《链上不翻车手册：防骗、防黑、防归零》

本手册包含：

✓ **区块链与加密货币基础** —— 帮助你理解区块链技术、代币分类、公私钥管理、钱包使用等核心概念。

✓ **常见骗局解析** —— 深入剖析资金盘、OTC 诈骗、钓鱼攻击、虚假交易所、NFT 骗局等高危陷阱，让你识破黑手。

✓ **安全防护策略** —— 从交易所到个人设备，从资产管理到社媒防骗，提供实用的防护指南，让安全成为习惯。

✓ **应急处理指南** —— 一旦遭遇资产被盗，如何止损、溯源、报警？本手册提供实战方案，助你最大化挽回损失。

无论你是区块链小白，还是资深玩家，本手册都将成为你在链上世界的安全指南，助你稳步前行，不翻车！

官网链接：https://pandaly.io

一、区块链基础概念

1.1 什么是区块链?

2008 年，中本聪发表了具有革命性的论文《比特币：一种点对点的电子现金系统》。该论文提出了一种全新的电子支付系统，其核心理念为：通过密码学技术而非传统信用机制，让任意双方在符合条件的情况下直接完成支付，免去对特定第三方机构的依赖。

从技术角度看，狭义的区块链是将数据区块按照时间顺序以链式结构连接起来，通过密码学技术确保其不可篡改与伪造，构建了一个分布式账本。

1.2 如何理解区块链?

为了让大家更清晰地理解区块链，可以通过以下生动的例子：

假设你是一位艺术家，创作了一幅价值连城的画作，并希望记录其所有权归属。若将画作交给某艺术品登记机构存档，理论上该机构可以随时更改记录，将画作的所有权转移给他人，这会导致你的权益丧失。

而如果采用区块链技术，你可以将画作的所有权信息记录在区块链上，并通过分布式网络中的多个节点（如全球艺术家协会、博物馆或收藏家组织）共同验证与存储该信息。通过共识机制，所有节点都认可该记录的真实性。

在这个过程中：

- **你是信息的发起者**；
- **画作的所有权信息与时间记录构成了一个“区块”**；
- **艺术家协会、博物馆等节点负责存储与验证信息**；
- **各区块按时间顺序链接，形成防篡改、公开透明的“区块链”。**

这种机制不仅确保了信息的安全性，还有效解决了传统单点信任系统中的篡改风险与信任问题，构建了更加可靠的记录方式。

1.3 区块链分类

区块链可以分为三大类：**公有链**、**私有链**和**联盟链。**以下是它们的具体区别与应用：

1. 公有链（Public Blockchain）

- **定义**：公有链是完全开放的区块链网络，任何人都可以参与，且节点之间是平等的。
- **特点**：
  - 去中心化，数据公开透明；

- 高安全性，但交易处理速度较慢。

- **例子**：
  - 比特币与以太坊是典型的公有链。
  - 例如：在比特币网络中，任何人都可以成为节点参与记账，所有交易历史都可以查看，确保公开透明。

2. 私有链（Private Blockchain）

- **定义**：私有链由单一机构或组织控制，只有授权节点才能访问数据或参与区块生成。
- **特点**：
  - 高度中心化，节点准入严格；
  - 交易速度快，隐私性强。
- **例子**：
  - 企业内部供应链管理系统。
  - 例如：某物流公司使用私有链记录货物运输过程，仅授权人员可以访问这些记录，确保商业机密不被泄露。

3. 联盟链（Consortium Blockchain）

- **定义**：联盟链由多个组织或机构共同维护与管理，节点准入与权限由联盟成员共同决定。
- **特点**：
  - 部分去中心化，访问权限受控；
  - 性能较高，数据透明度与隐私性平衡。
- **例子**：
  - 银行间清算系统。
  - 例如：R3 Corda 是一个典型的联盟链案例，全球多个银行和金融机构通过联盟链技术实现跨银行交易清算，提高效率并降低成本。

1.4 总结

- **公有链**：适合开放场景，强调去中心化与公开透明，如加密货币。
- **私有链**：适合封闭场景，强调隐私保护与高效性，如企业内部管理。
- **联盟链**：适合多方协作，兼顾效率与隐私，如行业合作与跨机构交易。

通过选择合适的区块链类型，可以在不同应用场景下最大化发挥区块链技术的优势。

1.5 那么区块链和加密货币到底是什么关系呢?

可以简单理解为：公有区块链是“技术”，加密货币是“应用”，由于区块链技术是去中心化的，需要有人主动参与维护和建设，所以诞生了加密货币用来奖励这些用户。

举例 1：以太坊网络（轨道）和 ETH 代币（火车）

1. **轨道的作用：**

以太坊提供了一个支持智能合约的区块链网络，就像铺好了一条专用的高速火车轨道，能承载更多功能和应用（比如 DeFi、NFT、DAPP）。

2. **火车的存在：**

ETH 是这个网络上的原生代币，就像火车上的燃料或票价：

a. 用户在以太坊上发交易或运行智能合约时，需要支付“燃料费”（GAS），这就是用 ETH 代币支付的。

b. 矿工或验证者处理这些交易，就能收到 ETH 代币作为奖励，从而激励更多人加入网络维护。

如果没有 ETH 这辆火车：

- 矿工没钱赚，不会维护轨道，区块链（**以太坊网络**）可能瘫痪；
- 用户无法支付手续费，轨道也会变成摆设，没人用。

举例 2：比特币网络（轨道）和 BTC（火车）

1. **轨道的作用：**

比特币是一个去中心化的支付网络，像是专门设计的货运轨道，只为转移“价值”而存在。

2. **火车的存在：**

BTC 是比特币网络的代币，主要功能是：

a. 作为价值传递的“货物”（比如跨国汇款）；

b. 激励矿工“维护轨道”——矿工通过“挖矿”获得 BTC 奖励，这让他们愿意提供算力，保护比特币网络不被攻击。

如果没有 BTC 代币：

- 矿工没了收益来源，就不会提供算力，轨道失去维护者，整个网络会崩塌。
- 没有用户需求（火车装货），轨道就沦为无用的摆设。

总结：

区块链（轨道）是加密货币运行的基础，而加密货币（火车）又为区块链提供经济激励和实际用途。没有轨道，火车跑不起来；没有火车，轨道也没人打理。两者相辅相成，彼此成就！

二、加密货币知识入门

2.1 加密基础知识

原生币与代币

2.1.1 原生币（如 BTC、ETH）的特点与作用　加密货币中的**原生币**，比如比特币（BTC）和以太坊（ETH），可以理解为整个区块链生态的核心驱动力。它们各自有独特的特点和作用，下面用大白话拆解一下：

原生币的特点

- **去中心化**：这类代币没有一个“老板”或“公司”在背后操控，一切都靠区块链网络运行。任何人只要有网络，都能参与。
- **稀缺性**：以比特币为例，最大供应量是 2100 万枚。这种“物以稀为贵”的特性给它带来了类似“数字黄金”的属性。
- **安全性高**：原生币的区块链底层技术通过密码学保证了交易和数据的安全性，基本不会被篡改或伪造（当然，钱包被盗就是另一码事，这个我们后面会讲）。

原生币的作用

- **价值存储**：比特币常被称为“数字黄金”，因为它可以长期保存价值，不受通货膨胀直接影响，类似一种避险资产。
- **支付功能**：比如比特币可以直接用来支付商品和服务。以太坊的 ETH 则是运行“智能合约”时的“燃料”，支付手续费用。
- **网络驱动力**：在以太坊网络生态中，ETH 代币是整个链条运转的动力来源。无论是运行去中心化应用（DApps）还是铸造 NFT，都需要用 ETH 支付手续费。
- **参与治理**：很多区块链项目会通过持币让用户参与网络的升级、规则制定等投票活动，原生币是“参与权”的体现。

举个例子：BTC vs ETH

- **BTC（比特币）**：

比特币的定位就是“数字黄金”，主要是价值存储和支付功能，功能比较简单，但网络最稳定，全球认可度高。

- **ETH（以太坊）**：

以太坊是一个更像“开发者乐园”的平台，ETH 不光能当钱用，还能支持各种复杂的应用，比如 DeFi（去中心化金融）、NFT 铸造等。

总结一句话：

原生币是区块链生态的“地基”和“燃料”。比特币更像是“储值的金砖”，以太坊则是“运行整个区块链经济的能源”。这两者代表了加密世界中最核心的价值逻辑。

2.1.2 代币（如 USDT、SHIB）的分类与用途

代币是建立在原生代币（如 ETH、BTC 等等）的公有区块链网络之上，代币是跑在公路上的车辆：它们依赖于原生代币的区块链网络来发行和运行，比如：

- **USDT** 是以太坊上的稳定币，用来转账。
- **SHIB** 是以太坊上的一种“搞笑代币”，靠社区炒作。

所有这些代币都是“搭建”在公路（ETH 网络）之上的，没有公路，它们无法独立存在。

代币的分类如下：

1. **稳定币（Stablecoin）**
    a. **特点**：价格和法币挂钩（如 1 USDT ≈ 1 美元）。
    b. **代表**：USDT、USDC、DAI。
    c. **作用**：
        i. **避险工具**：加密市场波动大，稳定币像“避风港”，可以锁定收益。
        ii. **跨境支付**：省掉银行中间费用，快速到账，尤其适合国际转账。
        iii. **交易中间桥梁**：交易所用稳定币作为通用货币，方便买卖其他币种。
2. **功能型代币（Utility Token）**
    a. **特点**：用来解锁某些区块链应用的功能，就像某种“使用券”。
    b. **代表**：BNB（币安交易手续费优惠）、MANA（元宇宙项目 Decentraland 中的代币）。
    c. **作用**：
        i. 支付平台手续费或服务费用。
        ii. 获取平台上的某些专属功能，比如优先权或奖励。
3. **治理代币（Governance Token）**
    a. **特点**：赋予持有人对项目治理的投票权，持有越多话语权越大。
    b. **代表**：UNI（Uniswap）、AAVE（Aave）。
    c. **作用**：
        i. 决定项目的未来发展，比如新功能上线、手续费调整等。
        ii. 激励社区参与，分红或奖励活跃用户。
4. **娱乐型代币（Meme Token）**

a. **特点**：社区驱动、投机性强，靠人气而非实际用途支撑。

b. **代表**：SHIB（柴犬币）、DOGE（狗狗币）。

c. **作用**：

i. 社区狂欢的象征，类似加密世界的“潮流文化”。

ii. 投机套利工具，可能暴涨暴跌，风险极高。

5. **资产支持型代币（Asset-backed Token）**

a. **特点**：每枚代币背后有对应实物资产，如黄金、房产。

b. **代表**：PAXG（黄金支持代币）。

c. **作用**：

i. 数字化拥有实物资产，更方便交易。

ii. 通过链上操作降低传统资产买卖的门槛。

代币的用途

1. **支付工具**

一些代币可以直接用于支付，比如 USDT 用来快速完成跨境支付。

2. **投资标的**

不同代币的用途、背景、社区实力不同，投资者会选择它们作为投机或长期投资的工具。

3. **平台功能支持**

功能型代币让你使用特定平台的功能，比如用 BNB 在币安上省手续费，用 MANA 在元宇宙里买地。

4. **权益参与**

治理代币持有者可以对项目的未来方向投票，还可能收到分红或奖励。

5. **社区文化**

像 SHIB、DOGE 这些代币，更多是依赖粉丝群体和社交传播形成了独特的文化氛围，适合短期炒作，但长期价值不一定能持续。

2.1.3 公钥、私钥与助记词

在区块链世界里，“公钥”、“私钥”和“助记词”是加密钱包的核心概念。

1. **公钥是什么?**

公钥就像你的银行账号。你可以告诉别人这个账号，让他们往里面转钱。它是公开的，别人只需要知道你的公钥，就可以向你发送资产。

专业点：

- 公钥是通过**私钥**生成的，是一种“一对一”的关系。
- 公钥可以用来生成地址，类似于你的“收款码”。
- 它是加密算法的产物，公开但安全。

2. **私钥是什么?**

私钥是用来“签字”的秘密钥匙，只有你自己知道。谁掌握了私钥，谁就拥有钱包里的资产。它是你的“超级权限”。

专业点:

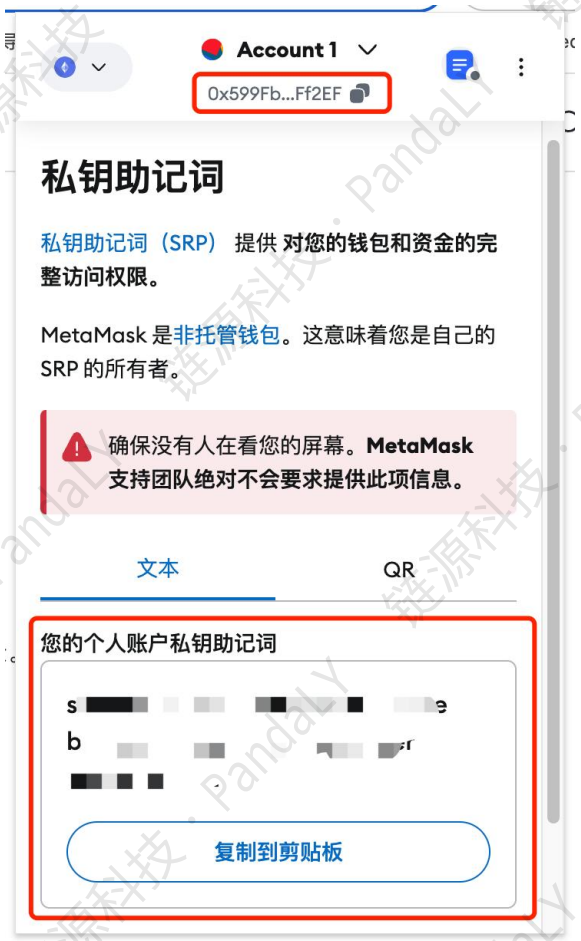
- 私钥可以用来生成公钥，但反过来无法通过公钥推导出私钥。
- 私钥不能泄露，一旦泄露，资产就可能被盗走。
- 私钥是钱包的核心，钱包里的资产其实并不“存在”你的钱包里，而是记录在区块链上，私钥是你访问这些资产的唯一凭证。

3. **助记词是什么?**

助记词是私钥的“备份工具”，由一组单词组成（通常是 12 个或 24 个）。它是私钥的翻译版，方便人类记忆和记录。

专业点：

- 助记词可以用来恢复钱包。
- 它是私钥的另一种表现形式，等同于你的“万能钥匙”。
- 助记词一旦泄露，别人也可以通过它恢复你的钱包并转走资产。



2.1.4 冷钱包与热钱包

在加密货币的世界里，“钱包”是每个玩家的必备工具。但钱包也有冷、热之分，选择正确的钱包类型，既能保护资产安全，又能满足交易需求。下面讲清楚这两者的区别和适用场景。

1. **什么是热钱包?**

热钱包就像你的手机支付 App（比如支付宝或微信钱包），随时连着互联网，能快速完成转账和交易。

- 热钱包是指联网的钱包，随时可以和区块链交互。
- 常见形式：手机钱包 App、交易所钱包、浏览器插件钱包（比如 MetaMask）。
- 特点：
  - **优点**：便捷，适合频繁交易和快速转账。
  - **缺点**：因为一直联网，容易被黑客攻击，安全性相对较低。

适用场景：

- 日常小额交易（比如转账、支付或抢购 NFT）。
- 用于交易所买卖、短期持币。

2. **什么是冷钱包?**

冷钱包就像你家里的保险箱，完全离线存放，无法通过互联网直接操作，需要你“亲自开箱”才能使用。

- 冷钱包是指完全离线的钱包，不能直接与区块链交互。
- 常见形式：硬件钱包（比如 Ledger、Trezor)、纸钱包、甚至是离线的专用电脑或手机。
- 特点：
  - **优点**：极高的安全性，因为离线状态下黑客无法接触。
  - **缺点**：使用较麻烦，交易时需要先“上线”（通过连接设备或导入私钥)。

适用场景：

- 长期持有大量资产（比如大额比特币、以太坊等)。
- 想要最大化安全性时（比如存储种子资产或家庭财富)。

冷钱包和热钱包的核心区别

对比项	热钱包	冷钱包
联网状态	持续联网，实时交互	离线存储，与区块链断开
安全性	易受黑客攻击，安全性低	不联网，极难被盗，安全性高
便捷性	使用便捷，适合频繁交易	使用麻烦，需要额外操作
成本	通常免费（交易所、App）	有硬件成本（硬件钱包）
适用对象	小额资产、频繁交易用户	大额资产、长期持有用户

2.1.5 链上交易 vs 交易所交易流程和逻辑解读

在加密货币世界，买币主要有两种方式：链上交易（On-Chain）和交易所交易（Off-Chain)。它们的操作流程和背后的逻辑各有特点。同时，充币与提币的操作以及交易费（Gas Fee）的计算也是新手常见的疑问。以下逐一解读。

链上交易买币

链上交易是直接在区块链上完成买卖，就像“逛市场直接和摊主交易”。

操作流程：

1. **准备钱包**
   a. 选择一个去中心化钱包（如 MetaMask 或 Trust Wallet），确保钱包有余额（比如 ETH、BNB）。
2. **连接去中心化交易所（DEX）**
   a. 打开 Uniswap、PancakeSwap 等平台，通过钱包授权连接。
3. **选择交易对**
   a. 输入你想要买的币种（比如用 ETH 买某种代币）。
   b. 注意检查代币合约地址，避免假币。
4. **设置交易参数**
   a. 输入购买金额，确认滑点范围（防止价格波动）。
5. **确认交易**
   a. 通过钱包确认交易，同时支付 Gas 费。
6. **等待区块确认**
   a. 等待矿工打包交易，完成后代币会显示在你的钱包中。

逻辑：

链上交易没有中间商，完全由智能合约执行。你用主流币兑换代币，交易信息公开透明，但需要 Gas 费作为网络操作成本。

交易所交易买币

交易所交易是把资产存入中心化平台（如 Binance、Coinbase），通过买卖订单完成交易，就像“去超市购物”。

操作流程：

1. **注册并充值**
   a. 在交易所注册账号，完成身份认证（KYC）。
   b. 通过银行卡或其他加密货币充值。
2. **选择交易市场**
   a. 进入交易界面，找到对应币种交易对（比如 BTC/USDT）。
3. **下单买币**
   a. 选择市价单（直接按当前价格买）或限价单（设置价格等候成交）。
4. **完成交易**
   a. 交易成功后，资产存放在交易所账户中。
5. **提币到钱包（可选）**

a. 如果需要更高安全性，将资产从交易所转到个人钱包。

逻辑：

交易所交易通过撮合系统完成交易，速度快，适合大额买卖，但资产托管在平台上，需信任平台安全性。

2.1.6 充币与提币的操作流程

充币（从钱包转到交易所）

充币是把钱从你钱包搬到交易所的账户里。

步骤：

1. 在交易所找到充币地址（比如 USDT-ERC20）。
2. 打开你的钱包，输入交易所地址和转账金额。
3. 确认交易，支付 Gas 费。
4. 等待区块确认后，资产会显示在交易所账户。

提币（从交易所转到钱包）

提币是从交易所把钱提到自己控制的钱包。

步骤：

1. 在钱包生成接收地址（比如你的 ETH 地址）。
2. 在交易所选择提币，输入接收地址和提币金额。
3. 确认提币请求（有些交易所需要双重验证）。
4. 支付提币手续费，等待交易完成。

2.1.7 交易费（Gas Fee）的意义与动态调整

Gas Fee 是你给矿工的“小费”，矿工帮你打包交易，你得付点辛苦费。

- Gas Fee = 交易操作的计算成本（Gas） × 当前 Gas 价格（Gwei）。
- 作用：
  - 确保网络运转，激励矿工/节点参与交易确认。
  - 防止网络被垃圾交易淹没。

Gas 费动态调整的逻辑

Gas 费就像打车费，路上车多（网络繁忙）时，费用高；路畅通时，费用低。

- **影响 Gas 费的主要因素：**
  - **网络拥堵：** 当大量用户同时发起交易，Gas 费会上升。
  - **交易复杂度：** 简单转账 Gas 低，复杂智能合约操作 Gas 高。
  - **矿工优先级：** Gas 费高的交易会优先被矿工处理。
- **节省 Gas 费的小技巧：**
  - 避开网络高峰（如 DeFi 热门事件时）。
  - 设置合理的 Gas 限制和价格。
  - 选择 Gas 费更低的链（如 Polygon、BSC）。

总结对比：链上 vs 交易所

对比项	链上交易	交易所交易
流程特点	去中心化，交易记录公开透明	中心化，依赖平台撮合
适用场景	适合购买新币种、去中心化理财	适合购买主流币种、大额交易
操作成本	需要支付 Gas 费	有交易手续费和提币费用
资产管理	完全掌握在自己手中	资产托管在交易所，需信任平台
风险	私钥保管不当风险高	平台被黑客攻击或跑路风险

2.1.8 建议

1. **日常小额交易+新币种：** 用链上交易，去中心化且灵活。
2. **大额交易+主流币：** 用交易所交易，方便且流动性好。
3. **安全优先：** 交易完后，提币到冷钱包长期保管。
4. **关注 Gas 费：** 及时查看链上拥堵情况，避免高峰时段交易。

2.2 系统学习区块链基础

2.2.1 区块链运行机制

区块链之所以能够安全运行，核心在于**共识机制**，也就是所有节点“如何达成一致”的规则。不同的区块链网络用不同的共识机制来决定谁能写入新数据。最经典的有 **POW（工作量证明）和 POS（权益证明）**，此外还有很多变种。下面简单解读这些机制的逻辑。

POW（工作量证明）——用算力说话

POW 就像“挖矿比赛”，矿工通过拼芯片的计算能力，算力解决数学题（哈希谜题），先解出来的人就有权写入新区块，并获得奖励（比如比特币）。

解出来的新区块有什么用?

简单来说，新区块的作用就是**记录所有交易和验证网络的合法性**，同时维护整个区块链的“账本”。可以把新区块想象成账本上的一页纸，上面记载了所有近期发生的交易。

再详细点解释：解出来的新区块的用处

1. **记录交易（账本更新）：**
    a. 比特币网络上，每当有人转账（比如小明给小红转 1 个 BTC），这个交易就会广播到全网。
    b. 矿工的任务是收集这些交易信息，验证是否有效（比如小明是否有 1 个 BTC），然后把有效的交易写进新区块。
    c. 解出新区块后，这个区块会成为区块链的一部分，永久记录交易信息。

比喻：区块就像账本的一页纸，矿工相当于会计师。只有解出新区块，交易信息才能正式记载在账本上并生效。

2. **维持网络安全（防止造假）：**
    a. POW 机制要求矿工通过大量计算（工作量）来竞争记账权，这种计算需要耗费电力和资源。
    b. 如果一个坏人想篡改某个区块，就得重新算出那一块之后的所有区块的哈希值，这需要巨大的算力，几乎不可能实现。

比喻：新区块像是一道锁，矿工解题是生成钥匙，只有正确的钥匙才能让新区块合法生效。解题难度高让坏人篡改的成本极高。

3. **发放矿工奖励（激励机制）：**
    a. 新区块被成功解出后，矿工会收到两部分奖励：
        i. **区块奖励：** 比如最初的比特币网络，每解一个新区块，矿工会获得 50 个比特币。这个奖励每隔约 4 年减半，现在是 6.25 个 BTC（2024 年）。
        ii. **交易手续费：** 区块中记录的每笔交易会附带少量手续费，矿工将收集这些费用作为额外奖励。

比喻：挖出新区块就像完成一项工作，矿工的工资就是比特币奖励和手续费。

总结：解出来的新区块解决了什么问题?

1. **记录了最新交易：** 把所有合法交易记到区块链上，成为账本的一部分。
2. **验证了交易合法性：** 通过矿工的计算和验证，确保区块链账本真实可信，防止伪造。
3. **提供了激励机制：** 矿工获得奖励，保障了整个网络持续运行。

换句话说，没有新区块，区块链网络就无法更新交易，也无法维持正常运行!

这就是新区块的重要性。

补充问题：为什么需要解题才能生成新区块?

解题 (哈希谜题) 是为了让生成新区块变得困难，保证每个新区块大约 10 分钟才生成一个 (比特币的设计目标)。如果生成区块太快，网络就容易被攻击，甚至失去价值。通过“挖矿难度”的动态调整，保证整个系统既安全又稳定运行。

怎么运行?

1. 矿工用计算机不停尝试解决一个复杂数学问题。
2. 谁先算出答案（工作量完成），谁就能添加新区块并获得奖励。
3. 其他节点验证这个区块的合法性后，将其加入区块链。

优点：

- 安全性高：芯片计算的算力集中，攻击成本高。
- 完全去中心化：任何人只要有算力都可以参与。

缺点：

- 耗能巨大：需要大量电力维持网络。
- TPS（每秒交易数）较低：交易速度慢。

代表： 比特币、以太坊 1.0（后来转为 POS)。

POS（权益证明）——用币权投票

POS 是“看谁币多”，谁的币多，谁就更有可能被选为记账者，成为记账的节点（在成为节点前需要把代币质押进去防止恶意行为)，可以产生新区块，相当于“持币者投票的竞争机制”。一旦智能合约发现节点出现——未能完成记账或者添加恶意未验证的交易进去，就会受到惩罚失去部分甚至全部的质押代币。

怎么运行?

1. 节点根据自己持有币的数量和时间“质押”代币。

2. 系统随机选出一个质押者来打包新区块，发放奖励。
3. 其他节点验证区块后完成交易记录更新。

优点：

- 节能环保：不需要大量计算力。
- 激励长期持币：减少抛售压力，稳定币价。

缺点：

- 币多者优势大：容易形成“富者恒富”局面。
- 去中心化弱化：少数大户可能控制网络。

代表： 以太坊 2.0、波卡、卡尔达诺（ADA）。

以太坊的模式及智能合约

1. 以太坊的模式：不仅仅是转账

如果比特币是区块链里的“电子黄金”（只能转账和存储价值），那么以太坊就是“区块链里的智能手机”。

它提供了一种平台，可以让开发者在链上部署各种“应用程序”（也叫去中心化应用，DApps）。

关键点：去中心化

这些应用不依赖传统的服务器，而是运行在全球成千上万的节点上，因此更难被关闭、篡改或攻击。

比喻：比特币像一个单一功能的计算器（只能加减法），而以太坊更像一部智能手机（可以运行各种 App，比如社交、游戏、交易）。

2. 智能合约：区块链上的“自动化程序”

智能合约是以太坊最核心的功能，简单来说，它是一种可以**自动执行的代码**，运行在以太坊区块链上。

它的作用是让交易或协议自动完成，无需人工干预或中间商。

特点：

1. **自动执行：**
   a. 一旦触发条件，代码会自动运行，不需要任何人批准。
   b. 例如，“如果你给我 1 个 ETH，我就把 NFT 转给你”——只要钱到了，NFT 就会自动转移。
2. **不可篡改：**
   a. 智能合约一旦部署，代码就被记录在区块链上，无法随意修改。
   b. **好处：** 增强信任。
   c. **坏处：** 如果代码有漏洞，黑客可能利用它，造成损失（比如之前的 DAO 事件）。
3. **去中心化：**
   a. 合约不依赖某个服务器或机构，而是运行在整个以太坊网络上，永不停机。

3. 以太坊与智能合约的实际应用

以下是以太坊和智能合约的一些实际应用场景：

① 金融领域：去中心化金融（DeFi）

通过智能合约，可以实现贷款、借贷、交易等功能。

- 比如用户可以在一个 DeFi 平台上借款，无需银行审批，抵押资产直接通过智能合约锁定。

② 数字资产：NFT（非同质化代币）

- 智能合约支持创建和交易 NFT，比如艺术品、游戏道具或虚拟土地。
- 每个 NFT 都是独一无二的，其所有权由智能合约记录。

③ DAO（去中心化自治组织）

- 通过智能合约，可以组建一种无领导的组织，所有规则都写在链上，按规则自动运行。
- 比如 DAO 成员投票决定如何花费组织资金，智能合约负责执行投票结果。

④ 游戏和虚拟世界

- 游戏开发者可以用智能合约制作完全去中心化的游戏，用户的虚拟资产真正属于自己，并可随时交易。

4. 以太坊的运行机制

以太坊的运行机制与比特币类似，但有些显著区别：

① 共识机制：POW → POS

- **过去：** 以太坊最初采用的是 POW（工作量证明）机制，类似比特币，通过矿工“挖矿”来确认交易。
- **现在：** 以太坊完成了“合并升级”（The Merge），转向 POS（权益证明）机制。
  - POS 不需要矿工竞争算力，而是让持有 ETH 的人质押资产参与验证，更节能环保。

② Gas 费：

以太坊交易需要支付 Gas 费，代表你使用网络资源的成本。Gas 费会根据网络繁忙程度动态变化，复杂的智能合约操作往往需要更高的 Gas 费。

5. 为什么智能合约和以太坊重要?

1. **打破传统限制：** 任何人都可以使用，以极低成本实现跨国交易和复杂协议。
2. **高度透明和安全：** 代码写在链上，大家都能看到。
3. **激发创新：** 以太坊是众多区块链应用的发源地，许多今天火爆的项目（比如 DeFi 和 NFT）都建立在以太坊上。

2.2.2 常见协议与标准

区块链上的代币其实就像一种特定规则下的数字资产。为了确保这些代币能够在同一平台上能够无缝交互，不同区块链设计了一些统一的标准。这些标准就像是一趟“语言规则”，让代币之间、代币和应用之间都能顺畅沟通。

常见的代币标准分为三类：**ERC20、TRC20 和 Solana** 的代币标准

1.ERC20（以太坊代币标准）

ERC20 是以太坊区块链上最常见的代币标准，可以看作是“以太坊上的通用代币模板”。

几乎所有运行在以太坊上的代币（比如 USDT、LINK 等）都基于 ERC20 标准。

ERC20 规定了代币应该具备的基础功能，例如：

- **查询代币总量：** totalSupply()

让大家知道这个代币一共发行了多少。

- **账户余额查询：** balanceOf(address)

让用户能查看某个地址的余额。

- **转账功能：** transfer(address, amount)

让用户可以直接发送代币。

- **授权转账：** approve() 和 transferFrom()

允许第三方应用或合约代替用户转账，比如在交易所充值。

ERC20 的意义：

ERC20 的统一规则让开发者无需从零设计代币逻辑，只需基于标准写智能合约，就能实现：

- **钱包兼容性：** 所有 ERC20 代币都能被以太坊钱包（如 MetaMask）支持。
- **轻松交易：** 在去中心化交易所（如 Uniswap）上，ERC20 代币可以快速上架交易。

2.TRC20（波场代币标准）

TRC20 是波场（TRON）区块链上的代币标准，与以太坊的 ERC20 非常相似。

为什么类似于 ERC20?

波场的设计初期参考了以太坊，因此 TRC20 基本复制了 ERC20 的规则和接口。TRC20 代币的基本功能（转账、余额查询、授权等）和 ERC20 几乎一模一样。

TRC20 的优势：

1. **高效率：** 波场网络采用的是 POS 共识机制，交易速度快，确认时间短。
2. **低成本：** TRC20 代币的转账手续费远低于以太坊网络 Gas 费。
    a. 比如 USDT 同时支持 ERC20 和 TRC20，很多用户更倾向于用 TRC20 转账，因为更便宜。

TRC20 的应用：

- 在波场网络上发行的 USDT 就是最著名的 TRC20 代币。
- 它也常用于游戏、博彩等 DApp 场景，因为交易快、费用低。

3.Solana 代币标准（SPL 标准）

Solana 的代币标准叫 SPL（Solana Program Library），是 Solana 区块链上的通用代币协议。

与 ERC20、TRC20 类似，SPL 标准规定了代币的基本功能，确保代币能在 Solana 网络上兼容使用。

SPL 的特点：

1. **超高速：**
   a. Solana 号称支持每秒处理数千笔交易（TPS），这是以太坊和波场远远无法企及的。
   b. 这意味着 SPL 代币的转账速度极快。
2. **低成本：**每笔交易的手续费通常不到 0.01 美元，适合高频交易和微交易场景。
3. **灵活性：**
   a. Solana 支持复杂的智能合约，可以用于 DeFi、NFT、游戏等多个领域。
   b. SPL 代币在这些场景中表现得尤为出色，比如著名的 Solana 生态 NFT 市场 Magic Eden。

SPL 的应用：

- **DeFi：** Solana 上的去中心化交易所（如 Raydium）广泛采用 SPL 代币。
- **游戏和 NFT：** Solana 生态中许多游戏和 NFT 项目都使用 SPL 代币作为奖励或交易媒介。

ERC20、TRC20 和 SPL 的对比总结

特性	ETH(ERC20)	TRX(TRC20)	Solana(SPL)
所属区块链	以太坊（Ethereum）	波场（TRON）	Solana
交易速度	慢（受网络拥堵影响）	快	极快
手续费	高（Gas 费）	低	极低
兼容性	应用广泛，支持多种钱包和平台	类似 ERC20，成本更低	高效生态，适合游戏和 NFT
常见应用	去中心化交易所、DeFi、NFT	跨境支付、游戏、稳定币	高频交易、NFT、链游、DeFi

2.2.3 区块链地址与交易

区块链地址和交易记录是区块链技术的核心部分。它们可以看作是你在区块链世界的“收款账号”和“账本记录”。以下从地址生成、用途到如何查询交易记录一一解读。

地址生成及用途

地址是什么?

区块链地址是一个类似“银行账号”的标识符，用于接收和发送数字资产。每种区块链（以太坊、波场、Solana 等）都有不同的地址格式。

地址是如何生成的?

生成区块链地址的过程一般涉及以下步骤：

1. **私钥生成：**
   a. 一个随机数通过加密算法生成私钥，私钥是你拥有资产的“钥匙”，绝对不能泄露。
2. **公钥生成：**
   a. 私钥通过椭圆曲线算法生成对应的公钥，公钥可以公开。
3. **地址生成：**
   a. 公钥再经过哈希处理，生成一个短一些、更方便使用的字符串，这就是区块链地址。

地址的用途：

- **接收资产：**
  - 比如朋友要给你转 ETH，他们需要知道你的以太坊地址。
- **发送资产：**
  - 转账时，需要输入目标地址。
- **查询资产：**
  - 地址关联的是链上的所有交易记录，可以公开查询余额和转账记录。

不同区块链地址的格式：

- **ERC20（以太坊）：**

地址以 0x 开头，后面是 40 个十六进制字符，例如：

0x4e6f7324e56a2F4dC356E12a486B37F9Dd98Bc60

- **TRC20（波场）：**

地址以 T 开头，例如：

TKNqGm3Dchng9b2nM4JpjVHZ59Wr5P9ZZp

- **Solana：**

地址由一串随机字母和数字组成，例如：

7SFG3n3kdyHCEvVmY5w9e2bAk8RtrnMsYZjQR9JovvhN

如何查询交易记录（通过区块链浏览器）

区块链浏览器是一个“公开账本查询工具”，你可以通过它查看地址的交易记录、余额、以及交易状态。不同区块链有自己的浏览器工具，以下分区块链介绍：

常用浏览器：

- **ERC20（以太坊）交易查询：**（https://etherscan.io）

  按回车后，你会看到：

  - 地址的余额（ETH 和其他 ERC20 代币）。
  - 交易记录：每笔交易的时间、发送方和接收方地址、金额、手续费等详细信息。

- **TRC20（波场）交易查询：**（https://tronscan.org）

  在搜索框输入你的波场地址（例如：TKNq...P9ZZp）。

  按回车后，你会看到：

  - TRX（波场主网币）的余额和交易记录。
  - TRC20 代币（如 USDT）的详细转账记录。

- **Solana（SPL 代币）交易查询：** Solscan（https://solscan.io）或者 Solana Explorer (https://explorer.solana.com)

  在搜索框输入你的 Solana 地址（例如：7SFG...vvhN）。

  你可以查看：

  - SOL 余额（Solana 主网币）。
  - SPL 代币（Solana 上代币）的转账记录，比如 USDC、NFT 交易等。

如果遇到一些交易信息，会出现多笔跨链、多笔追踪，这些基础浏览器使用起来并不是很方便，那么这个时候可能就会需要用到一些更高级的链上数据溯源工具，可以参考我们的链上溯源工具 MEME Catcher :https://pandaly.io/products/meme-catcher。

2.3 加密货币风险管理

必备基础

- 稳定币（USDT、USDC）与其用途
- 空气币的风险与识别方法

探索“黑暗数字森林”，有价值的“珍宝”（如比特币、以太坊）和危险的“陷阱”（如空气币）并存。需要了解基础概念和掌握风险管理方法，让你更安全、更自信！

2.3.1 稳定币：数字货币中的“定海神针”

稳定币是与现实世界的法定货币（如美元）挂钩的数字货币，它们价格稳定，常用作投资的“安全港”或交易中的“中间桥梁”。

常见的稳定币：

- **USDT（Tether）：**

最早的稳定币，市值最大，由美元储备支持。常见于各种区块链（ERC20、TRC20 等）。

- **USDC（USD Coin）：**

Coinbase 和 Circle 发行的稳定币，监管更严格，透明度较高。

用途：

1. **价值储存：**比如当市场波动剧烈时，将其他数字货币换成 USDT 或 USDC，锁定价值，避免资产缩水。
2. **便捷交易：**稳定币是交易所里常用的“交易对”货币，用于购买比特币、以太坊等。
3. **跨境支付：**稳定币可以跨国、快速、低成本转账，替代传统银行渠道。

风险提示：

- **信任风险：**稳定币的价值来源于发行方储备资产的支持。如果储备不足或管理不善，可能导致稳定币“脱锚”（价值不再等于 1 美元）。
- **合规性风险：**各国对稳定币的监管政策尚未统一，可能影响流通和交易。

2.3.2 什么是空气币？

空气币是一种没有实际价值、缺乏应用场景或技术支撑的加密货币。其发行方通常通过概念包装或市场炒作吸引投资者，但本质上是“空中楼阁”，甚至可能是彻头彻尾的资金盘骗局。

2.3.2.1 空气币的典型特征

1. **无实用价值**：项目白皮书往往充满夸张愿景，但没有清晰的技术落地方案，也缺乏实际应用或可行性技术。
2. **团队不透明**：团队成员身份模糊，无法查证真实履历，甚至可能使用假名或虚构经历。
3. **代币分布不合理**：项目方或内部团队掌控绝大多数代币，普通投资者难以公平获利。
4. **过度依赖营销**：项目主要通过社交媒体、KOL 造势，而非技术开发驱动，缺乏代码更新或实际应用进展。
5. **缺乏权威背书**：没有知名投资机构、行业合作伙伴或公信力审计机构支持。

6. **承诺高额回报**：以“零风险”“高收益”为噱头，吸引投资者入场，实则可能是庞氏骗局。

2.3.2.2 空气币的风险

- **价格崩盘**：由于没有实际价值支撑，价格容易被项目方或庄家操纵，导致短时间内暴跌。
- **资金受损**：投资者的资金可能被项目方转移，最终血本无归。
- **法律风险**：部分空气币项目可能涉及非法集资、诈骗等违法行为，投资者参与可能面临法律风险。
- **合规性问题**：许多空气币项目未进行任何法律合规性审查，一旦监管介入，投资者可能无法维权。

2.3.2.3 如何识别空气币?

1. **分析项目白皮书**

- 白皮书是否详细阐述了项目的技术方案、应用场景、经济模型?
- 是否只是大谈“改变世界”或“行业革命”，却没有技术细节?
- 如果连白皮书都没有，基本可以判定为骗局。

2. **查看项目实际进展**

- 是否有可用的产品或 MVP（最小可行产品）?
- 是否有真实的用户或合作伙伴，而非只是停留在 PPT 或概念阶段?

3. **验证团队背景**

- 核心团队成员是否可信? 在 LinkedIn 等平台是否能查到真实的行业履历?
- 是否有过成功的区块链项目经验?
- 是否有知名投资机构、行业合作伙伴的支持? 空气币项目通常会虚构不存在的合作伙伴。

4. **检查代币分布与流通**

- 代币分配是否合理? 如果 90% 以上的代币掌握在项目方手中，极可能是人为操控市场。
- 交易量是否真实? 是否存在“刷量”或“内循环交易”的迹象?
- **使用 MEME Catcher 地址分析**：查询代币的链上数据，例如持币地址是否过度集中，转账是否异常。

5. **审查安全性和代码审计**

- 是否有权威机构提供的代码审计报告?
- 是否有开源代码? 代码是否经常更新?
- 智能合约是否存在后门或漏洞?

6. **警惕“保本高收益”承诺**

- 合法投资不会承诺固定收益，特别是“每日返 10%”等超高回报承诺，几乎都是庞氏骗局。
- 查阅相关监管机构或社区的风险警示，避免陷入骗局。

如何实操审查一个加密货币是否是空气币?

1. **使用区块链浏览器分析链上数据**

- 在 Etherscan（以太坊）、BscScan（BSC）、OKLink 等区块链浏览器查询项目的智能合约地址，分析交易历史。
- 观察持币地址是否高度集中，是否存在异常大额转账或批量小额分发的情况。

2. **查阅审计报告**

- 通过 CertiK、SlowMist、PeckShield、Quantstamp 等知名安全审计平台，查看项目是否经过代码安全审计。
- 如果项目未经过任何审计或仅提供“伪审计报告”，需保持警惕。

3. **调研社交媒体和社区互动**

- 访问 Twitter、Reddit、Discord、Telegram，查看项目方的互动是否真实。
- 关注 GitHub 代码更新情况，判断开发是否活跃。
- 留意是否存在大量刷赞、机器人评论或删评的情况。

4. **充分利用 Web3 安全工具**

可以使用链捕手（ChainCatcher）提供的 Web3 工具导航，筛选行业内主流的安全工具：**https://www.chaincatcher.com/toolNav**

结论：在投资任何加密项目前，一定要做好充分的调查，避免成为空气币骗局的受害者。

2.3.3 风险管理

了解常见骗局：钓鱼网站、假项目方、假空投与空投钓鱼、假 OTC 交易骗局、假 KOL/假投资顾问骗局。

2.3.3.1 钓鱼网站（Phishing Scam）

骗局手法

伪造项目官网、钱包、交易所网站，引导用户输入助记词或私钥，盗取资产。

通过搜索引擎广告投放虚假网站（Google、Bing 等），使用户误入。

伪装成官方客服或管理员，在社交媒体、Telegram、Discord 等渠道发布恶意链接。

真实案例：Uniswap 伪造网站（2021）

2021 年，黑客通过 Google Ads 投放假的 Uniswap 网站广告，用户点击后进入一个与官网几乎一模一样的网站。

该网站诱导用户连接钱包，并要求进行一次授权交易（Approve），结果黑客立即转走了用户所有资产。

仅在短短几周内，该骗局导致超过 800 万美元的资产被盗。

如何防范

✓ **访问官网前核实域名**（推荐使用 Bookmark 收藏官方地址）。

✓ **开启钱包防钓鱼功能**（如 Metamask 的 **Phishing Detection**）。

✓ **不在陌生网站输入私钥或助记词**，官方团队不会索取此类信息。

✓ **验证官方社群链接**，使用 Twitter、Discord 官方认证标志核对身份。

2.3.3.2 假项目方（Fake Projects / Rug Pull）

骗局手法

发布精美白皮书，伪造知名团队背景，夸大合作伙伴关系。

通过 KOL 或名人营销（部分为付费推广），营造项目热度。

预售大量代币，吸引投资者后，迅速抛售代币（Rug Pull）。

伪造交易深度，通过机器人做市，制造“流动性良好”的假象。

真实案例：Squid Game（SQUID）币骗局（2021）

受《鱿鱼游戏》影响，SQUID 代币迅速走红，短短几天内价格从几美分涨至 2,800 美元。

项目方在高点突然撤走所有流动性，网站、社交媒体全部关闭，投资者无法卖出手中的代币。

最终，项目方卷走超过 **300 万美元**，并通过 Tornado Cash 混币服务洗白资金。

如何防范

✓ **查询团队背景**，通过 LinkedIn、GitHub、Twitter 查验是否真实存在。

✓ **检查代码开源情况**，是否提供智能合约审计（如 CertiK、SlowMist）。

✓ **分析代币分配**，如果大部分代币掌握在项目方或单一地址，风险极高。

✓ **使用链上工具检测风险**，如 Etherscan、Dune Analytics，查看大额地址是否异常转账。

2.3.3.3 假空投与空投钓鱼（Airdrop Scam）

骗局手法

在钱包地址上空投伪造代币，引导用户点击特定 DApp 或交互合约，授权盗取资产。

发送“官方”通知，要求用户连接钱包领取空投，实际是恶意合约。

真实案例：Fake MetaMask Airdrop（2022）

2022 年，大量用户在钱包中发现“MetaMask 官方空投”，引导他们到一个钓鱼网站领取奖励。

该网站要求用户签署交易，实际上是授予黑客完全的资金控制权限。

仅在短短几天内，该骗局导致超过 **500 万美元**的资产被盗。

如何防范

✓ **不要点击陌生代币的交互链接**，可在 Etherscan 手动隐藏可疑代币。

✓ **使用“Revoke”工具撤销钱包授权**，如 Revoke.cash 或 Debank。

✓ **官方空投通常不会主动联系你**，请到官方渠道核实是否真实存在。

2.3.3.4 假 OTC 交易骗局

骗局手法

在社群发布低价出售 USDT 等资产的信息，引诱用户私下交易。

伪造转账截图或假汇款信息，让用户误以为交易完成。

使用智能合约欺诈，如“闪电贷”方式操纵交易对手的资产。

真实案例：Telegram USDT OTC 诈骗（2022）

诈骗者在 Telegram 群里以 5%-10% 的折扣出售 USDT，吸引投资者通过 P2P 交易。

受害者转账后，骗子提供假冒的汇款截图，或直接拉黑受害者。

由于没有智能合约保障，受害者很难追回资产，诈骗金额累计超过 **2000 万美元**。

如何防范

✓ **使用可信 OTC 平台**，避免私下交易，确保交易流程受智能合约保护。

✓ **不要轻信“超低价格”**，市场价格不会无缘无故出现大额折扣。

✓ **收到款项后，务必确认资金已到账**，避免被撤回交易。

2.3.3.5 假 KOL/假投资顾问骗局

骗局手法

冒充知名 KOL 或投资机构，在 Telegram、Twitter、Discord 等社交平台推广空气币项目。

伪造明星或企业背书，如“XX 基金已投资”、“马斯克点赞”等虚假消息。

创建“内部交流群”，承诺短期高收益，引导投资者入场后抛售。

真实案例：Bitconnect 庞氏骗局（2016-2018）

Bitconnect 号称“自动交易机器人”，承诺每天 **40% 收益**，吸引全球投资者。

通过 KOL 推广、大型线下大会，形成“传销”式发展模式。

2018 年，Bitconnect 被美国 SEC 调查，最终崩盘，投资者损失超过 **25 亿美元**。

如何防范

✓ **检查社交账号认证标志**，避免关注假冒账号。

✓ **不要盲目信任 KOL 推荐**，很多 KOL 是收钱推广，并不代表项目可靠。

✓ **查验投资机构信息**，通过官网或链上数据核实是否真实参与。

2.3.4 如何应对黑天鹅事件

2.3.4.1 什么是黑天鹅事件?

黑天鹅事件具有以下特征：

难以预测：如 2020 年 3 月疫情导致 BTC 短时间内暴跌 50%。

影响巨大：例如 FTX 交易所倒闭，导致市场市值蒸发数千亿美元。

事后"合理化"：发生后人们往往能找出"合理"解释，但在事前难以预见。

历史上的黑天鹅事件：

时间	事件	BTC 影响
2013 年 4 月	Mt.Gox 交易所崩溃	-70%
2017 年 9 月	中国全面禁止 ICO	-40%
2020 年 3 月	新冠疫情爆发	-50%
2022 年 5 月	LUNA 崩盘	-35%
2022 年 11 月	FTX 破产	-25%

2.3.4.2 BTC 暴跌时的心理应对

认清市场周期，避免情绪化交易

市场是周期性的，暴跌通常是牛熊转换的结果，**不要因为短期恐慌而割肉。**

牛市 FOMO（害怕错过） 导致追高，暴跌时容易恐慌性抛售。

熊市 FUD（恐惧、不确定性、怀疑） 让人误以为 BTC 归零，从而错失低价买入机会。

应对策略：

✓ **保持冷静，不做情绪化交易**（牛市不贪，熊市不慌）。

✓ **回顾历史数据**，过去 BTC 也经历过多次暴跌，最终仍然创新高。

✓ **设定止盈止损策略**，避免暴跌时被恐惧控制。

确保资产安全，减少交易所风险

黑天鹅事件往往伴随着交易所暴雷，例如 FTX 破产后，用户无法取回资产。

应对策略：

✓ **分散存储资产**：长期持有的 BTC 放在 **冷钱包（如 Ledger、Trezor）**，交易资金放在 CEX 或 DeFi 钱包。

✓ **避免 All In 单一交易所**：使用多个交易所，如 Binance、OKX、Kraken，减少单点风险。

✓ **关注链上数据**：如 FTX 破产前，链上数据显示大额资金出逃，提前预警。

设定预案，避免暴跌时的非理性决策

市场暴跌时，许多人会 **割肉止损**，但历史证明，BTC 过去十年几乎每次暴跌后都能恢复。

应对策略：

✓ **提前制定"暴跌计划"**：设定跌幅到某个点时是否补仓、止损，避免临时决策。

✓ **采用分批买入策略（DCA）**：即便 BTC 继续下跌，仍能降低成本。

✓ **关注主流机构的操作**：如 MicroStrategy 在 BTC 暴跌时仍继续增持。

2.3.4.3 BTC 暴跌时的操作策略

短线交易策略

如果是短线投资者，可以通过技术分析和市场情绪判断 BTC 可能的底部：

支撑位买入，阻力位卖出：在历史支撑位（如 200 周均线）挂单买入，反弹时逐步卖出。

监测恐慌指数（Fear & Greed Index）：极端恐惧时往往是买入机会，极端贪婪时则需谨慎。

关注期货市场的资金费率：如果费率极度负值，代表市场过度看空，可能触发反弹。

示例策略：

BTC 触及 200 周均线（如 $20,000），买入 50% 资金。

如果继续下跌 10%（如 $18,000），再买入 25%。

如果再次跌破前低（如 $15,000），观察链上数据决定是否继续买入。

长线投资策略

对于长期持有者（HODLer），BTC 暴跌可能是一个 **加仓机会**，但需要控制风险：

定投策略（DCA，Dollar-Cost Averaging）：不管市场涨跌，每周或每月定期买入 BTC，平滑成本。

关注链上数据：如 MVRV 指标（市场价值/链上价值），当 MVRV <1 时，通常是买入机会。

避开杠杆：长期持有 BTC，切忌使用杠杆，防止爆仓清零。

示例策略：

2020 年 3 月 BTC 从 $10,000 暴跌至 $3,800，如果分批买入并持有至 2021 年牛市，最高可达 **$69,000**，回报超 **15 倍**。

2022 年 FTX 事件 BTC 从 $21,000 降至 $15,500，如果按照 DCA 策略买入，2023 年 BTC 反弹至 **$45,000**，收益翻倍。

2.3.4.4 黑天鹅事件的风险管理

在市场极端波动时，除了交易策略，良好的**风险管理** 是生存的关键。

✓ **预留 30%-50% 现金仓位**，避免资金全在市场，导致暴跌时无法补仓。

✓ **使用稳定币（USDT/USDC）做对冲**，可在熊市中转换部分资产到稳定币，降低波动性。

✓ **提前设定止损/止盈点**，如 20% 止损，50% 止盈，确保在剧烈波动中不会被情绪左右。

✓ **降低杠杆，避免爆仓**，在剧烈波动时，杠杆交易极易被清算，不要在极端行情下加仓杠杆。

✓ **分散投资**，如 BTC、ETH、蓝筹 DeFi 项目，不要重仓单一资产。

2.3.4.5 总结

如何在黑天鹅事件中生存?

保持冷静，不要被市场情绪影响，避免恐慌性卖出。

制定清晰的交易策略，无论短线还是长线，提前设定计划，避免临时决策。

分批买入，分散风险，不要一次性 All in，采用 DCA 策略降低成本。

避免杠杆和合约交易，市场极端波动时，杠杆交易极易爆仓。

保障资产安全，分散存放，减少交易所风险。

黑天鹅事件是币圈的常态，真正的赢家是那些 **冷静分析、提前布局，并坚守策略** 的人。

2.4 玩转 Web3：实际操作篇

Web3 世界提供了更加开放、去中心化的金融体系，但也伴随着较高的技术门槛和安全风险。这里将介绍 Web3 的基础操作，包括 **去中心化钱包、DEX 交易、流动性提供、热门赛道的参与策略**，帮助用户更安全、高效地探索 Web3。

2.4.1 去中心化钱包使用

去中心化钱包是进入 Web3 世界的必备工具，它不仅用于存储资产，还可以连接 DeFi、NFT、GameFi 等 DApp 生态。

1. **主流钱包推荐**

以下是几款常见的去中心化钱包：

钱包名称	特点	支持链
MetaMask	适合以太坊生态，兼容 EVM 链	ETH、BSC、Polygon、Arbitrum 等

Trust Wallet	移动端友好，多链支持	BTC、ETH、BSC、SOL、TRX 等
Rabby Wallet	专为 DeFi 设计，增强安全	ETH、BSC、Polygon、Arbitrum 等
Keplr Wallet	Cosmos 生态专用	ATOM、Osmosis 等
Phantom	Solana 生态专用	SOL、USDC、NFT 等

选择建议：

- 主要玩 **DeFi 和 NFT** 的用户，推荐 **MetaMask** 或 **Rabby**。
- 需要更强的移动端体验，可以选择 **Trust Wallet**。
- **Solana 生态用户** 建议使用 **Phantom**。
- **Cosmos 生态用户** 推荐 **Keplr**。

2. **助记词备份与防盗技巧**

助记词（Mnemonic Phrase） 是 Web3 钱包的核心，类似于银行账户的"主钥匙"。

一旦助记词泄露，资产可能被完全盗走！

助记词备份建议：

✓ **离线存储**：写在纸上，避免截图或存入云端。

✓ **物理备份**：用 **金属助记词牌**（如 Cryptosteel）防火、防水保存。

✓ **拆分存储**：将助记词拆成 2～3 份，分别存放不同地方。

✓ **不要输入在陌生网站**：**所有要求输入助记词的网站都是诈骗！**

常见钱包盗币手法：

- **钓鱼网站**：假冒 Uniswap、Opensea，诱导输入助记词。
- **假钱包 App**：下载来源不明的钱包，被植入后门。
- **空投骗局**：收到未知 Token，点击授权后资产被转走。

预防措施：

✓ **安装钱包前，检查官网 URL**（如 MetaMask 仅从 metamask.io 下载）。

✓ **不随意授权陌生合约**，定期使用 Revoke.cash 撤销权限。

✓ **使用硬件钱包（Ledger、Trezor）**，防止私钥被盗。

2.4.2 去中心化交易所（DEX）

DEX（去中心化交易所） 让用户在无须中介的情况下自由交易资产，并可提供流动性赚取收益。

1. **Uniswap / PancakeSwap 基础操作**

- **Uniswap（基于 ETH 生态）**
- **PancakeSwap（基于 BNB Chain）**

基础操作步骤：

1 进入 Uniswap（https://app.uniswap.org）或 PancakeSwap（https://pancakeswap.finance）。

2 连接钱包（MetaMask / Trust Wallet）。

3 选择要交换的代币（如 USDT → ETH），输入金额。

4 设置**滑点**（Slippage），通常 0.5%-1%，防止价格变动。

5 确认交易，等待链上完成（ETH 需支付 Gas 费）。

注意事项：

✓ **检查 Token 合约地址**，防止交易假币（可用 CoinGecko / Etherscan 查验）。

✓ **避免流动性低的代币**，交易时可能因滑点过大导致亏损。

✓ **跨链交易** 需要使用桥接（Bridge），如 Binance Bridge、Stargate。

2. **如何提供流动性（Liquidity）并获取收益**

在 DEX 提供流动性（LP）可以赚取交易手续费，但也有**无常损失**（Impermanent Loss）风险。

流动性提供步骤（以 Uniswap 为例）：

1 选择要提供流动性的交易对（如 ETH/USDT）。

2 进入 **Uniswap "Pool"** 页面，点击 "Add Liquidity"。

3 输入等值的两种代币（如 1 ETH + 2000 USDT）。

4 确认交易，获取 LP 代币（表示你的流动性份额）。

5 赚取交易手续费，LP 代币可随时赎回。

流动性挖矿收益计算：

- **交易手续费收益**（如 Uniswap V3 0.3% 费率）。
- **流动性挖矿奖励**（部分平台会额外奖励代币）。
- **无常损失风险**（如果某个代币价格剧烈波动，可能亏损）。

适合提供流动性的资产：

✓ **稳定币对（USDT/DAI、BUSD/USDC）**，低风险、低收益。

✓ **蓝筹币对（ETH/WBTC、BNB/USDT）**，收益高，但有无常损失风险。

2.4.3 参与热门赛道

Web3 的核心赛道包括 **NFT、DeFi、Meme 币**，但每个赛道的风险不同，参与前需做好研究。

1. **NFT：数字收藏品及交易平台**

- **NFT 代表数字资产所有权**，主要用于艺术、游戏、会员通行证等。
- **交易平台：**
  - **OpenSea**（ETH、Polygon、Solana 生态）
  - **Blur**（专业 NFT 交易者）
  - **Magic Eden**（Solana 生态）

操作步骤：

1 连接钱包到 OpenSea / Blur。

2 选择 NFT 项目，查看 **地板价、持有者分布、交易量。**

3 购买 NFT，支付 Gas 费。

NFT 交易注意事项：

✓ **避免 FOMO 追高**，NFT 价格波动大。

✓ **检查蓝筹项目**（如 BAYC、Azuki）是否有大资金持仓。

✓ **关注公链生态**，如 Solana NFT 在 Magic Eden 交易量更高。

2. **DeFi：流动性挖矿与稳定币借贷**

- **流动性挖矿**：AAVE、Compound、Curve 提供存款赚利息。
- **稳定币借贷**：USDT、DAI 可用于抵押借贷。

示例：

✓ **在 AAVE 存入 USDT**，赚取 4%～8% 年化收益。

✓ **抵押 ETH 借 USDC**，用于其他投资（注意清算风险）。

3. **Meme 币：小额高风险投资**

- **Meme 币（如 DOGE、SHIB、PEPE）** 主要靠社群驱动，投机性强。
- **参与策略**：
  - **小仓位**（不超过 5% 资产）。
  - **早期入场，涨幅过大及时止盈。**
  - **观察链上数据**，避免被项目方砸盘。

2.5 常用工具与资源

Web3 生态庞大，想要准确获取**链上数据、市场行情、投资情报**，需要掌握一些高效的工具和资源。本节将介绍**区块链浏览器、加密数据平台、学习资源**等，帮助用户更精准地做出投资决策。

2.5.1 区块链浏览器

区块链浏览器（Blockchain Explorer）是追踪链上交易、钱包资产、智能合约的核心工具。

1. 主流区块链浏览器

以下是几大公链的常用浏览器：

区块链	浏览器	网址
以太坊（Ethereum）	Etherscan	https://etherscan.io/
BNB Chain	BscScan	https://bscscan.com/
Polygon（MATIC）	PolygonScan	https://polygonscan.com/
Arbitrum	Arbiscan	https://arbiscan.io/
Solana	Solscan	https://solscan.io/
Bitcoin	Blockchain.com Explorer	https://www.blockchain.com/explorer

2. 区块链浏览器的常见用途

查询钱包地址（查看资产、历史交易）

跟踪交易状态（是否确认/失败、Gas 费用）

分析代币合约（查验是否为官方合约）

监控鲸鱼钱包（跟踪大户买卖动向）

使用示例：

查看钱包资产：

1.访问 **Etherscan**

2.在搜索栏输入钱包地址（如 0x...）

3.点击 “Token Holdings” 查看余额

查询某笔交易状态：

1.在 Etherscan 搜索交易哈希（Tx Hash）

2.检查交易状态（Success / Pending / Failed）

3.查看 Gas 费、交易详情

检查代币是否真实:

1.在 **CoinGecko / CoinMarketCap** 找到代币合约地址

2.在 **Etherscan/BscScan** 搜索该合约

3.确认持币地址分布，避免遇到假币骗局

2.5.2 加密数据平台

获取最新市场动态、币种信息、投资者情绪是投资决策的关键，以下是常用的**数据分析平台。**

2.5.2.1 主流市场数据平台

平台	功能	网址
CoinMarketCap	币种市值、交易量、历史数据	https://coinmarketcap.com/
CoinGecko	项目基本面、社交数据	https://www.coingecko.com/
CryptoQuant	链上数据分析（大户流动）	https://cryptoquant.com/
Glassnode	比特币、以太坊链上指标	https://glassnode.com/
Dune Analytics	自定义区块链数据查询	https://dune.com/
Nansen	智能资金流向分析	https://www.nansen.ai/

如何使用这些工具?

✓ **CoinMarketCap / CoinGecko**：查看币种价格、市值、历史走势

✓ **CryptoQuant / Glassnode**：分析比特币、以太坊链上资金动向（如矿工抛售、交易所流入）

✓ **Nansen**：追踪 VC、大户钱包买卖动态

✓ **Dune Analytics**：查询 DeFi 项目 TVL、用户增长情况

使用示例:

判断市场情绪（BTC、ETH 资金流向):

- 打开 **CryptoQuant**
- 观察 BTC 交易所存量（Exchanges Reserve）

- **上升**：大量 BTC 进入交易所，可能有抛售风险
- **下降**：BTC 退出交易所，长期持有（看涨信号）

查找潜力项目：

- 在 **Dune Analytics** 搜索热门 DeFi 项目（如 Uniswap、AAVE）
- 观察 TVL（总锁仓量）、活跃用户数量，判断是否值得参与

2.5.3 学习资源

币圈信息瞬息万变，想要紧跟行业动态，必须掌握优质的学习资源，包括**社交媒体、论坛、博客、视频教程**等。

2.5.3.1 Twitter（X）— 加密社区的核心

Twitter 是加密圈最活跃的平台，项目方、投资机构、KOL 都在这里发布信息。

✓ 关注行业大佬：

- **CZ Binance**（@cz_binance）- 币安创始人
- **Vitalik Buterin**（@VitalikButerin）- 以太坊创始人
- **Arthur Hayes**（@CryptoHayes）- BitMEX 创始人
- **Messari**（@MessariCrypto）- 加密研究机构

✓ 关注数据分析账户：

- **Lookonchain**（@lookonchain）- 鲸鱼资金流追踪
- **Nansen**（@nansen_ai）- 智能链上分析

✓ 关注 Meme 文化：

- **Elon Musk**（@elonmusk）- DOGE 相关动向

2.5.3.2 Reddit / Discord — 社区交流

- **Reddit r/cryptocurrency**（https://www.reddit.com/r/cryptocurrency/）- 讨论热点新闻、项目分析
- **Reddit r/ethtrader**（https://www.reddit.com/r/ethtrader/）- 以太坊交易讨论
- **各大项目 Discord**（如 Uniswap、AAVE）- 第一时间获取官方公告

2.5.3.3 YouTube / Web3 博主

- **Bankless**（DeFi、NFT、L2 生态）

- **Coin Bureau**（项目测评、投资策略）
- **DataDash**（加密市场分析）
- **a16z Crypto**（Web3 VC 观点）

学习建议：

✓ **新手可从 Coin Bureau 入手**（通俗易懂）

✓ **想深入研究 DeFi，可关注 Bankless**

✓ **每天花 10 分钟浏览 Twitter，了解市场热点**

2.6 安全小贴士

币圈的投资机会与风险并存，除了赚钱能力，**保护资产安全**更是生存的关键。本节将介绍密码学基础、防诈骗技巧以及钱包安全管理，帮助你在 Web3 世界中立于不败之地。

2.6.1 密码学基础：理解私钥的重要性

私钥（Private Key）是什么?

私钥是你的**区块链账户的唯一控制权**，掌握私钥就意味着掌握资产。

公钥 vs。 私钥

- **公钥**（Public Key）：公开的地址，别人可以用来向你转账
- **私钥**（Private Key）：类似银行密码，绝对不能泄露

助记词（Mnemonic Phrase）是什么?

助记词（12/24 个单词）是私钥的另一种表达形式，可以用来恢复钱包。

！ 丢失私钥 = 丢失资产，无法找回!

✕ **交易所不会索取你的私钥**，任何要求你提供私钥或助记词的行为都是骗局!

安全建议：

✓ **私钥离线存储**：写在纸上，保存在保险柜

✓ **不截图、不存云端**（Google Drive、iCloud）

✓ **使用硬件钱包**（Ledger、Trezor）

2.6.2 防止被骗：常见骗局解析

2.6.2.1 钓鱼网站 & 假钱包

骗子会创建**伪造的 MetaMask、Trust Wallet 网站**，诱导你输入助记词，导致资产被盗。

防范技巧：

- 访问官网**https://metamask.io/**，避免谷歌搜索误入假网站
- **不输入私钥或助记词**到任何网页
- **检查网址 HTTPS**，防止钓鱼攻击

2.6.2.2 伪装成客服或技术支持

骗子会冒充 Binance、MetaMask、Ledger 官方人员，在 Telegram、Discord 上联系你，要求你提供钱包信息。

防范技巧：

- **官方不会私信你！**任何私信都可能是骗局
- 在官方渠道（官网、推特）寻找客服支持
- **不点击陌生人的远程协助链接**

2.6.2.3 “免费空投”骗局

你会收到陌生钱包转来的“免费代币”，但当你去某个网站“领取奖励”时，系统会提示你签署一份交易，而这笔交易其实是**授权骗子转走你的所有代币！**

防范技巧：

- **不随便领取陌生代币**，尤其是**未知来源的 NFT 或空投**
- 使用 Etherscan 的 **Revoke Tool** 检查钱包授权状态
- **拒绝签署可疑合约**，如果不懂合约内容，就不要操作

2.6.2.4 假 KOL & “内幕群”

骗子假装成推特 KOL、大 V，宣传“稳赚不赔”的投资机会，引导你加入 VIP 群，在群里兜售骗局项目。

防范技巧：

- **DYOR（Do Your Own Research）**：不轻信 KOL，自己查项目信息
- **警惕承诺高回报的投资**，币圈没有“稳赚”
- **避免社交工程骗局**，骗子可能冒充你的朋友、知名人物

2.6.3 定期检查钱包安全性

1. 使用硬件钱包（冷钱包）

如果你持有**大额资产**，建议使用硬件钱包（Ledger、Trezor）离线存储，防止黑客入侵。

2. 启用多重签名（Multi-Sig）

多重签名（如 Gnosis Safe）可以要求**多个地址批准交易**，增加安全性。

3. 定期检查授权（Revoke 过期合约）

你可能在 DeFi、NFT 平台授权过钱包访问权限，但一些**恶意合约**可以随时提取你的资金。

✓ **使用 Revoke.tools 或 Etherscan 的 Token Approval 页面**检查授权情况。

✓ **移除不再使用的合约授权**，防止资产被盗。

2.6.4 总结

- **私钥和助记词**一旦泄露，资产无法找回
- **不点击陌生链接、不信免费空投、不加陌生群**
- **使用硬件钱包、多重签名，定期 Revoke 授权**

Web3 世界机遇无限，但安全第一，保护好你的资产才能笑到最后！

三、加密货币常见骗局

在这一部分，我们将带你走进币圈的迷雾，揭开那些层出不穷的骗局的面纱。我们不仅会深入分析这些骗局的特点，还会结合真实案例，帮助你快速识别并规避风险。

无论你是刚刚入场的“小白”，还是在币圈摸爬滚打多年的“老玩家”，总会有疏忽和大意的时候。但只要你了解得更多，眼光更敏锐，留意项目间的相似之处，便能为自己的资产增加一道保护屏障，避免落入不法分子的圈套。

事不宜迟，让我们从币圈最经典的骗局——**资金盘**说起，看看它是如何一步步诱骗投资者的。

3.1 资金盘骗局——什么是资金盘?

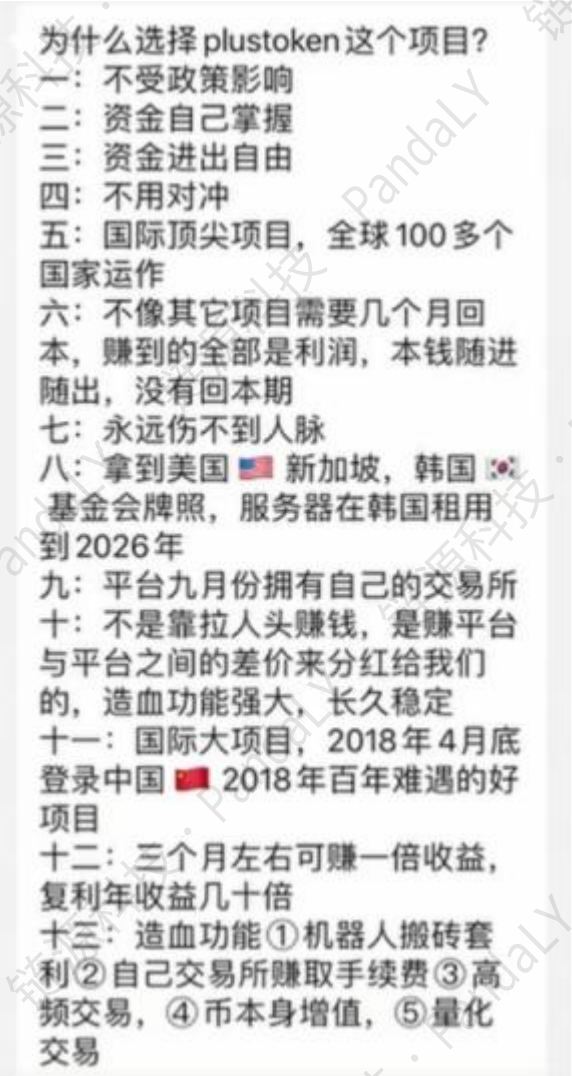
资金盘本质上是一种**庞氏骗局**，其运作方式与传统传销如出一辙，依靠新资金填补旧资金的缺口，最终形成一个不可持续的资金循环。

3.1.1 运作模式

1. **营造高大上的外衣**
   a. 通过包装豪华网站、线下聚会、赠送福利、免费旅游等手段，吸引投资者入局。
   b. 夸大宣传项目盈利模式，承诺**“高额回报”“稳赚不赔”**，吸引新资金流入。
2. **利用“人头奖励”机制**
   a. 投资者不仅能从自己的资金收益中获得回报，还能通过拉人头赚取佣金。
   b. 参与者发展下线，每拉一个人都会获得奖励，拉得越多，收益越高。
   c. 这种模式鼓励投资者疯狂拉新，形成金字塔式结构。
3. **初期制造“暴富”假象**
   a. 早期投入的用户确实会收到收益，让他们误以为项目真实可靠。
   b. 这些“成功案例”会被大肆宣传，进一步吸引更多人入场。
4. **崩盘跑路**
   a. 当项目方吸引足够多的资金后，往往会突然关闭网站、转移资金，投资者血本无归。
   b. 这类骗局的终点，往往是资金链断裂，受害者遍地。

3.1.2 典型案例：PlusToken

PlusToken 是币圈史上最著名的资金盘骗局之一，席卷**超过 10 亿美元**的加密资产，受害者遍布全球。



(图 1 PlusToken 微信群宣传文案)

3.1.2.1 骗局剖析

1. **打造“高端”形象**
   a. 2018 年 5 月 1 日，**PlusToken 网站（www.plToken.io）**正式上线。
   b. 项目方成立“**盛世联盟社区**”市场推广团队，利用互联网广告、线下会议、演唱会、旅游等方式疯狂宣传。
   c. 高调宣称其平台是“**国际顶级加密货币投资项目**”，并且拥有一项“**智能狗搬砖**”功能，号称可以在不同交易所之间**自动套利、稳赚不赔。**
2. **利用专业术语迷惑投资者**
   a. 由于“搬砖套利”听起来专业而神秘，许多人对其运行原理一知半解，便轻易相信。
   b. PlusToken 还聘请了一名湖南籍的年轻外国人，将其包装成“**联合创始人**”和“**谷歌高级工程师**”，提升可信度。
   c. 甚至让该外国人参加 2018 年 10 月日内瓦的世界数字经济论坛，增加“官方背书”光环。
3. **大规模营销**

a. 项目方投放纽约时代广场广告，制造国际影响力。
b. 微信群、社交媒体铺天盖地推广，营造一种“**身边人都在赚**”的氛围，刺激用户 FOMO 情绪（害怕错过）。
c. 截至崩盘前，已有 **269 万人**注册，每人支付 **500 美元** 开启“智能狗搬砖”功能，仅手续费就收割 **10 亿美元。**

4. **资金盘的真实运作**
   a. **初期**：项目方用后加入者的资金支付前期用户的“收益”，制造赚钱假象。
   b. **中期**：疯狂吸引更多投资者进场，并鼓励他们“复投”。
   c. **后期**：项目方设置提币限制，手续费高达 **5%**，进一步捆绑用户资金。
   d. **崩盘**：2019 年，项目方卷款跑路，导致无数投资者血本无归。

3.1.2.2 总结

✓ **不要相信“稳赚不赔”的投资项目** —— 任何高收益必然伴随高风险。

✓ **避免“拉人头”模式** —— 金字塔骗局的终点，往往是项目方跑路，投资者受害。

✓ **警惕无法验证的“黑箱”盈利模式** —— 真正的套利策略不会轻易向公众开放，尤其是“智能狗搬砖”这类模糊概念。

骗局破灭：神话终结，灰飞烟灭

纸终究包不住火，骗局的烈焰熄灭后，留给投资者的只有一地飞灰。

2019 年 6 月 27 日，PlusToken 以“区块链网络拥堵”为借口，悄然关闭提币通道，只留下充值窗口继续收割最后一批韭菜。对于那些沉浸在暴利幻象中的人来说，谁会想到这正是项目方准备跑路的信号？

当用户发现自己无法提现时，才终于意识到，“智能狗搬砖”从头到尾就是一个彻头彻尾的谎言。所有资金并未进行任何套利，而是直接流入了项目方的私人口袋，账户余额增长的数字，不过是自欺欺人的一串代码罢了。

这场骗局横行币圈近两年，最终在 2020 年 11 月 19 日迎来彻底崩盘。据苏州瑞亚会计师事务所统计，截至 2019 年 6 月 27 日，PlusToken 共计骗取了：

- 314,211 枚比特币（BTC）
- 117,450 枚比特现金（BCH）
- 96,023 枚达世币（DASH）
- 110 亿枚狗狗币（DOGE）
- 1,847,674 枚莱特币（LTC）
- 9,174,201 枚以太坊（ETH）
- 9.28 亿枚瑞波币（XRP）

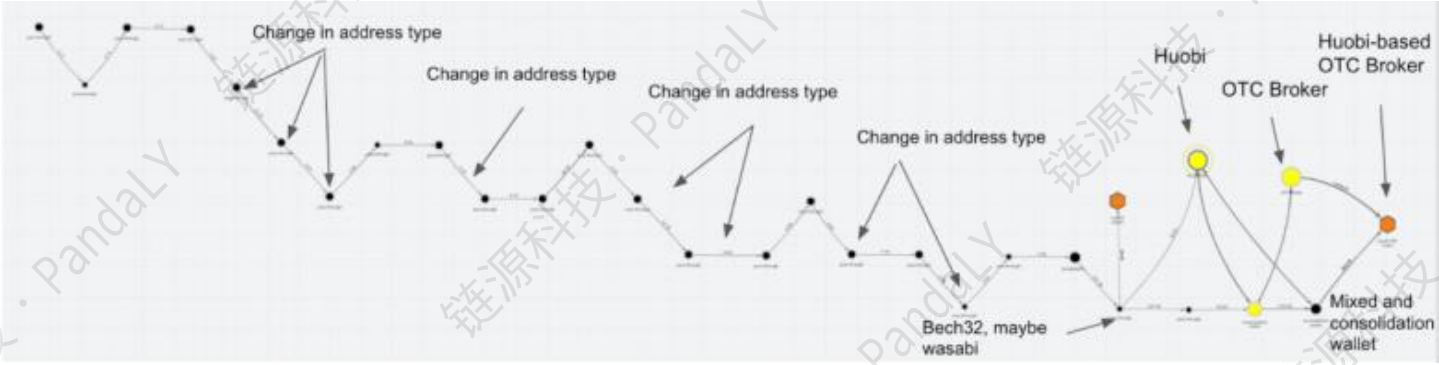
如果按照如今的市场价计算，这笔资金的规模，足以撼动整个加密市场。

资产转移：洗钱的黑暗路径

这些巨额加密资产的去向如何？314,211 枚 BTC 中，至少有 25,000 枚 BTC 的踪迹至今无法追踪。尽管区块链具有公开透明的特性，但骗子们并非毫无准备，他们使用了**混币器（如 Wasabi Wallet）**，借助 **CoinJoin 协议**将大额资金拆分成零散的小额交易，分散流入多个地址，以此掩盖资金来源。

尽管混币技术无法完全抹去交易痕迹，但它大大增加了追踪难度和成本。根据区块链数据分析公司 **Chainalysis** 的报告，PlusToken 的资金最终大部分流入了**火币（Huobi）上的 OTC 场外交易商**。这些 OTC 渠道的身份验证（KYC）要求较低，为骗子提供了变现的机会。

下图展示了 Chainalysis 对 PlusToken 资金流向的分析——从左上角的钱包开始，资金逐步向右扩散，对角线移动代表地址类型的变化，而垂直移动则表明混币技术的介入。

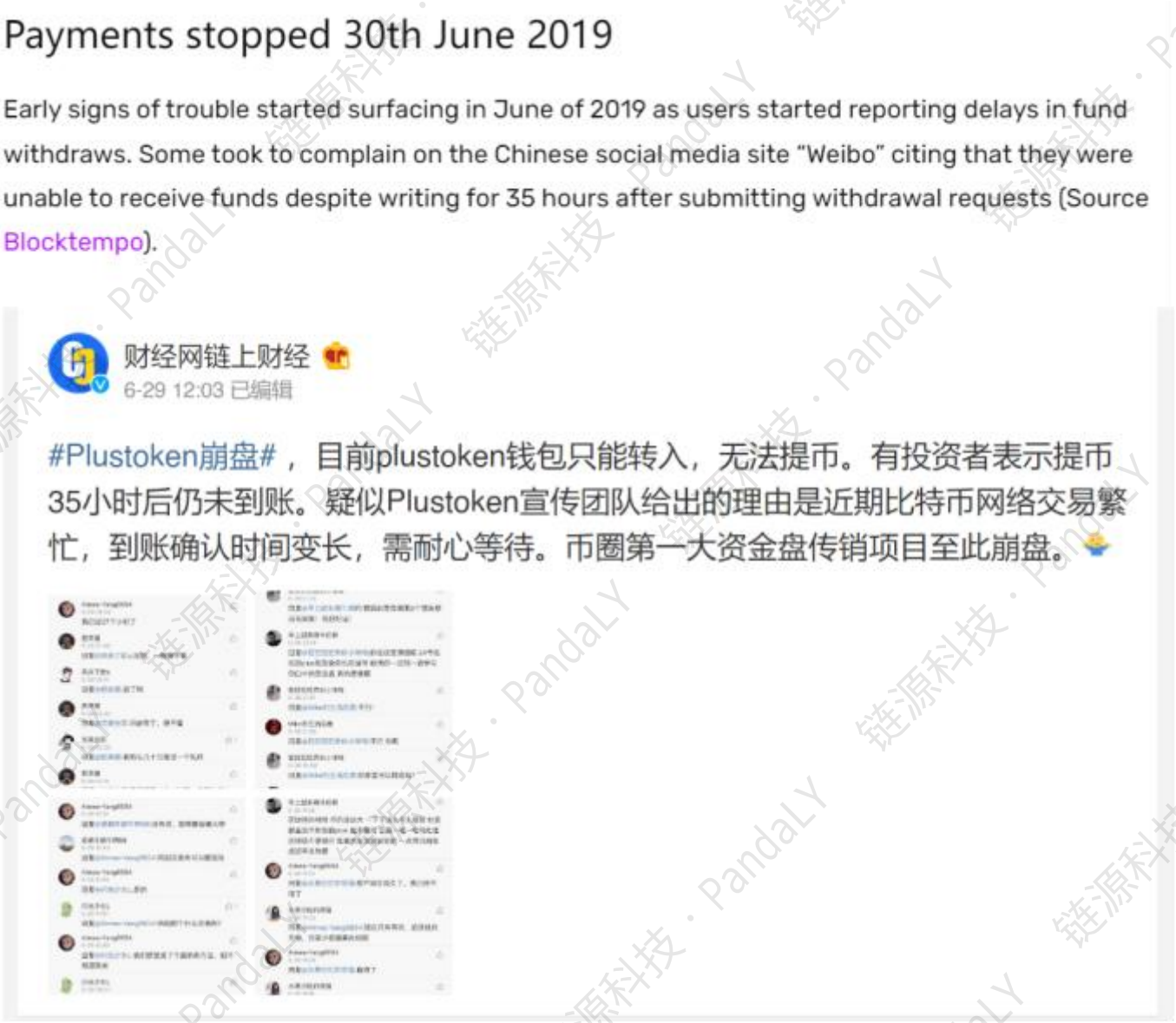


（图 2 Chainalysis 对 PlusToken 崩盘的追踪）

骗局的本质：新瓶装旧酒，币圈式传销

从 2018 年至今，类似的资金盘骗局层出不穷。你会发现，PlusToken 的本质**与加密货币毫无关系**，它只不过是打着区块链的旗号，复刻了一场数字时代的“现代传销”。它的运作模式依然是老一套：

- **金字塔式拉人头**：通过层层返利激励用户发展下线，让更多人参与其中。
- **铺天盖地的虚假宣传**：从社交媒体广告到线下活动，甚至投放纽约时代广场广告，营造出“国际顶级项目”的假象。
- **“高收益、零风险”承诺**：打着智能套利、稳定盈利的幌子，吸引投资者上钩。



（图 3 PlusToken 崩盘 ）

那么，**为什么明知道“天上不会掉馅饼”，仍然有成千上万的人上当?**

原因很简单——**骗局初期，有人真的赚到了钱。**

早期投资者的“财富神话”成为了骗局最好的广告，人们眼见他人利滚利、暴富翻倍，便产生了**“我不会是最后一个接盘的”**心理。可惜，欲望蒙蔽了理智，等到意识到骗局本质时，往往已是“为他人作嫁衣裳”。

莎士比亚曾说：“**每个人都有一份命运，但不是每个人都能逃避它。**”而在币圈，命运往往掌握在自己手中——你能否不被收割，取决于你的认知深度。

后记：警惕币圈的“资金盘幽灵”

PlusToken 不过是冰山一角，类似的骗局仍在币圈肆虐，披上不同的外衣，继续收割着新一轮的投资者。

在这个行业里，**“稳赚不赔”永远是最大的谎言。**

没有任何项目能**保证收益**，更没有人能**躺赚暴富。**你的每一次轻信，都可能成为骗子丰收的一次镰刀。

请记住：

你是否能在币圈立足，不取决于运气，而取决于你是否拥有足够的认知去避开这些陷阱。

希望你，**永远不要成为那个为别人买单的人。**

3.2 貔貅盘：吞噬财富的骗局

"无论你走多远，都无法逃避自己内心的欲望。" —— 卡尔·荣格

在加密货币的世界里，这句话体现得淋漓尽致，尤其是当我们谈到“貔貅盘”这种骗局时。

貔貅是中国文化中的一种神兽，传说它只吞不吐，寓意着财源滚滚，聚财不散。许多人相信貔貅能带来财富，甚至愿意将它作为自己的护身符。但当这个概念被引入币圈时，"吞噬"的就不是财富，而是每一个投资者的本金。

什么是貔貅盘?

貔貅盘，指的是**只能买，不能卖**的骗局。从表面上看，这种币的价格不断上涨，吸引投资者 FOMO（错失恐惧症）入场。然而，所有的上涨都只是数字游戏，等到投资者想要卖出时，才发现自己根本无法退出，而这时，骗局已经收割完毕。

这些骗局通常隐藏在**两类场景**下：

骗局类型 1：虚假项目吸引投资

骗子声称某个项目需要特定的代币才能参与，并提供一个合约地址让投资者兑换。投资者按照指示操作后，却发现兑换到的币无法出售，彻底被套牢，变成了一堆“死币”。

骗局类型 2：土狗币中的“虚拟财富”

某些 Meme（土狗）币，如 BSC、ETH、SOL 链上的新币种，会通过**永不下跌的 K 线图**制造“财富效应”。投资者看着币价狂飙，以为自己赚大钱了，直到想卖出时才发现**无法出售**，最终血本无归。

案例 1：BUSD 骗局——“财神爷”的悲剧

小帅，一个普通的币圈玩家，某天收到一个陌生人的私信：

“兄弟，我们有个赚钱的好项目，亲哥都不带，我就带你！想发财吗？”

小帅一听，眼睛一亮，心想：“机会来了！”毫不犹豫地回复：

“哥，你就是我亲哥！要是能带我赚钱，我认你当干爹！”

骗子乐开了花，立刻发来一个合约地址，并解释道：

“有个大客户愿意低价抛售 BUSD，但只接受特定渠道兑换的 BUSD，你只要先用 USDT 换成这种 BUSD，就能低买高卖，稳赚不赔！”

小帅一看，确实是 **BUSD**，而且带着**币安的 LOGO**，感觉很靠谱。骗子还补充：

“现在汇率差 8000USDT 能换 8050BUSD，多赚 50 刀，别犹豫！”

小帅心动了，立刻按照指示兑换。然而，当他尝试把 BUSD 换回 USDT 时，却弹出了***“该币种无法兑换”**的提示。

再去找骗子，发现已经被拉黑。他这才意识到，自己成了别人的“财神爷”，被骗得血本无归……

（图 4 BUSD 兑换）

技术分析：貔貅币的核心机制

骗子如何做到让受害者**无法卖币**？答案就在合约代码里。

打开 Solscan 查看该代币的合约，可以发现一个**关键函数**：

solidity

复制编辑

```
function transfer(address _to, uint256 _value) public returns (bool) {
    if(!tokenWhitelist[msg.sender] && !tokenWhitelist[_to]){
        require(tokenBlacklist[msg.sender] == false);
        require(tokenBlacklist[_to] == false);
        require(tokenGreylist[msg.sender] == false);
    }
    if(msg.sender == LP && ab && !tokenWhitelist[_to]){
        tokenGreylist[_to] = true;
        emit Gerylist(_to, true);
    }
}
```

关键词：Whitelist（白名单）

这个合约的机制非常简单：

- **只有在白名单上的地址**，才能转出代币；
- **普通投资者的地址不会被加入白名单**，因此他们买入的币根本无法出售；
- **骗子可以自由添加自己的钱包地址到白名单**，随时套现跑路。

而这些骗局的共性就是：**币价一直上涨**，但根本无法卖出。

（图 5 白名单函数）

案例 2：土狗貔貅币——EDU 骗局

小帅在币圈群里看到一条消息：

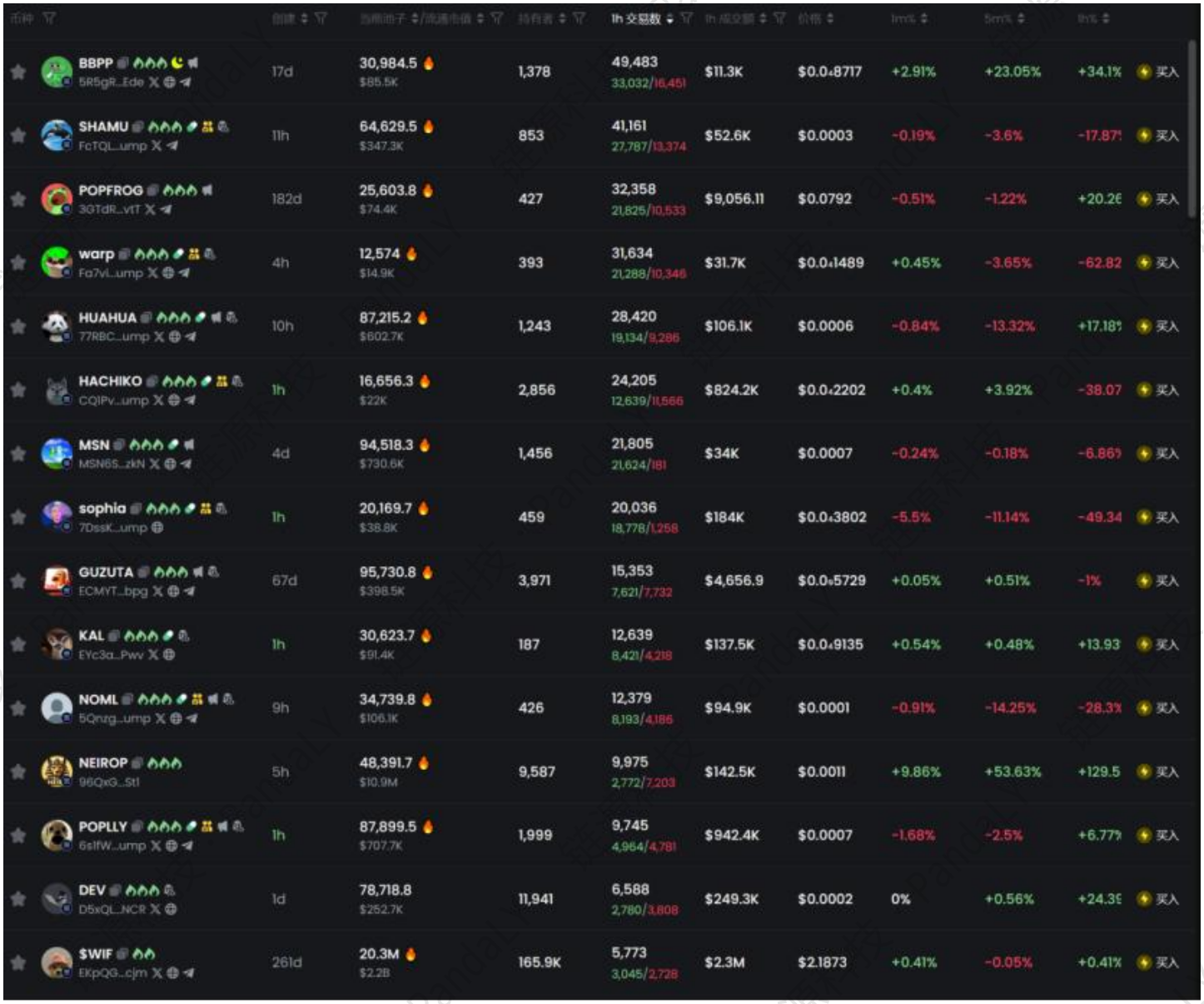
“兄弟们！EDU 币猛涨啊！10 倍收益，根本没跌，快冲！”

他打开合约地址一看，发现币价从 **0.05U 涨到 1U**，兴奋不已，立刻投了 100U 进去。

随后，币价飙升到 **3U**，小帅决定先卖掉本金，结果——**卖不出去！**

慌了的小帅回到群里，想找推荐这个币的人，却发现此人已经**被踢出群聊**。群主冷冷地说道：

“这是个貔貅盘，别浪费时间了。”



（图 6 土狗盘）

3.2.1 如何防范貔貅盘？

貔貅盘的核心问题在于**买入后无法卖出**，但实际上，**预防这种骗局并不难。**

1. **使用检测工具**

在购买任何新币之前，务必使用**防骗工具**检测合约：

- Coinscan.io
- honeypot.is

- Ave.ai

这些工具可以检测是否存在**无法卖出**的机制，如果检测结果显示“**Honeypot（蜜罐骗局）**”，就要果断放弃！

2. **避免跨链交易**

骗子常常引导受害者**通过跨链桥兑换**貔貅币，尤其是那些**不支持貔貅币检测**的跨链桥。所以，如果有人让你跨链兑换某种币，一定要提高警惕！

3. **观察交易记录**

- **正常的币种**：应该有**买入和卖出**交易，流动性正常；
- **貔貅盘**：只有**买入交易，没有卖出记录**，或卖出地址全是白名单用户。

在购买前，可以在 BscScan、Solscan 等区块链浏览器上检查交易记录，看看是否有人**成功卖出。**

4. **不要轻信“稳赚不赔”**

加密货币市场没有“稳赚不赔”这一说，凡是告诉你“**永远上涨**”的项目，99%都是骗局。

3.2.2 总结

貔貅盘的本质是利用 **FOMO 心理**，让投资者被快速上涨的数字蒙蔽双眼，等到想变现时才发现已被困住。

在币圈，**本金才是王道**，任何不透明、不允许卖出的代币，都应该果断避开！

所以，**在投资前，先问自己一句：如果不能卖出，你还能接受吗？**

3.3 OTC 场外交易骗局

OTC（Over The Counter，场外交易）指的是不通过公开交易所，而是私下达成的加密货币交易。这类交易不仅涉及 USDT，还涵盖许多尚未上线的代币。例如，在$Grass 发行前，场外市场就已经开始流通交易。

OTC 交易是将加密货币兑换为法币的重要途径，但也正因为其高流动性和缺乏监管，成为诈骗者活跃的温床。以下是几种常见的 OTC 骗局：

3.3.1 无 KYC 认证平台交易——高价诱惑，跑单骗局

OTC 的安全出入金方式较为有限，主要包括：

✓ 通过**币安神盾商家**交易；

✓ 依靠**知名 OTC KOL（大户）**撮合交易；

✓ **熟人介绍**的交易渠道。

一旦绕开这些安全渠道，资金损失的风险就大大增加。

骗局手法

骗子利用“高价收 U”吸引受害者，例如市场价 7 元/USDT，而他们声称 7.5 元/USDT 高价收购。这种信息常见于 Telegram、微信群，甚至一些小型 OTC 平台。

受害者可能在前几次小额交易中顺利成交，建立信任。但一旦涉及大额资金，骗子就会借故拖延，最终直接拉黑跑路。此外，他们还会发布**伪造的成功交易截图**，增强可信度，诱骗更多人上当。

如何防范?

保持警惕，拒绝过高报价，市场价的 U 价格不会大幅偏离。

不要相信陌生人的“成功交易截图”，很多是自动化程序批量生成的。

选择受信任的 OTC 渠道，避免无监管的平台交易。

3.3.2 USDT 跑分骗局——加密版洗钱陷阱

USDT 跑分起源于银行卡跑分，最初是为了洗钱，后来在加密货币领域变种升级。

骗局手法

跑分平台会要求用户**提供 USDT 钱包地址**，并声称通过代收代付赚取佣金（通常为 2%）。然而，受害者的钱包实际上被用于犯罪资金的流转。一旦涉及诈骗资金，钱包地址就会被交易所冻结，甚至可能引发刑事责任。

案例：SDS 聚富汇骗局

SDS 聚富汇曾以“高回报”为噱头，吸引用户存入 USDT。项目方宣称对接“稳定平台”，但实际上资金用于非法洗钱，最终 17 名操盘手被捕，涉案金额达 19 亿元。

如何防范?

⚠ **警惕任何“提供钱包地址就能赚钱”的项目**，99%是洗钱骗局！

⚠ **不要参与来历不明的 OTC 跑分平台**，否则可能被认定为共犯。

⚠ **避免使用私人钱包收款 USDT**，防止钱包被交易所冻结。

3.3.3 USDT 搬砖骗局——洗钱新模式

骗局手法

一些诈骗平台（如“U 摆渡”、“U 码头”）会在 Telegram 等渠道大肆宣传“高价收 U”，甚至承诺 9 元/USDT 的高回报。

但实际操作中，骗子会将你的银行卡号提供给诈骗团伙，被骗用户的资金会直接打到你的账户。最终，受害者报警，你的银行卡因**涉案资金流入**被警方冻结，你甚至可能面临法律责任。

如何防范?

避免在不明平台挂单交易，这些平台往往与诈骗团伙勾结。

切勿因高价诱惑而随意提供银行卡号或 USDT 地址。

收到异常资金后立刻报警，避免自己成为洗钱链条中的一环。

3.3.4 虚假付款信息——伪造截图、账户锁定骗局

这种骗局主要发生在 C2C 交易中，骗子利用各种手法制造付款假象，让卖家误以为收到款项，从而骗取 USDT。

套路一：伪造付款截图

骗子在交易页面点击“我已转账”，然后伪造一张银行转账截图，向卖家发送，并催促卖家放币。例如：

“你那边可能延迟了，我这边马上要爆仓，求你快点放币！”

如果卖家不核实到账情况，可能会直接放币，导致被骗。

套路二：银行 APP 锁定陷阱

骗子利用卖家的银行账户或手机号，在银行 APP 上多次输入错误密码，导致账户被暂时锁定。此时卖家无法查询是否到账，而骗子不断催促放币，最终骗取资金。

如何防范?

务必核实实际到账情况，不要仅凭截图或短信判断。

使用可信交易所的 C2C 平台，避免私下交易。

设置短信验证码或双重验证，防止账户被锁定。

3.3.5 空头支票骗局——香港 OTC 诈骗

骗局手法

骗子通常在香港 OTC 交易中使用空头支票。例如：

1 他们先用支票“挂账”，让受害者收到**“入账”短信**，但这并不代表到账。

2 在 24 小时到账前，骗子迅速要求卖家放币。

3 受害者放币后，骗子撤销支票或因账户资金不足导致跳票。

如何防范?

香港支票入账≠到账，必须等待 24 小时确认。

尽量使用现金或转账交易，避免支票付款方式。

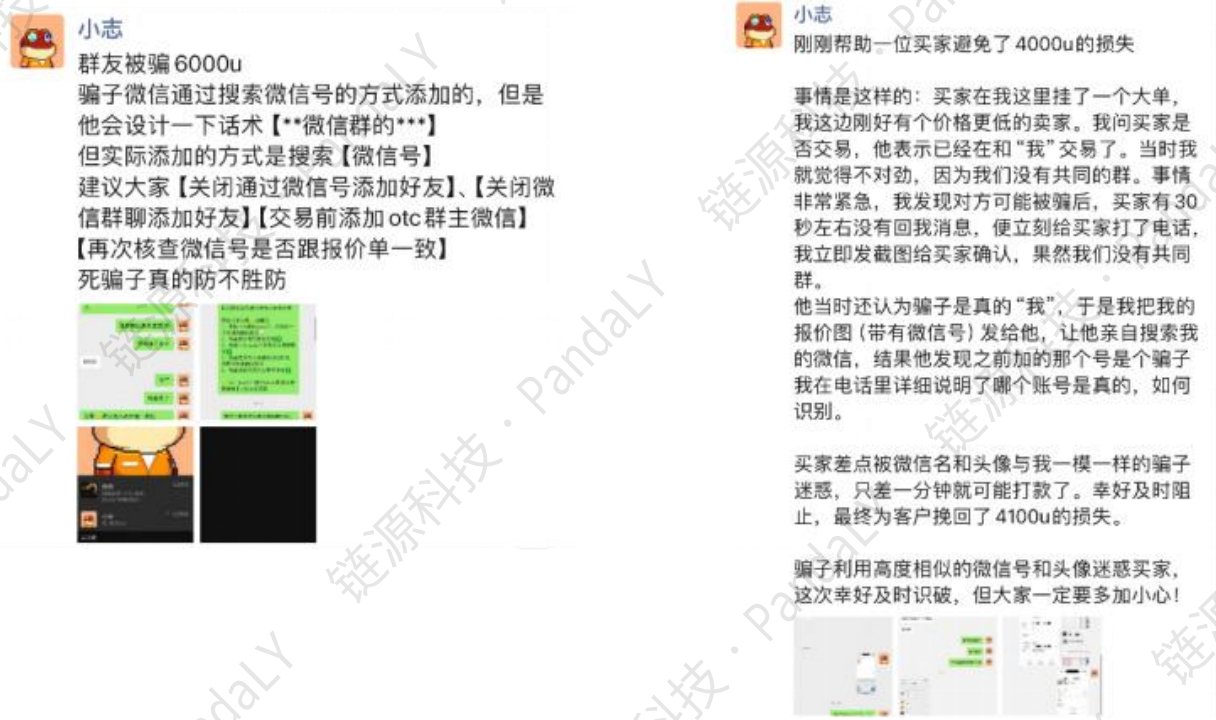
遇到大额交易时，务必在银行柜台核实到账情况。

3.3.6 假冒 KOL 买卖 USDT 骗局

骗局手法

骗子会伪装成知名 OTC KOL（如比特吴等），在群聊中复制他们的头像和昵称，主动联系用户进行交易。例如：

1 假冒 KOL 在群里发布“30 万 U 出售”信息，吸引受害者私聊。



（骗子模仿 kol 微信进行诈骗）

2 取得信任后，骗子会创建群聊，并拉入一个冒充 KOL 的“助手”。

（骗子在 Telegram 群里钓鱼）

3 受害者以为是正规交易，结果 U 转出后，对方立即拉黑跑路。

如何防范?

✓ **交易前核实微信号/Telegram ID**，KOL 不会私下主动找人交易。

✓ **多次确认交易地址**，不要轻信群聊中的信息。

✓ **警惕"高价收 U"噱头**，骗局往往从贪念开始。

3.3.7 总结

OTC 交易虽然方便，但风险极高，尤其是**无监管平台**、**高价收 U**、**跑分骗局**等情况。要避免被骗，务必：

✓ **使用主流交易所的 OTC 商家**，如币安神盾商家。

✓ **不贪高价，不走偏门交易**，骗子最擅长利用人性的弱点。

✓ **交易前多方核实身份**，避免成为骗局中的“猎物”。

币圈 OTC 水深，务必提高警惕！

3.4 钓鱼攻击

钓鱼攻击，顾名思义，就是攻击者用各种工具“钓”那些容易上钩的人。最早的钓鱼攻击主要指网络诈骗，通常通过假冒网站或邮件，诱导用户点击恶意链接，从而骗取个人信息。在区块链领域，钓鱼攻击的本质与传统钓鱼相同，都是冒充受害者信任的对象，例如常见的钱包网站、交易平台，甚至是曾经参与过的项目方，进行诈骗。攻击者通常会使用伪造的链接、假冒的社交媒体账号，甚至是看似正规的智能合约，诱导用户执行特定操作。一旦用户掉以轻心，输入私钥、助记词，或签署了恶意交易，资产就可能在不知不觉中被盗走。

3.4.1 案例解析：微信群的“空投”骗局

你是否遇到过类似的场景：在微信群里，某个熟悉的朋友或 KOL 突然发来一个“免费领取空投”的活动链接？网页看上去和你熟悉的某个项目官网几乎一模一样。你点击后，页面提示需要连接钱包并签名确认。你心想：“反正只是签名，应该没什么问题。”但就在你签名后，钱包里的资产却不翼而飞了……

这正是一个典型的**诱导签名**钓鱼攻击案例。许多用户对“签名”操作的风险认识不足，以为只是在“登录”网站，实际上，他们可能已经授权了攻击者转移资产的权限。

防范关键点：

✓ **仔细检查链接**：不要点击陌生人发来的链接，即使是熟人发的，也要确认是否被盗号。

✓ **避免轻易签名**：不熟悉的 DApp、陌生的签名请求，**不签、不授权、不交互。**

✓ **使用防钓鱼插件**：如 MetaMask 的 **PhishFort** 或 **Wallet Guard**，可帮助识别钓鱼网站。

3.4.2 五种常见钓鱼攻击手法

钓鱼攻击的形式多种多样，最常见的有以下五种：

3.4.2.1 垃圾币空投——利用假空投网站行骗

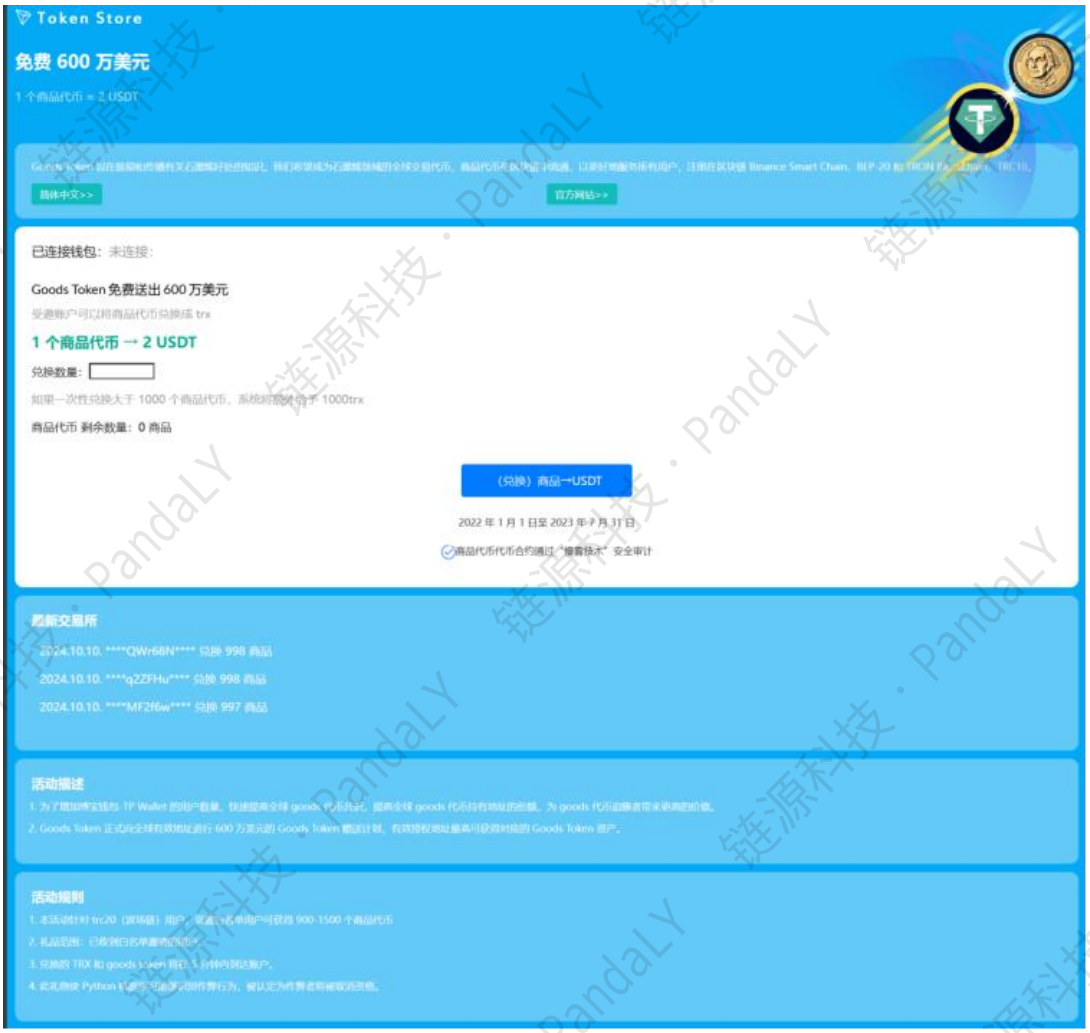
虚假空投分为垃圾币空投和假冒地址空投，我们先讲讲垃圾币空投。如果你的账户有钱的话，就有大概率会收到如下图的一些垃圾币。

feda6c76bbcec10...	TRC-10 转帐	65193586	2024/09/13 19:59:24	TUQyF6...cutExCZh	→ TVCG7q...PSHqqejq	hash.ist	1,000
281aa9090ff4a6d...	TRC-10 转帐	65101522	2024/09/10 15:15:00	TWmBCX...nskFRP8	→ TVCG7q...PSHqqejq	HX16.COM	8,888.88
a27c443c818580...	TRC-10 转帐	65100318	2024/09/10 14:14:48	THvB7V...Jq8eXCoKy	→ TVCG7q...PSHqqejq	video998.com	999
27dfe713ed3fbe3...	TRC-10 转帐	65098108	2024/09/10 12:24:12	TC4Nio...yxf9BseKP	→ TVCG7q...PSHqqejq	tron.ink	1,000,000
30fd38ec5f23855...	TRC-10 转帐	64853903	2024/09/02 00:46:45	TQBa8R...LNEXhWmq	→ TVCG7q...PSHqqejq	Pay.bi	8,888.88

垃圾币之所以称为垃圾币，是因为它是没有实际价值的，所以你没法把垃圾币换成其他的币。

这些垃圾币的目的是什么?

如果你仔细观察币的名称你就会发现，它的名称其实是一个网站。当你根据网址输入网站后，你会发现，这些网址确确实实是可以进入某些网页的，但这些网页都是一些垃圾的广告诈骗小网站。

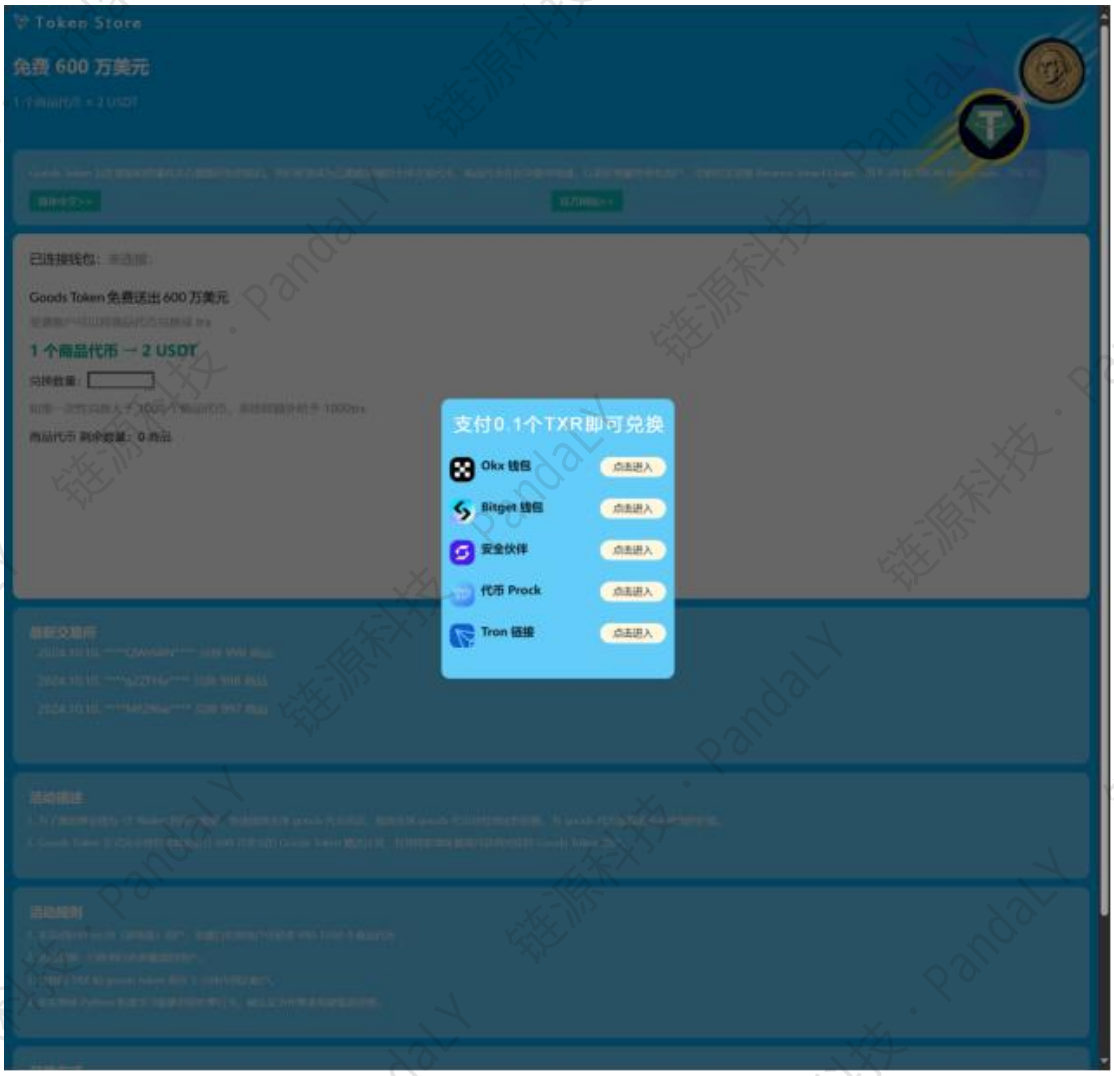


典型案例分析：

比如，我点进了 goods token （video998.com）这个网站，网站页面如下：

- 网站声称你可以免费领取他们的商品代币，而一个代币相当于 2USDT，并且下面最新交易所中还说，xxx 获得了 1000 个代币，相当于 2000USDT。

- 滑稽的是，它的代币领取时间是 2022 年的 1 月 1 日到 2023 年的 7 月 31 日，而我们现在已经是 2024 年了——他们连网页都懒得更新就直接搬上来行骗。
- 顺着它的网页点击“兑换”，弹出了几种选项，让我们选择钱包进行连接。但经过操作会发现，只有 Bitget 钱包能点开，并且点了 Bitget 也只是跳到了 Bitget 钱包的官方下载界面，下载后也并没有弹出任何签名的弹窗，看来这个网页是做到一半死于胎中了。



其他诈骗网站分析：

接着我们看看其他的网址。

赌博网站陷阱：我们点开 hash.ist 和 hx16.com，会发现进入的都是叫猜测哈希值来进行网赌的网站。相信只要你看过一些反诈骗宣传，你就会对这类网站敬而远之了，毕竟小钱不用跑，大钱跑不了。

第三方脚本工具：还有的网址会推荐你使用第三方脚本工具，比如说批量多发工具或是空投脚本工具等等。但由于这些多发工具大多都要上供助记词的，所以很可能造成助记词泄露的问题。

风险提示

或许大家会发现，这些垃圾小广告就跟我们邮箱收到的垃圾邮件一样，只是它们是专门面向于区块链方面的。当然，不管是不是区块链的小广告，我们都希望你不要点进去，毕竟都是一些三无网站。如果看完我说的这些话你

还点进去，那我可要把你挂推让所有人笑你了。

3.4.2.2 仿冒地址——伪造转账记录诱导误操作

如果你的地址经常有大额转账，且收付款地址相对固定，你有可能会收到莫名其妙的 0、0.01、0.001 等小额充值。仔细观察这些充值来源地址，你会发现，它们的尾号和你经常转账的地址尾号相同。如果你不加注意直接复制地址，很可能将资金转到骗子的地址上。

骗局原理

骗子会在区块链上查找经常有大额转账且收付款地址固定的用户，利用地址生成器仿造他们的常用收款地址，并多次向该用户的钱包转入小额资金。由于许多人习惯从历史交易记录中复制地址并只查看尾号，一旦稍不留意，就容易将资产转移到钓鱼地址。

如何防范?

- **添加地址白名单**：将常用的收款地址保存到通讯录或添加到白名单中。
- **谨慎复制地址**：不要直接复制历史交易记录中的地址。
- **多次确认地址**：每次转账前认真核对地址，确保与目标地址完全一致。

要牢记，区块链转账与支付宝不同，区块链转账是不可逆的，因此更需要细心核对，避免造成不必要的损失。

3.4.2.3 诱导签名——伪装成无害操作骗取授权

为什么 BTC 链不会有诱导签名问题?

BTC 链不会出现诱导签名骗局的情况，因为 BTC 不支持编写智能合约。而如果一个区块链支持编写智能合约，就可能出现诱导签名的风险。

常见语言案例：Solidity 钓鱼风险

Solidity 是区块链中最常见的智能合约编程语言，适用于 ETH 主链、ETH 二层链、ETH 三层链、BNB、Tron 等。凡是基于 Solidity 开发的链，都需要注意以下诱导签名骗局及其防范措施。

诱导签名与授权的区别

在了解诱导签名前，我们需要明确签名与授权的区别：

签名：签名是链上数据的确认或认可，通常不会直接涉及资产的转移。

授权：授权则赋予合约对你账户中资产的操作权限，一旦授权给恶意合约，资产就有可能被直接盗取。

诱导签名案例分析

诱导转账签名：一些钓鱼网站利用智能合约，诱导用户签名，表面上看是无害的操作，实际上可能暗含转账指令。

合约陷阱：用户可能被引导连接钱包并签署恶意合约授权，一旦签署，攻击者便能操控用户资产。

如何防范?

- **谨慎访问网站**：不随意点击不明链接或连接陌生网站。
- **仔细阅读签名内容**：签名前务必查看签名内容中是否涉及转账或授权。
- **限制授权范围**：在签署授权时，仅授予必要的权限，避免全权限授权。
- **定期管理授权**：使用安全工具检查并撤销不必要的授权。
- **后门工具**——伪装成空投脚本窃取助记词
- **上供助记词**——伪装成客服或 KOL 骗取私钥

3.4.2.4 诱导签名攻击解析

在深入探讨诱导签名攻击之前，我们需要明确一个基本概念： **BTC 链不会出现此类钓鱼情况**，因为 BTC 不支持智能合约的编写。然而，如果某条区块链支持智能合约开发，就可能面临诱导签名的风险。

Solidity 语言中的钓鱼案例

Solidity 是目前区块链中最常见的智能合约编程语言，被广泛用于 ETH 主链、ETH 二层和三层链、BNB、Tron 等。因此，所有使用 Solidity 开发的区块链，都可能受到以下诱导签名攻击方式的威胁。

签名（Sign）与授权（Authentication）的区别

在现实生活中，我们在银行取款时通常需要进行身份验证，例如人脸识别或签名确认。区块链世界中的**签名**（Sign）也承担类似的功能，用于证明你是某个钱包地址的所有者。而**授权**（Authentication）则是赋予某个地址特定权限的行为。

但签名≠授权。例如，当你连接 Magic Eden 并签署登录请求时，这只是一个**签名**操作，仅用于验证你的钱包地址归属权，并不会赋予 Magic Eden 任何资产操作权限。

在智能合约中，常见的授权方式有两种：

1. **带 Approve 关键字的函数**（常见于 ERC-20 代币和 ERC-721 NFT）

2. **带 Permit 关键字的函数**（支持链下签名授权）

3.4.2.4.1 Approve 机制与相关钓鱼手法

ERC-20 代币 Approve 机制

在 ERC-20 代币标准中，Approve 函数的作用是：

```
approve(spender, amount)
```

- spender：被授权地址，可以是智能合约地址或普通钱包地址。
- amount：被授权的代币数量。

完成 Approve 授权后，spender 便可通过 transferFrom(from, to, amount) 直接从授权账户转移代币。

钓鱼案例

曾有一个冒充“质押挖矿”的钓鱼网站，要求用户在确认交易时进行 Approve 操作。事实上，一旦用户签署该授权，攻击者便获得了无限制转移其代币的权限。

ERC-721 （NFT） 授权方式

NFT 主要有两种授权方式：

1. **Approve**：授权某个地址管理特定 NFT。

```
approve(to, tokenId)
```

1. **setApprovalForAll**：批量授权某个地址操作所有 NFT。

```
setApprovalForAll(operator, approved)
```

风险提示

setApprovalForAll 是 NFT 钓鱼的高危函数，骗子常利用其诱导用户授权，从而批量转移 NFT 资产。

3.4.2.4.2 Permit 攻击——隐蔽且高效的盗取手法

Permit 机制解析

Permit 机制源于 **EIP-2612**，允许用户通过**链下签名**的方式完成授权，而无需发起链上交易。

攻击案例

2023 年 5 月 11 日，推特用户“菠萝哥”遭遇 Permit 钓鱼。他只是简单地连接了一个钓鱼网站，并进行了签名，却发现资产被盗。

根本原因在于，菠萝哥在 5 月 10 日访问该钓鱼网站时，签署了 Permit 交易：

```
permit(owner, spender, value, deadline, v, r, s)
```

- owner：签名者（即用户本人）。
- spender：被授权地址（即攻击者合约）。
- value：授权金额。
- deadline：授权到期时间。
- v, r, s：签名参数。

攻击者随后调用 transferFrom，成功转移了菠萝哥的 USDC 资产。

Permit 相当于签署了一张空白支票，攻击者可以随意填写金额并兑现。

项目方也可能遭遇 Permit 攻击

不仅个人用户，项目方也可能因误用 Permit 而导致资金损失。例如，某项目方在未察觉风险的情况下，误签了一笔 Permit 授权，导致 3500 WU 代币被盗。

3.4.2.4.3 Permit2——更高效但更危险的授权方式

Permit2 机制解析

为了减少 Approve 交易的 Gas 费用，Uniswap 推出了 Permit2，实现更高效的代币授权管理。

与 Permit 相比，Permit2 具备以下特点：

支持批量授权，一次性赋予所有代币操作权限。

授权范围更广，不仅限于单个代币。

钓鱼案例：2024 年 9 月 15 日的空投骗局

某用户因轻信空投广告，在钓鱼网站上签署 Permit2 交易，结果导致价值 127,141 美元的 Neiro 代币被转走。

Permit2 本质上是**一键授权钱包内所有代币**，一旦被滥用，后果极其严重。

Permit2 交易结构

USDC.approve(permit2Address, type(uint256).max);

permit2Address：Permit2 授权合约。

type(uint256).max：设置授权额度为最大值。

攻击者可通过 permitTransferFrom 直接调用 transferFrom，将用户所有授权代币转走。

如何取消授权?

如果发现钱包被诱导签名，应立即撤销授权。

方法 1：使用 Revoke.Cash 检查和取消授权

访问 Revoke.Cash。

连接钱包，选择相应网络。

查看已授权记录，手动撤销高风险授权。

方法 2：检查 Permit 是否仍然有效

Permit 的有效性通常由 nonce 记录。若 nonce 已递增，说明 Permit 授权已生效，应立即采取措施。

nonce[tokenId] += 1;

用户可在区块链浏览器上查询 nonce 变化，若发现异常，应立即撤销授权。

3.4.2.5 总结

如何避免诱导签名陷阱?

警惕任何要求 Approve 或 Permit 授权的操作，特别是高额度授权。

避免随意连接陌生 DApp，慎重检查交易签名内容。

定期使用 Revoke.Cash 检查并清理无用授权。

提高安全意识，关注最新的钓鱼手法，防止被攻击者利用。

3.5 野鸡交易所与虚假平台

3.5.1 野鸡交易所

在进入币圈时，最关键的一步就是选择**合适的交易所**。主流交易所如币安、OKX 等，依靠多年积累的信誉和实力占据市场。但与此同时，也有一类交易所，它们的目标不是提供安全可靠的交易环境，而是**专门设计来收割用户**，这些我们称之为**野鸡交易所**。

野鸡交易所的运营模式多种多样，但无论如何包装，本质上都离不开“骗”字。它们往往通过以下几种方式吸引用户：

- **充值注册就空投**——制造免费送币的假象，实则套路新人入场。
- **配合 KOL 收割**——联合币圈大 V，利用社交平台造势，吸引更多资金进入。
- **高收益理财**——承诺远超正常市场水平的回报，实则资金盘套路。
- **上线垃圾币**——发布毫无价值的空气币，通过操控市场暴涨暴跌收割用户。
- **高杠杆合约**——利用高杠杆机制，在后台操控行情，强制用户爆仓。

接下来，我们拆解这些套路的细节，并结合实际案例，帮助大家提高警惕。

1. **充值注册就空投：免费送币是馅饼还是陷阱?**

许多交易所都会推出空投活动，即便是主流交易所，如币安、OKX 等，也会不定期提供奖励吸引新用户注册。然而，野鸡交易所则是借此大做文章，它们通过以下方式吸引用户：

- **注册即送空投币**——包括平台币以及所谓“和知名项目方合作的代币”。
- **拉人头奖励**——邀请好友注册、充值就能获得更多奖励，形成传销式裂变。
- **充值加送**——新用户充值后，平台会再赠送一定比例的代币，看似是稳赚不赔的机会。

这些空投币在初期通常会通过**人为操控拉升**，制造暴涨的假象，吸引更多用户进场。然而，等到用户充值资金达到一定规模后，平台会**突然砸盘**，甚至直接关闭提现通道，用户的资产也随之被锁死或清零。

典型案例 1：某空投交易所

某交易所以“注册即送价值 50U 代币”为噱头吸引大量用户，初期可小额提现，让用户产生信任。当用户尝试大额提现时，交易所则要求“先充值解锁提现权限”，一旦充值，账户就被封禁，客服失联，平台消失。

2. **配合 KOL 收割：你信的是 KOL，KOL 信的是交易所**

在微博、小红书等社交平台上，许多“币圈大 V”长期活跃。他们以精准预测走势、展示暴利收益等方式吸引粉丝，甚至营造出**“稳赚不赔”的神话**。而实际上，他们**很可能与野鸡交易所合作**，通过以下方式收割韭菜：

- **专推某交易所独家代币**——大 V 推荐的币种，只能在特定交易所交易，形成信息闭环。
- **持续喊单+晒单**——大 V 每天更新 K 线图，展示自己“精准预测”的能力，吸引更多人入场。
- **代币暴涨暴跌**——初期借势拉盘，用户追高买入，交易所再突然砸盘，让用户损失惨重。

收割完成后，大 V 们往往会甩锅：“币圈本来就是高风险市场，大家要学会控制仓位。”而他们自己早已全身而退，继续寻找新的交易所与割韭菜的机会。

典型案例 2：某 KOL 割韭事件

某微博大 V 在 2023 年合作推广一款新代币，承诺“团队长期运作，未来价值 10 倍以上”。短短一周，该币暴涨 500%，随后交易所开始疯狂砸盘，用户损失惨重。事后，大 V 删除所有推广内容，并发文称：“市场就是这样，有涨有跌。”

3. **高收益理财：真的稳赚不赔？其实是资金盘骗局**

年化收益 100%，敢投吗?

许多野鸡交易所推出“高收益理财产品”，承诺比主流交易所更高的年化回报，如：

- **一个月 20%收益**
- **三个月 40%收益**
- **一年 100%收益**

这些理财产品通常采用**资金盘模式**，即**用后来的用户资金支付前面的用户收益**，本质上是庞氏骗局。当资金链断

裂时，交易所就会找各种理由关闭提现，或直接跑路。

典型案例 3：某交易所跑路

某交易所曾推出“锁仓一年，稳定年化 100%”的产品，前期确实有用户收到收益，吸引更多资金流入。但一年后，交易所突然宣布“系统维护”，所有用户的资金被冻结，最终团队解散，官网关闭，用户损失惨重。

4. **上线垃圾币：你买的可能只是数据库里的数字**

主流交易所上线的新币通常需要严格审核，而野鸡交易所则**无门槛上币**，甚至**自己发币**，通过以下方式割韭菜：

- **人为操控 K 线**——后台控制代币涨跌，制造上涨假象，吸引用户接盘。
- **数据库币**——交易所直接在后台添加虚拟代币数据，币根本不存在区块链上。
- **砸盘收割**——当交易量足够大时，交易所会突然砸盘，让所有投资者爆仓。

5. **高杠杆合约：K 线你看得懂，后台你看不懂**

合约交易本身就存在高风险，而野鸡交易所进一步**推高杠杆倍数**，提供 **500 倍、1000 倍杠杆**，吸引用户赌性上头。更可怕的是，**交易所可以直接操控用户爆仓**：

- **后台操纵行情**——在其他平台没有波动的情况下，交易所 K 线突然剧烈波动，导致用户爆仓。
- **数据回滚**——交易所随意撤销已成交的交易，侵占用户利润。
- **拔网线**——用户交易时服务器突然卡顿，无法平仓，等网络恢复时已经爆仓。

3.5.2 虎符交易所

虎符交易所成立于 2017 年，2022 年暴雷，五年时间割韭菜无数，被誉为“野鸡交易所中的战斗机”。其套路之多令人咋舌：

经典案例 1：带单骗局

2021 年，一位用户报警称在虎符的带单群中被割 20 万人民币。带单老师在用户亏损后威胁称“你碰一下试试，我律师会联系你”。最终，警方查出该老师身份并绳之以法。

经典案例 2：传销币 ZILD

自称由 24 位俄罗斯博士开发的中心化协议，通过借钱产生代币和拉人头收益吸引用户。然而该项目本质是资金盘，披着加密货币外衣骗取投资者资金。

经典案例 3：资产被盗

“土豆儿事件”最为出名——一夜之间 11.3 个 BTC 和 30 个 ETH 被清空。虎符甩锅称用户未及时冻结资产，但专业人士认为可能是虎符内部作案。

经典案例 4：交易回滚

2021 年，虎符平台币暴跌，投资者低位抄底，但平台直接回滚交易并下架交易对，用户账户被冻结。最终平台退回了买入 USDT，但仍扣除了交易手续费。

经典案例 5：暴雷与跑路

2022 年 7 月 25 日，虎符宣布停止所有交易服务，并推出《债币转换方案》。高情商的说法是“转换方案”，低情商的说法则是“发了两个没用的币来忽悠用户资产”。

3.5.3 虚假交易所案例

2024 年 9 月 12 日，我们接到一位客户的咨询：“提现要交 25%税？”

经过调查，我们发现这是一个假币安交易所的骗局。受害者通过 KOL 推荐将京东卡换成 USDT 并充值到假交易所。提现时，平台以“需额外充值 25%个人所得税”拒绝提现。受害者这才意识到自己被骗。

这种假交易所骗术虽然拙劣，但仍能轻松欺骗缺乏经验的投资者，特别是年长用户。因此，科普此类骗局至关重要。

3.6 ICO 骗局

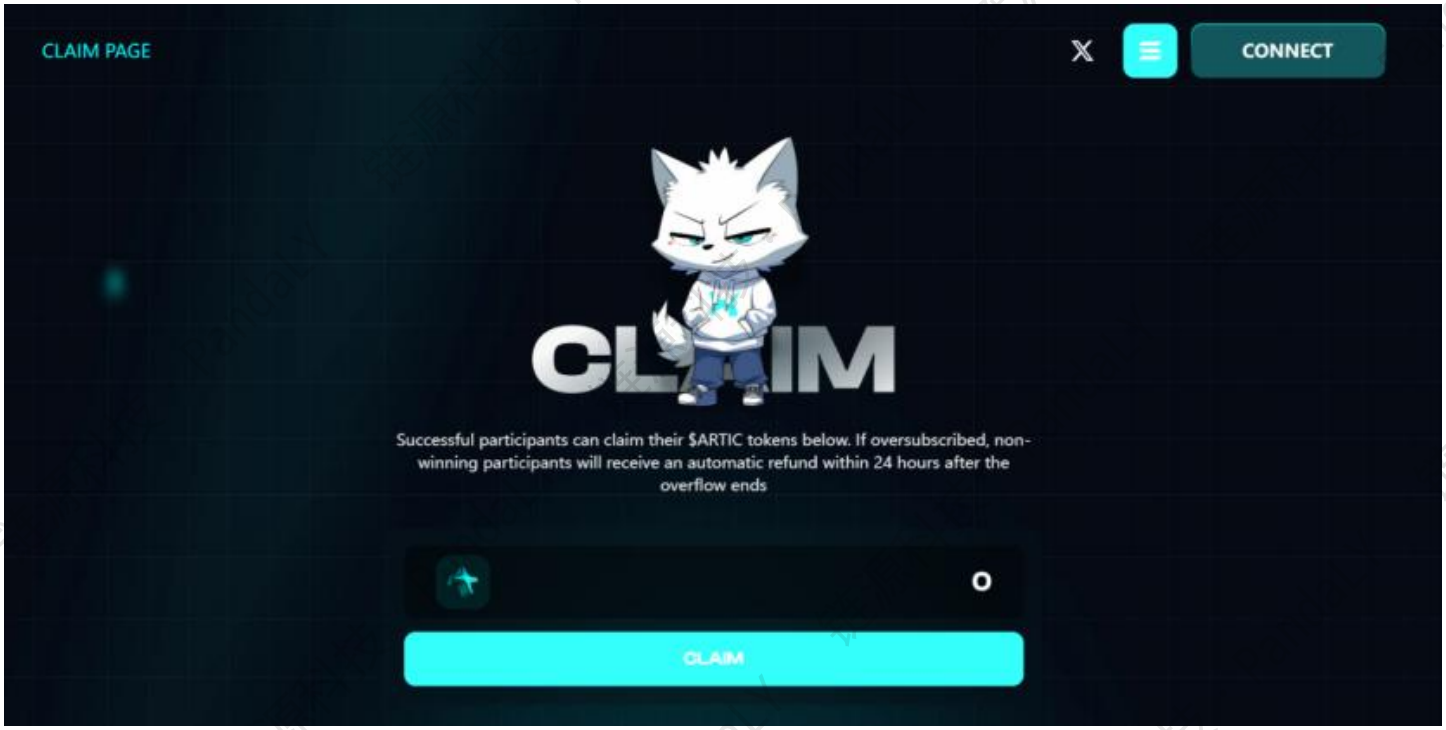
ICO 的基本概念

ICO（Initial Coin Offering）是指通过代币发行进行融资的方式。简单来说，投资者需要先将资金打入项目方提供的账户，待代币在区块链上部署后，再由项目方将代币发放给投资者。

然而，由于这种“先收钱，后办事”的模式存在天然风险，ICO 骗局在币圈层出不穷，尤其是在土狗盘频繁出现的 Solana 等链上环境。

典型案例 1：IBXtrade 跑路事件

2024 年 10 月 16 日，IBXtrade 官方 Twitter 发布了代币$ARTIC 的预售消息，并附带了官网链接。



不少知名 KOL 参与了转发，制造出强烈的市场热度。

10 月 18 日，IBXtrade 成功募集了 **161，216.10 SOL**，但并未按计划在约定时间发布代币。面对投资者的质疑，IBXtrade 在 Twitter 上承诺会为所有用户退款。

然而，不久后，IBXtrade 迅速删除所有社交媒体账号并卷款跑路，将募集到的 **SOL 提现至 Bybit 和酷币交易**

所。

KOL 的参与与背锅

IBXtrade 得以募集巨额资金的关键，在于通过以下手段营造出“优质项目”的假象：

1. **精心设计的网页**：页面布局专业，内容详尽，增加可信度。
2. **合理的社交媒体运营**：发布频率高，内容互动性强。
3. **KOL 频繁转发制造人气**：据调查，部分 KOL 被项目方许诺发币后的代币分配，部分则单纯蹭热点，但最终大部分人未拿到任何好处，还成为受害者攻击的目标。

分析与反思

IBXtrade 之所以成功骗取大量资金，是因为其为骗局披上了金玉其外的外衣。然而，表面的光鲜无法掩盖其脆弱的本质。一旦面对巨额资金的诱惑，项目方往往会选择直接卷款跑路。

其他相似案例：

币圈中，不透明的 ICO 项目数不胜数，尤其是土狗盘的项目方几乎不公开任何个人信息，仅留下一个无法追踪的地址，进一步增加了投资者识别风险的难度。

如何避免陷入 ICO 骗局?

1. **背调项目方信息**：查看项目成员是否公开透明，有无真实的社交背景。
2. **避免高风险投资**：对于完全不透明的项目保持高度警惕。
3. **止损意识**：哪怕误入骗局，也需果断止损，避免更大的损失。

警示总结

IBXtrade 事件再次提醒投资者，在币圈投资时不要被表面的华丽包装迷惑。务必保持理性判断，切勿轻信任何不透明的项目，以免落入骗局陷阱。

3.7 NFT 骗局

随着 NFT（非同质化代币）市场的火爆，各类骗局层出不穷。主要可归纳为两种类型：

1. **假冒盘 NFT 骗局**

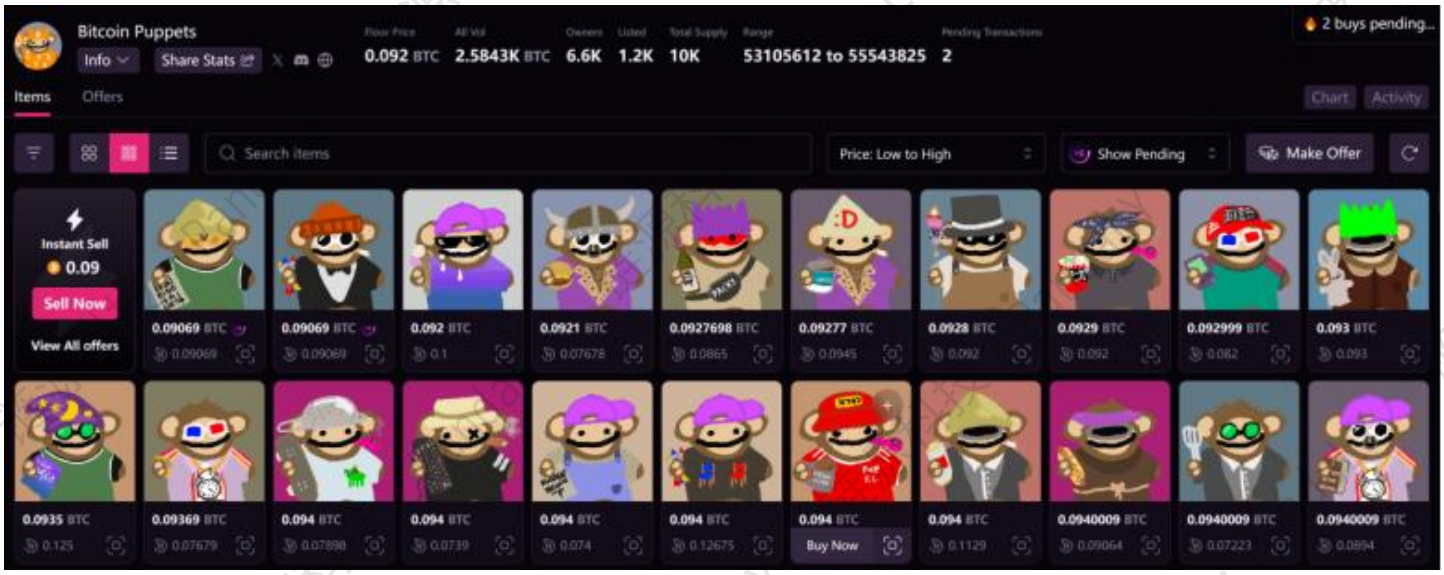
（1）仿盘 NFT

仿盘并非完全的假冒 NFT，而是对原 NFT 题材进行二次创作，并结合社区运营，试图打造成一个新的二创 IP。然而，成功打造二创 IP 的难度极高：

- **运营难度大**：二创项目需要持续的创意与资金支持。

- **认可度低**：原项目社区往往对仿盘抱有抵触心理。

因此，不少项目打着“二创”的旗号，实际上只是借用原项目热度来收割用户。



（正版 Bitcoin Puppets）

（蹭热度的各类 Puppets 仿盘）

（为正品，后为无价值仿盘）

（2）假冒 NFT

相比仿盘，假冒 NFT 才是最为恶劣、需要重点防范的骗局。当某个 NFT 项目具有较高热度时，骗子往往会发布外观极为相似的 NFT。

（官方发售完 NFT 后跑路）

典型案例分析

用户在 NFT 售卖平台搜索 NFT 时，往往会看到多个名字、图像相似的 NFT 项目：

- **正版 NFT**：图像设计与官方契合，具备市场流动性。
- **仿盘 NFT**：外观接近，打着“二创”旗号，流动性较差。
- **假冒 NFT**：完全复制正版外观，但没有任何价值，通常由项目方直接挂单。

购买假冒 NFT 的用户往往面临以下风险：

- **无市场流动性**：假冒 NFT 无法在市场上出售，除非用户自行挂单。
- **接盘概率接近零**：几乎没有买家愿意接手假冒 NFT。

如何避免购买“高仿”NFT?

1. **查看平台备注**：注意平台是否有标注项目为仿冒。
2. **验证官方链接**：通过项目方的官推获取官方链接，直接在官方平台交易。
3. **链上部署判断**：根据 NFT 所在链进行核对。例如：如果官方 NFT 部署在 Lina 链，而另一个项目部署在 Matic 链，则很可能为假冒。

总结

防范建议

1. **提高鉴别能力**：
   a. 谨慎对待夸大宣传和高额承诺。
   b. 核实项目信息的透明度。
2. **官方渠道交易**：始终选择项目方的官方渠道进行交易或铸造。
3. **链上核验**：通过区块链浏览器核实 NFT 的部署信息。

警示语：NFT 市场虽然充满机会，但也暗藏陷阱。投资者需保持理性，谨防掉入骗局陷阱。

四、加密货币社媒平台

看完以上的骗局后，相信各位都多多少少发现，需要多加留意的是人心而绝非技术。所以为了保护自己的资产安全，学会防范人比防范技术更加重要。

接下来我们来聊聊诈骗多发平台、术语、诈骗特征等。相信这会对你的资产保护大有帮助。

4.1 诈骗多发平台

根据我们接触和分析的案件，诈骗主要发生在以下几类平台：

1. **国内主流社媒平台**：微信、QQ、抖音、小红书等。
2. **国内高风险社媒平台**：Mostalk、Mosgram、Potato 等（如有新发现，请积极举报）。
3. **海外主流社媒平台**：X（原 Twitter）、Telegram、Facebook、Discord 等。

为何这些平台容易成为骗子的温床?

主要是因为**注册门槛低、缺乏实名验证机制。**

- 即使需要手机号等信息辅助注册，仍有许多方法可以规避实名验证，导致在平台上与骗子交流无法通过官方渠道追溯到对方真实身份。
- **海外平台情况更严重**：几乎没有任何实名认证要求，给骗子提供了更大的作案空间。

典型诈骗平台：Mosgram

Mosgram 是国内盛行的诈骗平台之一。在知乎上搜索“Mosgram”即可发现大量关于其涉及资金盘、刷单骗局和虚假交易所的曝光内容。

Mosgram 的特殊机制：

它具备**单方面清空聊天记录**的功能。当骗子发现无法再从你身上获利时，可以直接删除聊天记录，抹除证据。

4.2 诈骗话术剖析

有了诈骗平台，骗子接下来需要的就是“话术陷阱”来吸引受害者。以下是常见的诈骗话术与案例：

4.2.1 高收益承诺

案例：王先生在加密货币论坛看到某新币种宣传帖，声称投资 1 BTC 可在一个月内变成 3 BTC。他按对方指示购买该代币，但代币价格暴跌，交易平台也关闭，损失惨重。

话术：

- “投资这个新币种，回报率高达 300%！”
- “少量投资，快速实现财务自由！”

4.2.2 紧迫感

案例：张女士被加密货币交流群里的“限时投资机会”诱导，匆忙投入 5 ETH，不久后项目消失。

话术：

- “限时优惠，今天注册即可获得额外奖励！”
- “名额有限，抓紧机会，不要踏空暴富！”

4.2.3 社交证明

案例：李先生在币圈群里看到“投资达人”炫耀盈利截图，投了 2 BTC 后发现项目方跑路。

话术：

- “看群友的反馈，每个跟单的都赚麻了！”
- “成功案例在这里，不跟你就亏了！”

4.2.4 虚假身份

案例：吴先生在 X 上关注了一个自称知名投资者的账号，被推荐虚假代币项目，损失惨重。

话术：

- “我是币安官方投资人员，有内部消息！”
- “我们这边已经有大户入场，赶紧跟进！”

4.2.5 技术术语陷阱

案例：赵先生被“去中心化金融”项目的术语迷惑，投资后被骗 10 ETH。

话术：

- “这是基于 Layer-2 的跨链项目，安全性极高！”
- “我们的智能合约确保每笔交易透明！”

4.2.6 赠品和空投

案例：李小姐在电报群中参与空投活动，充值 1 ETH 后发现平台消失。

话术：

- “注册就送币，充值还有额外空投！”
- “参与空投，轻松赚钱！”

4.2.7 伪造支持团队

案例：陈先生因项目“团队介绍”被骗投资，发现信息全为造假。

话术：

- “我们有全球顶尖团队支持，通过权威审计！”
- “与知名交易所合作，项目必上币！”

4.2.8 情感操控

案例：小王因“币圈交友”被骗 20 ETH，对方消失。

话术：

- “我信任你才告诉你这个内幕消息。”
- “如果我们一起做这个项目，我们的未来会更好！”

4.3 社媒诈骗

1. **假冒 KOL 聊天记录**

骗子模仿 KOL 微信名称和头像，伪造推荐聊天记录，转发到微信群或 Telegram 群，利用 KOL 的知名度让群友上当。

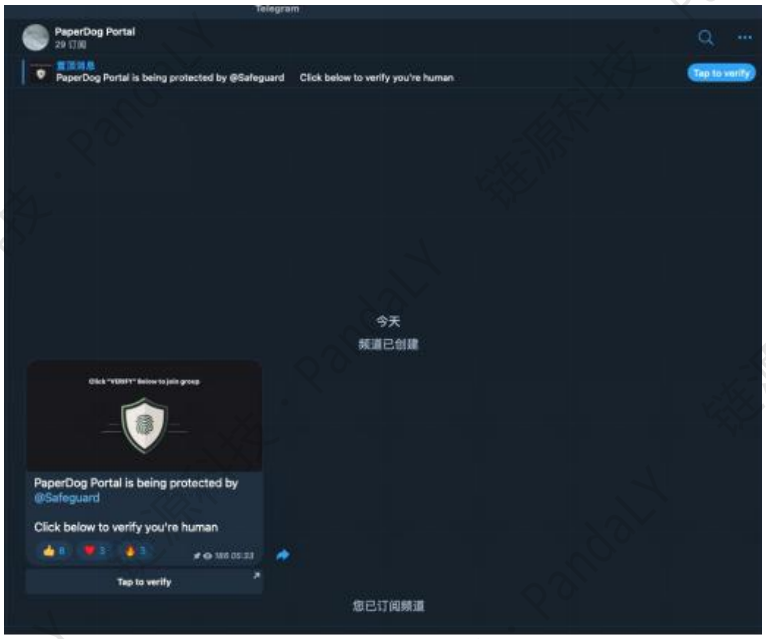
2. **Telegram 骗局**

Telegram 因用户隐匿性极强，成为灰色产业的温床。常见骗局包括：

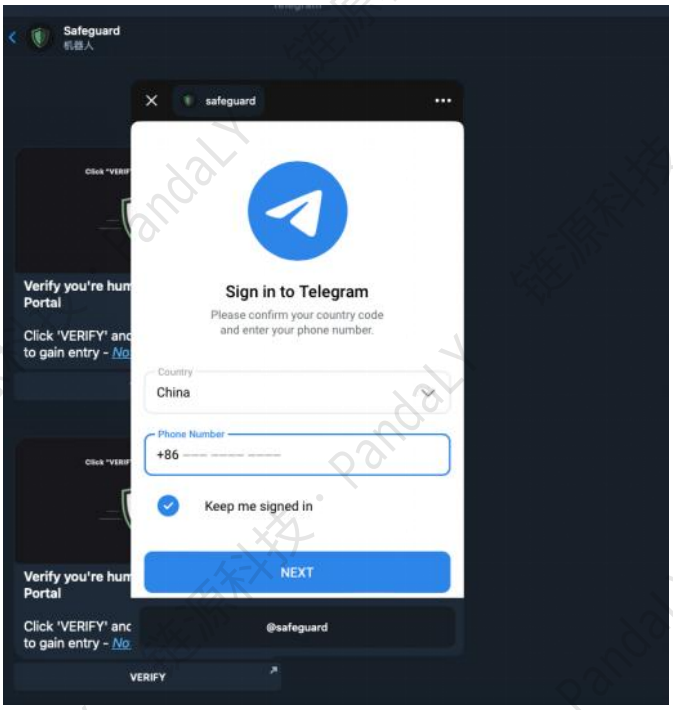
- **OTC 换 U**
- **诱导至虚假平台交易**
- **钓鱼链接**
- **发送割人项目**

特别提醒：**TG Bot 钓鱼**

骗子通过假冒的 TG Bot 要求导入钱包私钥，一旦导入即丢失资产。



当群友点击项目链接后，会弹出“TG 官方”的验证，要求填写手机号，重新登录。



群友没多想，填写了手机号码并填写了验证码进行登录。就在群友登陆后一瞬间，他的机器人钱包一直在不断弹窗，群友点进去机器人后还没来得及转移就被洗劫一空了。

4.3.1 防范建议

3. **选择合适的社交平台**

- **官方渠道下载 APP**：确保使用正规来源的 APP，避免下载钓鱼软件。
- **社交透明度**：涉及资产交易时选择具备身份验证机制的平台。
- **评估平台安全性**：确认平台是否提供两步验证及隐私保护功能。

4. **警惕高收益承诺与情感操控**

- **高收益骗局必是陷阱**：不存在“稳赚不赔”的投资项目。
- **远离网络亲密关系**：感情依赖可能导致判断失误。

5. **身份验证**

- **要求提供身份信息**：确保对方身份可查证。
- **银行流水验证**：判断资金来源是否正规。
- **核查社交媒体历史**：确保账户活跃且真实。

4.3.2 总结

骗局的本质永远是**利用人性中的贪婪与粗心**。技术再先进也只是工具，人性却是永恒的漏洞。

社媒连接了全球用户，也让诈骗无处不在。**增强自身防范意识**，学会鉴别信息来源，避免被贪婪蒙蔽双眼，是守护加密资产的第一步。

五、区块链生态的安全策略

在了解了区块链生态中的骗局之后，我们需要明确如何防范风险。本节将从两大方面提供安全策略：中心化交易所的安全策略和链上钱包的安全策略。

5.1 交易所安全

5.1.1 选择可信交易所

选择知名头部交易所（如币安、欧易）可以降低风险。 避免使用二三线交易所，原因包括：

- 提现速度慢
- 提现手续费高
- 垃圾币、传销币泛滥
- C2C 交易中可能涉及黑钱

5.1.2 启用 MFA（多因素身份验证）

MFA（Multi-factor authentication，多因素认证）通过多种验证手段提升账户安全性。启用 MFA 时，建议结合以下措施：

- **绑定邮箱和手机：** 注册完成后，启用 MFA 功能绑定邮箱和手机。
- **人脸识别：** 使用具有激光雷达功能的面部识别系统（如 iPhone 的 Face ID）。避免使用仅通过摄像头平面图像采集的安卓设备人脸识别。
- **指纹识别：** 指纹识别虽然便利，但存在在无意识状态下被滥用的风险，不建议单独使用。

5.1.3 更高安全性的 MFA

1. **支付 PIN 码：** 设置独立于其他平台的支付密码，切勿外露。
2. **身份验证器：** 推荐使用 Google Authenticator，其在本地生成验证码，避免验证码被拦截。

5.2 用户端安全

用户端主要涉及移动设备和电脑的安全策略。

5.2.1 移动设备安全

1. **应用下载：**

- 通过官方媒体提供的链接下载应用。
- iPhone 用户通过 App Store 下载，安卓用户通过 Google Play 下载。
- 避免使用不明来源的应用程序，以防粘贴板劫持等风险。

2. **Google Play 安全保护** 启用 Google Play 安全功能，以增强安卓设备的安全性。
3. **应用锁** 对涉及资金的应用添加独立于锁屏的应用锁密码。
4. **谨慎使用公共 Wi-Fi** 避免在公共 Wi-Fi 环境中传输敏感信息，以免信息被截获。
5. **私钥与助记词存储：**

- 不要将助记词存储在备忘录、微信、QQ 或相册中。
- 避免在手机中复制私钥，以防第三方粘贴板窃取。

6. **应用权限管理** 定期检查并关闭不常用应用的文件、相册访问权限。
7. **谨防陌生推送和链接** 避免点击陌生短信、邮件中的链接，以防钓鱼和恶意程序下载。

5.2.2 电脑安全

1. **防病毒软件** 安装并定期更新防病毒软件，如微软官方电脑管家。
2. **下载管理** 避免下载陌生文件，尤其是。exe 格式文件。建议建立专门下载文件夹并定期检查。
3. **浏览器安全：**

- **插件管理：** 避免安装可疑插件，定期检查并移除不必要的扩展。
- **勿在浏览器登录交易所：** 交易所登录建议使用官方 App，以防敏感信息泄露。
- **选择合适浏览器：** 推荐使用 Chrome 和 Edge，并开启增强型保护功能。
- **选择合适搜索引擎：** 使用 Google 和 Bing，避免使用百度搜索区块链相关内容。

- **浏览器版本管理：** 选择稳定版本，避免使用存在已知漏洞的版本。
- **缓存清理与自动填充：** 定期清理缓存，关闭自动填充功能。

4. **数据备份** 定期离线备份钱包数据及其他重要文件，并考虑加密存储以提高安全性。

通过以上策略，可以有效提升在区块链生态中的安全防护能力，确保资产安全。

5.3 项目安全

在参与任何项目时，**安全性**是最核心的考量因素。项目安全不仅关乎资金安全，还直接影响项目的长期发展和可持续性。以下将从多个维度详细分析如何评估项目的安全性，帮助参与者做出明智决策。

1. **项目方官方社媒账号**

重要性：社交媒体是项目方与社区互动的重要渠道，其活跃度和透明度直接反映了项目的可信度。

评估方法：

- 验证项目方的官方社交媒体账号（如 Twitter、Telegram、Discord 等），确保其真实性和活跃度。
- 关注发布内容的质量，包括技术更新、项目进展、社区活动等。
- 查看互动情况（如点赞、评论、转发）以及社区反馈，判断项目的受欢迎程度和用户信任度。
- 警惕“僵尸账号”或虚假互动，这些可能是项目方试图制造虚假热度的信号。

2. **项目方官网链接**

重要性：官方网站是项目方展示其专业性、技术能力和透明度的窗口。

评估方法：

- 访问项目方的官方网站，检查其设计、功能及用户体验。
- 确保网站使用 **HTTPS 协议**，以保障数据传输的安全性。

- 查看网站内容的完整性，包括项目介绍、团队成员、白皮书、技术文档和路线图。
- 注意网站是否提供清晰的联系方式（如邮箱、地址）以及法律声明（如隐私政策、服务条款）。

3. **项目方社群评价**

重要性：社区是项目生态的重要组成部分，用户的真实反馈是评估项目安全性的重要依据。

评估方法：

- 加入项目的官方社区（如 Telegram 群组、Discord 频道、Reddit 论坛等），观察用户的讨论内容。
- 关注社区中是否有负面反馈或争议，尤其是关于资金安全、团队诚信或技术问题的讨论。
- 警惕“过度宣传”或“盲目吹捧”的现象，这些可能是项目方操纵舆论的迹象。

4. **项目方背景**

重要性：团队背景是项目成功的关键因素之一，优秀的团队能够有效降低项目风险。

评估方法：

- 研究项目团队成员的背景，包括其教育经历、职业履历和过往项目经验。
- 查看团队是否公开了完整的成员信息（如 LinkedIn 资料），并验证其真实性。
- 关注项目是否有知名顾问或合作伙伴，这些信息可以增强项目的可信度。
- 警惕匿名团队或信息不透明的项目，这些可能是高风险信号。

5. **项目方融资情况**

重要性：融资情况反映了项目的资金实力和发展潜力，透明的融资信息有助于评估项目的可持续性。

评估方法：

- 审查项目的融资历史，包括融资轮次、融资金额和投资者名单。
- 了解资金的用途，确保项目方有明确的资金分配计划（如技术开发、市场推广、运营成本等）。
- 查看融资的透明度，包括是否公开了投资协议或资金使用报告。
- 警惕过度依赖单一投资者或资金来源的项目，这些可能存在集中风险。

6. **项目安全审计**

重要性：安全审计是确保智能合约和系统安全性的关键步骤，能够有效降低技术风险。

评估方法：

- 确认项目是否进行了第三方安全审计，并查看审计报告的内容。
- 选择由知名审计机构（如 CertiK、SlowMist、PeckShield 等）进行的审计，确保其专业性和可信度。
- 关注审计报告中指出的问题及其修复情况，判断项目方对安全问题的重视程度。
- 警惕未经过安全审计或审计报告不透明的项目，这些可能存在严重的技术漏洞。

7. **项目参与方法**

重要性：清晰的参与流程是保障用户权益的基础，复杂的流程或模糊的规则可能隐藏风险。

评估方法：

- 了解项目的参与方式，包括代币购买、治理投票、质押挖矿等。
- 确保所有流程清晰明了，避免潜在的陷阱或误导性信息。
- 查看项目的法律合规性，确保其符合所在国家或地区的监管要求。
- 警惕高收益承诺或“零风险”宣传，这些往往是骗局的常见特征。

8. **风险提示**

在参与任何项目时，务必牢记以下原则：

- **不参与不了解的项目**：如果对项目的技术、团队或商业模式不够了解，切勿盲目参与。
- **警惕诱导性宣传**：当他人不断诱导你参与某个项目时，务必保持冷静，独立分析项目的风险和收益。
- **分散投资风险**：避免将所有资金投入单一项目，分散投资可以有效降低风险。
- **持续学习与更新**：区块链行业变化迅速，保持对行业动态的关注和学习，提升自身的判断能力。

5.4 总结

在区块链领域，**“小心驶得万年船”**是永恒的原则。通过全面的项目安全分析，参与者可以有效降低风险，保护自身权益。我们始终建议用户在参与任何项目前，进行充分的调研和风险评估，确保资金安全和投资回报。

六、资产管理及保护

随着区块链资产的快速发展，钱包管理已成为资产管理的核心环节之一。合理地使用冷钱包和热钱包能够有效降低安全风险，保护数字资产。

6.1 钱包管理及使用

6.1.1 冷钱包与热钱包的区别

冷钱包：

- 与互联网完全隔离的存储设备，适用于长期存储和资产保护。
- 常见形式包括硬件钱包和纸钱包。
- 优点：安全性极高，几乎不受黑客攻击影响。
- 缺点：操作较为复杂，不适合频繁交易。

热钱包：

- 始终连接互联网的数字钱包，适合频繁交易和快速访问资产。
- 常见形式包括手机钱包、桌面钱包和在线钱包（如 MetaMask、Unisat)。
- 优点：功能丰富，支持代币查看、添加、兑换、以及与项目合约交互。
- 缺点：易受黑客攻击、钓鱼网站和恶意软件的威胁。

6.1.2 冷热钱包的安全建议

由于热钱包的长期联网特性，存在较高的安全风险，我们建议仅在其中存放频繁交易所需的少量资金。常见的安全风险包括：

- **黑客攻击**：恶意代码可能窃取私钥。
- **钓鱼网站**：通过伪装官网骗取用户授权。
- **服务商故障**：钱包提供商问题可能导致资金损失。

建议：分散资产存储，不将大额资金长期存放于热钱包中。

如果你是某个币种的长期持有者，建议将该币存入冷钱包，以避免在线环境下的风险。冷钱包的两种实现方式如下：

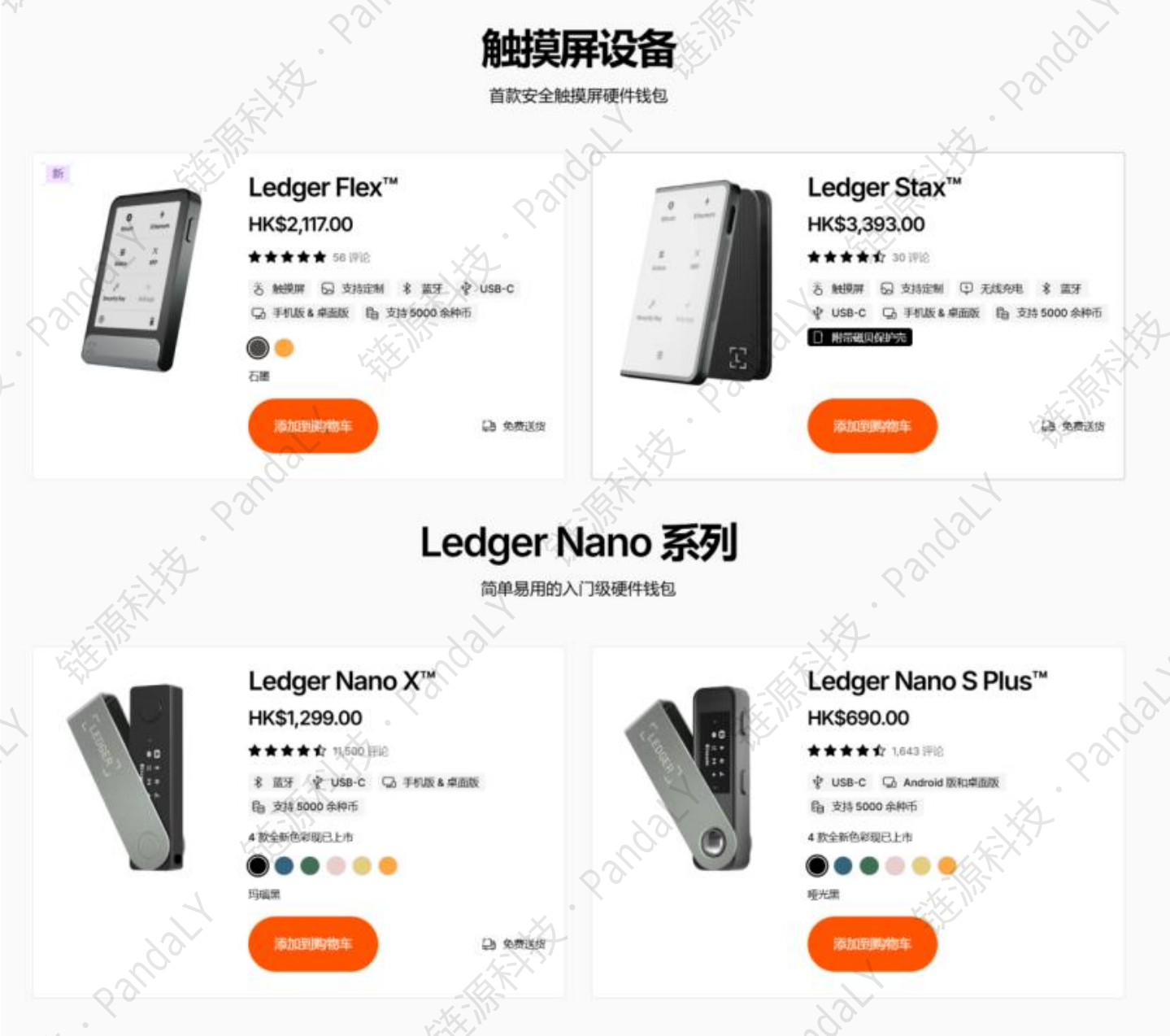
纸钱包：

- 在钱包应用中生成助记词或私钥，将其手抄记录并妥善存放。
- 适合简单的资产存储，不涉及频繁交易。

硬件钱包：

- 购买如 Ledger 等知名厂商的硬件钱包。
- **优势**：支持多种币种、提供透明签名功能，具备密码保护与离线交易功能。

建议：在硬件钱包中查看资产和进行签名时，可以明确了解交易风险敞口，确保每笔交易都在用户掌控之中。



6.1.3 冷热钱包使用策略

- **长期投资策略**：将大额加密货币存入冷钱包。
- **短期交互策略**：使用热钱包进行项目参与和链上交互。
- **资金隔离策略**：避免频繁使用冷钱包与热钱包交互，将冷钱包视作定期存折，减少转账频次。
- **风险防范策略**：将项目交互中涉及的少量资金通过交易所或其他热钱包进行提币操作，避免直接使用冷钱包。

6.1.4 钱包备份及安全策略

钱包备份是数字资产管理的重要环节。错误的备份方式会带来严重安全隐患，例如将助记词保存在备忘录、TXT 文档、截图等方式都存在被黑客窃取的风险。

热钱包备份

- 常用钱包：建议手抄助记词并妥善存放。
- 不常用钱包：可以暂时存放于设备本地的备忘录或文档中，但务必避免截图。

冷钱包备份

- 采用手写方式记录助记词或私钥，并存放在安全的物理位置。

警告：绝不将助记词或私钥存储在联网应用中，否则容易造成严重的资产风险。

6.2 项目交互与钱包使用

当参与陌生项目时，建议采取以下措施：

1. **项目背调**：优先了解项目方的背景与透明度。
2. **新建钱包**：若无法完成详细背景调查，建议创建新的热钱包进行交互，隔离核心资产。
3. **隐私保护**：可通过交易所提币进行交互，以避免项目方跟踪地址。

注意：创建新钱包仅作为资金隔离与隐私保护的下策，不可完全规避风险，尤其在大额投资时应确保项目调研充分。

6.3 指纹浏览器的风险

指纹浏览器是运行于服务器中的浏览器，用户通过远程访问进行操作。由于支持批量节点管理功能，许多“撸毛”KOL 将其作为主力工具。然而，指纹浏览器也存在严重的安全隐患。

6.3.1 典型案例：比特浏览器资产被盗事件

2023 年 8 月 26 日，多名加密社区 KOL 与成员发现其在比特浏览器中使用的钱包被盗，损失总额高达 150 万美元。链上数据显示，所有被盗类型均为私钥泄露。

比特浏览器官方声明称，由于服务端缓存遭到黑客入侵，开启扩展数据同步的用户钱包存在被盗风险。黑客通过服务端缓存获取用户同步至服务器的钱包私钥，导致资产损失。

警示：使用指纹浏览器时应极度谨慎，毕竟用户仅购买了服务器的使用权，服务提供商仍可能监控用户的个人信息与钱包数据。

B	C	D	E	F	G	H
被盗金额(大约)	是否使用wps存储私钥	系统（win /mac）	使用比特浏览器还是ads	总撸毛账号	被盗账号	被盗链
1500U	是	盗版win10	比特浏览器	50	13	全链
0.5E	是		比特浏览器	50	50	全链
4e	用过		比特浏览器	100	48	全链
统计中	没用过		比特浏览器	10	9	zks+op+bnb
统计太多	没用过		比特浏览器	3060	统计在算	全链
10000U	曾经用过，中途换了office		比特浏览器	40	40	全链，但只偷gas币，没偷linea
统计中	没用过		比特浏览器，最近一个月转为ads			马蹄
没算	曾经用过		比特浏览器			
没算				63	63	zks
60000U左右	用过		比特浏览器	150	140左右	全链 质押的没盗
0.54e	否		比特浏览器	20	1	Zks
没算	用过 但不存私钥		比特浏览器	1200	179	全链
40u	没有	win	比特浏览器	3	3	全链
统计中	未用过，只通过microsoft offic	windows	比特浏览器	70	统计中，目前被盗34个	全链eth被盗
3200u	用过	windows	比特浏览器	17	17	全链
2000U	没用过	Mac	比特浏览器	10	9个开了同步扩展程序数据的被盗/1个没开的没被盗	全链
1000U	用过	win	比特浏览器	7	6	全链
1000u	是	windows	比特浏览器	50	10	zks+主网
10E	是	windows	比特浏览器	50	50	全链
30E	否	windows	比特浏览器	100	100	全链
统计中	是	windows	比特浏览器			zks
0.18eth	否	windows	比特浏览器	20		zks arb linea

6.3.2 总结

数字资产管理中，冷钱包与热钱包的合理配置是降低资产风险的关键。投资者需要根据自身需求制定适当策略，同时避免使用高风险工具，确保资产安全。

6.4 Web2 隐私安全

无论是传统电信诈骗还是 Web3 诈骗，仔细研究后会发现，这些骗局都离不开 Web2 技术。因此，Web2 的隐私安全对保护数字资产至关重要。以下我们将从账号的创建到使用的平台，为你提供最佳的安全方案。

6.4.1 账号的创建与管理

在国内，账号注册通常以手机号为主，而在海外，大多数平台则使用邮箱注册。不论使用哪种方式，手机号和邮箱的安全性都是防范诈骗的关键。一旦这些信息泄露，你的账号将面临严重风险。

6.4.2 如何保护手机号

1. **避免公开手机号**

不要随意在线上或线下场合泄露自己的手机号，以免被滥用或用于骚扰轰炸。

2. **防范 SIM 卡交换攻击**

SIM 卡交换攻击的实施步骤如下：

黑客冒充你向运营商申请更换 SIM 卡。一旦成功，他们即可控制与你手机号相关的账户，例如银行、电子邮件等，甚至可能完全锁定你的账号。

3. **防范措施：**
   a. 为 SIM 卡设置 PIN 码，并在手机中同步激活 SIM 卡锁功能。
   b. 向运营商设置恢复短语，但确保从未公开这些问题的答案（如“我是甜豆花党还是咸豆花党”）。

6.4.3 如何保护邮箱

1. **使用强密码**

一个强密码应包含：

   a. 至少 12 个字符，包含大写字母、小写字母、数字和特殊符号；

   b. 避免使用常见信息，如生日或简单序列（如“123456”）；

   c. 每个平台使用独特的密码，避免密码重复使用。

2. 如果难以管理复杂密码，可以使用密码管理器，如 Google 或 Apple 提供的工具。

3. **注册新平台时使用新邮箱**

对于不熟悉的新平台，可创建单独的邮箱注册，既能保护隐私，也能隔离潜在风险。

4. **警惕钓鱼邮件**

   a. **链接**：不要轻易点击陌生邮件中的链接，检查其真实 URL。

   b. **附件**：避免打开不明附件，尤其是 。exe 文件或含有宏的文档。

   c. **发件人地址**：核实发件人是否真实，伪装邮件通常会使用相似但假冒的地址。

6.4.4 跨平台安全性

社交媒体和其他平台的账号往往相互绑定，一个账号被盗可能导致多个平台受到波及。例如，国内用户常使用微信登录抖音或爱奇艺，而海外用户则常用 Gmail 登录 YouTube、X 等平台。

6.4.4.1 常见隐患

1. **账号关联性**

多平台绑定是跨平台安全的最大隐患。一旦邮箱账号泄露，攻击者不仅能访问邮箱，还可通过密码找回功能控制其他平台账号。

2. **弱密码与重复使用**

使用相同或简单密码会让攻击者轻易入侵多个账户。

3. **单一身份认证（1FA）**

即使启用两步验证（2FA），若邮箱和平台账号密码相同，黑客仍能通过邮箱获取验证码，突破 2FA。

6.4.4.2 防范措施

1. **独立管理密码**

每个平台都使用独特密码，尤其是邮箱、社交媒体和交易所等重要账户。

2. **定期更新密码**

定期更换密码，确保新密码与旧密码完全不同，且符合强密码要求。

3. **防范社交工程攻击**

不要轻信伪装客服的电话或邮件，不要随意提供个人信息。

4. **监控账号活动**

定期检查安全日志和登录历史，对异常活动保持警觉。许多平台会提供登录提醒功能（如新设备登录通知），及时关注这些提示。

5. **分层安全策略**

根据平台重要性设置不同的安全措施：

a. **财务相关平台**：使用硬件密钥、冷钱包存储等高级保护手段。

b. **社交媒体**：启用 2FA，并确保密码不易破解。

5.3 网络安全

家用 WiFi 安全 家用 WiFi 不仅仅是连接网络的工具，它也是个人隐私和数据的第一道防线。因此确保家用 WiFi 的安全至关重要。

1. **复杂密码设置：**

请使用包含数字、字母和符号的复杂密码，避免使用“123456”这类简单密码，以降低被暴力破解的风险。

2. **定期更换密码：**

每隔三到六个月更换一次 WiFi 密码，确保密码的时效性和安全性。

3. **更改默认 SSID：**

将 WiFi 的默认网络名称（SSID）更改为不包含任何个人信息的名称，避免透露设备品牌等信息。

4. **隐藏网络 SSID：**

在路由器设置中隐藏网络 SSID，减少被陌生设备扫描到的机会。

5. **关闭远程管理功能：**

关闭路由器的远程管理功能，避免黑客通过网络访问你的路由器。

个人数据管理

在网络时代，个人数据变成了商品和攻击目标，因此合理管理和保护个人数据至关重要。

1. **定期清理信息：**

定期检查自己在各个平台上的个人信息，删除不必要的账户和数据。

2. **限制平台权限：**

关闭不必要的应用权限，特别是对位置信息、通讯录和存储权限的访问。

3. **使用数据伪装：**

在注册不太可靠的平台时，可以使用虚拟号码和临时邮箱地址，避免使用真实信息。

隐私政策的审查

1. **阅读隐私政策：**

虽然大多数隐私政策冗长复杂，但尽量关注数据收集和共享条款。如果平台要求过多的个人信息或存在数据滥用风险，建议谨慎使用。

2. **定期检查隐私设置：**

不同平台提供的隐私选项不同，建议定期检查并调整自己的隐私设置。

避免点击不明链接

1. **链接核查：**

将鼠标悬停在链接上查看其实际地址，避免点击钓鱼链接。

2. **提高警惕：**

对于陌生邮件、短信或社交媒体中的链接，尤其是声称需要验证账户或提供奖励的信息，务必三思而后点。

定期备份数据

1. **使用云存储：**

选择可靠的云存储平台（如 Google Drive、OneDrive）进行备份。

2. **外部硬盘备份：**

定期将重要数据复制到外部硬盘，以防止设备故障导致的数据丢失。

谨慎下载与安装软件

1. **官方渠道下载：**

只从官方网站或官方应用商店下载软件，避免从不明来源获取应用。

2. **拒绝破解软件：**

破解软件可能包含恶意代码和木马，容易导致个人数据泄露。

5.4 社媒安全

随着社交平台的普及，个人隐私泄露的风险大幅提升。正如扎克伯格曾说过的那句“你已经没有隐私了，克服克服吧！”，我们在数字化时代需要更加谨慎地保护自己的隐私信息。

隐私泄露案例分析 例如，2020 年 7 月 30 日，北京互联网法院判决微信读书和抖音存在个人信息侵权问题。微信读书自动关注好友并默认公开读书记录，而抖音通过手机号推荐“可能认识的人”。这些做法让用户在不知情的情况下暴露了个人信息。

在海外，这一问题更加严重。不法分子可以通过收集社交平台上的个人信息反向推测出银行卡号、住址等敏感数据。这种环境为诈骗和社媒攻击提供了便利条件。

隐私保护建议

3. **谨慎填写个人信息**

线上泄露的主要来源是各类社交平台和应用程序。在注册时，务必仔细考虑是否有必要提供身份证号、居住地址等敏感数据。如果不是必要信息，尽量避免填写。

4. **虚假信息的巧妙使用**

在不可靠的平台上注册时，可以适当填写虚假信息，避免使用真实住址和号码。这样即使数据被泄露，风险也能降到最低。

5. **管理 App 权限**

安装 App 时，注意权限要求。如果应用请求访问相册、摄像头、位置等与功能无关的权限，应及时撤销。

6. **定期清理账户信息**

定期检查社交媒体账户及应用中存储的个人数据，清除不必要的信息和长期不用的账户。

7. **慎重同意隐私协议和条款**

在注册时，至少了解数据收集和共享部分。如果隐私条款过于宽泛或存在明显的数据滥用风险，建议放弃使用该平台。

总结 数字化时代的隐私安全是一场长期战役。我们需要在家用 WiFi、网络使用、个人数据管理和社媒平台中建立起全面的安全意识，通过密码管理、权限控制、隐私策略等方式，全方位提升自身的信息安全等级。

七、被盗怎么办

7.1 识别骗局

发现资产被盗后，首要任务是确认资产被盗的原因：是否参与了资金盘，误入貔貅盘，或在 OTC 交易中被骗？是否点击了钓鱼网页，或遭遇了 ICO 募资跑路？下面我们将详细介绍如何识别不同类型的骗局。

7.1.1 资金盘

资金盘的特征通常较为明显。如果一个项目具备以下特征，应当提高警惕并远离：

- **回报异常高：** 若项目承诺的回报远高于市场平均水平，特别是宣称“每天几百分比的回报”，通常是资金盘的典型标志。
- **缺乏透明度：** 资金盘往往没有明确的项目背景或产品说明，运营模式也缺乏透明解释。当要求查看平台经营数据时，通常无法提供有效信息。
- **急于让你入金：** 资金盘平台会催促用户快速入金，甚至设置时间限制，诱使用户在未经过深思熟虑的情况下做出决策。
- **无法提现：** 投入资金后，平台可能会设置各种提现限制，导致用户无法提取资金。

7.1.2 貔貅盘

貔貅盘的主要特征是购买的代币无法卖出。以下方法可以帮助识别：

- **使用检测工具：**
  - **ETH 貔貅检测器：** https://www.coinscan.com/
  - **BSC 貔貅检测器：** https://honeypot.is/
- 在这些网站的搜索栏中输入代币合约地址即可判断是否为貔貅盘。
- **SOL 链貔貅盘的检测方法：**
  - **检查流动性：** 如果代币的流动性极低，很可能是貔貅盘。
  - **查看社交媒体和社区信息：** 访问代币的官方推特或社区，验证合约信息是否与实际情况相符。例如搜索 BUSD 仿盘，可以轻松发现假币。

7.1.3 钓鱼攻击

如果点击了不明网站并进行签名操作，随后资产在未授权的情况下被转移，很可能是遭遇了钓鱼攻击。

- **回忆不明链接和广告：** 回想是否收到不明来源的链接或广告，尤其是在 Telegram 群组或 Twitter 中。如果曾点击，应保存该网站的网址。
- **查看是否有恶意签名：** 根据前文案例判断签名类型。如果签名涉及 Approve 或 Permit 等操作，很可能是

钓鱼链接。

- **查看链上数据：** 检查链上记录是否包含 Approve 或 Permit 操作，若有则很可能遭遇钓鱼攻击。
- **确认是否为官方网站：** 检查是否曾在非官方网站输入私钥，并验证访问的网址是否为官方地址。

7.1.4 野鸡交易所及平台

如果发现所在平台无法提现、兑现承诺的收益，或网站关闭，很可能遇到了野鸡交易所或平台。

- **平台信誉差：** 缺乏足够的用户基础，网络上评价较少或充斥负面评论。
- **无法提现：** 交易完成后无法提现，或平台突然封锁提现功能。
- **过低手续费：** 提供异常低或零手续费的交易服务。
- **伪造市场数据：** 虚假交易所通常会伪造交易量和市场数据。

7.1.5 NFT 骗局

如果发现购买的 NFT 无法出售，可能遭遇了假冒盘或虚假 NFT 项目。

- **仿盘项目：** 检查是否有类似的官方 NFT 项目，确认是否买到了蹭热度的仿盘项目。
- **假冒 NFT：** 核对官方推特的合约地址，与 NFT 合约地址进行比对。
- **缺乏透明度：** NFT 骗局项目通常没有足够的公开信息，项目方往往隐藏身份。而正规 NFT 项目通常会进行团队信息公开、审计和宣传。

7.1.6 总结

通过上述特征分析与判断，可以有效识别各类骗局，帮助受害者第一时间了解自身所遇到的风险，为后续止损和资产追踪打下基础。

7.2 止损

在区块链中，交易几乎不可逆，因此止损尤为重要。

7.2.1 立即进行资产转移

发现钱包被盗后，不要慌张，立即检查未被盗取的资产并进行转移。转移过程中需注意拉高 GAS 费，以提高交易优先级。

7.2.2 抢跑

在区块链中，矿工根据 GAS 费优先打包交易。当与骗子在同一区块进行资产转移时，GAS 费越高，矿工打包交易的概率越大，资产转移速度也会领先于骗子。

7.2.3 GAS 转移

如果钱包中还有 Token，但无法保证抢在骗子前转移，可以通过转移 GAS 的方式防止资产被盗，即每进来一笔 GAS 就立即转走。但该方法在出块速度较快的链上效果有限。

7.2.4 NFT 与 Token 转移

确保将钱包内的 NFT 及 Token 进行转移。有时骗子仅盗取用于支付 GAS 的代币或特定代币（如 USDT），其他资产可能未被转移。可紧急转移未被盗取的资产到其他钱包。

7.3 收集证据并报案

止损后应立即收集证据并保护现场。

7.3.1 现场保护

- **电脑中病毒：** 立即断网但不要关机，以免无法重新开机。
- **钓鱼网站：** 保存域名并存储网页文件（若有能力）。
- **社媒被骗：** 保存骗子在社媒上的信息及聊天记录。
- **资金盘或杀猪盘：** 保存聊天记录及盘的信息，包括宣传文案、承诺回报、地址和联系方式。

7.3.2 报案

收集完信息后立马报案。国内司法程序不可避免，警方的帮助能为交易所冻结账户或提供信息提供法律依据。

7.4 追踪溯源

联系警方的同时，应进行溯源调查。区块链上的所有信息都是可查的，黑客的行为总会留下痕迹。

7.4.1 溯源分析

溯源包括链上和链下两个部分：

- **链上分析：** 追踪黑客的资产转移、洗钱和攻击手法。
- **链下分析：** 分析黑客的设备或服务器 IP、身份信息和设备信息。

通过一系列分析，最终形成黑客画像，为司法单位抓捕黑客提供关键线索。

八、结论

在 Web3 快速发展的浪潮中，区块链技术为全球用户带来了创新的金融和数字资产管理方式。然而，这一领域的去中心化特性也吸引了大量网络犯罪分子，他们利用技术漏洞和用户认知差距设下各种陷阱，危害行业生态。

作为一家专注于区块链安全的公司，我们深知保护数字资产安全的重要性。我们不仅目睹了加密世界的辉煌，也面对过无数用户因诈骗、黑客攻击等事件而遭受的损失。我们相信，没有安全就没有行业的持续发展。

为了提升用户的安全意识并帮助行业建立更健康的生态环境，我们撰写了这份白皮书，系统性地分析了区块链领域的常见诈骗手段和防范措施。希望借助我们的经验与技术积累，为用户提供更加全面的安全指引。

面对日益复杂的安全威胁，我们呼吁行业内的所有参与者：

1. **提高安全意识**：在进行任何链上操作前，保持警觉，了解潜在的风险，避免因贪心或粗心落入陷阱。
2. **选择可靠的安全合作伙伴**：通过专业的安全服务与解决方案，降低被攻击和诈骗的风险。
3. **共同构建安全生态**：安全不仅是个体的责任，更需要全行业的合力。我们期待与项目方、投资者及用户携手合作，共同打造一个更加安全与值得信赖的 Web3 生态环境。

区块链的未来光明且值得期待，但前提是我们需要共同捍卫这片数字空间的纯净。PandaLY 将始终秉持专业精神，持续为行业安全贡献力量，助力每一位用户在 Web3 中放心探索与创新。