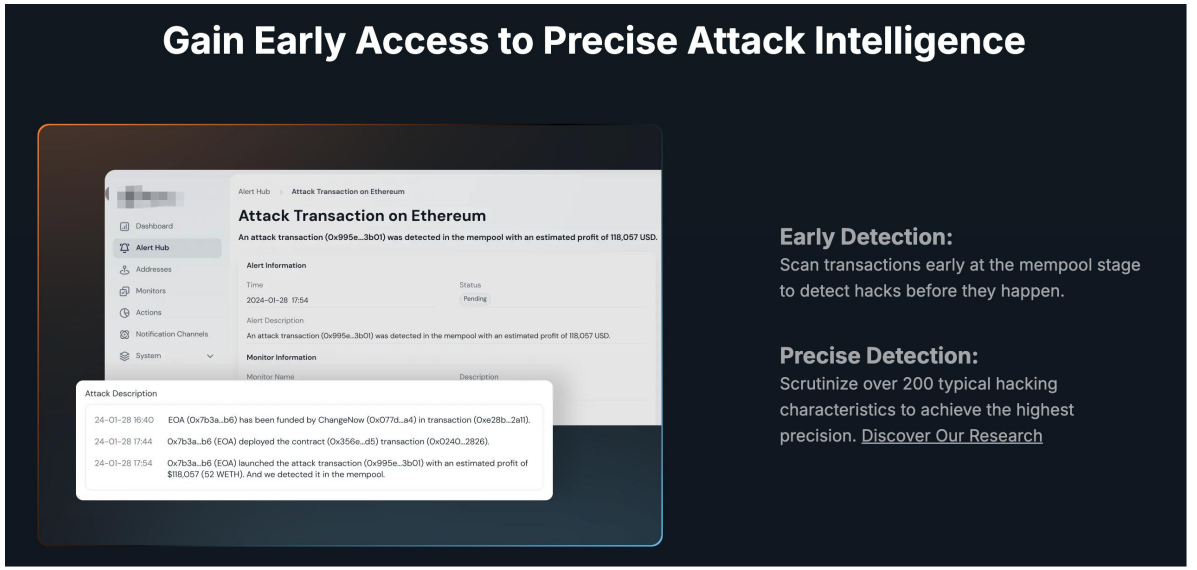
为用户提供安全无缝的链上服务

https://nebula-graph.com.cn

业务背景

- **链上安全事件频发，亟需高效追踪与溯源手段：**Web3 生态中攻击事件频繁发生，导致大量资产损失，急需追踪资金流向、快速定位攻击路径与核心地址。
- **加密资产合规监管趋严，链上资金需可视化审计：**随着全球对加密资产监管加强，交易所、钱包等机构需满足资金来源与去向的合规审查，具备可视化、结构化的资金链路展示能力，支持反洗钱（AML）与制裁风险识别。
- **匿名性强、跳转频繁的链上资金路径增加分析复杂度：**攻击者常使用多跳地址、混币工具隐藏身份，传统手段难以还原真实流向，亟需依赖资金流向图与标签化数据提供清晰、可交互的路径图谱，辅助安全分析与风控决策。





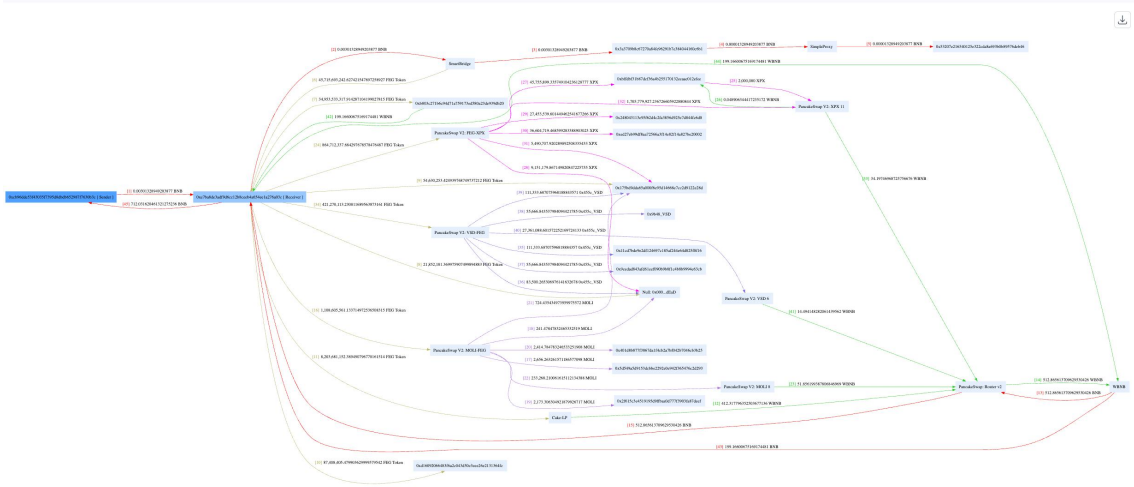
技术挑战

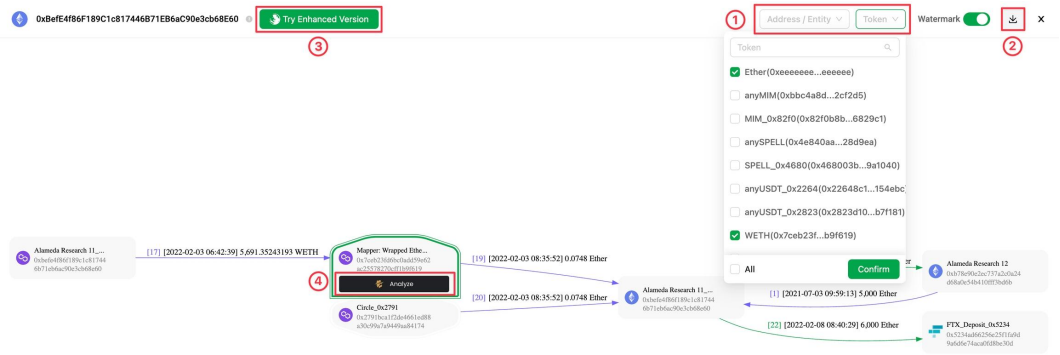
- **性能瓶颈限制业务扩展：**在高并发的复杂路径分析等场景下存在性能瓶颈，无法充分满足大规模图数据深度分析和交互式查询的业务需求，影响系统的稳定性与响应效率。
- **查询语言表达能力有限，制约复杂分析需求：**现有图查询语言在复杂业务场景中的表达能力存在不足，需要写大量的代码来表达，重复用代码调用图数据库以及处理中间过程数据，从而导致性能瓶颈更加明显。
- **集群资源隔离能力弱，易发生资源抢占：**在混合负载运行环境下，图计算与查询任务间缺乏有效的资源隔离机制，容易出现资源竞争与任务干扰，降低整体系统的可用性与性能稳定性。

为用户提供安全无缝的链上服务

基于 NebulaGraph 的解决方案

- **分布式图数据库集群部署：**提供 3节点企业版集群，每台配置：48Core、256GB 、3TB SSD，支持横向扩展，满足大规模数据并发访问和未来容量增长需求。
- **构建超大规模资金流向图：**基于链上转账数据与地址标签信息，构建超3亿节点、10 亿边的资金流图，支撑资金流转路径分析、账户画像、地址聚类等复杂风控应用。
- **高性能图计算与实时写入能力：**借助灵活的 GQL 查询语言与子图计算引擎，实现实时数据写入与秒级查询响应，支持引入多维风控特征、动态规则





应用价值

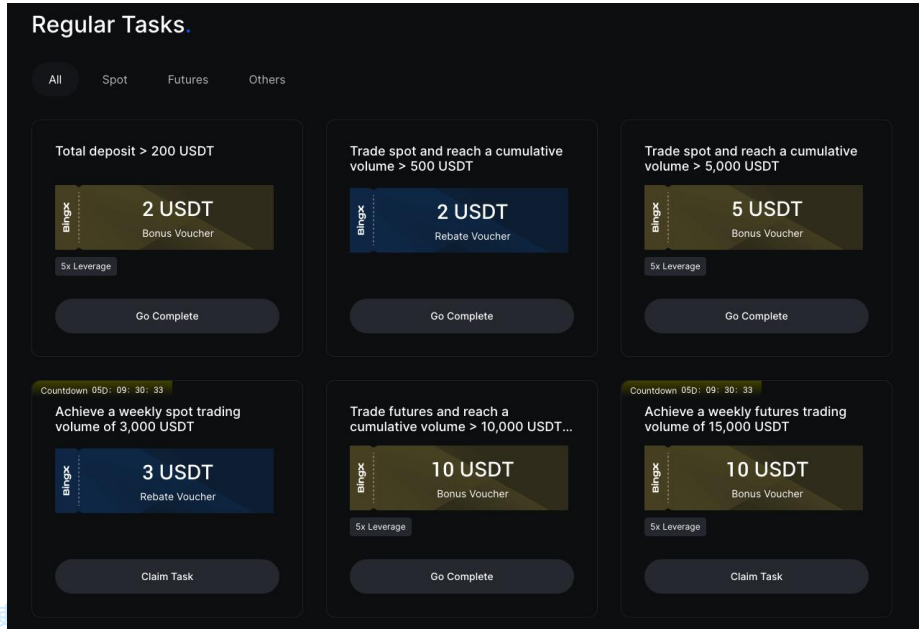
- **保障稳定的业务服务：**系统稳定支撑高并发请求，所有 API 指标结果 1.5 秒内可返回，满足实时交互场景下的服务质量要求。
- **充分释放硬件性能：**相比开源版本，单条 Query 时延更低，使用内存更少，QPS 提升显著，极大提升硬件资源利用率，实现更优算力支撑。
- **简化复杂场景开发运维：**通过标准化 GQL 查询接口，显著降低复杂业务逻辑的开发与维护成本，无需额外代码实现复杂逻辑推理。

某 Web3 交易所：实时营销反作弊

业务背景

为吸引新用户并促进交易，交易所主要采用以下策略：

- **高激励奖金与空投活动**:分层奖池设计，覆盖大额投资者与小散用户，刺激广泛参与。
- **质押奖励**：要求用户质押,绑定用户资产，提升用户留存率。
- **交易竞赛与任务**：用户交易指定资产可瓜分奖池，连续签到交易额外奖励现金
- **社交裂变机制**：要求用户转发活动帖、标记好友并提交钱包地址，利用社交关系链扩散交易所影响力。



Top加密货币现货交易所

CoinMarketCap基于流量，流动性，交易量以及对所报告交易量合理性的置信度对交易所进行排名和评分。 阅读全文

现货 | 衍生品 | DEX（现货） | DEX（衍生品） | 借贷

#	交易所	Trading volume(24h)	平均流动性	每周访问次数	市场数量	# 货币	法币支持
1	Binance	¥98,893,160,586	933	9,399,435	1999	519	EUR, GBP, BRL and +8 more
2	Bybit	¥17,673,361,175	720	3,427,103	1223	734	USD, EUR, GBP and +3 more
3	Coinbase Exchange	¥12,103,283,350	787	27,905	438	298	USD, EUR, GBP
4	Upbit	¥8,213,120,101	383	1,326,820	520	255	KRW
5	OKX	¥11,056,331,379	775	5,315,049	1037	346	AED, ARS, AUD and +43 more

业务挑战

- **高激励驱动的黑产渗透**：Web3 交易所通过空投、交易竞赛等高奖励活动吸引用户（如 Bybit 的 10,000 USDT 奖池、CoinW 的 9 万美元交易挑战），但黑产通过批量注册地址、伪造身份等手段套取奖励，**导致 80% 的空投奖励被 5% 的地址获取**。
- **匿名性与协同作弊：**链上地址无需实名认证，攻击者可通过**“设备农场”**控制数百个地址形成“羊毛军团”，通过多层转账混淆资金路径，传统规则引擎难以识别群体行为。
- **跨平台攻击复杂性：**黑产利用交易所间风控力度差异，实施“链跳混币-场外现金”的闭环交易，单一平台数据无法全局追踪
- **误报率高**：正常用户使用VPN可能被误判为高风险

某 Web3 交易所：实时营销反作弊

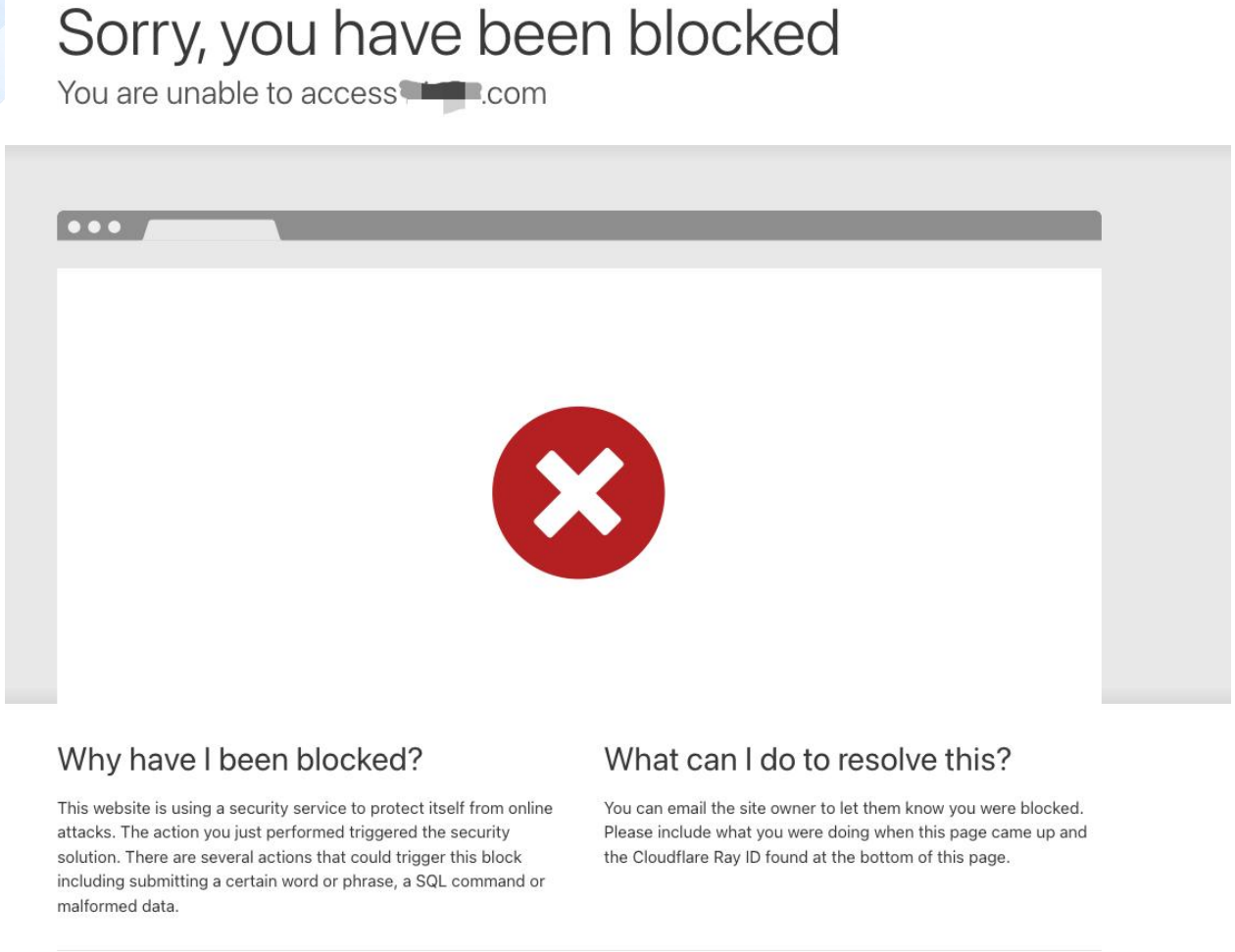
实时营销反作弊的技术挑战

- **数据规模与性能**：需处理百亿级地址节点和千亿级交易边，传统SQL数据库3跳查询延迟超10秒，无法满足毫秒级风控需求。
- **复杂关系建模**：黑产行为呈现星型聚合（多地址向同一提币地址集中转账）、环形交易（资金闭环回流）等拓扑结构，关系数据库难以高效匹配。
- **实时更新与计算**：交易峰值达10万笔/秒，需在ms级时延内完成风险地址的N度关联扫描

基于 NebulaGraph 的解决方案

- **分布式 NebulaGraph 图数据库集群部署：提供 3节点企业版集群**，每台配置：**32Core、128GB 、2TB SSD**，支持横向扩展，满足大规模数据并发访问和未来容量增长需求。
- **构建用户-设备-活动图谱**：交易所内用户信息、设备信息、活动优惠券信息构成一整张异构图，将用户、设备与优惠券进行连接。最终图中包含 **3000w 点、20 亿边**。
- **NebulaGraph 图数据库成为风控核心**：关系推理能力弥补了规则引擎和 AI 模型的不足
  - **团伙欺诈识别**：NebulaGraph 图数据库可构建多度关系网络，**发现分散账户间的隐蔽关联**，助力识别“设备农场”操控的虚假账户群（如 100 个账户通过同一出口IP关联）批量薅取平台奖励
  - **动态风险传导分析与实时决策能力**：当单一地址被标记为高风险时，图数据库可扩散扫描其N度关联账户，提前拦截潜在威胁。**相较关系型数据库的小时级分析，与其他图数据库的分钟级分析，NebulaGraph 图数据库将响应时间压缩至毫秒级，提高了风控系统实时决策能力**
  - **实现复杂业务逻辑**：风控算法具有较为复杂的业务属性，传统图数据库实现业务逻辑需开发人员针对性开发业务代码，多轮调用图数据库计算结果，导致计算延时较高；**NebulaGraph 图数据库支持使用 ISO-GQL 查询语言直接完成复杂业务逻辑开发，节约开发成本，提高开发效率**。同时，单次调用图库完成业务逻辑，提升计算效率

某 Web3 交易所：交易所内实时营销反作弊



业务价值

- **风控精准度提升**：误报率降低至 **5%** 以下，通过关联算法识别“单点正常、群体异常”的地址簇。
- **实时风控能力**：百亿级图谱中 **3** 跳查询延迟**<50毫秒**，盗号交易拦截时间从分钟级压缩至毫秒级。
- **跨平台联防**：融合多交易所黑名单数据，图数据库追踪跨链洗钱路径效率提升10倍。
- **成本优化**：相比传统方案，**存储空间减少 40%，计算资源消耗降低 60%**

NebulaGraph | VELODB

Deep Relationships & Real-Time Analytics:

Architecting Modern Financial Data Stacks

深度关联与实时分析下的金融新范式

August 22, 2025 13:30

Hong Kong

扫码报名
香港 nMeetUP

感谢观看
Q&A

https://nebula-graph.com.cn

GitHub: vesoft-inc/nebula

Twitter: @NebulaGraph

Facebook: @NebulaGraph

https://discuss.nebula-graph.com.cn

微信公众号

开源项目